N° 207

SÉNAT

SESSION ORDINAIRE DE 2023-2024

Enregistré à la Présidence du Sénat le 13 décembre 2023

PROPOSITION DE RÉSOLUTION EUROPÉENNE

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

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*,

PRÉSENTÉE

Par Mmes Audrey LINKENHELD, Catherine MORIN-DESAILLY et M. Cyril PELLEVAT,

Sénatrices et Sénateur

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

EXPOSÉ DES MOTIFS

Mesdames, Messieurs,

Le 18 avril dernier, la Commission européenne présentait un nouveau « paquet » d'initiatives visant à renforcer l'architecture européenne de cybersécurité[1], comprenant une proposition de règlement COM(2023) 209 final ayant pour objectif d'améliorer la solidarité européenne dans le domaine de la cybersécurité, une seconde proposition de règlement COM(2023) 208 final tendant à étendre le champ de la certification européenne de cybersécurité[2] et une communication COM(2023) 207 final annonçant la création d'une Académie européenne de cybersécurité.

La proposition de règlement COM(2023) 209 final fait seule l'objet de la présente proposition de résolution.

I) La cybersécurité, un enjeu politique majeur dans des sociétés hyperconnectées

Le recours aux technologies numériques, pour les administrations, les entreprises et les particuliers, engendre en retour un risque accru d'exposition aux cyberattaques. Pour faire face à ces menaces, autant la France que l'Union européenne se sont dotées d'un cadre juridique solide.

A) Les cybermenaces, une réalité aux contours variés

Une cybermenace peut être définie comme *« toute circonstance, tout événement ou toute action potentiels susceptibles de nuire ou de porter autrement atteinte aux réseaux et systèmes d'information, aux utilisateurs*

---

[1] Selon l'Agence nationale de la sécurité des systèmes d'information (ANSSI), la cybersécurité est l'« état recherché pour un système d'information lui permettant de résister à des évènements issus du cyberespace susceptibles de compromettre la disponibilité, l'intégrité ou la confidentialité des données stockées, traitées ou transmises et des services connexes que ces systèmes offrent ou qu'ils rendent accessibles. ».

[2] En pratique, la certification de cybersécurité concerne les produits, les services et les processus TIC (c'est-à-dire appartenant à un réseau ou à un schéma d'information). La proposition de règlement COM (2023) 208 tend à viser également les « services de sécurité gérés », services de conseil et d'assistance dans le domaine de la gestion des risques de cybersécurité (aptes à proposer des réponses aux incidents cyber, à effectuer des tests de pénétration, à établir des audits de sécurité…) dans le champ d'application de cette procédure de certification.

de tels systèmes et à d'autres personnes, ou encore de provoquer des interruptions de ces réseaux et systèmes »[1], c'est-à-dire une menace d'action hostile pesant sur les systèmes d'information d'une entité publique ou privée. Le onzième rapport de l'Agence européenne pour la cybersécurité[2] (ci-après ENISA), publié en octobre 2023, met en évidence huit groupes de menaces se caractérisant par l'importance qu'elles ont acquise au fil des années et les effets significatifs qu'elles peuvent avoir.

Les huit principales cybermenaces selon l'ENISA

– **les logiciels rançonneurs** (ou *« ransomware »*), c'est-à-dire un type d'attaque dans laquelle les attaquants prennent le contrôle d'un système informatique et exigent une rançon en échange du rétablissement de son fonctionnement ;

– **les logiciels malveillants** (ou « *malware* »), destinés à exécuter une action malveillante pouvant avoir des conséquences sur la confidentialité, l'intégrité ou la disponibilité d'un système ;

– **l'ingénierie sociale**, c'est-à-dire les actions visant à exploiter l'erreur humaine ou le comportement humain dans le but d'accéder à des informations ou à des services, telles que le hameçonnage et toutes ses déclinaisons (hameçonnage ciblé, hameçonnage visant des cibles haut-placées, hameçonnage téléphonique), les attaques dites de point d'eau[3], l'appâtage ...etc. ;

– **les violations des données personnelles**, définies à l'article 4.12 du règlement général sur la protection des données (RGPD) comme *« toute violation de la sécurité entraînant, de manière accidentelle ou illicite, la destruction, la perte, l'altération, la divulgation non autorisée de données à caractère personnel transmises, conservées ou traitées d'une autre manière, ou l'accès non autorisé à de telles données »*[4] ;

– **les attaques par déni de service**, qui rendent impossible l'accès aux ressources d'un système, à la suite par exemple d'une sollicitation excessive du service ou de l'infrastructure du réseau ;

---

[1] *https://eur-lex.europa.eu/legal-content/FR/TXT/?uri=CELEX%3A32019R0881&qid=1700661241510 art.2*

[2] *ENISA Threat Landscape 2023*

[3] *Une attaque de point d'eau (*watering hole attack*) consiste à piéger un site internet légitime pour atteindre les visiteurs, lesquels sont la véritable cible de l'attaquant.*

[4] *https://www.cnil.fr/fr/reglement-europeen-protection-donnees/chapitre1#Article4*

– **les perturbations** touchant internet et les communications électroniques et se traduisant par des pannes, des coupures, des fermetures ou des censures ;

– **la manipulation de l'information** ;

– et **les attaques sur la chaîne d'approvisionnement**, attaques combinées ciblant en parallèle clients et fournisseurs.

Le dernier « panorama de la cybermenace » publié par l'Agence nationale de la sécurité des systèmes d'information (ci-après ANSSI) indique que *« Le niveau général de la menace se maintient en 2022 avec 831 intrusions avérées contre 1082 en 2021. Si ce nombre est inférieur à celui de 2021, cela ne saurait être interprété comme une baisse du niveau de la menace. En effet, si une chute de l'activité liée aux rançongiciels a bien été observée par l'ANSSI sur les opérateurs régulés publics et privés à l'exception des hôpitaux, elle n'illustre pas l'évolution générale de cette menace cyber qui se maintient à un niveau élevé en se déportant sur des entités moins bien protégées »* [1].

Protéiforme, la cybermalveillance s'illustre en particulier, selon les observations de l'ANSSI, par les tendances suivantes :

– la poursuite de la **convergence des outils et des techniques des différents profils d'acteurs malveillants**, les attaquants « étatiques » se rapprochant des méthodes employées par les cybercriminels, notamment par l'utilisation de « rançongiciels » à des fins de déstabilisation politique ;

– la recherche d'accès discrets et pérennes aux réseaux des victimes ; sont ainsi ciblés les équipements périphériques (routeurs, pare-feu), les fournisseurs, les sous-traitants et les organismes de tutelle ;

– la hausse des actes liés aux « rançongiciels » en 2022, touchant particulièrement les très petites entreprises (TPE) et les petites et moyennes entreprises (PME) (40 % des « rançongiciels » traités par l'ANSSI), les collectivités territoriales (23 %) et les établissements publics de santé (10 %) ;

– les intrusions à des fins d'espionnage, qui ont représenté la principale catégorie de menaces dans lesquelles les équipes de l'ANSSI ont été impliquées en 2022 ;

[1] *https://www.cert.ssi.gouv.fr/uploads/CERTFR-2023-CTI-001.pdf*

– et l’opportunité que constituent pour les attaquants les usages numériques non maîtrisés et les faiblesses en matière de sécurisation des données.

B) Les cadres juridiques français et européen de cybersécurité

1) La stratégie nationale française en matière de cybersécurité

La France a défini en 2015 une stratégie nationale pour la sécurité numérique s’articulant autour de cinq piliers :

– garantir la souveraineté et assurer la sécurité des infrastructures critiques en cas d’attaque informatique majeure ;

– protéger tous les citoyens et lutter contre la cybercriminalité ;

– sensibiliser, former, informer ;

– faire de la sécurité numérique un facteur de compétitivité ;

– contribuer à l’avènement d’une souveraineté numérique européenne et au renforcement des capacités de pays alliés.

Actualisée à deux reprises, en 2017 puis en 2021, la stratégie française se veut aujourd’hui « d’accélération » et vise ainsi le triplement du chiffre d’affaires du secteur cyber et la création de 37 000 emplois d’ici 2025. Dotée d’un plan de financement supérieur à un milliard d’euros, la stratégie s’articule désormais autour de quatre axes :

– le développement de solutions souveraines et innovantes de cybersécurité ;

– le renforcement des synergies entre les acteurs de la filière ;

– le soutien à la demande (individus, entreprises, collectivités et État), notamment *via* la sensibilisation de la population française aux questions de cybersécurité, tout en faisant la promotion des offres nationales ;

– et la formation aux métiers de la cybersécurité.

La cybersécurité s’organise autour de plusieurs acteurs, au premier rang desquels le **Premier ministre**, qui **définit et coordonne l’action en**

matière de cybersécurité[1]. Sont également chargés de la stratégie française :

– **l'ANSSI**, qui assure la fonction d'autorité nationale de défense des systèmes d'information, conformément à l'article L. 2321-1 du code de la défense ;

– **le ministère des armées**, qui veille à la protection des réseaux essentiels et à l'intégration du combat numérique au sein des opérations militaires ;

– et **le ministère de l'intérieur**, qui lutte contre toutes les formes de cybercriminalité, visant les institutions, les intérêts nationaux, les acteurs économiques, les collectivités publiques et les particuliers.

En tant qu'autorité nationale chargée de la cybersécurité, l'ANSSI poursuit quatre missions principales :

– **la défense** des systèmes d'information critiques, des victimes de cyberattaques d'ampleur et du pays ;

– **l'expertise** en matière de (1) sécurité des technologies et des systèmes d'information, (2) d'identification des menaces et des risques dans le cyberespace et de développement des instruments visant à les contrer ;

– **la communication *via* le partage** (1) de recommandations, solutions et outils avec les acteurs de cybersécurité, (2) l'échange d'informations sur la réponse aux menaces au sein des réseaux de coopération, (3) la formation des agents et opérateurs, (4) le développement des connaissances par l'encouragement à la création de filières et formations dédiées à la cybersécurité et (5) la sensibilisation des citoyens aux risques ;

– **l'accompagnement** (1) à la création d'une doctrine et d'un écosystème en matière de cyberdéfense et (2) le soutien aux différents acteurs, autorités et opérateurs.

---

[1] *Aux termes des articles L. 2321-1 du code de la défense, « dans le cadre de la stratégie de sécurité nationale et de la politique de défense, le Premier ministre définit la politique et coordonne l'action gouvernementale en matière de sécurité et de défense des systèmes d'information. Il dispose à cette fin de l'autorité nationale de sécurité des systèmes d'information qui assure la fonction d'autorité nationale de défense des systèmes d'information ».*

S'agissant des secteurs sensibles, la loi de programmation militaire 2014-2019[1] a imposé aux opérateurs d'importance vitale (OIV) le renforcement de la sécurité des systèmes d'information critiques qu'ils exploitent et dénommés systèmes d'information d'importance vitale (SIIV). Près de 200 entités, dont la liste est couverte par le secret de la défense nationale, sont ainsi classées comme OIV et sont soumises aux obligations de déclaration et de notification des incidents y relatives.

Au niveau régional, l'ANSSI coordonne le réseau des *Computer Security Incident Response Team* (CSIRT), centres de réponse aux incidents cyber au profit des entités de leur périmètre géographique. Outre les réponses aux incidents, les équipes des CSIRT régionaux opèrent aussi des missions de prévention, de sensibilisation et d'accompagnement.

2) L'architecture européenne de cybersécurité

L'architecture européenne de cybersécurité, instituée par la directive visant à assurer un niveau élevé de cybersécurité dans l'ensemble de l'Union européenne (ou directive SRI 2 ou NIS II, en anglais)[2] et le règlement (UE) 2019/881[3], repose sur une coopération institutionnelle et opérationnelle forte entre États membres et Union européenne. À l'échelle européenne, la cybersécurité s'articule autour de plusieurs entités et procédures.

a- La dynamique politique

La Commission européenne dirigée par Mme Ursula von der Leyen a, dès 2019, fait de l'adaptation de l'Europe « l'ère du numérique », l'une des six grandes ambitions politiques de son mandat. La Présidente de la Commission rappelait ainsi dans son dernier discours sur l'état de l'Union que *« l'Europe a*[*vait*] *(...) joué un rôle pionnier dans la gestion des risques liés au monde numérique »*[4].

Dans ce cadre, la Commission n'a cessé de vouloir conforter les exigences de cybersécurité. Après l'impulsion donnée par sa prédécesseure, dans la recommandation du 13 septembre 2017 sur la réaction coordonnée

---

[1] *https://www.legifrance.gouv.fr/loda/id/JORFTEXT000028338825/*

[2] *Directive (UE) 2022/2555 du Parlement européen et du Conseil du 14 décembre 2022 concernant les mesures destinées à assurer un niveau élevé commun de cybersécurité dans l'ensemble de l'Union, modifiant le règlement (UE) n° 910/2014 et la directive (UE) 2018/1972, et abrogeant la directive (UE) 2016/1148 (directive SRI 2), non encore transposée en France.*

[3] *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 la certification de cybersécurité des technologies de l'information et des communications, et abrogeant le règlement (UE) n° 526/2013 (règlement sur la cybersécurité).*

[4] *https://ec.europa.eu/commission/presscorner/detail/fr/speech_23_4426*

aux incidents et crises de cybersécurité majeurs[1], la Commission a voulu donner consistance à la stratégie européenne par la création d'une unité commune de cybersécurité, dont la mission est d'apporter une réponse coordonnée et une assistance en cas d'incident et de crise cyber à grande échelle.

En complément, la stratégie de cybersécurité de l'Union, adoptée en décembre 2020 par la Commission européenne et le Service européen pour l'action extérieure (SEAE), a affirmé la nécessité de renforcer la coordination européenne dans le domaine de la cyberdéfense et la coopération et la constitution des capacités. En novembre 2022, ces mêmes acteurs ont dessiné les contours de la politique de l'Union européenne en matière de cyberdéfense, en prônant une coopération autant militaire que civile[2].

Le champ d'application du cadre juridique applicable à la cybersécurité est toutefois encadré par les traités

Afin de se conformer aux traités et de respecter les exigences de souveraineté nationale, le cadre juridique, posé pour l'essentiel par la directive 2022/2555 précitée (dite NIS II), s'applique *« sans préjudice de la responsabilité des États membres en matière de sauvegarde de la sécurité nationale et de leur pouvoir de garantir d'autres fonctions essentielles de l'État »* et ne s'applique donc pas *« aux entités de l'administration publique qui exercent leurs activités dans le domaine de la sécurité nationale, de la sécurité publique, de la défense ou de l'application de la loi, y compris la prévention et la détection des infractions pénales, ainsi que les enquêtes et les poursuites en la matière »*[3].

Cette stratégie européenne repose sur des organes bien identifiés, sur un cadre réglementaire complet et sur des financements disponibles.

b- <u>Les procédures et dispositifs constituant l'architecture européenne de cybersécurité</u>

L'architecture européenne repose sur un cadre juridique conséquent, d'une part, et sur divers outils visant à mettre en œuvre ces dispositions législatives, d'autre part.

---

[1] *https://eur-lex.europa.eu/legal-content/FR/TXT/?uri=CELEX:32017H1584*
[2] *https://www.consilium.europa.eu/fr/policies/cybersecurity/*
[3] *Considérant 8.*

*** Le paquet législatif relatif à la cybersécurité**

L'Union européenne a progressivement bâti un cadre juridique visant à lutter contre des cybermenaces d'autant plus importantes que notre société est hyperconnectée.

La directive SRI 2 (ou NIS II)[1], qui doit être transposée par les États membres au plus tard en octobre 2024, s'appuie sur les acquis de la directive précédente (NIS I) tout en élargissant la protection contre les cybermenaces. Elle comprend ainsi trois dispositions essentielles :

– **elle impose des obligations de cybersécurité, de contrôle et d'information** renforcées **à des secteurs critiques** définis comme « entités essentielles » (fournisseurs d'énergie, secteur de la santé...) ou comme « entités importantes » (entreprises agro-alimentaires ou chimiques...) ;

– **elle exige de chaque État membre la définition d'une stratégie nationale** et la désignation d'au moins une autorité compétente chargée de veiller à l'application de la réglementation de cybersécurité et invitée à échanger ses informations sur une base volontaire ;

– et elle demande aux États membres **l'institution de centres de réponse aux incidents de sécurité informatique (CSIRT)** pour surveiller les cybermenaces, les vulnérabilités et les incidents au niveau national, activer les messages d'alerte et apporter une assistance aux entités essentielles attaquées.

En complément, la proposition de règlement dite « cyber-résilience »[2], qui a fait l'objet d'un accord entre les États membres et le Parlement le 30 novembre 2023, tend à harmoniser les règles de cybersécurité à respecter par les produits (ordinateurs, téléphones…) et les systèmes informatiques (VPN, antivirus…) lors de leur mise sur le marché, ainsi que les obligations des fabricants lors de leur conception, de leur développement et de leur production, les exigences essentielles applicables aux fabricants durant l'intégralité du cycle de vie du produit, ainsi que les informations à fournir aux utilisateurs.

Enfin, le règlement établissant des mesures destinées à assurer un niveau élevé commun de cybersécurité dans les institutions, organes et organismes de l'Union a été définitivement adopté le 21 novembre 2023[3].

---

[1] *https://eur-lex.europa.eu/legal-content/FR/TXT/PDF/?uri=CELEX:32022L2555*
[2] *https://eur-lex.europa.eu/legal-content/FR/TXT/HTML/?uri=CELEX:52022PC0454*
[3] *Textes adoptés - Mesures destinées à assurer un niveau élevé commun de cybersécurité dans les institutions, organes et organismes de l'Union - Mardi 21 novembre 2023 (europa.eu)*

Ce texte est la réponse apportée par la Commission à l'avis de la Cour des Comptes de l'Union européenne, qui avait jugé dans un rapport spécial de mars 2022 sur la cybersécurité de ces institutions, organes et agences[1] que **le niveau de préparation des institutions européennes était** « ***globalement insuffisant*** » par rapport aux menaces. La Cour des Comptes européenne avait pointé qu'*« il n'exist*[ait] *pas de cadre juridique pour la sécurité de l'information et la cybersécurité dans les IOAUE* [institutions, organes et agences de l'Union européenne] » puisque ces domaines ne relevaient pas de la législation européenne en matière de cybersécurité. Elle regrettait également qu'aucune information exhaustive sur le montant consacré à la cybersécurité par ces institutions ne soit disponible.

*** Les outils permettant une traduction en faits des dispositions législatives**

La mise en œuvre du cadre juridique européen passe non seulement par des programmes financiers, mais aussi des instruments de certification et politiques.

En matière **d'investissements**, 20 % du plan de relance *« NextGenerationEU »*[2] devaient être consacrés à la transformation digitale de l'Europe, incluant la cybersécurité[3]. En outre, la recherche sur la sécurité numérique a été intégrée autant dans le plan Horizon 2020 que dans son successeur, Horizon Europe. Enfin, le programme pour une Europe numérique prévoit pour la période 2021-2027 un investissement de 1,9 milliard d'euros dans les capacités de cybersécurité et le déploiement à grande échelle d'infrastructures et d'outils de cybersécurité dans l'ensemble de l'Union européenne[4].

S'agissant enfin de la **certification de cybersécurité des produits, services et des processus TIC**, le règlement européen 2019/881 précité établit un cadre de certification **harmonisé à l'échelle européenne. Ainsi, la procédure s'inscrit** dans le cadre d'un schéma européen arrêté par l'ENISA, tandis que les autorités nationales (l'ANSSI en France) sont chargées du contrôle et de l'émission des certificats de niveau d'assurance élevé.

---

[1] *https://www.eca.europa.eu/Lists/ECADocuments/SR22_05/SR_cybersecurity-EU-institutions_FR.pdf*
[2] *https://op.europa.eu/fr/publication-detail/-/publication/d3e77637-a963-11eb-9585-01aa75ed71a1/language-fr p.11*
[3] *Dans son discours sur l'état de l'Union prononcé le 13 septembre 2023, Mme Ursula von der Leyen a indiqué que ce taux avait été dépassé.*
[4] *Précisons que le domaine de la cybersécurité relève également du programme InvestEU, qui utilise l'investissement public pour obtenir des investissements supplémentaires du secteur privé.*

c- Les acteurs de la cybersécurité européenne

La coopération européenne en matière de cybersécurité repose sur plusieurs intervenants.

* **L'agence de l'Union européenne pour la cybersécurité (ENISA)** a été créée en 2004. Son mandat a progressivement été étendu au fil des ans pour aujourd'hui recouvrir, conformément aux articles 5 à 12 du règlement (UE) 2019/881 précité, huit missions :

– l'élaboration et la mise en œuvre de la politique et du droit de l'Union européenne dans le domaine de la cybersécurité ;

– le renforcement des capacités, notamment par l'assistance des États membres et des autres structures et institutions ;

– la coopération opérationnelle au niveau des institutions de l'Union européenne, des États membres, des entités ainsi que la réalisation d'exercices de cybersécurité ;

– la participation à l'élaboration et à la mise en œuvre de la politique de l'Union en matière de certification de cybersécurité des produits, services et processus des technologies de l'information ;

– la connaissance des technologies et l'information du public ;

– la sensibilisation du public aux risques et l'éducation à la cybersécurité ;

– la recherche et l'innovation, notamment en conseillant les institutions européennes sur les axes à privilégier et en contribuant au programme stratégique de recherche et d'innovation ;

– et la coopération internationale avec les pays tiers et les organisations internationales afin d'encourager la coopération internationale sur les problèmes de cybersécurité.

* **Le centre de compétences en matière de cybersécurité** (ci-après CECC)[1], instauré en 2021, a pour mission d'aider l'Union européenne à conserver et à développer les capacités technologiques et industrielles en matière de cybersécurité. Avec l'appui du réseau des centres nationaux de

[1] *Règlement (UE) 2021/887 du Parlement européen et du Conseil du 20 mai 2021 établissant le Centre de compétences européen pour l'industrie, les technologies et la recherche en matière de cybersécurité et le Réseau de centres nationaux de coordination*

coordination (CNC), le CECC est le nouveau cadre de soutien à l'innovation et à la politique industrielle dans le domaine de la cybersécurité. À ce titre, il est chargé (1) de prendre les décisions stratégiques en matière d'investissement, (2) de mettre en commun les ressources de l'Union et de ses États membres afin d'améliorer et de renforcer les capacités technologiques et industrielles en matière de cybersécurité et (3) de soutenir le déploiement de solutions innovantes en matière de cybersécurité.

* **Les réseaux spécifiques**, à l'instar du groupe de coopération européen(SRI), chargé d'établir des lignes directrices politiques, du réseau des autorités de préparation et de gestion des crises cyber (réseau européen EU-CyCLONe), responsable de la prévention des crises ou du réseau des centres de réponse aux incidents de sécurité informatique dans sa déclinaison nationale (CSIRT) ou européenne (CERT-UE), sont enfin des outils de coopération opérationnelle et de partage d'informations entre les différentes entités concourant à la cybersécurité à l'échelle européenne.

*

II) La proposition de règlement COM(2023) 209 final

Traduisant la volonté de la Commission européenne d'améliorer la coordination des États membres en matière de cybersécurité et de cyberdéfense dans un contexte d'accroissement des menaces cyber à la faveur de la guerre en Ukraine et des actions d'espionnage menées par la Chine, le « paquet » d'initiatives visant à **renforcer l'architecture européenne de cybersécurité** a été présenté le 18 avril 2023.

Ce paquet est constitué :

– de la proposition de règlement COM(2023) 209 final ayant pour objectif d'améliorer la solidarité européenne dans le domaine de la cybersécurité, qui fait l'objet de la présente analyse ;

– de la proposition de règlement COM (2023) 208 final tendant à étendre le champ de la certification européenne de cybersécurité ;

– et de la communication COM(2023) 207 final annonçant la création d'une Académie européenne de cybersécurité.

La proposition de règlement est fondée sur l'article 173, paragraphe 3, et l'article 322, paragraphe 1, point a), du traité sur le fonctionnement de l'Union européenne (TFUE). Elle est organisée en cinq chapitres déclinant trois piliers présentés ci-après : la mise en place d'un « cyberbouclier »

européen, un mécanisme d'urgence et un mécanisme d'analyse des incidents.

A) Un « cyberbouclier européen » pour mieux détecter les menaces et accroître l'échange d'informations

Le chapitre II de la proposition de règlement établit le « cyberbouclier » européen comme une *« infrastructure paneuropéenne interconnectée de centres d'opérations de sécurité »* (COS, ou *SOC* en anglais). Chaque État membre devrait désigner au moins un COS, qui pourrait également participer à un COS transfrontière[1].

Un COS national serait un *« point de référence et d'accès à d'autres organisations publiques et privées au niveau national en vue de collecter et d'analyser des informations sur les menaces et incidents de cybersécurité »*.

Après appel à manifestation d'intérêt, et suite à une sélection opérée par le centre de compétences européen en matière de cybersécurité (CECC), un COS pourrait être sélectionné pour acquérir conjointement avec lui, des équipements et des infrastructures de cybersécurité. À ce titre, il pourrait bénéficier de subventions européennes versées par le centre (pour un montant allant jusqu'à 50 % des coûts pour les COS nationaux et à 75 % des coûts pour les COS transfrontières).

En outre, les COS nationaux seraient amenés à participer à un COS transfrontière dans un délai de deux ans. À défaut, ils ne bénéficieraient plus des aides européennes précitées. En pratique, trois États membres au moins, qui accepteraient de réunir leurs COS nationaux en un *« consortium d'hébergement »*, s'engageraient à échanger entre eux des informations pertinentes au sein de cette structure. Ces informations incluraient les cybermenaces, les incidents évités, les vulnérabilités, ...*etc*. si ce partage était nécessaire pour prévenir ou détecter des incidents ou pour renforcer le niveau de cybersécurité. Ces échanges d'information seraient encouragés par l'exigence d'un haut niveau d'interopérabilité entre leurs systèmes, dont les conditions pourraient être définies par recours à des actes délégués.

---

[1] *Le chapitre I définit un COS transfrontière comme « une plateforme multinationale qui rassemble, au sein d'une structure de réseau coordonnée, les COS nationaux d'au moins trois États membres qui forment un consortium d'hébergement, et qui est conçue pour prévenir les cybermenaces et les incidents et pour soutenir la production de renseignements de haute qualité, notamment par l'échange de données provenant de différentes sources, publiques et privées, ainsi que par le partage d'outils de pointe et le développement conjoint de capacités de détection, d'analyse, de prévention et de protection en matière de cybersécurité dans un environnement de confiance ».*

Ayant connaissance d'un incident de cybersécurité majeur potentiel ou en cours, les COS transfrontières seraient tenus de partager ces informations *« sans retard injustifié »*, avec le réseau EUCyCLONe, le réseau des CSIRT et la Commission européenne.

Enfin, les états membres participant au dispositif de « cyberbouclier » seraient tenus de veiller à la sécurité de ce dernier, en s'assurant du niveau élevé de sécurité des données et de sécurité physique de l'infrastructure, d'une part, et en veillant à la bonne gestion du dispositif de sorte qu'il soit possible de le protéger contre les menaces, d'autre part. En outre, les échanges d'informations avec des entités qui ne sont pas des organismes publics des États membres ne devraient pas nuire aux intérêts de l'Union européenne.

B) Un mécanisme d'urgence pour conforter la solidarité européenne en cas de crise de cybersécurité

Le chapitre III instaure le mécanisme d'urgence en matière de cybersolidarité. Celui-ci vise à *« améliorer la résilience de l'Union face à des menaces de cybersécurité majeures ainsi qu'à [l'y] préparer et à atténuer, dans un esprit de solidarité, les effets à court terme des incidents ou des crises de cybersécurité importants et majeurs »*.

Sont ainsi incluses dans le mécanisme d'urgence envisagé :

– les mesures **d'assistance mutuelle** entre les autorités compétentes des États membres ;

– les **mesures de préparation aux menaces**, incluant des tests coordonnés pour les secteurs hautement critiques. La liste des secteurs dont les entités peuvent être soumises à un tel test serait dressée par la Commission européenne, après consultation du groupe de coopération SRI et de l'ENISA ;

– les **mesures de réaction**, pour faire face aux incidents de cybersécurité importants ou majeurs et pour permettre le rétablissement immédiat des activités, comprenant l'intervention d'une réserve européenne de cybersécurité. Cette dernière consisterait en *« services de réaction aux incidents fournis par des fournisseurs de confiance sélectionnés »* dans le cadre d'une passation de marché public selon des critères tenant par exemple à la fourniture de prestations de services répondant au plus haut degré de compétence professionnelle, à l'exigence de haute intégrité, de transparence, offrant des garanties en matière de protection des informations sensibles ...*etc*.

Ces services seraient déployables dans un État membre confronté à une crise, à sa demande. En pratique, les demandes d'intervention au titre de la réserve seraient formulées auprès de la Commission européenne, qui évaluerait la demande avec l'expertise de l'ENISA et selon des critères tels que la gravité, le type de structures touchées ou les conséquences probables en cas de demandes concomitantes. Les pays tiers pourraient également demander une assistance à la réserve de sécurité, sous certaines conditions.

Les rapporteurs de la commission des affaires européennes notent également que cette réserve de cybersécurité européenne aurait vocation à intervenir, outre dans les États membres et les institutions européennes, dans des États tiers qui en auraient fait la demande, sans limitation géographique, dès lors qu'ils auraient passé un accord d'association avec l'Union européenne et que ce dernier viserait leur participation au programme pour une Europe numérique.

Cette aide interviendrait sur demande, du moment où l'État a épuisé ses capacités nationales de réponse, et après désignation d'un point de contact unique et la fourniture d'informations suffisantes sur les capacités et actions de cybersécurité mises en œuvre.

À titre d'exemple, depuis le début de la guerre en Ukraine, trois États européens non membres de l'UE ont subi des attaques d'ampleur : l'Albanie, qui a eu recours à l'aide américaine, le Monténégro et la Macédoine du nord.

S'agissant du fonctionnement pratique du dispositif, la Commission européenne *« assume(rait) la responsabilité globale de la mise en œuvre de la réserve de cybersécurité de l'Union »*. À ce titre, elle en définirait les priorités et l'évolution, superviserait sa mise en œuvre et s'assurerait, entre autres, de sa cohérence et de sa complémentarité avec les autres mesures de soutien et les actions et programmes de l'Union européenne. L'ENISA pourrait se voir confier par voie de convention de contribution, le fonctionnement et l'administration de la réserve.

C) Un mécanisme d'analyse des incidents de cybersécurité afin de tirer les leçons des crises

Le chapitre IV instaure un **mécanisme d'analyse des incidents de cybersécurité**. Dans ce cadre, à la demande de la Commission européenne, du réseau EU-CyCLONe ou du réseau des CSIRT, l'ENISA serait chargée de rédiger un rapport qui analyserait et évaluerait les menaces, les vulnérabilités et les mesures d'atténuation, suite à un incident de cybersécurité important ou majeur.

Ce rapport d'analyse et d'évaluation devrait contenir un bilan des enseignements tirés et s'accompagnerait de recommandations lorsque ce serait utile. Il serait remis au réseau des CSIRT, à EU-CyCLONe et à la Commission européenne.

À ces trois piliers s'ajoutent des **dispositions relatives au financement du dispositif,** puisque la proposition tend à modifier le règlement (UE) 2021/694[1] instituant le programme pour une Europe numérique afin d'y insérer les dispositions relatives au « cyberbouclier » et à son financement. L'exposé des motifs de la proposition indique à ce titre que le montant disponible pour des actions de cybersécurité dans le cadre du programme pour une Europe numérique serait porté à 842,8 millions d'euros, grâce à une réaffectation de 100 millions d'euros prévus pour d'autres objectifs du même programme.

Enfin, des actes délégués et d'exécution en nombre sont prévus afin de répondre aux finalités suivantes : *« préciser les conditions de l'interopérabilité entre les SOC transfrontières[2], déterminer les modalités procédurales du partage d'informations relatives à un incident de cybersécurité majeur, potentiel ou actuel, entre les SOC transfrontières et les entités de l'Union[3], établir des exigences techniques pour garantir un niveau élevé de sécurité des données et de sécurité physique des infrastructures et protéger les intérêts de l'Union en matière de sécurité lors de l'échange d'informations avec des entités qui ne sont pas des organismes publics des États membres[4], préciser les types et le nombre de services de réaction aux incidents requis pour la réserve de cybersécurité de l'Union[5], et préciser davantage les modalités d'attribution des services d'aide de la réserve de cybersécurité de l'Union[6] »*.

III. La position de la commission des affaires européennes du Sénat

Les rapporteurs de la commission des affaires européennes souhaitent avant tout souligner leur **soutien de principe à tout dispositif visant à lutter contre les cybermenaces et la cybermalveillance. Pour autant, si l'objectif est louable et certaines dispositions bienvenues, d'autres**

---

[1] *Règlement (UE) 2021/694 du Parlement européen et du Conseil du 29 avril 2021 établissant le programme pour une Europe numérique et abrogeant la décision (UE) 2015/2240.*
[2] *Article 6.*
[3] *Article 7.*
[4] *Article 8.*
[5] *Article 12.*
[6] *Article 13.*

suscitent de réelles interrogations et méritent une vigilance de la part du Sénat.

A) Un objectif louable de renforcement de la coopération et de la solidarité en cas d'incident majeur

1) Une volonté de lutte contre la cybermalveillance, fléau de nos sociétés modernes

La numérisation accrue de nos sociétés, bien que bénéfique à de nombreux égards, est aussi une aubaine pour les pirates, réseaux criminels voire acteurs étatiques hostiles. L'ENISA évalue le risque actuel à un niveau 3 sur une échelle de 5, soit un risque substantiel. L'ANSSI, quant à elle, souligne que les administrations publiques, les établissements de santé et les TPE/PME font partie des cibles privilégiées des cyber attaquants.

À titre d'exemple, la mairie de Lille a été victime fin février 2023 d'une cyberattaque d'envergure, qui a paralysé l'ensemble du réseau informatique. Outre le vol de données personnelles, certains agents ont ensuite reçu des demandes de rançon. Le préjudice total était estimé à 1,7 million d'euros six mois après l'attaque.

Face à cette menace diffuse mais permanente, la coopération et l'entraide entre les États membres en matière de cybersécurité apparaissent nécessaires et constituent un prérequis pour tendre vers un espace numérique sûr. **Les rapporteurs de la commission des affaires européennes soutiennent donc l'objectif affiché de la présente proposition.**

2) La réserve européenne de cybersécurité, une coopération public-privé qu'il convient de bien encadrer

Traduction à l'échelle européenne d'un système qui fonctionne assez bien en France, **la réserve européenne de cybersécurité** complèterait utilement « l'offre nationale » visant à répondre aux cyber incidents. Les rapporteurs insistent sur le fait que l'intervention de cette réserve représenterait une solution de dernier recours et qu'en appui de leur demande d'intervention de la réserve, États membres comme États tiers devraient justifier des mesures prises par eux-mêmes en réponse à l'incident.

Bien sûr, les rapporteurs souhaiteraient, idéalement, que les moyens propres aux États membres, suffisent sans besoin de recourir à des entreprises privées, craignant de plus que cela ne favorise une concurrence industrielle au-delà du cercle européen.

Néanmoins, la mise en place d'une réserve privée peut être un instrument précieux et rassurant, à la condition, bien sûr, que ces missions soient assurées par des entreprises prestataires fiables. Pour garantir cette fiabilité des prestataires, les entreprises concernées devraient être sélectionnées par appel d'offres selon des critères tenant par exemple à la fourniture de prestations de services répondant au plus haut degré de compétence professionnelle, à l'exigence d'intégrité et de transparence, offrant des garanties en matière de protection des informations sensibles, *etc*.

C'est déjà le mode opératoire que l'ANSSI suit à l'échelon national pour répondre aux cyberattaques contre les établissements de santé ou les collectivités territoriales. L'avantage d'un tel dispositif est d'assurer une coordination publique et stratégique des actions. Néanmoins, pour pallier tout risque de fuite ou d'ingérence étrangère, les rapporteurs de la commission des affaires européennes appellent à ce que des critères très stricts soient définis, au nom de la préservation des intérêts nationaux et fondamentaux des États membres. Ils souhaitent, tout comme le Parlement européen, n'inclure dans la réserve que des prestataires ayant leur siège social dans l'Union européenne, dans l'Espace économique européen, ou dans un pays tiers associé à l'Union européenne et partie à l'accord sur les marchés publics de l'Organisation mondiale du commerce (OMC).

Les rapporteurs de la commission des affaires européennes appellent également de leurs vœux la montée en puissance des prestataires européens afin d'assurer à terme l'autonomie stratégique de l'Union européenne, accompagnée d'une augmentation des ressources de l'ENISA par un plan de recrutement de cyber-experts européens.

Ils souhaitent aussi que les États membres s'assurent de l'intégration de sanctions pénales et non pénales, adaptées afin de punir le vol, la diffusion non autorisée d'informations confidentielles et l'espionnage qui pourraient découler de l'activation du mécanisme d'urgence.

Ils veulent souligner que la France doit elle-même poursuivre le renforcement de ses capacités à prévenir les cyberattaques et à y répondre.

Tout en soutenant le principe d'une possibilité d'intervention de la réserve européenne dans les pays tiers associés à l'Union européenne et participant au programme pour une Europe numérique qui seraient confrontés à une crise cyber, les rapporteurs de la commission des affaires européennes souhaitent que les modalités d'intervention de la réserve soient précisées dans la présente proposition, en cas de demandes d'intervention simultanées d'États membres et de pays tiers, en prévoyant

en particulier une priorité bénéficiant aux États membres puis, aux pays tiers candidats à l'adhésion à l'Union européenne. »

3) Le retour d'expérience, une nécessité pour progresser

Le mécanisme d'analyse des incidents, en ce qu'il permet un retour d'expérience nécessaire et invite à tirer des enseignements des crises cyber, est un élément bienvenu de la présente proposition. Ce retour d'expérience serait opéré par l'ENISA, mandatée par la Commission européenne, le réseau EU-CyCLONe ou le réseau des CSIRT. Dans la préparation de son rapport, l'ENISA bénéficierait de la collaboration des parties prenantes concernées.

Les rapporteurs de la commission des affaires européennes soutiennent le principe de cette analyse, mais invitent toutefois à en clarifier les principes, ainsi que la rédaction de l'article 18 qui en précise les modalités, pour deux raisons. D'une part, il serait nécessaire de bien distinguer ce mécanisme d'analyse des incidents effectué par l'ENISA de celui opéré par le réseau EU-CyCLONe, qui a déjà pour mission, aux termes de l'article 16 de la directive SRI 2 *« d'évaluer les conséquences et l'impact des incidents de cybersécurité majeurs et des crises en question et de proposer d'éventuelles mesures d'atténuation »*.

D'autre part, il est essentiel de confirmer et d'insister sur le rôle des États membres dans cette analyse *ex-post*.

B) Des points de vigilance pour la commission des affaires européennes

1) Une complexification de l'architecture européenne de cybersécurité sans valeur ajoutée flagrante

L'ajout d'un échelon supplémentaire à une architecture européenne de cybersécurité déjà conséquente surprend. D'autant plus que le cadre juridique actuel de la directive 2022/2555 semble cohérent et complet, prévoyant en particulier la mise en place d'un réseau de centres d'intervention pour se préparer aux crises cyber (réseau européen pour la préparation et la gestion des crises cyber (EU-CyCLONe)) et pour y répondre (réseau des centres de réponse aux incidents de sécurité informatique (CSIRT)), les modalités d'échange des informations pertinentes et une coordination des réponses en cas d'incident. **Outre la complexification du schéma, le risque de doublon est important.**

C'est ce que souligne la Cour des comptes de l'Union européenne dans un avis sur la proposition publié le 5 octobre 2023 : *« Dans ces*

conditions, nous estimons que la proposition de règlement est de nature à rendre plus complexe l'ensemble du paysage de l'UE en matière de cybersécurité. Il existe un risque de double emploi entre les SOC et le réseau des CSIRT déjà en place. Certes, dans la section 1 de l'exposé des motifs, la Commission déclare que les plateformes SOC transfrontières devraient constituer une nouvelle capacité venant compléter le réseau des CSIRT, mais nous observons des similitudes au niveau de certaines des tâches et de certains des objectifs assignés aux SOC nationaux, aux SOC transfrontières, aux CSIRT et au réseau des CSIRT ».

Lors des auditions menées par les rapporteurs de la commission des affaires européennes, les autorités françaises, au premier rang desquelles l'ANSSI, semblaient dans un premier temps sceptiques quant à la pertinence d'un COS national, avant d'accepter, dans un second temps, cette nouvelle entité sous réserve de sa réorientation afin d'en faire, non un « clone » des CSIRT, mais un outil à leur service.

Le scepticisme demeure de mise s'agissant des COS transfrontières, dont les contours, missions et obligations semblent encore flous. En outre, se pose la question de la pertinence de créer des réseaux pour échanger des informations sur des sujets hautement sensibles. Le bon sens et la prudence voudraient en effet les échanges sur les vulnérabilités des systèmes soient limités à quelques interlocuteurs pertinents, et non à l'ensemble des acteurs concourant à la cybersécurité européenne.

Enfin, se pose la question de la pertinence du calendrier prévu. En effet, la directive SRI 2, adoptée en décembre 2022, doit être transposée dans le droit interne des États membres d'ici octobre 2024. Ce texte est donc très récent et n'est pas encore pleinement opérationnel, ce qui empêche actuellement de tirer des conclusions quant à son efficacité ou ses lacunes présumées. Il paraît donc prématuré de vouloir déjà le compléter, comme le désire la Commission, voire le « doublonner ». Enfin, il est regrettable que la Commission européenne ait cette fois opté pour un règlement, c'est-à-dire un texte d'effet direct qui s'impose aux États membres sans marge d'appréciation de leur part.

2) Un champ d'application aux contours flous qui pourrait empiéter sur les compétences propres des États membres

La question du champ d'application exacte du texte reste imprécise et la répartition des responsabilités entre les acteurs incertaine : l'emploi de termes novateurs et non strictement définis tels que *« responsabilité première des États membres »* peuvent avoir des conséquences lourdes

pour les États membres, à l'instar d'une tentative d'empiètement sur leurs compétences propres.

Rappelons que la défense et la sécurité intérieure sont des prérogatives nationales et qu'il convient de préserver la responsabilité exclusive qui revient aux États membres en ces domaines.

Ainsi, aux termes de l'article 4, paragraphe 2, du traité sur l'Union européenne (TUE), « *la sécurité nationale reste de la seule responsabilité de chaque État membre* ».

Pour résoudre ces difficultés et se conformer au principe de subsidiarité, la proposition de règlement devrait donc reprendre la clause de délimitation et d'exclusion posée par l'article 2 de la directive 2022/2555 précitée. Elle devrait ainsi :

– s'appliquer *« sans préjudice de la responsabilité des États membres en matière de sauvegarde de la sécurité nationale et de leur pouvoir de garantir d'autres fonctions essentielles de l'État, notamment celles qui ont pour objet d'assurer l'intégrité territoriale de l'État et de maintenir l'ordre public »* ;

– ne pas s'appliquer *« aux entités de l'administration publique qui exercent leurs activités dans les* domaines *de la sécurité nationale, de la sécurité publique, de la défense ou de l'application de la loi, y compris la prévention et la détection des infractions pénales, ainsi que les enquêtes et les poursuites en la matière »*.

3) Une absence d'étude d'impact qui pénalise l'analyse de la proposition de règlement

Deux choix de méthode sont regrettables : l'absence d'analyse d'impact qui rend difficile l'appréciation de la sincérité du dispositif, d'une part, et le recours aux actes d'exécution, d'autre part.

En premier lieu, **la proposition ne contient pas d'étude d'impact** au motif de *« l'urgence »* invoquée pour présenter le texte. Si les rapporteurs de la commission des affaires européennes comprennent les circonstances ayant poussé à privilégier la rapidité, il n'en demeure pas moins que l'absence d'étude d'impact nuit à la clarté de la démarche de la Commission européenne et empêche une analyse sincère du dispositif, d'une part, et de conclure rapidement à la nécessité du « cyberbouclier » européen envisagé, d'autre part.

Conformément à une position de principe du Sénat, les rapporteurs souhaitent plus généralement rappeler *« la nécessité pour la Commission européenne d'appuyer ses initiatives législatives par des analyses d'impact systématiques afin d'en contrôler la nécessité et la proportionnalité »*[1]. En outre, *« les lignes directrices de la Commission pour une meilleure réglementation préconisent de procéder à des analyses d'impact et de consulter les parties prenantes dans le cadre de l'analyse complète des options de conception et de mise en œuvre des interventions »*, souligne la Cour des comptes de l'Union européenne.

Ainsi, en l'état des données, sans analyse d'impact, les informations relatives au financement du dispositif n'apportent aucune garantie de pérennité. Certes, on peut tout à fait imaginer qu'un programme de financement de la cybersécurité figurera dans le prochain cadre financier pluriannuel, eu égard à l'importance du sujet, mais il existe une véritable incertitude sur le financement des COS nationaux et transfrontières. En outre, comme le souligne la Cour des comptes de l'Union européenne, il n'existe que *« peu d'informations sur les options d'intervention possibles et sur les coûts induits par le règlement proposé »*.

En second lieu, les rapporteurs de la commission des affaires européennes regrettent **un renvoi fréquent, voire exessif, aux actes d'exécution** de la Commission européenne, par la proposition de règlement, prévus à l'article 291 du traité sur le fonctionnement de l'Union européenne (TFUE)[2].

En pratique, de tels actes d'exécution :

– arrêteraient les modalités de l'interopérabilité entre les COS/SOC transfrontières (article 6) ;

– établiraient les procédures de partage d'informations entre les COS/SOC transfrontières et le réseau EU-CyCLONe, le réseau des CSIRT et la Commission européenne (article 7) ;

– définiraient les exigences techniques permettant aux États membres d'assurer la sécurité du « cyberbouclier » (article 8) ;

---

[1] *Résolution européenne n° 69 (2022-2023) du Sénat sur le programme de travail de la Commission européenne pour 2023, en date du 13 mars 2023.*

[2] *« Les États membres prennent toutes les mesures de droit interne nécessaires pour la mise en œuvre des actes juridiquement contraignants de l'Union. Lorsque des conditions uniformes d'exécution des actes juridiquement contraignants de l'Union sont nécessaires, ces actes confèrent des compétences d'exécution à la Commission (…). »*

– décideraient des types et du nombre de services de réaction nécessaires pour la réserve de cybersécurité de l'Union européenne et des modalités d'attribution des services d'aide fournis par cette réserve (articles 12 et 13).

Dans ce dernier cas, il s'agit de fait de confier à la seule Commission européenne le pouvoir d'arrêter les modalités d'intervention de la réserve européenne de cybersécurité, ce qui semble excessif, le législateur européen ne paraissant pas, en l'espèce, avoir épuisé ses compétences.

En effet, de tels actes d'exécution échappent au contrôle par les parlements nationaux et il semble nécessaire que les modalités d'intervention précitées puissent être fixées dans le corps même de la proposition de règlement.

Proposition de 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

① Le Sénat,

② Vu l'article 88-4 de la Constitution,

③ Vu le traité sur l'Union européenne, en particulier son article 4,

④ Vu le traité sur le fonctionnement de l'Union européenne, en particulier ses articles 173 et 322,

⑤ Vu le règlement (UE) 182/2011 du Parlement européen et du Conseil du 16 février 2011 établissant les règles et principes généraux relatifs aux modalités de contrôle par les États membres de l'exercice des compétences d'exécution par la Commission,

⑥ Vu 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),

⑦ Vu le règlement (UE) 2021/694 du Parlement européen et du Conseil du 29 avril 2021 établissant le programme pour une Europe numérique et abrogeant la décision (UE) 2015/2240,

⑧ Vu le règlement (UE) 2021/887 du Parlement européen et du Conseil du 20 mai 2021 établissant le Centre de compétences européen pour l'industrie, les technologies et la recherche en matière de cybersécurité et le Réseau de centres nationaux de coordination,

⑨ Vu la directive (UE) 2022/2555 du Parlement européen et du Conseil du 14 décembre 2022 concernant des mesures destinées à assurer un niveau élevé commun de cybersécurité dans l'ensemble de l'Union, modifiant le règlement (UE) n° 910/2014 et la directive (UE) 2018/1972, et abrogeant la directive (UE) 2016/1148 (directive SRI 2),

⑩ Vu la proposition de règlement du Parlement européen et du Conseil établissant des mesures destinées à assurer un niveau élevé commun de cybersécurité dans les institutions, organes et organismes de l'Union COM(2022) 122 final,

⑪ Vu la proposition de règlement du Parlement européen et du Conseil concernant des exigences horizontales en matière de cybersécurité pour les produits comportant des éléments numériques et modifiant le règlement (UE) 2019/1020, COM(2022) 454 final,

⑫ Vu la proposition de règlement tendant à étendre le champ de la certification européenne de cybersécurité, COM(2023) 208 final,

⑬ Vu la proposition de règlement ayant pour objectif d'améliorer la solidarité européenne dans le domaine de la cybersécurité, COM(2023) 209 final,

⑭ Vu la communication du 18 avril 2023 annonçant la création d'une Académie européenne de cybersécurité, COM(2023) 207 final,

⑮ Vu l'avis 02/2023 du 5 octobre 2023 de la Cour des Comptes de l'Union européen sur une 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,

⑯ Vu la résolution européenne du Sénat n° 109 (2017-2018) du 26 mai 2018 sur la proposition de règlement du Parlement européen et du Conseil 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,

⑰ Vu le rapport d'information n° 458 (2017-2018) de M. René DANESI et Mme Laurence HARRIBEY, au nom de la commission des affaires européennes du Sénat, intitulé *la cybersécurité : un pilier robuste pour l'Europe numérique*,

⑱ Vu la communication en date du 5 juillet 2023 de Mme Laurence HARRIBEY, sénatrice, devant la commission des affaires européennes du Sénat, sur la conformité au principe de subsidiarité de la proposition de règlement européen établissant des mesures pour renforcer la solidarité et les capacités dans l'Union européenne à détecter les menaces et les incidents liés à la cybersécurité, à s'y préparer et à y répondre COM(2023) 209,

⑲ *Sur la proposition de règlement et ses objectifs :*

⑳ Considérant que la cybersécurité est un enjeu politique majeur d'autant plus fort que le recours au numérique est massif dans les sociétés contemporaines ;

㉑ Considérant en effet que l'une des conséquences du développement de la numérisation de l'économie et des sociétés européennes est la vulnérabilité croissante de l'Union européenne et de ses États membres à l'égard des cyberattaques ;

㉒ Considérant que, selon l'ENISA, la menace cyber pesant sur l'Union européenne est aujourd'hui substantielle, et que ce niveau s'est accru depuis le début de la guerre en Ukraine ;

㉓ Considérant que, pour la France, selon l'Agence nationale de la sécurité des systèmes d'information (ANSSI), les cyberattaques touchent particulièrement les administrations publiques, les établissements de santé, les PME-TPE, mais fragilisent également les démarches du quotidien de nos concitoyens ;

㉔ Considérant que ces menaces et ces attaques sont le fait, non seulement de « pirates » et de réseaux criminels mais également d'acteurs étatiques hostiles aux États membres de l'Union européenne désireux de fragiliser cette dernière ;

㉕ Considérant, par conséquent, que la coopération et l'entraide entre les États membres en matière de cybersécurité sont nécessaires et constituent un prérequis pour tendre vers un espace numérique sûr ;

㉖ Salue le fait que l'Union européenne a pris conscience de cette nécessité et a su se doter d'un cadre juridique solide et complet pour bâtir une architecture européenne de cybersécurité ;

㉗ Rappelle que cette architecture a été établie par le règlement (UE) 2019/881 du 17 avril 2019, qui a renforcé l'ENISA, et la directive (UE) 2022/2555 du 14 décembre 2022, dite SRI 2, qui, d'une part, a imposé des obligations de cybersécurité aux entités essentielles et, d'autre part, institué des organes opérationnels pour la coopération et l'échange d'informations ;

㉘ Prend acte du souhait de la Commission européenne de renforcer de nouveau cette architecture avec la présente proposition de règlement ; s'interroge sur l'opportunité de la présentation d'un nouveau texte européen modifiant les relations et les missions des acteurs de la cybersécurité seulement quatre mois après l'adoption définitive de la directive SRI 2 ; soutient néanmoins l'objectif de cette dernière en ce qu'elle traduit la volonté d'une coopération accrue et pérenne en matière de cybersécurité à l'échelle européenne ;

㉙ *Sur l'absence d'analyse d'impact accompagnant la proposition et ses conséquences sur l'évaluation de la nécessité de la réforme :*

㉚ Déplore l'absence d'analyse d'impact accompagnant la proposition de règlement car cette absence fragilise la sincérité de la présentation de la Commission européenne, empêche l'estimation des financements nécessaires à la mise en œuvre de la réforme et rend difficile l'évaluation de la valeur ajoutée du dispositif envisagé ;

㉛ *Sur le champ d'application du règlement proposé :*

㉜ Considérant que la rédaction des articles 1er et 2 de la proposition de règlement est ambiguë en ce qu'elle n'exclut pas explicitement les domaines de la sécurité nationale et de la défense nationale de son champ d'application ;

㉝ Considérant en outre que l'article 1er, paragraphe 3, précité évoque une « responsabilité première » des États membres et non exclusive dans le domaine de la sécurité nationale ;

㉞ Rappelle que conformément aux traités, et en particulier, l'article 4 du traité sur l'Union européenne (TUE) qui stipule que « *la sécurité nationale reste de la seule responsabilité de chaque État membre* », la sécurité nationale et la défense nationale demeurent des domaines relevant de la compétence exclusive des États membres ; considère qu'il ne saurait être question d'inclure les États membres dans un dispositif d'échange massif et obligatoire d'informations avec un nombre étendu de partenaires, qui, paradoxalement, affaiblirait la cybersécurité de l'Union européenne ;

㉟ Invite le Gouvernement à s'assurer de la compatibilité des dispositions de la présente proposition avec celles de la directive SRI 2 ; et demande la reprise explicite, au sein de son article 1er, des paragraphes 6 et 7 de la directive SRI 2 précitée, afin de préciser, d'une part, que son dispositif serait « *sans préjudice de la responsabilité des États membres en matière de sauvegarde de la sécurité nationale et de leur pouvoir de garantir d'autres fonctions essentielles de l'État, notamment celles qui ont pour objet d'assurer l'intégrité territoriale de l'État et de maintenir l'ordre public* », et, d'autre part, qu'il ne s'appliquerait pas « *aux entités de l'administration publique qui exercent leurs activités dans les domaines de la sécurité nationale, de la sécurité publique, de la défense ou de l'application des lois* » ;

㊱ *Sur le financement de la présente proposition de règlement :*

㊲ Considérant que le budget des actions de cybersécurité dans le cadre du programme pour une Europe numérique a été augmenté de 100 millions d'euros par une réaffectation des fonds, passant ainsi de 743 à 843 millions d'euros ;

㊳ Constate, comme le confirme l'avis 02/2023 rendu par la Cour des comptes de l'Union européenne, que l'information sur le financement de cette réforme est partielle et, en particulier, que la proposition ne contient pas d'estimation du coût total escompté de l'établissement et de la mise en œuvre des mesures envisagées ; demande en conséquence, à la Commission européenne de faire toute la transparence sur ces coûts ;

㊴ Observe également que la Commission européenne souhaite pouvoir déroger au principe d'annualité budgétaire dans l'utilisation des fonds européens dédiés à ce dispositif ; incite la Commission européenne à limiter cette dérogation au principe d'annualité aux seules activités non planifiables, à savoir la réserve européenne de cybersécurité et l'assistance mutuelle, puisque ces dernières ne seraient mises en œuvre que pour faire face à des évènements imprévisibles ;

㊵ Rappelle la nécessité de financements pérennes, nationaux et européens, pour garantir l'efficacité de la coopération européenne dans le domaine de la cybersécurité ;

㊶ Regrette que la réorientation des fonds visant à financer le présent dispositif se fasse au détriment d'autres actions essentielles comme l'éducation digitale ou le programme Erasmus+, qui ont pour objectif de développer les compétences numériques de nos concitoyens et d'éviter « l'exclusion numérique » ;

㊷ *Sur la création d'un « cyberbouclier » européen :*

㊸ Considérant que la cybermenace ne peut, par nature, être complètement contrée et que le « risque zéro » n'existe pas dans le domaine de la cybersécurité ;

㊹ Considérant que l'architecture européenne actuelle, résultant de la directive précitée SRI 2, comporte déjà de multiples acteurs chargés de la coordination politique, tels que le groupe de coopération européen, de la prévention et de la gestion des crises cyber, tels que le réseau EU-CyCLONe, et de la réponse aux incidents, tels que les centres de réponse aux incidents de sécurité informatique (CSIRT) ;

㊺ Considérant que la présente proposition prévoit la mise en place d'un « cyberbouclier » européen, infrastructure paneuropéenne qui serait constituée de centres opérationnels de sécurité (COS), nationaux et transfrontières, et devrait doter l'Union européenne de capacités avancées de détection, d'analyse et de traitement des données relatives aux cybermenaces ;

㊻ Considérant que chaque État membre devrait mettre en place un organisme public dénommé COS national, qui aurait une double fonction de « radar » pour détecter en amont les incidents de cybersécurité et de point de référence pour d'autres organisations publiques et privées au niveau national ;

㊼ Considérant que ces COS nationaux pourraient procéder à des acquisitions d'outils et d'infrastructures en matière de cybersécurité conjointement avec le Centre de compétences européen en matière de cybersécurité (CECC), et, à cette occasion, bénéficier d'une aide financière européenne couvrant jusqu'à 50 % des coûts d'acquisition et 50 % des coûts opérationnels ;

㊽ Considérant que trois États membres au moins, représentés par leurs COS nationaux, pourraient s'unir au sein d'un consortium d'hébergement pour former un COS transfrontière ;

㊾ Considérant que ces COS transfrontières, en cas d'acquisition conjointe avec le CECC, pourraient bénéficier d'aides financières d'un montant à hauteur de 75 % des coûts d'acquisition des outils et infrastructures et de 50 % des coûts opérationnels ;

㊿ Considérant que ces COS transfrontières seraient tenus d'échanger des informations pertinentes, y compris sur les vulnérabilités, les incidents évités, et les cybermenaces, non seulement entre eux mais également, « sans retard injustifié », avec le réseau des CSIRT, le réseau EU-CyCLONe et la Commission européenne, en cas d'information relative à un incident de cybersécurité majeur ;

(51) Considérant qu'à défaut de rejoindre un COS transfrontière dans les deux ans, un COS national perdrait le bénéfice de toute aide européenne ;

(52) Approuve la volonté exprimée par la Commission européenne d'améliorer la détection des cyberincidents et des cybermenaces au niveau européen ;

(53) Estime que la notion de « cyberbouclier » est trompeuse et qu'il devrait lui être préférée celle, plus honnête, de « cybersentinelle » ;

(54) Observe que la Cour des comptes de l'Union européenne, dans son avis 02/2023 précité, a indiqué que la présente proposition était de nature à « *rendre plus complexe l'ensemble du paysage de l'Union européenne en matière de cybersécurité* » et précisé qu'il existait un risque de « *double emploi entre les centres opérationnels de sécurité (COS) et le réseau des CSIRT déjà en place* » ;

(55) Souligne également que l'appel de Nevers des ministres de l'Union européenne en charge des télécommunications, rendu public le 9 mars 2022 sous présidence française du Conseil de l'Union européenne (PFUE), a encouragé le renforcement de la coopération et de la solidarité européennes dans le domaine de la cybersécurité en s'appuyant sur les réseaux existants ;

⑯ Rappelle à cet égard la nécessité pour les collectivités territoriales comme pour les administrations et les entreprises d'anticiper les crises de cybersécurité en élaborant un plan de continuité des activités (PCA) ;

⑰ Estime enfin que l'architecture européenne de cybersécurité, pour être pleinement efficace, doit être compréhensible par tous les acteurs de la société, citoyens comme entreprises ;

⑱ Demande la préservation de l'architecture européenne de cybersécurité existante et le renforcement des organes de coopération déjà en place ;

⑲ Recommande en conséquence le retrait du dispositif des COS, dont la nécessité et la pertinence n'apparaissent pas évidentes, et l'intégration explicite des fonctions envisagées pour ces structures au sein des compétences des CSIRT ; insiste sur la pertinence de l'échelon régional pour la mission de réponse aux incidents informatiques confiée aux CSIRT ; souhaite le développement de la coopération entre CSIRT régionaux d'États membres frontaliers ;

⑳ S'interroge sur la pertinence de la présence systématique de la Commission européenne dans les échanges d'informations sensibles prévus par l'article 7 de la proposition, eu égard à son absence de compétence opérationnelle dans le domaine de la cybersécurité et alors même qu'elle siège déjà en tant qu'observateur au sein du réseau EU-CyCLONe ;

㉑ *Sur le mécanisme d'urgence :*

㉒ Considérant que la présente proposition prévoit l'institution d'un mécanisme d'urgence, composé à titre principal d'une réserve européenne de cybersécurité, appelée à intervenir en cas de crise, à la demande d'un État membre, sur décision de la Commission européenne, et en dernier recours ;

㉓ Considérant que la réserve européenne de cybersécurité pourrait également bénéficier, sur demande, aux pays tiers ayant désigné un point de contact unique et fourni des informations suffisantes sur leurs capacités et actions de cybersécurité ;

㉔ Considérant que la réserve européenne de cybersécurité serait constituée d'entreprises privées sélectionnées par appels d'offres en tant que fournisseurs de confiance, sous réserve que les intéressées remplissent des critères de compétence technique et de garantie de la confidentialité des données ;

⑮ Considérant que les entreprises intervenant dans le cadre de la réserve bénéficieraient d'un préfinancement destiné à garantir leur disponibilité en cas d'incident et que, en cas de non utilisation de ces fonds, ces derniers pourraient être réorientés vers des actions de préparation ;

⑯ Prend acte du soutien du Gouvernement à ce mécanisme d'urgence fondé sur une alliance public/privé, qui s'inspire de l'organisation française de cybersécurité constituée autour de l'ANSSI ; constate néanmoins que ce modèle résulte d'une insuffisance des moyens dévolus aux autorités nationales compétentes en matière de cybersécurité ;

⑰ Prend note de la possibilité laissée à des entreprises extra-européennes d'intervenir au sein de la réserve européenne de cybersécurité dans les infrastructures critiques d'un État membre faisant face à une crise cyber ; relève que cette possibilité représente un risque non négligeable d'ingérence étrangère dans le fonctionnement de ces entités ; constate que l'instauration d'une telle possibilité répond à la dépendance actuelle de l'Union européenne ; observe que cette dépendance ne saurait subsister au regard de ses ambitions d'autonomie stratégique ;

⑱ Recommande par conséquent de n'inclure dans la réserve que des prestataires ayant leur siège social dans l'Union européenne, dans l'Espace économique européen ou dans un pays tiers associé à l'Union européenne et partie à l'accord sur les marchés publics de l'Organisation mondiale du commerce (OMC) ;

⑲ Appelle en conséquence l'Union européenne à soutenir les prestataires européens et à favoriser leur « montée en puissance », en vue d'assurer son autonomie stratégique ; demande en complément, une augmentation des ressources de l'ENISA par un plan de recrutement de cyber-experts européens ; ajoute que la France doit elle-même poursuivre le renforcement de ses capacités à prévenir les cyberattaques et à y répondre ;

⑳ Souhaite en outre que le dispositif envisagé impose aux États membres de fixer des sanctions effectives, proportionnées et dissuasives afin de punir le vol, la diffusion non autorisée d'informations confidentielles et l'espionnage qui pourraient découler de l'activation du mécanisme d'urgence ;

⑦① Constate que l'article 17 de la présente proposition prévoit que la réserve européenne de cybersécurité pourrait également intervenir dans un pays tiers associé à l'Union européenne, à la demande de ce pays et à condition que l'accord d'association signé entre les deux parties mentionne une telle intervention ; estime cependant nécessaire de préciser dans la présente proposition, les modalités d'intervention de la réserve en cas de demandes simultanées d'États membres et de pays tiers, en prévoyant en particulier une priorité pour les États membres puis, pour les pays tiers candidats à l'adhésion à l'Union européenne ;

⑦② *Sur le mécanisme d'analyse des incidents de cybersécurité :*

⑦③ Considérant que la proposition tend à confier à l'ENISA une mission d'analyse des incidents de cybersécurité, à la demande de la Commission européenne, du réseau EU-CyCLONe et du réseau des CSIRT ;

⑦④ Approuve le principe d'un tel mécanisme qui favorise la coordination des organes mentionnés en les faisant bénéficier mutuellement de « retours d'expérience » sur les crises et en leur permettant d'en tirer des enseignements pour l'avenir ;

⑦⑤ Remarque toutefois que la directive SRI 2 confie déjà une telle mission au réseau EU-CyCLONe et souhaite en conséquence une clarification de la rédaction du dispositif envisagé afin d'éviter les « doublons » ;

⑦⑥ Souhaite confirmation de la pleine intégration des États membres à cette revue des incidents de cybersécurité effectuée par l'ENISA, *via* leur contribution à l'analyse des incidents et leur information sur les conclusions de cette analyse ;

⑦⑦ *Sur l'ampleur des renvois aux actes d'exécution :*

⑦⑧ Relève que le recours aux actes d'exécution est prévu à l'article 291 du traité sur le fonctionnement de l'Union européenne (TFUE) ; souligne que ce recours est justifié quand il est nécessaire d'assurer des conditions uniformes d'exécution des actes juridiquement contraignants de l'Union européenne ; constate cependant, qu'en renvoyant à des actes d'exécution la fixation des types et du nombre de « services de réaction aux incidents » nécessaires pour activer la réserve de cybersécurité de l'Union européenne, jusqu'à celle des modalités d'attribution des services d'aide fournis par cette réserve, les articles 12 et 13 de la proposition confèrent à la Commission européenne des compétentes d'exécution abusives ;

⑲ *Sur l’état de préparation des institutions européennes aux menaces de cybersécurité :*

⑳ Rappelle que la Cour des comptes de l’Union européenne constatait en 2022 que l’état de préparation des institutions européennes aux menaces de cybersécurité était « globalement insuffisant », insistant en particulier sur l’absence de lignes directrices et de protocoles opérationnels, ainsi que sur la rareté des formations délivrées à leurs personnels ;

㉑ Salue en conséquence l’adoption définitive de la proposition de règlement COM(2022) 122 final établissant des mesures destinées à assurer un niveau élevé commun de cybersécurité dans les institutions, organes et organismes de l’Union européenne.

㉒ Invite le Gouvernement à faire valoir cette position dans les négociations au Conseil.