ASSEMBLÉE NATIONALE

XV^e LÉGISLATURE

Compte rendu

Commission des affaires européennes

Jeudi
14 novembre 2019
9 h 30

Compte rendu n° 111

Présidence de Mme Sabine Thillaye
Présidente

ASSEMBLÉE NATIONALE

COMMISSION DES AFFAIRES EUROPÉENNES

Jeudi 14 novembre 2019

Présidence de Mme Sabine Thillaye, Présidente de la Commission

La séance est ouverte à 9 h 43.

I. Table ronde sur la cybersécurité en présence de M. Juhan Lepassaar, directeur exécutif de l'ENISA, M. Steve Purser, directeur des opérations de l'ENISA, M. Jean-Baptiste Demaison, président du conseil d'administration de l'ENISA, et M. Cyril Cuvillier, sous-directeur adjoint de la stratégie de l'ANSSI

Mme la Présidente Sabine Thillaye. La cybersécurité, sujet de la table ronde qui nous réunit aujourd'hui, est d'une brûlante actualité. 80 % des entreprises européennes auraient été victimes d'attaques informatiques, ce qui pose la question de l'action de l'Union européenne en matière de prévention de celles-ci, mais aussi en termes de réaction. La cybersécurité est également un enjeu technologique et industriel majeur car elle constitue un marché qui ne doit pas être abandonné aux entreprises américaines ou chinoises.

Pour nous éclairer sur ces enjeux ainsi que sur la politique européenne en matière de cybersécurité, nous accueillons M. Juhan Lepassaar, directeur exécutif de l'ENISA, l'Agence européenne de cybersécurité, M. Steve Purser, directeur des opérations de l'ENISA, M. Jean-Baptiste Demaison, président du conseil d'administration de l'ENISA et M. Cyril Cuvillier, sous-directeur adjoint de la stratégie de l'ANSSI, l'Agence nationale de la sécurité des systèmes d'information.

M. Juhan Lepassaar, directeur exécutif de l'ENISA. Je tiens en préalable à vous remercier pour cette invitation à présenter le point de vue de l'ENISA sur la cybersécurité et la France pour le soutien qu'elle apporte à notre Agence. Je souligne également la très bonne coopération entre l'ENISA et les différentes agences nationales, parmi lesquelles l'ANSSI.

Je commencerai mon intervention par rappeler que l'Union européenne avait une opportunité unique d'établir un cadre de régulation qui pourrait devenir une norme internationale en matière de cybersécurité. Elle l'a saisie en adoptant la directive SRI qui constitue le cadre actuel de protection des infrastructures critiques contre les attaques informatiques : réseaux énergétiques, de transport, de santé, financiers… L'Union européenne est la seule à disposer d'un tel cadre, utile aux États membres comme aux citoyens, qui doit certes être renforcé et opérationnalisé. Quant à l'Acte sur la cybersécurité, entré en vigueur cette année, il représente une opportunité à saisir pour accroître la production et la distribution de produits et services liés à la cybersécurité.

S'agissant maintenant plus précisément de l'ENISA, celle-ci a deux missions principales. La première est d'aider l'Union européenne et les États membres à avoir une approche commune des enjeux liés à la cybersécurité. Par exemple, s'agissant de la 5G, l'ENISA a contribué, avec la Commission européenne et les États membres, à cartographier et évaluer les risques, ainsi qu'à déterminer les moyens de les réduire. L'ENISA assure également le secrétariat du réseau des CSIRT européens, qui permet l'échange d'informations et d'expériences sur les attaques informatiques. En d'autres termes, même si tous les experts européens ne travaillent pas pour elle, l'ENISA a un rôle majeur d'animation de la communauté cyber européenne.

La deuxième mission de l'ENISA est la certification en matière de cybersécurité. Plus précisément, elle travaille, par l'intermédiaire de groupes de travail composés notamment d'experts nationaux, à établir des normes communes de certification, pour les objets connectés ou les réseaux systémiques.

M. Steve Purser, directeur des opérations de l'ENISA. L'ENISA, qui ne dispose que de 70 collaborateurs, est avant tout une agence de coopération. Elle travaille étroitement avec les Agences nationales de cybersécurité ainsi qu'avec les entreprises privées. Parmi les sujets dont elle s'occupe, je voudrais citer l'intelligence artificielle, la 5G, l'économie et la souveraineté numérique, les *fake news*, l'économie de la cybersécurité et la sécurité informatique.

Pour l'intelligence artificielle, vous êtes sans doute au courant que la Commission étudie actuellement la partie éthique du sujet. L'ENISA, avec son conseil d'administration, a défini une première tâche pour l'année prochaine, qui est principalement de comprendre l'intelligence artificielle (IA) du point de vue de la cybersécurité, et d'assurer une base de cybersécurité dans l'IA elle-même. Beaucoup de gens parlent de garantir la sécurité grâce à l'IA ; pour notre part, nous voulons être certains que l'IA elle-même est bien sécurisée.

Je pense que nous serons rapidement dans les contenus : comment combattre la *fake logic* par exemple ? Cela m'amène à un commentaire très important : le sujet qui revient sans cesse est celui de la sécurisation des logiciels dès leur conception, puis au cours de leur existence. C'est très difficile, mais je pense que c'est à la base de beaucoup de problèmes.

Plusieurs choses nous empêchent de faire cela. Le nombre de lignes de codes dans une voiture est d'environ 100 millions à l'heure actuelle. Vous imaginez le travail nécessaire pour sécuriser un tel volume. Or, on cherche aussi des méthodes économiquement viables, qui marchent en un temps et à un coût raisonnables.

Je ne vais pas beaucoup parler de la 5G, mais simplement dire que c'est d'une complexité énorme. Il faut procéder lentement mais sûrement. Ce n'est pas un concept fixe : les normes évoluent au jour le jour, ce qu'il faudra prendre en compte. La sécurité a trois aspects : les gens, les processus et la technologie. En l'espèce, le processus est très important.

Je souhaiterais insister sur la notion d'autonomie stratégique numérique. Cela signifie que chaque État membre contrôle sa propre infrastructure, tout comme l'Union européenne. Cela ne signifie pas que les États membres doivent fabriquer totalement les infrastructures, mais qu'ils contrôlent la chaîne d'approvisionnement et que rien n'est ajouté dans leurs produits sans leur consentement.

J'aimerais également évoquer le concept de souveraineté numérique. Il correspond à l'idée qu'en Europe, et c'est très vrai de la France, il y a une compétence très poussée en matière de cybersécurité. On peut l'utiliser en lien avec notre politique industrielle et pour stimuler nos marchés. Vous avez sans doute constaté le lancement de discussions sur un *Cloud* européen, Gaia.

Enfin, les *fake news* et la désinformation sont un sujet important. Vous vous interrogez peut-être sur le rapport avec la sécurité informatique. En réalité, nous nous préoccupons de tout ce qui est trompeur (le *bad looking good)*. Les fausses nouvelles ne font pas exception. Nous avons un rôle à jouer en la matière.

Pour finir, j'aimerais dire quelques mots de la dimension économique de la cybersécurité. L'Union européenne et les États membres dépensent des sommes considérables mais il existe très peu d'instruments pour en mesurer l'impact. Il faut essayer de trouver des données sur le retour sur investissement. Les études, quand elles existent, sont insuffisantes. Quelqu'un doit commencer à vous donner les informations de base relatives aux effets de vos décisions, tant au niveau macro que microéconomique.

Vous avez sans doute entendu parler du débat sur les ordinateurs quantiques, qui vont changer la sécurité d'une façon radicale. Dès qu'on a un ordinateur quantique, le système de cryptographie est mis à plat. Depuis longtemps, nous travaillons sur la réponse, qu'est la cryptographie post-quantique. À mon avis, cela mérite d'être défendu. Nous serons dans quelques années dans une situation difficile, si nous ne réagissons pas. Sur le calcul quantique en lui-même, beaucoup de gens préconisent de l'utiliser pour faire de la cryptographie. Toutefois, il faut être prudent : à l'ENISA, nous ne voyons pas la pertinence de ce procédé très coûteux pour le moment.

L'ENISA est ici pour vous soutenir, en tant qu'État membre, mais aussi comme État qui dispose d'une agence de cybersécurité très développée. Nous sommes à l'écoute de vos conseils

M. Cyril Cuvillier, sous-directeur de la stratégie de l'ANSSI. Nous sommes très heureux d'avoir été conviés ce matin et qu'un rapport d'information ait été rédigé pour informer les parlementaires.

Je souhaite dire quelques mots sur la manière dont l'état de la question cyber est perçu à l'échelle européenne. La législature précédente a fait un énorme travail en posant des fondations. Cependant, chaque sujet qui a avancé n'est que le premier étage d'une structure à consolider. Nous devons faire preuve de vigilance et ne pas passer immédiatement aux sujets suivants. Il faut encore rationaliser, piloter, améliorer les démarches entreprises.

D'abord, nous avons renforcé la résilience de l'Union face aux risques cyber. Il faut évidemment citer la directive NIS (ou SRI). Elle s'intéresse au cadre de sécurité sur les infrastructures dites critiques. En France, nous avions un modèle déjà bien développé pour les infrastructures vitales, mais l'Europe a commencé à parler d'opérateurs essentiels à la prospérité économique. Cette démarche a très bien démarré et elle se poursuit ; un de nos rôles dans les prochaines années est d'observer comment cela se poursuit.

La question est la façon de résoudre des crises à l'échelle européenne. Nous avons réalisé qu'il fallait pouvoir échanger entre nous à un niveau plus opérationnel et plus stratégique, de manière à ce que les États membres réfléchissent entre eux. La France a

accueilli le 2 juillet dernier un exercice de cette nature, avec la grande majorité des directeurs d'agences et de structures nationales. Il va probablement avoir à nouveau lieu, parce que nous nous sommes rendu compte qu'il était nécessaire d'avoir ce niveau de préparation aux crises.

Au cours de cette législature, nous nous sommes aussi rendu compte que la sécurité des institutions européennes elles-mêmes doit faire l'objet d'une vigilance régulière. Il ne faut pas prendre la sécurité comme acquise, comme en témoignent certains incidents qui ont fait l'objet de communications officielles.

Enfin, je souhaite aborder la question de la résilience. Le travail a beaucoup avancé dans le domaine de l'édification d'un réseau industriel. Comment faire émerger une industrie apte à répondre au défi de la confiance dans le domaine du numérique ? La législature qui se termine a donné lieu à une expérimentation autour d'un partenariat public privé. Ce sujet va perdurer sous la forme d'un texte sur un centre de compétences, qui vise à mieux structurer les compétences dans le temps, mieux flécher les budgets de recherche. L'objectif est de faire émerger un réseau industriel pour répondre au défi d'autonomie stratégique dans le domaine du cyber. Nous devons être très aidants dans la relation dans la relation entre nos moyens budgétaires et les moyens de l'industrie.

Le troisième point, qui n'est pas à négliger, est le développement d'outils diplomatiques. Nous avons vu que les crises ont une dimension diplomatique. Les politiques ont besoin que nous sachions les accompagner d'une lecture technique. Des textes ont été générés au cours des dernières années.

Nous sommes persuadés que l'échelle européenne est la bonne pour traiter ces sujets. En même temps, nous nous assurons que les textes intègrent des exceptions de souveraineté, par exemple dans le cas de la certification des produits cryptographiques. Dans les domaines régaliens, nous souhaitons pouvoir mener les projets qui nous semblent nécessaires. Toutefois, de manière générale, pour rendre les producteurs responsables, en appeler à des démarches qui standardisent les efforts qu'on leur demande, l'Union européenne est le bon niveau.

Nous l'avons vu avec le RGPD : la force d'un texte de ce périmètre a été absolument magistrale dans la prise de conscience des responsables. On peut alors obtenir un impact réel.

L'ENISA est une agence qui est au cœur de cela car elle apparaît, au sein des entités de l'Union européenne, comme un lieu vers lequel se tourner lorsque des questions se posent. Les parlementaires européens veulent savoir ce qu'est la « *blockchain* », le « quantum » et tous ces concepts complexes. Il faut donc que nous ayons un centre qui soit non pas expert mais en capacité de repérer que tel État membre a écrit un texte intéressant sur ce sujet et que c'est ce texte-là qu'il faudrait lire en premier, que tel État membre dispose de compétences qui peuvent nous aider à appréhender le sujet.

Sur la 5G, l'ENISA se pose en animateur d'un effort collectif des États membres pour rédiger un document qui analyse le risque, non pas dans l'idée de dessaisir les États du problème mais de proposer de le résoudre, en invitant les États à développer leurs expertises, leurs analyses de risque, leurs stratégies politiques. L'ENISA a montré au cours des dernières années le rôle remarquable qu'elle a joué. Quand on considère par exemple la question de la sensibilisation de nos concitoyens, l'ENISA organise un mois européen de la cybersécurité tous les ans. Quand nous parlons de renforcer le rôle des étudiants dans l'informatique et

le cyber, il s'agit d'un challenge européen animé par l'ENISA. La France s'inscrit, comme les autres États, dans cette démarche, les incitant à s'inscrire à ce challenge et les étudiants se prêtent à cet exercice.

Il faut que nous apprenions à nous entraîner à l'échelle européenne et l'ENISA encadre la mise en œuvre de « cyber Europe », exercice de dimension européenne très utile pour convenir de méthodes partagées. Nous avons également évoqué le réseau de CERT qui profite beaucoup du soutien de l'ENISA.

Il faut aller au-delà et nous nous réjouissons que l'ENISA, après plusieurs mandats provisoires, se soit installée dans un mandat définitif, durable, sous la forme d'une agence européenne. Nous sommes heureux que la France, en la personne de Jean-Baptiste Demaison, se soit vue à nouveau confier la présidence du conseil d'administration de l'ENISA. Monsieur Demaison occupait déjà cette fonction et a été renouvelé à l'unanimité par ses collègues, signe d'une réelle adhésion à sa démarche de travail. Cette démarche vise à continuer les efforts par lesquels l'ENISA doit impliquer les expertises des États membres pour fédérer ce travail, comprendre les nouveaux sujets et aider les États à renforcer leurs capacités.

M. Jean-Baptiste Demaison, président du Conseil d'administration de l'ENISA. Le Conseil d'administration de l'ENISA est composé de vingt-huit États membres et de deux représentants de la Commission européenne. Notre travail est de doter l'ENISA d'un programme de travail et plus généralement d'orientations stratégiques guidant son action. Je suis par ailleurs également agent de l'ANSSI et conseiller du sous-directeur à la stratégie de cette agence nationale.

Les précédents intervenants ont parlé des défis politiques et technologiques pour l'Europe, de l'enjeu de la souveraineté numérique de l'Union européenne et de l'autonomie stratégique en matière de sécurité. Je crois que nous abordons en 2020 une nouvelle ère pour la cybersécurité européenne. Le cadre européen de certification devrait permettre à l'avenir de relever significativement le niveau de sécurité des solutions et services numériques utilisés par les administrations, les entreprises et les citoyens européens. Il s'agit d'un pas de géant et l'ENISA est appelée à jouer un rôle central et opérationnel dans le fonctionnement de ce réseau. C'est une nouvelle ère, car l'enjeu est gigantesque pour relever le niveau de cybersécurité de l'ensemble de l'Union. L'ENISA devra plus que jamais jouer un rôle de facilitatrice active qui ne se contente pas de mettre les gens autour de la table, mais qui fasse émerger une expertise européenne et progresser les États membres dans leurs capacités nationales, tout en renforçant la coopération entre les agences nationales en matière opérationnelle.

J'utilise le concept « d'agence-plateforme », qui permet de prendre et rendre le meilleur à la communauté européenne. Ce changement dans le panorama des défis pour la cybersécurité occupe beaucoup le conseil d'administration. Je conclurai en disant que l'enjeu dans les mois à venir est de doter l'agence d'une nouvelle stratégie, afin de fixer des objectifs à cinq ans. Nous nous félicitons de la nomination de Juhan Lepassaar comme nouveau directeur exécutif de l'agence. Il s'agit d'un moment pivot pour l'agence et nous ferons en sorte d'accompagner le nouveau directeur exécutif dans ses missions face aux défis évoqués.

Mme la Présidente Sabine Thillaye. Est-ce que ce sujet de la cybersécurité, auquel nous avons donné un cadre, prend suffisamment en compte les PME et les personnes physiques ? Nous avons tous une responsabilité quant à l'utilisation des outils informatiques à

notre disposition. Une revue juridique parlait de « monstre doux » pour désigner ces technologies. Nous nous faisons d'une certaine manière happer par les facilités que tous ces outils nous offrent, sans tenir compte de la nécessité de se protéger en tant que personne privée. Je souligne que pour les PME il est parfois complexe de s'informer et de faire les démarches nécessaires.

M. Juhan Lepassaar, directeur exécutif de l'ENISA. La cybersécurité ne s'applique pas uniquement aux entreprises informatiques ou à l'industrie. Sa fonction primaire est de protéger la société. L'ENISA travaille sur la sensibilisation dans toute l'Europe avec différentes mesures, par exemple le mois « cyber ». Nous collaborons avec des entités européennes et nationales pour avoir des supports de sensibilisation à distribuer dans l'Union européenne. Mais la tâche la plus importante pour l'ENISA et pour toutes les autorités de cybersécurité est de promouvoir la cybersécurité par défaut, intégrée dans les solutions. Il vaut toujours mieux sécuriser l'infrastructure avant une crise, plutôt que de retourner en arrière et d'essayer de réparer les failles.

Intégrer la sécurité dans la conception des outils est une tâche que je prends très à cœur et c'est une nécessité qui découle de l'acte de cybersécurité. Il nous incombe de trouver des mécanismes pour faire en sorte que les fabricants créent des outils qui soient déjà sécurisés. On ne peut pas présumer que les consommateurs soient experts dans la cybersécurité et sachent déjà comment protéger les services qu'ils utilisent. Il y a des fonctionnalités basiques que tout le monde connaît, comme mettre à jour les logiciels régulièrement, ce qu'il faut faire car cela protège les systèmes. Mais cela devrait être automatique.

Mme la Présidente, vous avez parlé des PME : lorsqu'on met en œuvre ce nouveau cadre de régulation, il faut toujours garder les PME à l'esprit. L'acte sur la cybersécurité, en ce qui concerne la certification, a déjà une approche proportionnée. Il y a différents niveaux de certification : on peut avoir une auto-certification, plus simple pour les PME, puis un niveau supérieur qui serait une certification validée par un tiers, ce qui coûte plus cher et prend plus de temps. Toutes les PME n'ont pas le temps ou les moyens nécessaires pour se faire certifier par un tiers. Il est nécessaire d'aider les PME, les petits employeurs et les *start-up* à se sécuriser et à utiliser le cadre de régulation. Un système d'auto-certification constitue la première étape.

M. Éric Bothorel, rapporteur. Avant d'entrer dans le détail au travers du rapport qui m'a été confié, je voudrais revenir sur plusieurs points qui ont été évoqués. Le directeur de l'ANSSI voit la cybersécurité comme « positive » ou « heureuse ». Il me semble que dans les expressions évoquées jusqu'ici on retrouve un élément important, à savoir la nécessité de considérer la cybersécurité comme un vecteur potentiel de développement économique, au travers la capacité à faire émerger des standards. L'exemple le plus concret est celui du règlement général de protection des données (RGPD), qui est un modèle qui s'exporte. Il est nécessaire qu'au sein de l'Union européenne puissent émerger des standards ambitieux, à la hauteur de l'état de la menace. Ces standards doivent être reconnus à l'échelle internationale et exportables.

Il est parfois difficile de faire adhérer nos concitoyens, en particulier les PME, et à leur faire prendre conscience des risques auxquels ils s'exposent, avec des outils de plus en plus interconnectés et immatériels. Il y a trente ans, nous étions majoritairement dans un système « *hardware* » et la garantie de sécurité d'un produit reposait avant tout sur la chaîne d'approvisionnement, la fabrication des composants et le jeu de puces. Aujourd'hui, nous

sommes passés à un système beaucoup plus immatériel et il a été rappelé combien de millions de lignes de codes il existe dans une automobile. C'est vrai pour presque l'ensemble des systèmes. C'est ce à quoi l'Assemblée nationale a été sensibilisée dans le cadre de l'examen du texte de loi sur la 5G dont je fus le rapporteur. La 5G constitue une avancée technologique qui repose aussi sur le fait que les infrastructures sont de plus en plus immatérielles et totalement évolutives, avec des mises à jour permanentes.

C'est dire si la capacité qu'ont les agences, et notamment la plus belle d'entre elles, l'ANSSI (pardon pour les autres !), dépend des crédits votés par le législateur. Notre responsabilité n'est donc pas seulement de commenter ou de subir l'actualité, mais aussi de prendre des initiatives et d'allouer des moyens aux agences à qui l'on confie ce genre de missions. Nous avons aussi su largement déléguer à l'ANSSI, confiants dans ses compétences, pour lui permettre de faire sur la 5G ce qu'elle a fait déjà fait sur la 3G et la 4G.

Il faut prendre conscience des difficultés posées par les menaces hybrides, que l'on va rencontrer de plus en plus. Ces menaces sont appelées « hybrides » parce qu'elles émanent d'États ou de proto-États et conjuguent les nouvelles technologies et des moyens conventionnels. En Arabie Saoudite, une simple attaque par drone sur quelques puits pétrolifères a causé de grands désordres. Une autre problématique nouvelle : la sécurisation des processus électoraux dans un contexte de *fake news*, où le vraisemblable devient le vrai et où les régimes politiques et les opinions publiques sont susceptibles d'être manipulés.

Ainsi l'ENISA a-t-elle un rôle indispensable d'animation auprès de l'ensemble des agences nationales, dans une logique à la fois offensive (se prémunir contre les risques futurs) et défensive (se prémunir contre les risques actuels). Il faut toujours penser au volet anticipation et au volet protection.

Je termine en disant qu'il est fondamental que, tout en recherchant un bon niveau de sécurité, nous traduisions nos efforts au niveau économique. La cybersécurité en tant que domaine de recherche est un relais de croissance pour toutes les entreprises européennes qui travaillent dans ce secteur, et qui sont parmi les meilleures au monde. Il faudra pouvoir construire des champions industriels de la cybersécurité européenne.

M. Jean-Louis Bourlanges. J'ai peine à intervenir dans un domaine où, comme disait Aristide Briand, « je suis d'une ignorance encyclopédique ». Je dois dire que si j'étais candidat à la Commission européenne sur ces questions, il n'y aurait aucun risque qu'on me reproche une familiarité excessive avec le secteur…

Une question donc d'une innocence absolue : celle de la subsidiarité. Sans remettre en cause l'utilité de votre travail, qu'est-ce qui, dans ce que vous faites, doit être fait spécifiquement au niveau européen ? C'est un domaine où la compétence de droit commun revient en principe aux États membres, et où l'Union européenne n'a qu'une compétence d'attribution conditionnée par le principe de subsidiarité. Quelle est la spécificité de l'intervention au niveau européen par rapport à l'intervention des États au niveau national ?

Mme Christine Hennion. Il est important de maintenir et de développer nos capacités technologiques et industrielles dans la cyber, à la fois pour nous protéger et pour construire cette économie du monde de la cyber qui nous permettra d'avoir notre indépendance numérique européenne.

Comme le souligne le rapport de notre collègue, les moyens de l'ENISA sont encore très limités, et sans doute insuffisants ; par ailleurs la directive SRI (2016) est une première étape vers le chemin qui nous permettra de disposer de l'ossature de la cybersécurité au niveau européen, mais il y a un manque de coordination entre certaines instances internationales (l'ONU, l'OTAN, Interpol…), dont les compétences et les missions ne sont pas toujours bien définies et partagées. Saluons tout de même certaines initiatives de la Commission européenne : le nouveau cadre du « paquet cyber » qui prévoit un élargissement du mandat de l'ENISA et une augmentation de ses moyens ; un cadre de certification à construire pour avoir un espace de sécurité uniforme ; le nouveau centre de compétence industrielle, technologique et de recherche en matière de cybersécurité.

Comment construire progressivement et pragmatiquement le cadre de cybersécurité par le « paquet cyber » ? Comment, en tant que parlementaires nationaux, pouvons-nous contribuer à la mise en place de ces nouvelles missions au niveau européen ?

M. André Chassaigne. Je dirai d'abord à mon collègue Bourlanges, avec qui nous avons l'habitude d'échanger, qu'il faut sortir de l'ignorance encyclopédique, ce qui suppose certes de faire des efforts intellectuels, voire une « révolution copernicienne »…

Je voudrais revenir sur le travail fait par la commission de la Défense, avec le rapport de Bastien Lachaud et d'Alexandra Valetta-Ardisson publié en juillet 2018 à la suite d'une mission d'information sur la cyberdéfense. Ce rapport insistait sur la nécessité d'accompagner les efforts d'harmonisation de la certification au niveau européen. Il s'appuyait sur le fait que le système européen de certification vise à garantir la sécurité d'utilisation des produits et des services dans l'environnement numérique en veillant à ce qu'ils respectent les exigences de cybersécurité, les certificats délivrés devant être reconnus dans tous les États membres. D'où ma première question : y a-t-il aujourd'hui des avancées concrètes à propos de la reconnaissance des certificats dans les États membres ?

Deuxième question : cette certification harmonisée, si elle prospère, doit être effectuée sur la base de critères exigeants, et non en fonction du « plus petit dénominateur commun ». Êtes-vous sensible à ce risque de « tirer vers le bas » les exigences de cybersécurité au lieu de les renforcer ?

Troisième observation : le rapport de la commission de la Défense souhaitait « mener une diplomatie normative active, afin de promouvoir les modèles et les valeurs de la France dans le domaine cyber ». Cette « diplomatie » devrait permettre de développer l'influence normative de la France à l'international. Est-ce que cette diplomatie se limite aux pays de l'Union européenne, ou ne touche-t-elle pas plus largement à l'OTAN ? Peut-on espérer un jour – mais sans doute est-ce un rêve – qu'il puisse y avoir un corpus juridique international commun au niveau mondial, organisé autour de l'ONU ?

Mme Aude Bono-Vandorme. Le 31octobre dernier, le Centre européen de lutte contre la cybercriminalité et l'ENISA ont organisé une simulation afin de tester le protocole de réaction d'urgence de l'Union européenne face aux cyberattaques transfrontalières affectant les secteurs privé et public. Vos analyses ne sont certes pas terminées, mais quelles sont vos premières impressions sur la mutualisation des moyens et l'efficacité de la réaction conjointe des pays qui ont participé à cette simulation ?

M. Cyril Cuvillier, sous-directeur adjoint de la stratégie de l'ANSSI. Je réponds à M. Bourlanges au sujet de la subsidiarité. Quelle action spécifique y a-t-il à mener à

l'échelle européenne ? Je prends l'exemple de la démarche de certification. À une échelle trop petite, il est difficile de structurer le marché autour des règles attendues quant aux équipements et aux façons de les installer, de les maintenir ou de les retirer du service lorsqu'ils sont obsolètes, etc. Ces questions sont extrêmement importantes. Dès le début, lorsqu'on achète un équipement et qu'on le met en service, il faut s'assurer qu'il a été bien conçu et que son installation est conforme aux meilleures pratiques. C'est ce qu'on appelle la *security by default*.

Or aujourd'hui, nos entreprises ont toutes des zones de chalandise qui dépassent la France. Les jeunes entreprises, en particulier, ont besoin d'une zone économique plus grande pour saisir des opportunités sur un domaine technologique très vaste. Pour aider ces entreprises, il faut leur apporter de la clarté quant aux règles que l'on souhaite édifier. C'était l'objet du texte très ambitieux sorti l'an dernier sur le schéma de certification. L'objet de ce texte n'était pas de dire comment certifier tel ou tel équipement, mais d'organiser le travail à 28 pour parvenir à mettre en place un schéma de certification. C'est ce que l'on fait à l'échelle européenne et que l'on ne peut pas faire à l'échelle nationale : convenir des règles du jeu grâce auxquelles les États membres vont se mettre d'accord, reconnaître leurs centres de certification respectifs et s'assurer que ces centres soient indépendants des entreprises dont ils doivent certifier les produits. Il ne doit en effet pas y avoir d'intéressement à certifier. S'il y a dans un pays européen un centre de certification aux prestations coûteuses et aux exigences assouplies, cela ne fonctionne pas. Il était nécessaire de créer la confiance dans notre capacité à observer nos centres respectifs, à les reconnaître, à préciser leurs compétences et à fixer des prérequis techniques.

C'est pour cette raison que ce texte était très ambitieux. Il entendait à la fois traiter les besoins du quotidien, avec des niveaux de certification peu coûteux à établir, et installer des schémas de certification de haut niveau pour protéger les produits qui peuvent être attaqués par des menaces de très haut niveau. Les règles du jeu pour l'élaboration des schémas de certification sont en place. L'ENISA va avoir un rôle particulier pour accompagner les États membres dans leur rédaction.

M. Juhan Lepassaar, directeur exécutif de l'ENISA. Au sujet de la subsidiarité, il faut être clair sur la répartition des responsabilités entre le niveau européen et le niveau national.

Je vais m'appuyer sur une métaphore simple. S'il y a un incendie, ce n'est pas l'ENISA qui va venir éteindre l'incendie, cela relève de la responsabilité des autorités nationales. L'ENISA est là pour s'assurer qu'il y ait des mécanismes d'alerte incendie dans les établissements, que les pompiers sont bien formés et elle aide les différentes brigades de pompiers, lorsque l'incendie est important, à échanger les informations pour qu'elles puissent mieux se préparer. Elle est également là pour les aider à tirer les enseignements de l'événement. C'est la mission de l'échelon européen.

L'échelon national est le premier à aller sur le terrain, mais nous souhaitons qu'il y ait une coordination toujours plus poussée. Je suis ravi de constater que l'ANSSI appelle de ses vœux la mise en place de mécanismes européens.

Les parlements nationaux ont un rôle à jouer pour s'assurer que la cybersécurité reste au cœur des priorités des gouvernements. Il ne s'agit en effet pas uniquement d'une question technologique, mais d'une question hautement stratégique et politique.

Deuxièmement, le cadre de certification de cybersécurité soulève la question du type de produits et de services devant relever de cette certification. Chaque État membre est représenté au sein du groupe de certification européen qui discute des catégories de produits et services qui doivent être certifiés en priorité. Il faut certes identifier les lacunes, mais c'est aussi une question de priorités politiques. Je serais intéressé de connaître celles des parlements nationaux.

L'ENISA a également un rôle à jouer pour ce qui concerne l'identité numérique. Un mécanisme de rapport des incidents a été mis en place, qui nous permet de tirer des enseignements de nos vulnérabilités afin de s'assurer que les identités numériques nationales soient préservées. Il nous faut évaluer ce cadre, l'améliorer et peut-être l'inscrire dans le cadre général de lutte contre la cybercriminalité.

Des questions très spécifiques ont été posées sur la certification. Je rappelle que l'ENISA est une agence qui relève du marché intérieur ; elle n'a pas compétence en matière de défense nationale. L'ENISA est dotée de la capacité d'aider les États membres et l'Union Européenne en matière de coopération internationale, mais elle n'est pas chef de file. C'est aux États membres de faire appel à l'ENISA. Celle-ci ne peut pas avoir une approche proactive, mais elle est toujours là pour aider à définir une approche commune et apporter son expertise.

M. Steve Purser, directeur des opérations de l'ENISA. Pour répondre correctement à la question posée sur l'exercice de simulation, il faut revenir au point de départ, en 2010, lorsque nous avons commencé les exercices.

Le premier exercice, en 2010, était relativement simple. Nous cherchions à répondre à trois questions : en cas d'urgence, savons-nous qui appeler dans un autre pays ? Si oui, connaissons-nous son niveau de responsabilité et ses possibilités de réaction ? Enfin, quels sont les protocoles utilisés pour échanger les informations ? Cet exercice a révélé que nous étions très peu préparés : les résultats ont été mauvais sur chacun des trois points.

La bonne nouvelle, c'est que, depuis 2010, plusieurs exercices ont montré que nous savions désormais très bien répondre à ces trois questions. Les *standard operating procedures* ont bien évolué, notamment grâce à l'ANSSI et aux autres agences. Les protocoles ont été testés à de multiples reprises. Ils ont notamment été utilisés à l'occasion des crises de *WannaCry* et *NotPetya*, au cours desquelles ils se sont avérés relativement efficaces. Les conséquences de ces attaques auraient été pires si nous n'avions pas utilisé ces procédures. Nous avons encore un long chemin à parcourir, mais nous sommes relativement bien positionnés.

Pour en revenir à la question de Mme Bono-Vandorme, il y a eu un exercice il y a deux ou trois semaines pour tester le protocole développé par Europol. J'ai eu des retours très positifs, mais j'insiste sur le fait qu'il ne s'agit que d'un premier pas.

En Europe, nous n'avons pas de *cyber-tsar*, de contrôle centralisé. Nous travaillons ensemble, avec une réponse multilatérale. Les États membres ont fait un excellent travail en concevant un système qui nous permet de réagir très rapidement. Il nous reste à le rendre encore plus rapide, à hiérarchiser les informations transmises et à s'assurer de l'émergence d'une véritable communauté. Il est extrêmement important que les gens se connaissent pour que les choses avancent plus rapidement.

M. Cyril Cuvillier, sous-directeur adjoint de la stratégie de l'ANSSI. Les enjeux en matière de cybersécurité sont également débattus dans plusieurs enceintes internationales, notamment au sein du groupe de travail de l'ONU sur le désarmement. En 2017, le dernier rapport de ce dernier n'avait pas été très conclusif. J'espère que le prochain le sera, en particulier sur les modalités d'application du droit international dans le cyberespace. Sur ce point, la position française est très claire : il doit s'appliquer. Parmi les autres enceintes pertinentes en matière de cybersécurité, je citerai l'OSCE ou l'OCDE, où la France est représentée par le ministère des Affaires étrangères.

M. Jean-Louis Bourlanges. Vous avez évoqué la séparation du militaire et du civil en matière de cybersécurité. N'y aurait-il pas, à l'inverse, une logique à les réunir ?

M. Cyril Cuvillier, sous-directeur adjoint de la stratégie de l'ANSSI. La notion de « Défense » doit être précisée. Pour nous, la cyberdéfense signifie se défendre contre une attaque et non pas attaquer afin de mettre hors d'état de nuire ceux qui nous attaquent. Là n'est pas le travail de l'ANSSI. J'ajoute qu'il est nécessaire pour nous de maintenir des relations de confiance avec les entreprises qui doivent être assurées que les informations qu'elles nous transmettent ne pourront pas être utilisées contre elles.

M. Éric Bothorel, rapporteur. La doctrine en France est en effet de distinguer entre la cyberdéfense et la cybersécurité. En effet, certaines technologies nécessaires pour protéger les infrastructures militaires ne sont pas utilisables dans les domaines civils, notamment parce qu'elle devrait être conciliée avec les droits fondamentaux comme la liberté d'expression. Certes, cyberdéfense et cybersécurité peuvent s'enrichir mutuellement, mais c'est la force de la France que de maintenir une distinction entre les deux.

II. Présentation du rapport d'information de M. Éric Bothorel sur l'avenir de la cybersécurité européenne

Mme la Présidente Sabine Thillaye. Je propose à nos invités de rester parmi nous pour la présentation du rapport d'information et je les invite à réagir s'ils le souhaitent. M. le rapporteur, vous avez la parole.

M. Eric Bothorel, rapporteur. Le rapport que je vais vous présenter aujourd'hui porte sur l'avenir de la cybersécurité européenne, à l'aune des changements législatifs intervenus récemment dans l'Union. Ces changements ont fait l'objet de la table ronde qui a précédé la présentation du rapport, aussi ne reviendrai-je pas dans le détail sur le contenu de l'Acte de cybersécurité européen ou sur la directive SRI qui l'a précédé.

Ce travail m'a conduit à réaliser une large consultation d'acteurs concernés par l'introduction de l'Acte de cybersécurité européen, avec près d'une trentaine d'auditions menées, aussi bien à Paris qu'à Bruxelles, Athènes et Madrid. Ces auditions ont permis de recueillir la position des principales institutions publiques impliquées par la mise en œuvre de l'Acte de cybersécurité, ainsi que des acteurs majeurs du secteur privé.

Selon la Commission européenne, 80 % des entreprises européennes connaissent au moins un « incident de cybersécurité » par an. Dans certains États membres de l'Union, jusqu'à 50 % des crimes perpétrés interviendraient dans le champ de la cybercriminalité. Les cybermenaces peuvent prendre des formes multiples, comme en rend compte le rapport sur l'état de la menace liée au numérique en 2019 du Ministère de l'intérieur français : *typosquatting*, rançongiciels, chevaux de Troie d'administration à distance, *cryptojacking* et autres *botnets*. La liste est longue et ne cesse de s'allonger.

Autant de termes peu familiers aux oreilles des non-initiés qui composent la majorité des utilisateurs, mais qui représentent pourtant des menaces bien réelles, et aux conséquences potentiellement très graves. Force est de constater que l'écart reste encore trop grand aujourd'hui dans le public entre l'usage au quotidien des réseaux, très répandu, et la perception des dangers, qui reste encore bien trop faible. Comme si les actes délictueux commis dans le cyberespace n'avaient pas d'implications concrètes dans la « vraie vie » : or, rien n'est plus faux.

De plus, la multiplication des objets connectés et des services en ligne sera renforcée par de futurs réseaux techniquement plus performants mais aussi peut-être plus vulnérables en termes de sécurité du fait de leurs caractéristiques propres (avec leur plus grande surface d'exposition aux risques, la part croissante jouée par leur dimension logicielle les soumettant à de nombreuses mises à jour). La cybersécurité est donc non seulement un enjeu actuel et souvent sous-estimé, mais devrait également devenir un sujet majeur pour les années à venir dans une société toujours plus numérisée.

La France occupe une place tout à fait spécifique sur le terrain de la cybersécurité en Europe, car elle dispose d'une expertise ancienne et reconnue, expertise plus particulièrement incarnée par son agence nationale, l'ANSSI. Mais la force d'une chaîne se mesurant à l'aune de son maillon le plus faible, une coopération de qualité entre les autorités européennes responsables de ce sujet dans leur pays apparaît déterminante. Jusqu'à récemment, l'existence même de telles autorités n'était pas acquise dans tous les États membres de l'Union, et lorsqu'elles existaient, toutes n'avaient pas la puissance de frappe de l'agence française.

La législation européenne récente (la directive SRI et l'Acte de cybersécurité) s'est donc employée à remédier à cela, en cherchant à concilier le respect de la souveraineté des États membres sur ce sujet très régalien avec une collaboration européenne efficace sous la houlette d'une agence dédiée à la sécurité des réseaux, l'ENISA.

Selon votre rapporteur, cet enjeu majeur doit évidemment être considéré sous l'angle de la sécurité et de la défense des intérêts à la fois nationaux et européens. Mais sa dimension économique ne doit pas être négligée : la cybersécurité peut aussi être source de prospérité, et l'Union européenne a tout à gagner à présenter un front cohérent et uni pour affronter la concurrence mondiale et proposer des standards faisant référence.

C'est pourquoi notre rapport porte sur les deux volets de l'Acte de cybersécurité : sécuritaire et opérationnel avec le renforcement de l'ENISA, et plus économique avec l'introduction d'un système européen de certification pour la cybersécurité.

À partir des observations recueillies lors des auditions et de l'étude des textes adoptés dans le cadre de l'Acte de cybersécurité européen, le rapport d'information se

propose donc, d'abord, de présenter l'émergence des grands enjeux de la cybersécurité en Europe ces dernières années et les tendances en termes de menaces.

L'élaboration de réponses européennes coordonnées aux problèmes de cybersécurité par les pouvoirs publics se heurte en effet à deux écueils : le foisonnement des institutions destinées à répondre aux menaces sur le plan international d'une part, et la difficulté à évaluer et caractériser les atteintes à la cybersécurité d'autre part.

La cybersécurité étant par nature un sujet ne connaissant pas de frontière, sa prise en compte par les organisations internationales se fait de façon foisonnante et peu coordonnée, conduisant à un véritable « patchwork institutionnel » de la cybersécurité. En tracer les contours permet au rapport de mettre en lumière le chemin qui reste à parcourir pour une véritable coordination internationale, à la hauteur des enjeux. Encore faut-il être en mesure d'évaluer ceux-ci : le développement au sein de l'Union européenne d'un indicateur de mesure de la cybersécurité apparaît en effet comme un prérequis indispensable à l'affirmation d'un modèle européen de cybersécurité. Cet indicateur devrait répondre à des critères de scientificité ouverts et permettre de mesurer les progrès réalisés d'une année sur l'autre, notamment grâce aux outils mis en place pour garantir la cybersécurité au niveau de l'Union. L'ENISA publie un rapport annuel d'évaluation des menaces : à l'avenir, il pourrait être intéressant que ce rapport fasse l'objet d'une plus grande publicité, par le biais d'une présentation au Parlement européen par exemple. Ce rendez-vous régulier pourrait être mis en place dès à présent avec le début du mandat des députés européens, et constituer ainsi un temps de discussion annuel qui contribuerait à la sensibilisation autour des enjeux de la cybersécurité européenne.

Le rapport cherche également à montrer comment une Agence européenne de la cybersécurité renforcée pourra contribuer à rationaliser une architecture de la cybersécurité européenne encore trop éclatée. Votre rapporteur salue le renforcement de l'ENISA mais appelle à la vigilance sur les contours du rôle que l'Agence devra endosser, afin que soient conciliées au mieux les exigences de coopération européenne et de respect de la souveraineté des États membres. L'ENISA ne doit pas devenir l'organe supranational de la cybersécurité en Europe, mais peut et doit assurer un rôle utile de coordination et de mobilisation des compétences nationales.

La diversité des instances nationales nous conduit à proposer que soit désignée dans chaque État membre une personnalité politique de référence, susceptible d'offrir une meilleure visibilité aux enjeux de cybersécurité. Il pourrait s'agir en France de créer un ministère de plein exercice, qui permettrait une véritable incarnation politique des problématiques de cybersécurité, tant sur le volet sécuritaire qu'industriel.

Le rapport examine également les modalités dans lesquelles s'inscrira la certification européenne créée par le nouveau règlement : si la certification de cybersécurité peut constituer un avantage comparatif essentiel pour l'Union, elle n'emporte pas moins certaines difficultés dont il faut être conscient. La certification introduite par le règlement sur la cybersécurité représente une véritable opportunité de croissance pour l'Europe sur le marché de la cybersécurité, à condition qu'elle favorise la convergence vers les plus hautes exigences. Pour cela, le rapport appelle à la bonne prise en compte des acquis existants et attire l'attention sur les problématiques de périmètres et de durabilité des schémas d'évaluation de certification. En effet, dans un domaine, le numérique, où les mises à jour sont nombreuses et les évolutions rapides, la certification devra tenir la gageure de réconcilier réactivité et stabilité

La mise en œuvre de l'Acte de cybersécurité offre à l'Union européenne l'occasion historique de répéter l'établissement d'un standard, tel que celui qu'elle a réussi à proposer pour la protection des données personnelles avec le RGPD. Il lui faut pour cela capitaliser sur les réussites des meilleurs acteurs en son sein, et réussir à faire converger secteurs public et privé dans la promotion de l'intérêt européen. C'est le sens du modèle que ce rapport vise à défendre.

Le rapport présenté aujourd'hui devant notre Commission cherche donc à présenter les dernières avancées dans la législation européenne sur la cybersécurité tout en soulignant les difficultés qui pourraient survenir lors de la mise en œuvre de ces textes, difficultés inhérentes au paysage institutionnel complexe, à la sensibilité de ce sujet pour la souveraineté des États et au caractère très évolutif du secteur du numérique. Il cherche ainsi à contribuer à la diffusion d'une certaine culture autour des enjeux de cybersécurité à un moment charnière pour la vie de l'Union européenne, avec l'arrivée récente des nouveaux députés au Parlement européen et la prise de fonction prochaine de la Commission européenne. Je vous remercie.

Mme la Présidente Sabine Thillaye. M. le rapporteur, vous avez évoqué la place de la France, qui semble plutôt avancée sur ces sujets. Quels sont les États membres avec un niveau d'implication moindre ? Quels sont les plus avancés ? Par ailleurs, avons-nous une idée des zones géographiques d'où proviennent les principales menaces ?

M. Éric Bothorel, rapporteur. Nous parlions tout à l'heure de diplomatie ; je vais tenter d'être diplomate dans ma réponse. Il ne vous aura pas échappé que l'harmonisation dans l'Union européenne n'est pas encore parfaite. Il ne serait pas surprenant qu'au niveau des moyens, des outils, il y ait encore une certaine hétérogénéité. Loin de moi l'idée de désigner ici des pays, mais l'idée que la force d'une chaîne repose sur son maillon le plus faible est aujourd'hui pleinement partagée.

Cela a été rappelé : au-delà des infrastructures, ce sont les pratiques et les cultures, ainsi que la prise en compte des risques cyber par les politiques, qui contribuent à l'effort. L'objectif est de parvenir au même niveau de prise de conscience. La certification est aussi un moyen de mettre du collaboratif et de l'échange entre les pays, en bilatéral comme en multilatéral au sein de l'Union européenne. Le nivellement doit en tout cas se faire par le haut.

M. Jean-Louis Bourlanges. Puisque vous évoquez des problèmes d'harmonisation, y aurait-il une possibilité théorique d'élever juridiquement, à travers éventuellement une révision du traité, de créer une véritable compétence d'harmonisation en la matière ? On est là face à des procédures de coopération qui marchent plus ou moins bien. Une avancée institutionnelle, même si elle n'est pas réaliste aujourd'hui, serait-elle utile ?

Mme Christine Hennion. Lorsque le RGPD a été adopté, les pays ont investi dans leurs agences et ont décuplé le nombre de leurs membres. Cela a notamment été le cas en Irlande. Dans tout ce paquet cyber, y a-t-il des textes qui pourraient amener les pays européens à se sentir contraints à investir ? Ou faut-il aller plus loin dans les textes pour qu'il y ait ce réflexe ?

M. Juhan Lepassaar, directeur exécutif de l'ENISA. Comme je l'ai dit, tous les États membres ont transposé la directive SRI. Tous les États membres ont adopté une stratégie nationale sur la cybersécurité, qui contient une partie dédiée au renforcement des

capacités et des ressources. De fait, ils ont renforcé les ressources allouées, sans que ce soit suffisant.

La Commission européenne est encore en cours d'évaluation des mesures mises en place. C'est une question qui restera en suspens pour la prochaine Commission, qui entreprendra une analyse de la mise en œuvre de la directive SRI.

Il existe un groupe de coopération SRI, très efficace, et nous avons vu à partir de leurs travaux sur la 5G qu'ils produisent des résultats très intéressants. Les contributions des États membres, à travers ce réseau de coopération SRI, ont été très pertinentes. Aujourd'hui, je pense que les États membres se rendent compte que la cybersécurité est vitale pour eux. Les capacités de l'ENISA, qui reste une petite agence mais dont l'effectif a été augmenté de quasiment 50 %, montrent l'engagement de l'Union européenne en la matière.

M. Cyril Cuvillier, sous-directeur de la stratégie de l'ANSSI. Dans les expériences qui ont précédé ce schéma de certification, on avait déjà des réalisations d'une dizaine d'États membres ou plus. Ils avaient pris pour habitude de reconnaître mutuellement leurs centres de certification. Nous allons poursuivre cet effort afin d'avoir de plus en plus de centres de certification à travers l'Europe. Nous devons aussi aider des centres à monter en compétence, pour qu'ils puissent évaluer des choses de plus en plus sophistiquées. Pour moi, ce sera progressif.

Dans un second temps, je voudrais préciser qu'il ne s'agit pas, pour moi, d'un domaine qui ressort uniquement de la sphère publique. Il y a bien des domaines dans lesquels les acteurs privés développent des standards et des efforts de certification. Nous allons voir se croiser un effort horizontal de certification générique avec des verticales sectorielles, qui témoignent d'initiatives de qualité. Il y aura un défi pour articuler cette lecture des risques pour les sociétés que fait le politique ou l'acteur public, avec la lecture de qualité que l'opérateur privé cherche à atteindre. Cela peut devenir, et nous le souhaitons, un argument de vente pour les entreprises que de savoir valoriser les efforts qu'elles font pour livrer sur le marché des services et des produits de qualité.

M. Éric Bothorel, rapporteur. Tout ce qui permettra d'adopter, à l'échelle de l'Union, un référentiel pour encadrer ces éléments de certification, à l'image de ce que l'on a fait avec le RGPD, est bienvenu. Ce sont des métiers relativement récents : entre les pratiques allemandes et françaises, par exemple, qu'il s'agisse de délais ou de gratuité, il y a des divergences. L'idée est de mettre en commun les meilleures pratiques. Il faut parvenir à garantir un niveau d'exigence suffisamment élevé pour les infrastructures, afin d'être suffisamment sereins par rapport aux menaces. À terme, en effet, si l'on peut avoir une initiative législative à l'échelon pertinent qui est celui de l'Europe, ce sera positif.

À l'issue de la discussion, la commission a *autorisé* la publication du rapport.

III. Examen de textes soumis à l'Assemblée nationale en application de l'article 88-4 de la Constitution

Sur le rapport de la Présidente Sabine Thillaye, la Commission a examiné des textes soumis à l'Assemblée nationale en application de l'article 88-4 de la Constitution.

- **Textes actés**

Aucune observation n'ayant été formulée, la Commission *a pris acte* des textes suivants :

➢ *Transports, politique spatiale*

- Proposition de décision du conseil relative à la position à prendre, au nom de l'Union européenne, au sein de l'Organisation de l'aviation civile internationale en ce qui concerne la révision de l'annexe 17 ("Sûreté") (amendement 17) de la convention relative à l'aviation civile internationale **(COM(2019) 577 final - E 14421).**

- **Textes actés de manière tacite**

La Commission *a* également *pris acte de la levée tacite de la réserve parlementaire,* du fait du calendrier des travaux du Conseil, pour les textes suivants :

➢ *Politique de développement*

- Proposition de décision du Conseil relative la position à adopter par l'Union européenne au sein du Comité des ambassadeurs ACP-UE en ce qui concerne l'adoption d'une décision d'adopter des mesures transitoires en vertu de l'article 95, paragraphe 4, de l'accord de partenariat ACP-UE **(COM(2019) 550 final - E 14410).**

➢ *Politique étrangère et de sécurité commune(PESC)*

- Décision du Conseil modifiant la décision (PESC) 2016/2382 instituant un Collège européen de sécurité et de défense (CESD) **(12540/19 LIMITE - E 14375).**

La séance est levée à 11 h 27.

Membres présents ou excusés

Présents. – Mme Aude Bono-Vandorme, M. Éric Bothorel, M. Jean-Louis Bourlanges, M. André Chassaigne, Mme Yolaine de Courson, Mme Christine Hennion, Mme Caroline Janvier, Mme Sabine Thillaye

Excusés. – Mme Marietta Karamanli, M. Joaquim Pueyo