ASSEMBLÉE NATIONALE

XV^e LÉGISLATURE

Compte rendu

Commission des lois constitutionnelles, de la législation et de l'administration générale de la République

Mardi
10 avril 2018
Séance de 16 heures 45

Compte rendu n° 62

SESSION ORDINAIRE DE **2017-2018**

Présidence de Mme Yaël Braun-Pivet, *Présidente*, et de Mme Sabine Thillaye, *Présidente de la commission des Affaires européennes*

ASSEMBLÉE NATIONALE

La réunion débute à 16 heures 55.

Présidence de Mmes Yaël Braun-Pivet, Présidente, et Sabine Thillaye, présidente de la commission des Affaires européennes.

La Commission entend, en audition conjointe avec la commission des Affaires européennes, M. Julian King, commissaire européen chargé de l'Union de la sécurité.

Mme la présidente Yaël Braun-Pivet. La commission des lois et la commission des affaires européennes ont le plaisir d'accueillir conjointement M. Julian King, commissaire européen chargé de l'Union de la sécurité. Je vous souhaite la bienvenue, monsieur le commissaire.

Vous avez déjà été entendu par nos deux commissions réunies le 23 novembre 2016 sur les questions dont vous avez la charge : la sécurité, la lutte contre le terrorisme, contre la radicalisation et contre la criminalité organisée. Vous savez combien est grand leur retentissement dans notre pays, qui a été récemment à nouveau durement frappé par le terrorisme.

La France ne vous est pas étrangère puisque, avant d'occuper les fonctions qui sont les vôtres aujourd'hui, vous étiez ambassadeur du Royaume-Uni à Paris. Votre parfaite maîtrise de notre langue vous permettra de vous adresser à nous en français.

Je précise que les questions relatives à l'asile et à l'immigration, qui nous ont beaucoup occupés la semaine dernière, ne font pas partie de votre portefeuille.

Nombre des enjeux dont il est question doivent être appréhendés à l'échelle de l'Union, nous avons déjà eu l'occasion de le constater en transposant dans notre droit diverses dispositions d'origine européenne dans le domaine de la sécurité et ce, encore très récemment, avec la loi du 26 février 2018.

Je vais céder la parole à la présidente de la commission des Affaires européennes, Mme Sabine Thillaye. Les députés présents qui le souhaitent pourront ensuite vous interroger.

Mme la présidente Sabine Thillaye. Monsieur le commissaire européen, depuis 2015, les États membres et les autorités européennes ont pris conscience qu'il fallait profondément changer de politique pour mettre en œuvre une Europe qui protège. Votre nomination en septembre 2016 en tant que commissaire pour l'Union de la sécurité a symbolisé ce changement de cap qui vise à intégrer les questions de sécurité extérieure dans la stratégie pour la sécurité intérieure de l'Union européenne. En effet, dans de nombreux domaines comme la propagande sur Internet ou le retour en Europe des combattants venus de Syrie, l'actualité internationale a d'importantes répercussions sur la sécurité des citoyens européens.

Je voudrais évoquer tout d'abord l'action de l'Union européenne en matière de lutte contre le terrorisme. Le 8 mars dernier, la Commission européenne et le comité des régions ont invité les maires des grandes villes d'Europe pour consolider les défenses urbaines face au terrorisme. Lors de cette réunion, vous avez souligné que ce n'était pas aux citoyens de changer leur mode de vie mais aux autorités publiques de réduire les moyens d'action des terroristes en renforçant la sécurisation des espaces publics. Comment l'Union européenne peut-elle y contribuer ? Quels sont les autres axes d'action de l'Union européenne en matière

de terrorisme ? Pouvez-vous préciser les mesures que la Commission européenne souhaite proposer pour mieux contrôler le commerce d'armes à feu destiné aux civils et la vente de produits pouvant être détournés pour la fabrication d'explosifs ?

Dans la lutte contre le terrorisme, la question du partage entre États membres des informations contenues dans les fichiers de police et de sécurité est cruciale. Toutefois, l'on constate actuellement de fortes disparités dans la manière dont les États membres alimentent les fichiers de sécurité tels que le système d'information Schengen (SIS), le fichier d'information sur les visas ou bien les bases de données Europol. Comment inciter les États à avoir une réelle culture du partage des informations ? Comment améliorer la fiabilité du système d'information Schengen pour identifier les personnes présentant des profils à risque terroriste ?

Pour terminer, je voudrais vous interroger sur le rôle croissant des agences dans le domaine de la sécurité. Je citerai Europol, Eurojust, Frontex ou encore le Centre d'analyse du renseignement de l'Union européenne. Comment voyez-vous votre rôle vis-à-vis de ces agences ? Comment ces organismes peuvent-ils être contrôlés démocratiquement sans que ce contrôle ne nuise à l'efficacité de leur action ?

Enfin, j'en viens à l'action extérieure de l'Union européenne en matière de lutte contre le terrorisme, à la suite des conclusions du Conseil des affaires étrangères du 19 juin 2017. Comment renforcer la coopération entre les professionnels engagés dans les missions relevant de la politique de sécurité et de défense communes et les agences européennes chargées de la justice et des affaires intérieures ? Il paraît primordial de renforcer les liens entre les acteurs militaires, les diplomates et les services répressifs pour rendre la lutte contre le terrorisme plus efficace.

M. Julian King, commissaire européen chargé de l'Union de la sécurité. Je vous remercie de votre invitation, madame la présidente de la commission des Lois, madame la présidente de la commission des Affaires européennes.

Pour commencer, je tiens à présenter mes condoléances aux familles des victimes de l'attentat de Trèbes et, au nom de tous mes collègues de la Commission, je salue le courage dont a fait preuve le colonel Beltrame.

C'est un grand honneur de pouvoir débattre aujourd'hui avec vous des questions relatives à la sécurité intérieure de l'Union européenne, à la lutte contre le terrorisme mais aussi aux cyber-menaces.

Le Président Juncker considère que le développement de relations plus étroites avec les parlements nationaux est une priorité et je soutiens totalement cet engagement. C'est lors d'échanges tels que celui que nous avons aujourd'hui que ces relations peuvent se développer. Je vous remercie pour vos rapports et résolutions sur les sujets touchant à la sécurité. La Commission apprécie vivement ces contributions et en tient compte au cours du processus législatif. La sécurité est une des principales préoccupations des citoyens européens.

Nous faisons face aujourd'hui à deux principaux types de menaces stratégiques pesant sur notre sécurité.

Il s'agit, d'une part, de la menace terroriste, qui reste à un niveau élevé et qui est en constante évolution. Nous assistons en effet à l'augmentation d'attaques dites « à bas coûts »

commises à l'aide de moyens simples et accessibles comme les voitures ou les couteaux par des individus isolés, souvent radicalisés au sein de certaines communautés ou en ligne.

Il s'agit, d'autre part, des risques croissants liés à la cybersécurité. Les attaques augmentent dans un contexte de croissance exponentielle de la vulnérabilité de nos sociétés et de nos systèmes du fait de la numérisation et de l'avènement du « tout connecté ». La cyber-menace est également en constante évolution et, comme on ne cesse de le constater, revêt une importance de plus en plus stratégique puisque ces nouveaux outils sont aujourd'hui largement utilisés par des acteurs ou puissances hostiles à des fins de destruction, de sabotage mais aussi de déstabilisation politique – le Président Macron en a été victime durant sa campagne électorale. Ils peuvent mettre en danger le fondement même de nos démocraties. C'est pourquoi je partage le constat de la France sur le fait que la propagation rapide de fausses nouvelles constitue un enjeu crucial, en particulier lors de périodes électorales.

Il est clair que la sécurité relève en premier lieu de la responsabilité des États membres, mais la nature transnationale des menaces qui pèsent sur nous requiert une réponse forte au niveau européen. C'est dans ce cadre que j'ai été nommé en septembre 2016 commissaire européen chargé de l'Union de la sécurité. Le travail que je mène depuis, avec mes collègues, vise à apporter aux États membres le soutien et les outils nécessaires afin de renforcer la lutte contre le terrorisme, la radicalisation et les cyber-menaces.

J'évoquerai dans un premier temps nos actions concernant la menace terroriste.

Ces dernières années, la France ainsi que plusieurs autres États membres comme le Royaume-Uni, l'Allemagne, la Suède, la Finlande, la Belgique, l'Espagne ont été la cible d'attaques terroristes qui ont causé des centaines de morts et encore davantage de blessés. L'Europe a répondu. Face à la menace du terrorisme, les États membres ont renforcé leur coopération. Les terroristes et les criminels ne connaissant pas de frontières nationales, nous devons apporter des réponses à la hauteur de cette menace et travailler ensemble de manière plus étroite au niveau européen. Grâce au travail que nous menons pour construire une véritable Union de la sécurité, de réels progrès ont été faits pour réduire l'espace dans lequel les terroristes peuvent opérer, pour renforcer notre résistance collective et pour répondre aux causes profondes liées au phénomène de radicalisation, en ligne et dans les communautés.

Afin de réduire les moyens d'action des terroristes, nous avons renforcé la législation européenne concernant les armes à feu, les explosifs et le financement du terrorisme.

Les terroristes cherchent à exploiter les vulnérabilités et les failles existantes. Les armes à feu ayant servi durant les attaques de Paris en janvier 2015 ont été mal neutralisées et ont pu ainsi être réactivées. C'est la raison pour laquelle nous avons révisé la directive sur les armes à feu, en nous basant largement sur la législation française existante – et je remercie la France d'avoir d'ores et déjà transposé cette directive dans son droit national. Nous avons aussi revu à la hausse les critères de désactivation des armes à feu. Et nous travaillons, avec le soutien de l'agence Europol, à la lutte contre le trafic illicite d'armes dans les Balkans occidentaux car certaines des armes des attaques du 13 novembre provenaient de cette région.

Les explosifs tels que le peroxyde d'acétone ont également été utilisés dans plusieurs attaques terroristes, que ce soit à Paris, Manchester ou encore Bruxelles. Nous devons réduire la possibilité pour les terroristes d'avoir accès aux substances permettant de les fabriquer. Après avoir adopté une recommandation en octobre dernier, nous présenterons la semaine

prochaine une révision du règlement relatif aux précurseurs d'explosifs afin de mettre les substances les plus dangereuses hors de portée du grand public.

Les terroristes doivent également rassembler et déplacer des fonds, souvent rapidement, pour commettre leurs attaques. C'est pourquoi nous avons adopté en décembre 2016 trois propositions en cours de négociation pour compléter le cadre juridique sur le blanchiment de capitaux, les mouvements illicites d'argent liquide et le gel et la confiscation d'avoirs. L'accord politique récemment trouvé sur la cinquième directive anti-blanchiment rendra également obligatoire dans tous les États membres la mise en place de registres bancaires centralisés – la France s'en est déjà dotée. Dans quelques jours, nous ferons une proposition afin de faciliter l'accès des forces de l'ordre à ces registres car les informations financières sont cruciales pour les enquêtes relatives au terrorisme et doivent être obtenues dans des délais rapides.

Au-delà des moyens d'action, nous avons également agi pour limiter les déplacements des terroristes, notamment leur entrée sur le territoire européen lors des retours d'Irak et de Syrie. Ainsi, nous avons adopté une réforme du code frontières Schengen, en place depuis avril 2017, qui permet de contrôler systématiquement à travers les bases de données toute personne entrant et sortant de l'espace Schengen. En outre, nous avons proposé la mise en place de deux nouveaux fichiers : le fichier entrées-sorties qui permettra d'enregistrer les entrées et sorties de l'espace Schengen des ressortissants d'États tiers ; le fichier ETIAS (*European Travel Information and Authorization System*), équivalent européen de l'ESTA (*Electronic System for Travel Authorization*), afin de pouvoir contrôler en amont les personnes dispensées de visa arrivant sur notre territoire. Et dans quelques jours, nous ferons une proposition afin de renforcer la sécurité des documents d'identité, notamment en introduisant des éléments biométriques car nous savons que certains des terroristes ont utilisé de faux documents pour se déplacer.

À travers la directive relative à la lutte contre le terrorisme, adoptée au mois de septembre 2017, nous avons érigé en infraction pénale des actes tels que le financement du terrorisme, le fait de dispenser ou de recevoir un entraînement au terrorisme et celui de voyager à des fins de terrorisme.

Afin de pouvoir identifier en amont les personnes dangereuses tentant de venir en avion sur le territoire européen, nous avons adopté le PNR (*Passenger name record*) européen, et nous travaillons aujourd'hui activement à sa mise en œuvre dans tous les États membres avant le 25 mai prochain, date limite de transposition. Le PNR français est déjà opérationnel, j'ai d'ailleurs visité l'« Unité Information Passagers », et je remercie la France pour le soutien opérationnel et technique qu'elle a apporté à d'autres États membres dans la mise en place de leur PNR. Encore une fois, la mise en œuvre est cruciale, car il faut que tous les PNR nationaux soient installés pour que le système européen soit pleinement efficace et opérationnel.

Nous avons mis en place le premier corps européen de garde-frontières et de garde-côtes, composé de 1 700 personnes qui assistent les autorités nationales dans leurs fonctions aux frontières extérieures de l'Union.

Cet ensemble de mesures vise à renforcer la sécurisation de nos frontières extérieures mais, pour qu'elles soient pleinement efficaces, il est indispensable qu'elles soient mises en œuvre par les États membres.

Renforcer notre résilience collective est également crucial dans la lutte que nous menons contre le terrorisme. Pour cela, l'information est clé, comme vous l'avez souligné, madame la présidente. Au niveau européen, le partage d'information a été fortement renforcé entre les États membres.

Tout d'abord, le système d'information Schengen (SIS) est davantage consulté et mieux alimenté par les États membres. Il contient désormais 75 millions d'alertes sur des personnes ou des objets recherchés et a été consulté 4 milliards de fois en 2016. La France en est un des principaux contributeurs. De plus, la réforme du SIS que nous avons également adoptée l'an dernier vise à renforcer l'utilisation de la biométrie et à rendre obligatoire la notification par les États membres, dans le système, d'alertes relatives au terrorisme obligatoires.

Le terroriste de Marseille et celui de Berlin étaient enregistrés sous plusieurs dizaines d'identités différentes dans plusieurs bases de données européennes. Afin que cela ne soit plus possible, et, pour assurer un meilleur partage de l'information, nous avons proposé au mois de décembre dernier de mieux interconnecter nos différents systèmes d'information sécuritaires et migratoires européens. Nous comptons sur le soutien de la France pour que cette proposition soit adoptée d'ici à la fin de l'année.

Le renforcement de la coopération opérationnelle entre les services répressifs des États membres est également un élément participant au renforcement de notre résilience collective. L'Union européenne a fourni aux États membres un appui et des outils pour ce faire, notamment à travers les agences comme Europol ou Eurojust. Ainsi, Europol a mis en place dès 2015, à la suite des attentats de Paris, un centre européen sur la lutte contre le terrorisme. Depuis lors, ce centre a apporté un soutien opérationnel à d'autres États membres victimes d'attaques terroristes, notamment dans le cadre des enquêtes post-attentat, à travers 439 opérations en 2017.

Je veux aussi mentionner ici le renforcement important de la coopération entre les services de renseignement des États membres, alors que j'entends encore trop souvent dire qu'elle n'existe pas. Elle existe bien, en dehors des structures institutionnelles de l'Union européenne, à travers le Groupe antiterroriste (GAT), qui réunit les services de renseignement des vingt-huit États membres dans le cadre d'une plateforme physique établie aux Pays-Bas. Récemment, ils ont mis en place une base de données visant à renforcer le partage d'informations relatives aux terroristes djihadistes. Aujourd'hui, nous travaillons à renforcer la coopération entre le GAT et Europol.

Malgré tous les outils et le soutien que nous apportons aux États membres pour mieux prévenir une attaque, le risque zéro, il faut être clair, n'existe pas. C'est pourquoi nous avons adopté au mois d'octobre dernier un plan d'action relatif à la protection des espaces publics, accompagné d'un soutien financier d'un montant de 120 millions d'euros. Un premier appel à projets a été lancé l'an dernier et nous sommes en train d'examiner les propositions reçues, dont plusieurs émanent de villes françaises. D'autres appels seront lancés au cours de l'année.

Cela m'amène à souligner l'importance du rôle des villes et de l'échelon régional et local dans la lutte contre le terrorisme. Le 8 mars dernier, nous avons organisé à Bruxelles la première conférence européenne des maires pour la protection des espaces publics, à la suite de l'initiative prise par la ville de Nice au mois de septembre 2017, à laquelle j'ai participé, avec le ministre de l'intérieur, M. Collomb. Il est en effet fondamental d'impliquer nos

territoires dans la lutte contre le terrorisme car ce sont les premiers concernés en cas d'attaque. Si nous voulons continuer à faire de nos villes et de nos lieux de loisirs des espaces ouverts, nous devons mettre en place les moyens permettant d'assurer leur protection. Le partage d'expérience est essentiel dans ce domaine. Nous avons ainsi mis en place un Forum des exploitants d'espaces publics pour encourager les partenariats public-privé dans le domaine de la sécurité et favoriser les échanges avec les exploitants privés, tels les responsables de salles de concert ou les loueurs de véhicules.

Au-delà des actions que nous menons pour empêcher les terroristes de nous attaquer, nous agissons également en amont, aux racines du problème, notamment sur la prévention et la lutte contre la radicalisation, en ligne et dans nos communautés.

L'Union européenne est, selon moi, l'échelon pertinent pour lutter contre la radicalisation en ligne, qui ne connaît pas de frontières. Nous avons dès 2015, avec la mise en place d'un Forum européen de l'internet, rassemblé les États membres et les opérateurs internet, pour travailler ensemble sur le retrait des contenus terroristes en ligne. Europol a également mis en place une unité spécialisée, qui détecte les contenus terroristes illicites en ligne et les signale aux opérateurs pour que ces derniers les retirent. Des progrès ont été faits dans ce cadre mais nous devons aller plus loin.

Nous avons adopté au début du mois de mars dernier une recommandation demandant aux opérateurs internet de détecter et retirer des contenus terroristes de manière plus efficace et rapide. Nous les appelons notamment à retirer les contenus terroristes qui leur sont signalés par la police dans l'heure suivant leur notification et à déployer des moyens automatiques visant à détecter ces contenus, permettre leur retrait rapide et empêcher leur réapparition. Nous allons dans les prochains mois évaluer la mise en œuvre de ces recommandations par les opérateurs internet, et nous serons prêts à légiférer si nécessaire ; il faut vraiment avancer. Il est également important de promouvoir les contre-discours positifs en ligne. Nous avons mis en place un programme européen de quelque 10 millions d'euros afin d'aider nos partenaires de la société civile à élaborer des récits alternatifs positifs en réponse à la propagande terroriste.

Mais les phénomènes de radicalisation s'observent également dans nos communautés ou en prison. Beaucoup de terroristes, nous le savons, ont été un temps en prison. Encore une fois, l'échelon régional et local est crucial : ce sont les élus locaux, les responsables associatifs, les éducateurs, les surveillants de prison qui peuvent le mieux détecter les premiers signes de radicalisation. L'Union européenne peut apporter un soutien en facilitant le travail de coopération et d'échanges de bonnes pratiques. C'est le travail du réseau européen de sensibilisation à la radicalisation (RAN), qui apporte un soutien aux acteurs locaux en les aidant à développer des stratégies adaptées. Le RAN a ainsi développé un manuel sur les retours et la prise en charge des combattants terroristes étrangers et leurs familles.

Afin de renforcer les liens entre les praticiens de terrain et les politiques publiques, nous avons mis en place un groupe d'experts de haut niveau sur la radicalisation. Ce groupe a récemment proposé une série de recommandations sur la lutte contre la radicalisation, notamment en prison, mais également sur le traitement du retour des femmes et des enfants des zones de combat. Il est important que la France partage avec d'autres États membres son expérience dans ce domaine.

En ce qui concerne la deuxième menace à laquelle nous faisons face, la menace cyber, l'année 2017 a été celle d'une prise de conscience. Elle a été marquée par l'ampleur,

inédite, d'attaques comme WannaCry et NotPetya, et par une prise de conscience de leur capacité à proliférer d'une manière extrêmement rapide et à se jouer des frontières. Nous avons aussi pris conscience des risques que présentent les innombrables objets déjà connectés et les 50 milliards qui le seront d'ici à 2020. Et nous avons constaté l'implication croissante d'acteurs étatiques dans les attaques cyber ainsi que de la dimension de plus en plus politique et géopolitique des cyber-menaces, y compris à travers des manœuvres de propagande et de désinformation reposant sur l'utilisation des nouveaux services et outils technologiques, encore une fois récemment illustrée par l'affaire Cambridge Analytica.

Afin de doter l'Europe des outils adéquats pour faire face aux cyberattaques, nous avons proposé une large panoplie de mesures destinées à renforcer la cybersécurité dans l'Union européenne. Cette nouvelle approche stratégique, présentée au mois de septembre dernier, a plusieurs objectifs : accroître notre résilience, stimuler l'innovation technologique, renforcer la dissuasion en améliorant la traçabilité et la responsabilisation et tirer parti de la coopération internationale pour promouvoir notre cybersécurité collective. Permettez-moi de souligner tout d'abord qu'une étape importante dans le renforcement de notre sécurité collective est en train d'être franchie avec la mise en œuvre de la directive relative à la sécurité des réseaux et des systèmes d'information, dite « NIS » (*Network and Information Security*), qui doit être finalisée d'ici au mois de mai. Je remercie les autorités françaises de l'avoir transposée. Les États membres ont ensuite jusqu'au mois de novembre pour identifier les opérateurs de services essentiels. Nous attendons beaucoup de ce nouveau cadre réglementaire, notamment pour favoriser une plus grande harmonisation du niveau de préparation des États membres de l'Union ainsi que davantage d'échanges d'informations et de coopération.

Pour aller plus loin, nous avons aussi proposé au mois de septembre de nouvelles mesures visant à mettre en place une agence européenne pour la cybersécurité dotée de compétences plus étendues ainsi qu'un système européen de certification. S'agissant de l'agence européenne pour la cybersécurité, l'idée est de renforcer l'actuelle Agence européenne chargée de la sécurité des réseaux et de l'information (en anglais, *European Union Agency for Network and Information Security*, ENISA), ce qui devrait permettre à terme un meilleur soutien aux États membres, par exemple dans la mise en œuvre de la directive NIS. L'agence européenne renforcée que nous avons proposée servira à mieux structurer la coopération entre États membres et, par la suite, à favoriser la montée en compétences de ceux qui en ont le plus besoin. Cela bénéficiera à tous, dans la mesure où cela permettra de créer un espace européen plus sûr et mieux préparé.

S'agissant de notre proposition de créer un cadre de certification de cybersécurité à l'échelle de l'Union européenne, l'objectif est de créer les conditions nécessaires pour qu'un certificat obtenu par un produit dans un État membre soit automatiquement, et à des conditions très précises, reconnues dans tous les États membres. Cela permettra de stimuler le marché européen de la cybersécurité et d'accroître la confiance des utilisateurs.

Dans cette perspective, nous devons nous assurer que notre modèle est apte à répondre aux différents besoins et niveaux de sécurité. Notre proposition s'appuie sur ce qui a déjà été accompli dans ce domaine, notamment par la France. Il est important que les schémas de certification existants – qui, dans certains cas, regroupent déjà plusieurs États membres – puissent avoir une dimension véritablement paneuropéenne.

Enfin, pour améliorer notre résilience, nous avons proposé un plan de réponse coordonnée en cas de cyberattaques de grande ampleur.

Nous prévoyons d'autres initiatives dans les mois à venir. Nous avons ainsi pour objectif de renforcer considérablement la recherche et développement en matière de cybersécurité afin d'accroître notre autonomie stratégique. Nous avons déjà lancé en 2016 un partenariat public-privé qui devrait générer presque deux milliards d'euros d'investissements d'ici à 2020. Là aussi, il est nécessaire d'agir sans tarder pour renforcer et élargir cette initiative. C'est pourquoi nous lancerons prochainement un réseau de centres de recherche et de compétences en matière de cybersécurité au niveau des États membres, qui sera accompagné d'un centre européen similaire.

Autre volet important de notre action, il faut une réponse pénale plus efficace face à la cybercriminalité. Dans la lutte très inégale que nous menons contre la cybercriminalité, un des obstacles principaux concerne les difficultés rencontrées pour l'obtention des preuves électroniques, qui sont le plus souvent disséminées hors des frontières nationales et sont extrêmement volatiles. Au-delà des crimes en ligne, de nouveaux outils permettront de rendre plus efficaces tous les types d'enquêtes pénales impliquant des preuves électroniques, notamment en matière de terrorisme. Nous adopterons la semaine prochaine une proposition en ce sens.

Nous agissons également pour renforcer notre réponse politique et diplomatique aux cybermenaces. Les États membres mettent actuellement en œuvre un nouveau cadre stratégique, qui prévoit différents types de réponses aux actes cyber malveillants émanant d'acteurs étatiques, lesquelles peuvent aller jusqu'à des sanctions économiques.

Enfin, nous contribuons à renforcer la coopération internationale. On ne peut plus dissocier, en effet, les questions de cybersécurité des enjeux globaux en matière de sécurité et de défense. La Commission européenne a notamment présenté, en avril 2016, un cadre commun pour mieux lutter contre les menaces hybrides. Nous travaillons en coopération avec l'OTAN, notamment à travers le centre européen sur les menaces hybrides, qui a été créé à Helsinki, et nous avons réalisé l'an dernier un premier exercice parallèle et coordonné entre l'Union européenne et l'OTAN sur la base d'un scénario de menaces hybrides.

Dans le même temps, nous sommes confrontés à une autre forme de menace utilisant les moyens cyber, qui est peut-être plus pernicieuse encore : la prolifération des fausses informations et de la désinformation en ligne. Les acteurs se trouvant derrière ces campagnes font d'internet un nouveau vecteur pour leurs stratégies – qui, elles, ne sont pas nouvelles. Leur but est de déstabiliser nos démocraties de l'intérieur et de remettre en cause nos valeurs. Il en résulte aussi des risques réels pour notre sécurité. C'est un problème complexe qui exige une réponse résolue et multidimensionnelle.

Il est urgent et essentiel de renforcer la transparence des plateformes internet non seulement en ce qui concerne les contenus sponsorisés, qui doivent être mieux identifiés, mais aussi le fonctionnement des algorithmes, afin de lutter contre « l'enfermement algorithmique ». Il s'agit notamment de favoriser une utilisation plus responsable et éthique de ces outils, en particulier grâce à une limitation de l'exploitation des données personnelles à des fins spécifiques, notamment politiques. La Commission européenne a mis en place un groupe d'experts qui a rendu ses conclusions en mars. Nous les étudions actuellement et une communication sera prochainement présentée sur cette question.

Pour conclure, je voudrais souligner que l'unique réponse possible aux menaces terroristes et cyber est collective, c'est-à-dire européenne : aucun État membre ne peut lutter seul contre le terrorisme. L'Union européenne est là pour soutenir, aider et apporter des outils

communs. C'est une des priorités de la Commission pour l'année 2018 et je pense que ce sera aussi le cas pendant le prochain mandat. Nous sommes en ligne avec les propositions françaises de faire de la sécurité une des priorités du prochain cadre financier pluriannuel.

Je compte sur vous pour travailler à la mise en œuvre des politiques et des décisions européennes au niveau national : tout ce que nous faisons au plan européen ne sert à rien si ce n'est pas mis en œuvre de manière effective dans les États membres.

M. Joaquim Pueyo. J'ai été très intéressé par votre intervention, qui montre bien à quel point la Commission européenne est consciente des besoins en matière de sécurité : vous avez dressé un panorama très complet de ce que l'on doit faire pour lutter contre toutes les formes de criminalité, en particulier le terrorisme – le fichier PNR, les gardes-frontières et les gardes-côtes, le renforcement de la coopération entre tous les territoires, ou encore la recherche.

Ce qui me gêne un peu, est que les contributions nationales ont été réduites dans le cadre financier pluriannuel (CFP) 2014-2020. S'agissant du prochain CFP, pour lequel les discussions commencent, il y aura des besoins importants. Si l'on veut donner du sens à l'Europe, il faut expliquer à nos concitoyens que la sécurité européenne a un prix. On doit renforcer les frontières extérieures afin que l'on ne puisse plus dire de l'Europe qu'elle est une passoire pour la criminalité transfrontière ou les déplacements des terroristes. Il faudra donc augmenter le budget de la sécurité intérieure, comme celui de la défense. Dans ces conditions, ne faudrait-il pas réfléchir aux ressources de l'Union européenne ?

Dans la perspective de la campagne électorale de 2019, il faudra expliquer à nos concitoyens ce que vous avez dit : je pense que ça les intéresserait beaucoup. Vous soulignez la nécessité de contre-discours, mais avec quels moyens ? Il en existe déjà, mais ils sont insuffisants. En ce qui concerne le renforcement de la politique de prévention à l'égard des jeunes, que vous appelez de vos vœux, il y a déjà Erasmus, mais là aussi cela ne suffit pas. Afin que l'Europe gagne, il faut non seulement mettre sur le tapis ce que vous nous avez dit, mais également expliquer que l'on devra accroître le budget européen.

Voilà ce que je voulais dire en tant que membre de la commission des Affaires européennes. Vous savez que nous œuvrons pour améliorer la coopération européenne, qui est indispensable à un moment où les droits humains ne sont pas respectés et où ce sont plutôt les dictatures qui prennent le pas sur les démocraties. Il est grand temps que la démocratie que représente l'Union européenne agisse et soit un peu plus forte.

M. Pieyre-Alexandre Anglade. Vous avez évoqué le scandale Cambridge Analytica : cette entreprise est accusée d'avoir utilisé les données d'au moins cinquante millions d'utilisateurs et d'avoir joué un rôle crucial notamment au Royaume-Uni au moment du vote sur le *Brexit*. Si c'est vrai, nous sommes face à une menace extrêmement grave pour le fonctionnement de nos démocraties et il est de la responsabilité de la Commission de tout faire pour empêcher que les pays européens soient menacés par des tentatives de déstabilisation émanant d'acteurs ayant intérêt à affaiblir l'Europe.

Il y a deux dimensions à prendre en compte dans cette affaire. La première concerne la lutte contre les *fake news* et la désinformation. Dans ce domaine, la position de la Commission européenne n'est pas toujours claire : la Commissaire Mariya Gabriel plaide pour une autorégulation alors que vous défendez une approche plus contraignante, si j'ai bien compris. J'aimerais donc savoir quelle est la position de la Commission. Le deuxième aspect

est la protection de la vie privée et des données personnelles. Le débat est moins axé sur ce sujet, alors que tout est très lié. Les Européens, et les Français en particulier, sont attachés à la protection de leurs données personnelles. Vous savez que ce sont les Français qui sollicitent le plus Google pour le droit à l'oubli. Dans le contexte du scandale Cambridge Analytica, que fait concrètement la Commission européenne ? Vous avez cité le « paquet » proposé en septembre : depuis, une enquête a-t-elle été menée par la Commission ?

J'en viens à la lutte contre le terrorisme. La commission spéciale du Parlement européen sur le terrorisme a auditionné hier Jean-Charles Brisard, président du centre d'analyse du terrorisme (CAT). Selon lui, il y aurait entre 50 000 et 70 000 personnes radicalisées sur l'ensemble du continent européen et l'Union européenne aurait connu l'an dernier 62 incidents terroristes, dont 15 ont été perpétrés, soit un événement de ce type tous les six jours. Estimez-vous que ces chiffres sont crédibles ? Cela correspond-il aux estimations de la Commission ?

M. Ludovic Mendes. Vous avez évoqué le renforcement de la coopération en matière de migration et de sécurité, grâce aux fichiers, notamment pour lutter contre les multi-identités. Dans ce domaine, que fait-on en ce qui concerne les citoyens européens ? J'ai personnellement une identité pour l'état civil français, une autre pour l'état civil portugais et une troisième pour l'état civil espagnol, avec trois noms de famille différents. Les fichiers biométriques et photographiques des logiciels utilisés en Europe ne sont pas liés. Je ne pense pas être fiché au titre du risque terroriste et je ne suis pas en situation d'immigration, mais il y a quand même des questions à se poser. Comment ferons-nous demain pour suivre les ressortissants européens entrant et sortant de l'espace Schengen ? Par ailleurs, quand l'agence Frontex disposera-t-elle d'une vraie force, d'au moins 5 000 agents, lui permettant d'effectuer correctement le travail sur le territoire européen à la place des garde-côtes et des gardes-frontières nationaux ? Quand discutera-t-on aussi de la création d'une police européenne ? Cela faisait partie des projets des Pères fondateurs de l'Union européenne, mais ce sujet a été complètement oublié car les pouvoirs régaliens sont entre les mains des États membres et des nations. Quand commencera-t-on à poser les jalons d'une police européenne ?

M. Guillaume Larrivé. Merci pour la grande précision de vos propos sur le retrait des contenus illicites sur internet. Vous nous avez dit que la Commission s'était saisie de cette question en 2015, qu'Europol y travaille aussi, que la Commission a émis des recommandations le mois dernier, dans lesquelles elle demande aux opérateurs d'accélérer les retraits de contenus illicites, et qu'elle est prête à légiférer. Sur ce sujet, j'ai présenté ici même une proposition de loi au nom de l'opposition, il y a quatre ans, et les gouvernements qui se sont succédé depuis ont fait évoluer la législation nationale. J'ai le regret de dire qu'elle reste très largement inopérante, même si nous avons voté des dispositions qui prévoient théoriquement le blocage des sites internet appelant au djihad et obligent, théoriquement aussi, les opérateurs à retirer les contenus illicites. S'il y a un sujet sur lequel on voit que l'Europe peut avoir une valeur ajoutée importante, c'est bien la négociation avec les opérateurs, notamment les GAFA, voire le recours à la contrainte à leur égard. Il est urgentissime de progresser sur ces deux plans. J'aimerais savoir quelle est la position de la Commission dans ce domaine, où l'on a parfois le sentiment que les États membres sont assez démunis quand il s'agit d'agir efficacement.

M. Julian King, commissaire européen. Merci de l'intérêt que vous manifestez pour ces questions. Comme je l'ai dit au début de mon intervention : ce sont les États membres qui demeurent en première ligne pour lutter contre les menaces terroristes et les menaces cyber ; reste que, selon moi, il est un certain nombre d'actions que nous devons

mener de façon plus collective – au niveau de l'Union européenne –, afin d'aider les États à faire face à ces menaces. Et c'est seulement avec le soutien des Parlements que nous pourrons avancer. Il est en effet arrivé que nous trouvions un accord politique mais que son application soit insuffisante.

En ce qui concerne le budget, monsieur Pueyo, j'hésite un peu à vous répondre car je ne serai malheureusement plus là… Cela reviendrait à me mêler des dépenses des autres. Vous avez toutefois complètement raison. La sécurité est l'une des premières priorités pour nos concitoyens. Il faut réagir et, pour renforcer la lutte contre le terrorisme, contre les menaces cyber et pour accentuer nos efforts dans le domaine de la défense, il faut un budget adéquat. Il ne me revient pas de fixer tous les chiffres. La Commission européenne a déjà lancé quelques propositions s'agissant d'un budget de la défense. Si tous les États membres sont d'accord, alors nous pourrons avancer.

Nous faisons déjà pas mal de choses dans la lutte contre les menaces cyber, en matière de recherche notamment ; mais nous devons renforcer notre coopération et cela aura un coût. Quant à la lutte contre le terrorisme, certaines mesures ne sont pas onéreuses – réseaux de soutien, échanges de bonnes pratiques… – et se révèlent très utiles. D'autres mesures en revanche, et j'y insiste, ont un coût : on veut renforcer la protection de nos espaces publics et l'on a débloqué 120 millions d'euros, mais ce n'est pas assez car la demande des villes est bien supérieure aux fonds engagés. Il faudra donc, je le répète, prévoir un budget.

J'en viens aux agences : on connaît Eurojust, Europol… mais il en existe également de nombreuses dans le domaine cyber. Or nous allons créer une agence européenne de la cybersécurité. Ici aussi, pour que ces agences soient vraiment efficaces, il faut prévoir un budget. On parle beaucoup de l'échange d'informations. Je suis complètement d'accord sur la nécessité d'encourager les États membres à partager l'information, encore faut-il que l'échange soit utile et pour cela que les fichiers fonctionnent. Ainsi avons-nous fait des propositions sur l'interopérabilité des systèmes afin qu'un agent de police ou un agent travaillant à la frontière extérieure de l'Europe ait accès en temps réel aux informations dont il a besoin – un tel dispositif aura un coût, là encore, et qui ne sera pas que de quelques centaines de millions d'euros.

Je réponds à présent à la question de M. Pieyre-Alexandre Anglade sur les fausses informations et en particulier sur l'affaire Cambridge Analytica. Je trouve cette histoire choquante. Pour la Commission, Mme Jourová l'a souligné, il est inacceptable que des données personnelles appartenant à Facebook aient pu être détournées. Selon les derniers chiffres publiés par ce groupe, sur 87 millions de personnes concernées, on compte au moins 2,5 millions d'Européens. C'est beaucoup trop. La commissaire Jourová a demandé des clarifications à Sheryl Sandberg, directrice des opérations de Facebook – qui a manifesté sa volonté de collaborer avec la Commission. On verra quelle suite y sera donnée mais nous ne laisserons pas tomber.

L'affaire Cambridge Analytica montre que la protection des données personnelles est étroitement liée à la préservation du débat démocratique. Je suis d'accord avec vous pour considérer que le règlement général sur la protection des données personnelles, qui entrera en vigueur fin mai, arrive, et c'est le moins que l'on puisse dire, au moment opportun. Mais, là encore, tous les États membres doivent l'appliquer – ce qui n'est pas gagné. En principe ces nouvelles règles vont rendre les entreprises du numérique plus responsables dans leur manière de gérer les données, sous peine de se voir infliger, vous l'avez souligné, des amendes importantes – dont nous aurons besoin pour alimenter le budget.

D'une manière plus générale, dans les quelques semaines à venir, nous allons faire des propositions au sujet des fausses informations. Une de mes collègues commissaires, Mme Gabriel, a constitué un groupe d'experts dont nous sommes en train d'étudier les propositions avant de proposer nous-mêmes des mesures structurelles, de long terme, touchant en particulier à l'éducation, à l'indépendance et à la qualité des médias. J'espère que nous allons également trouver un accord sur des mesures plus immédiates : nous devons renforcer la transparence, surtout s'agissant des contenus sponsorisés mais également de la façon dont est « *boostée* » telle ou telle information. Je suis convaincu que c'est très important au moment des élections. D'ici aux élections européennes de 2019, précisément, nous allons lancer le débat et il appartiendra ensuite aux États membres de nous indiquer comment ils entendent agir. Et, là encore, nous n'allons pas laisser tomber.

On m'a interrogé sur les identités multiples, y compris pour les ressortissants européens. Les bases de données que nous sommes en train d'établir et de consolider concernent pour la plupart des ressortissants des pays tiers. Toutefois, le système d'information Schengen concerne aussi les ressortissants européens. Les autorités françaises ont récemment fait part de leur souhait d'un nouvel instrument permettant d'enregistrer le franchissement des frontières extérieures par les ressortissants européens aussi bien que par les ressortissants des pays tiers. Nous sommes convenus de lancer un travail préparatoire qu'accompagnera une étude de suivi afin de savoir si le dispositif envisagé respecte le cadre européen de protection des données. Cette question est donc sur la table.

En ce qui concerne la police européenne, nous avons déjà sensiblement accru la coopération entre les forces de police, à travers l'échange d'informations notamment, mais aussi à travers le renforcement de l'académie consacrée à l'entraînement de toutes nos forces de police. Ce sont les premiers pas.

Pour ce qui est du retrait des contenus illicites – liés au terrorisme – nous y travaillons depuis un moment. Les GAFA ont compris que c'était essentiel pour eux aussi. J'estime que cette question mérite en effet d'être traitée à vingt-huit – vingt-sept à l'avenir – parce que tout le monde sait que si l'on ne trouve pas une solution au niveau européen, il y a un risque de fragmentation avec des législations qui partent un peu dans tous les sens. Je suis très fier que nous ayons défini, pour la première fois, ensemble, au niveau européen, des objectifs très précis, très opérationnels sur cette question des contenus terroristes. Nous avons rédigé des recommandations : utilisation des outils automatisés de détection et de retrait, amélioration de la coopération avec les grandes plateformes, qui font d'ailleurs beaucoup de progrès, mais aussi avec les plus petites, afin de parer au risque de migration des contenus incriminés, coopération systématique avec les forces de l'ordre... Nous allons examiner jusqu'à la fin mai les progrès accomplis pour réaliser ces objectifs très précis. En cas de progrès insuffisants, nous avons la possibilité de relancer la question d'une législation. Si nous n'avons pas entamé de processus législatif, c'est parce que c'est compliqué et long – or il s'agit ici d'avancer vite.

Mme Coralie Dubost. Ma première question porte sur la politique de l'Union européenne vis-à-vis des Balkans occidentaux. Nous savons que ces derniers sont des partenaires de premier ordre pour l'Union et à plusieurs titres : certains sont candidats à l'adhésion, d'autres jouent un rôle majeur dans la régulation des flux migratoires et la prévention du terrorisme. La zone des Balkans apparaît aujourd'hui comme un espace régional par lequel transitent des combattants qui rentrent de Syrie ou d'Irak et ce sont aussi des pays où le trafic d'armes est très important en raison de la présence de stocks dans les pays de l'ex-Yougoslavie.

Aussi pouvez-vous nous préciser quelle est la politique de l'Union européenne pour renforcer la coopération policière entre ces pays et l'Union ? Europol doit déployer prochainement des officiers de liaison en Serbie, au Monténégro et en Albanie : quel sera leur rôle précis et quelle est l'implication d'Europol dans les Balkans ?

Par ailleurs, en matière d'échange de données personnelles avec les pays tiers, Europol négocie actuellement des accords avec des États tiers, comme la Turquie ou l'Égypte, pour l'échange de données personnelles en vue de lutter contre le terrorisme ou le trafic de migrants, mais aussi pour lutter contre le trafic d'armes et la contrefaçon de marchandises. Pouvez-vous nous confirmer que, pour être validés, ces accords devront d'abord être adoptés par le Conseil de l'Union à la majorité qualifiée après approbation du Parlement européen ?

Je m'interroge sur la manière dont les États membres, qui restent propriétaires des informations qu'ils transmettent à Europol, vont pouvoir s'opposer à ce que certaines interventions fassent l'objet d'échanges avec des États tiers dont ils estiment qu'ils ne présentent pas les garanties de respect de l'État de droit. Il paraît en effet un peu théorique de prévoir dans ce mandat de négociations avec la Turquie que plusieurs autorités publiques indépendantes chargées de la protection des données auront à surveiller l'usage fait par ce pays des données personnelles et devront veiller à ce qu'il ne transmette pas ces données à des pays tiers, eux non autorisés. N'est-il pas un peu illusoire de penser qu'une autorité indépendante non turque va pouvoir mener des investigations en Turquie, et sera en mesure de recueillir les plaintes des personnes sur l'utilisation abusive des données personnelles qui les concernent ?

D'une manière générale, la Commission européenne, dans un souci sécuritaire, en cherchant à renforcer une coopération policière avec des États tiers qui ne partagent en rien le respect des valeurs démocratiques, ne risque-t-elle pas d'aller un peu trop loin ? Quel serait le prix de la sécurité à payer en la matière ?

M. Alexandre Freschi. Monsieur le commissaire européen, je veux d'abord vous dire que c'est avec regret que nous devrons nous passer de votre accent si élégant dans quelques mois…

Dans le treizième rapport sur les progrès accomplis dans la mise en place d'une union de la sécurité réelle et effective, la Commission souligne avoir adopté, le 17 janvier dernier, une recommandation spécifique invitant les États membres « *à prendre de nouvelles mesures pour renforcer l'esprit critique, l'éducation aux médias et les valeurs communes, afin d'accroître le sentiment commun d'appartenance au niveau local et national* ».

De plus, afin de renforcer la cohésion sociale, mais aussi de lutter contre la désinformation, la Commission a annoncé en janvier qu'elle souhaitait prendre des mesures visant à accroître les échanges virtuels entre écoles, notamment grâce au réseau eTwinning, mis en place avec succès, et à stimuler la mobilité scolaire au moyen du programme Erasmus +.

Mes questions sont aussi en lien avec la commission des Affaires culturelles et éducatives dont je suis membre. Comment la Commission pense-t-elle mettre en place ces mesures ? Comment pense-t-elle pouvoir accroître les échanges européens ? Enfin, comment mesurer l'impact effectif des échanges éducatifs européens dans le cadre de la lutte contre la désinformation ?

Mme Constance Le Grip. Monsieur le commissaire, ma question porte sur la cybersécurité. Dans votre propos liminaire, vous avez longuement fait état de la stratégie ambitieuse de la Commission européenne en matière de renforcement de la cybersécurité en Europe. Dans la droite ligne du discours sur l'état de l'Union de Jean-Claude Junker du 13 septembre dernier, un paquet cybersécurité a ainsi été présenté, et nous en saluons l'objectif et la pertinence. Une réelle prise de conscience s'est opérée, y compris au sein des institutions communautaires, sur la nécessité d'avoir une stratégie européenne totalement coordonnée, à la fois sur le plan défensif et sur le plan offensif.

Je souhaite évoquer plus particulièrement l'un des outils de cette panoplie, à savoir le règlement ayant vocation à la fois à pérenniser l'Agence européenne chargée de la sécurité des réseaux et de l'information (ENISA), à en accroître les compétences, et à créer un cadre européen légal de certification. La commission des Affaires européennes de notre assemblée s'est déjà penchée sur ces sujets dans un rapport récent. Nous devons être parfaitement conscients du haut niveau de compétence, d'expertise et de maîtrise technique qui existe dans plusieurs pays européens, notamment la France et l'Allemagne. Ils sont dotés d'organes nationaux extrêmement pointus et reconnus au plan européen en matière de lutte contre les cyberattaques : je pense à l'Agence nationale de la sécurité des systèmes d'information (ANSSI) en France et au BSI en Allemagne, qui collaborent d'ailleurs étroitement.

Dès lors, il nous apparaît un peu hasardeux d'envisager, dans le cadre du renforcement et de l'extension des compétences de l'ENISA, une dépossession de certaines des agences nationales d'autres pays en matière de maîtrise et d'établissement des certificats légaux de cybersécurité. En d'autres termes, nous craignons que l'harmonisation d'un niveau de certification au plan européen n'aboutisse éventuellement à un affaiblissement du niveau de protection et des labels de qualité extrêmement protecteurs qui existent. En France, l'ANSSI dispose d'une expertise incontestable, avec une certification de sécurité de premier niveau (CSPN) dont la valeur est largement reconnue, et l'agence française a également mis au point, en collaboration avec le BSI, le nouveau label commun *European Secure Cloud*.

Par-delà la nécessité de coordonner, d'échanger et d'aider à faire progresser les pays qui ne sont pas encore dotés de structures nationales en matière de certification optimale, nous sommes quelques-uns à avoir des doutes et des inquiétudes face à l'affaissement du niveau de protection qui pourrait résulter de la volonté d'aboutir à une certification européenne harmonisée. À tout le moins, il nous semble qu'une démarche de certification à plusieurs niveaux, avec des évaluations et des processus différents selon les catégories de produits, pourrait constituer une réponse plus appropriée ; il conviendrait alors de laisser principalement aux agences nationales la possibilité de continuer à délivrer ces certifications de cybersécurité performantes.

Mme Marie-France Lorho. Monsieur King, vous déclariez le 28 août dernier, dans le journal *Nice Matin*, qu'aucun État ne peut lutter seul contre le terrorisme. Sur ce point, nous ne pouvons qu'être parfaitement d'accord avec vous. Toutefois, l'Union européenne, ou plus exactement une partie des dirigeants des États de l'Union européenne, a fait le choix de rompre les liens et de provoquer une escalade de commentaires agressifs au sein même de notre union et à l'extérieur. Aussi, j'aimerais vous demander comment nous envisageons aujourd'hui les liens de sécurité avec des pays comme la Pologne et la Hongrie.

Je suis également un peu inquiète face à la mise en œuvre depuis quelques années d'une diplomatie de réprobation. Nous avons, historiquement, des partenaires importants en matière de prévention du terrorisme : en ce qui concerne la Russie, notre collaboration avec

cet État a-t-elle été endommagée par l'escalade des condamnations actives lors de l'affaire Skripal ? Enfin, en janvier dernier, l'Italie recevait M. Ali Mamlouk, chef des renseignements syriens, qui aurait communiqué des listes de terroristes rentrés en Italie. Une telle collaboration est-elle mise en œuvre au niveau européen ?

Mme Marietta Karamanli. Monsieur le commissaire, Mme Dubost a évoqué plusieurs sujets concernant le rôle d'Europol ; après une réunion interparlementaire lors de laquelle nous avons échangé sur ce point, nos inquiétudes sont réelles.

À la suite des attentats terroristes commis à Madrid en 2004, le Conseil européen avait adopté une déclaration sur la lutte contre le terrorisme et, parmi les mesures prévues, figurait la création d'un poste de coordinateur pour la lutte contre le terrorisme. En mars 2016, ce coordinateur avait rendu un rapport sur l'état d'avancement des mesures. Depuis, aucun nouveau document circonstancié n'a été rendu public, alors même que les parlements nationaux sont aujourd'hui de plus en plus impliqués en la matière. Monsieur le commissaire, où en est l'amélioration opérationnelle entre les systèmes de sécurité des différents États – une amélioration que le coordinateur estimait nécessaire il y a déjà deux ans, compte tenu de l'état de faiblesse du système ?

Mme Christine Hennion. Monsieur King, après que l'affaire Microsoft contre le gouvernement américain a défrayé la chronique il y a quelques mois, les États-Unis ont voté dans le cadre du budget américain une nouvelle loi extraterritoriale, le *Cloud Act*, qui leur permet à nouveau d'accéder à des données – ne concernant *a priori* que des citoyens américains.

Cette nouvelle loi n'est pas sans poser certains problèmes, ne serait-ce qu'en raison du fait qu'elle prévoit la possibilité pour les autorités américaines de négocier avec d'autres gouvernements des accords bilatéraux pour des échanges d'information sans recourir au juge pour faire valider la demande. Quelle peut être la position de l'Union européenne sur cette loi qui suscite déjà beaucoup de controverses ? Quelle est votre première réaction à ce sujet.

Mme Françoise Dumas. Monsieur le commissaire, le treizième rapport sur les progrès accomplis dans la mise en place d'une union de la sécurité réelle et effective témoigne de l'importance accordée par la Commission à la lutte contre le terrorisme. Si je salue les mesures proposées, visant à prévenir la radicalisation, à accompagner la sécurisation des espaces publics et à renforcer la sécurité à nos frontières, l'expérience de la France nous montre qu'il est difficile de dissocier l'action intérieure et la sécurité extérieure dans le combat contre le terrorisme – c'est tout le sens de l'intervention effectuée par la France et ses partenaires au Sahel.

Le Président Macron ayant affirmé sa volonté de créer une force européenne d'intervention, j'aimerais savoir quel est l'état d'avancement de la réflexion menée au sein de la Commission européenne sur le lien entre sécurité intérieure et extérieure.

M. Julian King, commissaire européen. Je suis d'accord avec Mme Dubost pour considérer que la coopération avec les Balkans est absolument essentielle pour notre sécurité : soit on exporte plus de sécurité vers les Balkans, soit on s'expose à ce que les Balkans exportent plus d'insécurité vers nos pays. Une partie des quelque 800 ressortissants des Balkans qui sont partis en Irak et en Syrie finiront par revenir en Europe, et il faut compter aussi avec les ressortissants d'autres pays qui peuvent traverser cette zone. La lutte contre le trafic d'armes représente donc un défi particulier dans les Balkans, du fait que celles-ci s'y

trouvent en très grand nombre pour les raisons que je viens d'évoquer : il y a plus d'armes par habitant en Serbie que dans n'importe quel autre pays d'Europe. Ils doivent également faire face à la radicalisation de leurs communautés.

Il faut donc impérativement renforcer notre collaboration avec ces pays. Nous avons adopté en février un plan d'action et un sommet se tiendra au mois de mai. Le travail avec nos agences, Europol, Eurojust et Frontex, sera renforcé, afin de tisser des liens avec les autorités nationales. Il faut aussi, et cela me tient à cœur, accompagner le développement de leurs moyens de lutte contre la cybercriminalité.

Il est vrai qu'Europol est désormais autorisé à ouvrir des négociations avec des pays comme l'Algérie, l'Égypte, Israël, la Jordanie, le Liban, le Maroc, la Tunisie et la Turquie. Vous avez très précisément décrit le processus : une fois les négociations arrivées à leur terme, il faut un vote au Conseil et un avis du Parlement, afin de s'assurer que nos valeurs fondamentales sont pleinement respectées.

Vous m'avez interrogé sur le partage d'informations. Même s'il existe un accord, il revient aux États membres, responsables de leurs données, d'autoriser le partage avec un pays tiers.

Monsieur Freschi, je transmettrai votre question à M. Tibor Navracsics, commissaire en charge de l'éducation, de la culture, de la jeunesse et de la citoyenneté…

Madame Le Grip, nous travaillons étroitement avec l'ANSSI. Comme vous l'avez dit, la France, l'Allemagne, le Royaume-Uni sont bien plus avancés que d'autres pays en la matière. Mais notre objectif est de relever le niveau dans tous les pays européens. C'est la raison pour laquelle nous avons proposé le processus de certification.

Plusieurs niveaux sont concernés, depuis les produits interconnectés de base – souvent produits en Chine, un défi pour nous tous – jusqu'aux investissements stratégiques, qui requièrent un tout autre niveau de sécurité. Il est clair que l'agence européenne de cybersécurité n'a pas vocation à remplacer les agences nationales ; c'est en collaborant avec celles-ci que nous parviendrons à relever le niveau de sécurité de toute l'Union européenne.

Madame Lohro, je ne suis pas certain qu'il y ait eu une escalade après l'attaque contre Sergei et Ioulia Skripal à Salisbury. Nous coopérons avec la Russie, sur une base technique, surtout dans la lutte contre le terrorisme. Il est vrai que la Russie souhaite voir développer ces coopérations : sa proposition est sur la table et sera étudiée par les États membres et la commission. Je rappelle que les travaux d'Europol sont désormais soumis à un contrôle renforcé des parlementaires.

Madame Karamanli, si j'ai bien compris, vous faites référence aux rapports rédigés par M. Gilles de Kerchove. Les États membres donnant des informations dans le cadre de leur participation au fichier, il arrive que ces rapports fassent l'objet d'une classification. Pour autant, je tiens à être aussi ouvert que possible. C'est la raison pour laquelle nous avons lancé, l'an passé, une revue des mesures que nous avons prises dans le domaine de la sécurité depuis quinze ans. Je tiens à votre disposition les résultats, qui ont été publiés.

Madame Hennion, c'est vrai, le Congrès américain vient d'adopter le *Cloud Act*. Nous rencontrons les mêmes problèmes et il nous faut accéder aux preuves électroniques, qui se trouvent de plus en plus souvent hors de nos territoires. La semaine prochaine, nous

présenterons des propositions très détaillées, apportant ainsi une réponse européenne à ce problème international.

Madame Dumas, je travaille étroitement avec Mme Federica Mogherini. Nous sommes convaincus que les questions de sécurité extérieure et celles de sécurité intérieure se rejoignent. Nos moyens et le cadre juridique dans lequel nous travaillons ne sont pas les mêmes, mais une approche globale est nécessaire – je pense notamment à notre action au Mali et à la prise en compte des efforts du pays pour limiter l'émigration.

Je vous remercie de vos questions et de l'attention que vous portez à ces sujets.

Mme la présidente Sabine Thillaye. Monsieur le commissaire, merci de nous avoir éclairés et de nous avoir apporté la confirmation que les États membres se saisissent, ensemble, des questions de sécurité.

Mme la présidente Yaël Braun-Pivet. À mon tour, je vous remercie, monsieur le commissaire.

La réunion s'achève à 18 heures 20.

——ϕπϕπ——

Membres présents ou excusés

Présents. - M. Erwan Balanant, Mme Yaël Braun-Pivet, M. Xavier Breton, M. Vincent Bru, M. Éric Ciotti, M. Jean-Michel Clément, Mme Coralie Dubost, Mme Nicole Dubré-Chirat, Mme Isabelle Florennes, Mme Paula Forteza, M. Philippe Gosselin, M. Dimitri Houbron, M. Sébastien Huyghe, M. Guillaume Larrivé, M. Philippe Latombe, Mme Marie-France Lorho, Mme Alexandra Louis, M. Jean-Louis Masson, M. Stéphane Mazars, M. Jean-Michel Mis, M. Paul Molac, Mme Danièle Obono, M. Jean-Pierre Pont, M. Rémy Rebeyrotte, M. Robin Reda, M. Hervé Saulignac, M. Jean Terlier, M. Arnaud Viala, M. Cédric Villani, M. Jean-Luc Warsmann

Excusés. - M. Philippe Dunoyer, M. Jean-Michel Fauvergue, Mme Marie Guévenoux, M. Mansour Kamardine, Mme Maina Sage, Mme Alice Thourot, M. Guillaume Vuilletet

Assistaient également à la réunion. - M. Pieyre-Alexandre Anglade, Mme Sophie Auconie, M. Éric Bothorel, Mme Fannette Charvier, Mme Yolaine de Courson, Mme Françoise Dumas, M. Alexandre Freschi, Mme Christine Hennion, M. Christophe Jerretie, M. François-Michel Lambert, Mme Constance Le Grip, M. Ludovic Mendes, M. Joaquim Pueyo, Mme Liliana Tanguy, Mme Sabine Thillaye, M. Jean-Pierre Vigier