COMMISSION
EUROPÉENNE

Bruxelles, le 13.6.2018
COM(2018) 470 final

COMMUNICATION DE LA COMMISSION AU PARLEMENT EUROPÉEN, AU CONSEIL EUROPÉEN ET AU CONSEIL

Quinzième rapport sur les progrès accomplis dans la mise en place d'une union de la sécurité réelle et effective

I. INTRODUCTION

Le présent document est le quinzième rapport sur les progrès accomplis dans la mise en place d'une union de la sécurité réelle et effective; il fait état de l'évolution de la situation en ce qui concerne deux piliers principaux: d'une part, lutter contre le terrorisme et la criminalité organisée et contre les moyens sur lesquels ils s'appuient, et, d'autre part, renforcer nos défenses et notre résilience face à ces menaces.

À la suite de l'attaque à l'agent neurotoxique commise à Salisbury, le Conseil européen[1] a déclaré en mars 2018 que «l'Union européenne [devait] renforcer sa résilience aux risques de nature chimique, biologique, radiologique et nucléaire («risques CBRN»), y compris en intensifiant sa coopération avec ses États membres ainsi qu'avec l'OTAN». Il a invité la Commission et la haute représentante à faire progresser les travaux en la matière et à rendre compte, d'ici sa réunion de juin 2018, des progrès qui auront été réalisés. Le présent rapport d'étape s'inscrit dans le cadre de la réponse à cet appel, parallèlement à une communication conjointe[2] intitulée «Accroître la résilience et renforcer la capacité à répondre aux menaces hybrides» et à un rapport conjoint[3] sur la mise en œuvre du cadre commun en matière de lutte contre les menaces hybrides, de juillet 2017 à juin 2018. Il dresse un bilan et présente les prochaines étapes de la mise en œuvre du plan d'action[4] visant à améliorer la préparation aux risques en matière de sécurité chimique, biologique, radiologique et nucléaire, adopté en octobre 2017. Dans le cadre des mesures relevant de l'union de la sécurité conçues pour renforcer la protection contre le terrorisme et la résilience face à celui-ci, le plan d'action a suivi une approche préventive fondée sur l'idée selon laquelle les menaces que font peser les substances chimiques, biologiques, radiologiques et nucléaires constituaient des risques qui, même s'ils présentent un faible degré de probabilité, auraient des conséquences lourdes et durables au cas où un attentat serait perpétré. Dans l'intervalle, l'attentat survenu à Salisbury, ainsi que l'inquiétude grandissante devant l'intérêt des terroristes pour de telles substances et leur capacité à les utiliser tant sur le territoire de l'UE qu'en dehors[5], ont mis en évidence la réalité de la menace que représentent les matières chimiques, biologiques, radiologiques et nucléaires. Cet état de fait renforce encore la nécessité urgente de mettre ce plan d'action intégralement en œuvre, en portant une attention renouvelée aux menaces chimiques.

En outre, le présent rapport expose également la situation actuelle concernant la suppression des **contenus à caractère terroriste en ligne** dans le droit fil de la recommandation de la Commission de mars 2018[6], ainsi que la voie à suivre par la Commission en matière de **prévention de la radicalisation** dans le prolongement du rapport final du groupe d'experts à haut niveau sur la radicalisation. L'attaque commise à Liège le 29 mai 2018 rappelle une nouvelle fois l'importance de la lutte contre la radicalisation étant donné que, d'après les autorités belges, son auteur avait été en contact avec des personnes radicalisées. Le présent rapport recense également plusieurs mesures visant à améliorer la **sûreté dans le transport ferroviaire de voyageurs**. Enfin, il fait le point sur la mise en œuvre des autres dossiers prioritaires, notamment l'**interopérabilité des systèmes d'information**, dossier dans lequel

---

1 http://www.consilium.europa.eu/media/33484/22-euco-final-conclusions-fr.pdf.
2 JOIN(2018) 16 final du 12.6.2018.
3 JOIN(2018) 14 final du 12.6.2018.
4 COM(2017) 610 final du 18.10.2017.
5 Le rapport d'Europol sur la situation et les tendances du terrorisme (TE-SAT) de 2017, p. 16, peut être consulté à l'adresse suivante: www.europol.europa.eu/sites/default/files/documents/tesat2017.pdf. Voir également les déclarations du directeur général de l'Organisation pour l'interdiction des armes chimiques: www.globaltimes.cn/content/1044644.shtml.
6 C(2018) 1177 final du 1.3.2018.

deux propositions de modification, adoptées par la Commission en même temps que le présent rapport, permettront aux colégislateurs de dégager un accord avant la fin de l'année. Le présent rapport fait également le point sur la transposition et la mise en œuvre de la directive relative aux données des dossiers passagers à la suite de l'expiration, le 25 mai 2018, de son délai de transposition, sur la mise en œuvre des actions prises pour renforcer la cybersécurité et contrer le financement du terrorisme, ainsi que sur les évolutions récentes quant à la dimension extérieure de la sécurité.

Les **propositions présentées par la Commission pour le cadre financier pluriannuel 2021-2027** dans sa communication intitulée «Un budget moderne pour une Union qui protège, qui donne les moyens d'agir et qui défend»[7] rendent également compte du fait que les nouvelles menaces en matière de sécurité appellent de nouveaux types d'actions, soulignant que la sécurité revêt en soi une dimension transfrontière et plurisectorielle et qu'une réponse forte et coordonnée s'impose donc au niveau de l'UE. La Commission propose de multiplier par un facteur de 1,8, par rapport à la période actuelle (2014-2020), les fonds destinés à la sécurité intérieure. Les éléments permettant de relever les nouveaux défis en matière de sécurité sont en cours de définition dans diverses propositions législatives sectorielles présentées au titre du cadre financier pluriannuel.

II. UNE MEILLEURE PRÉPARATION AUX RISQUES EN MATIÈRE DE SÉCURITÉ CHIMIQUE, BIOLOGIQUE, RADIOLOGIQUE ET NUCLÉAIRE

1. État d'avancement de la mise en œuvre du plan d'action

Les menaces en matière de sécurité chimique, biologique, radiologique et nucléaire (CBRN) sont complexes et peuvent évoluer rapidement, comme en témoigne l'attaque à l'agent neurotoxique commise à Salisbury. Si les organisations terroristes n'ont pas utilisé d'agents CBRN en Europe, il existe cependant des éléments crédibles suggérant qu'elles pourraient avoir l'intention de se procurer des matières ou des armes CBRN et qu'elles développent actuellement les connaissances et les moyens nécessaires pour les utiliser. Le plan d'action d'octobre 2017 visant à améliorer la préparation aux risques en matière de sécurité chimique, biologique, radiologique et nucléaire, qui a été présenté en réaction à ces menaces, met l'accent sur la mise en commun du savoir-faire et des capacités au niveau de l'UE pour améliorer la préparation opérationnelle sur tout le territoire de l'Union. **Des avancées tangibles** ont été enregistrées dans la mise en œuvre de ce plan d'action, des mesures ayant été prises dans plusieurs domaines afin d'atteindre les quatre objectifs qu'il poursuit, à savoir: réduire l'accessibilité des matières CBRN; garantir une meilleure préparation et une meilleure capacité de réaction aux incidents de sécurité CBRN; resserrer les liens intérieurs et extérieurs en matière de sécurité CBRN avec les principaux partenaires régionaux et internationaux de l'Union; et approfondir nos connaissances en matière de risques CBRN.

Premièrement, dans le cadre des efforts déployés pour réduire l'accessibilité des matières CBRN, l'Union intensifie les **mesures prises par les autorités douanières pour prévenir l'entrée illicite de matières CBRN**. Les systèmes d'information sur les marchandises sont essentiels pour renforcer la surveillance et le contrôle, fondé sur une analyse des risques, des chaînes d'approvisionnement internationales. Aussi la Commission procède-t-elle actuellement à une mise à niveau de grande ampleur du système d'informations anticipées sur les marchandises et de gestion des risques en matière douanière par la réorganisation des actuels systèmes nationaux entretenant des liens peu étroits en un système informatique intégré à grande échelle. Le nouveau système sera centré sur le répertoire commun de données

[7] COM(2018) 321 final du 2.5.2018.

commerciales, qui sera en mesure de recevoir des informations en temps réel et de meilleure qualité sur les marchandises. Il assurera l'interconnexion entre les systèmes d'évaluation des risques des autorités douanières nationales. Le nouveau système sera relié à des milliers d'autres parties intervenant dans les opérations de logistique internationale telles que les transitaires, les prestataires de services logistiques ou les opérateurs postaux, tous modes de transport confondus, qui alimentent le système en précieuses données relatives aux marchandises qui ne sont aujourd'hui pas disponibles. Son objectif est de couvrir l'ensemble des risques douaniers, dont les menaces que représentent les matières CBRN.

Deuxièmement, pour ce qui est de renforcer le degré de préparation et la résilience, les États membres accroissent leur **capacité à détecter les matières CBRN** afin d'aider à prévenir les attaques CBRN. À l'initiative de la Commission, un consortium d'experts nationaux **a analysé les failles des équipements de détection** pour quelque 70 types différents de scénarios CBRN. Le rapport d'analyse des failles a été communiqué aux États membres et discuté avec ceux-ci, démarche qui a contribué à orienter les futurs besoins en matière de recherche et leur a permis d'arrêter des décisions éclairées sur les stratégies de détection et de prendre des mesures opérationnelles pour combler les failles mises en évidence. L'analyse fait aussi apparaître le besoin manifeste pour l'UE de se doter de normes techniques applicables aux équipements de détection. S'appuyant sur les conclusions de l'analyse, et se servant du cadre du groupe consultatif dans le domaine CBRN[8] créé à la faveur du plan d'action, la Commission œuvrera à la normalisation européenne des équipements de détection CBRN. En outre, les États membres devraient dresser des inventaires des stocks de contre-mesures médicales essentielles, des capacités en matière de laboratoires, de traitements et autres. La Commission coopérera avec les États membres pour cartographier régulièrement la disponibilité de ces stocks dans l'ensemble de l'UE afin d'améliorer l'accès à ceux-ci et leur déploiement rapide en cas d'attaque CBRN. Pour se préparer aux conséquences d'une attaque CBRN et les gérer, il est indispensable d'accroître la coopération et la coordination entre les États membres, dont les autorités chargées de la protection civile. Le mécanisme de protection civile de l'Union peut jouer un rôle essentiel dans ce processus, dans le but de renforcer la capacité collective de préparation et de réaction de l'Europe.

Troisièmement, le plan d'action CBRN met l'accent sur la nécessité d'une **coopération étroite avec les organisations et partenaires internationaux principaux**. Les 28 et 29 juin 2018, la Commission, en coopération avec le ministère de l'énergie des États-Unis, organisera un atelier UE-États-Unis sur la sécurité des sources radioactives. La Commission œuvre aussi actuellement au renforcement des capacités des institutions et communautés dans le domaine CBRN dans les pays partenaires du voisinage européen. En outre, l'Union prend des mesures concrètes pour développer une **coopération plus étroite avec l'OTAN** sur la question CBRN, y compris sur la préparation du secteur civil. Des représentants de l'UE ont assisté en tant qu'observateurs à un atelier organisé par l'OTAN sur la coopération civilo-militaire en réaction à une attaque terroriste CBRN de grande ampleur. Par ailleurs, l'UE et l'OTAN envisagent de créer un module de formation conjoint de sensibilisation à l'intention des décideurs dans le domaine CBRN. De surcroît, l'UE devrait examiner des mesures visant à garantir le respect des règles et normes internationales prohibant l'utilisation d'armes chimiques, notamment en se dotant d'un éventuel régime de sanctions propres à l'UE sur les

[8] Afin de faciliter la coopération entre les États membres, la Commission a créé un nouveau **groupe consultatif en matière de sécurité CBRN**, composé des coordonnateurs nationaux de la sécurité CBRN. Ces coordonnateurs servent de points de contact pour la Commission dans le domaine CBRN dans chaque État membre. Le groupe, qui s'est réuni pour la première fois en janvier 2018, se réunira à nouveau en juillet 2018 pour discuter de l'évolution de la politique CBRN au niveau de l'UE et coordonner les activités entreprises par les États membres.

armes chimiques. **En matière de transport**, la Commission et les États membres collaborent avec des partenaires internationaux pour renforcer la préparation du système européen de sûreté aérienne à combattre les menaces CBRN. Ces travaux ont abouti à la constitution d'une liste d'actions pour faire face aux menaces CBRN visant l'aviation.

Quatrièmement, une réaction efficace aux risques CBRN exige des connaissances spécialisées à tous les niveaux, de sorte qu'il est indispensable d'intensifier la **mise en commun et le partage des expertises**. Constitue un exemple de bonne pratique le centre de formation CBRN-E d'Europe centrale[9], créé en 2016 à Budapest par huit États membres[10]. Il vise à partager, élargir et approfondir les connaissances du personnel de première intervention en matière de CBRN-E, son expérience et ses compétences en organisant des formations et des exercices à son intention. Par ailleurs, la Commission a évalué favorablement une proposition de projet portant renforcement de cette coopération par la création d'une unité mobile de première intervention CBRN-E/«bombe sale», déployable – sur demande – en cas d'incident CBRN-E. Le **domaine de la criminalistique** illustre bien la nécessité de créer des capacités collectives. La collecte d'éléments de preuve et leur traitement dans une zone contaminée étant extrêmement difficiles, des installations spécialisées sont indispensables. Le Centre commun de recherche de la Commission élabore actuellement des initiatives dans ce domaine avec des ressources de criminalistique nucléaire afin de partager des connaissances spécialisées sur les capacités correspondantes. Sur la base des conclusions de l'analyse des failles précitée, la Commission collabore également avec le groupe consultatif CBRN afin de recenser les domaines dans lesquels il convient de mettre en commun les capacités de détection.

Cinquièmement, les **formations et exercices** sont des moyens permettant le partage efficace de l'expertise sur les risques CBRN. Dans le cadre du projet eNotice financé par l'UE, une base de données[11] répertoriant plus de 200 initiatives de formation pertinentes a été mise à disposition, offrant un aperçu des possibilités de formation proposées dans l'ensemble de l'Union. Les États membres sont encouragés à utiliser au mieux les possibilités de formation CBRN disponibles. En outre, utilisant pleinement le centre européen de formation à la sécurité nucléaire, la Commission a lancé une vaste campagne de formation à l'intention des experts douaniers de l'UE qui manipulent des équipements sophistiqués de détection nucléaire et de radiation le long des frontières extérieures, dans les ports et aéroports. Par ailleurs, la Commission a évalué de manière positive une proposition de projet portant élaboration d'un programme harmonisé de formation au domaine CBRN destiné aux primo-intervenants et au personnel médical. Pour ce qui est des exercices pratiques, au début de l'année 2018, l'**exercice de simulation Chimera**, organisé par la Commission, a réuni les secteurs de la santé, de la protection civile et de la sécurité sur tout le territoire de l'Union afin de tester la planification de la préparation et de la réaction transfrontières sur la base d'un scénario fictif impliquant la dissémination volontaire d'une maladie transmissible. Cet exercice à l'échelle de l'UE a contribué à soutenir le renforcement des capacités transsectorielles et a amélioré l'interopérabilité et la coordination entre les secteurs de la santé, de la protection civile et de la sécurité au niveau de l'UE et des États membres. En outre, le partage des expertises s'étend également au **secteur privé**, compte tenu de l'ampleur des conséquences que pourrait avoir une attaque CBRN sur les opérateurs de ce secteur. Un projet de l'industrie[12] visant à

9 L'acronyme CBRN-E signifie chimique, biologique, radiologique, nucléaire et explosif.

10 La République tchèque, l'Allemagne, la Croatie, la Hongrie, l'Autriche, la Pologne, la Slovaquie et la Slovénie.

11 https://www.h2020-enotice.eu/static/roster.html.

12 Le projet était intitulé «eTraining Against CBRN Terrorism: the development of a CBRN Online Training» (formations en ligne en matière de lutte contre le terrorisme CBRN: élaboration d'une

sensibiliser le personnel de sécurité, principalement dans le secteur aérien, est à l'origine d'un outil d'apprentissage en ligne qui fournit des informations essentielles aux personnes qui sont en contact avec des matières et agents CBRN.

2. Renforcement des actions de lutte contre les menaces chimiques

Le recours éventuel à des produits chimiques dans les attentats terroristes prend une importance grandissante dans la propagande terroriste. Cela s'ajoute à des préoccupations qui se sont fait jour en rapport avec le complot terroriste découvert en Australie en juillet 2017, et à l'utilisation récente de produits chimiques dans un théâtre. C'est pourquoi la Commission **accélère la mise en œuvre d'autres actions de lutte contre les menaces chimiques** dans le cadre général du plan d'action CBRN, en s'appuyant sur les progrès accomplis dans l'analyse des failles qui minent les capacités de détection et dans l'échange de bonnes pratiques au sein du groupe consultatif en matière de sécurité CBRN.

Lors d'une réunion classifiée avec les experts des États membres en mars 2018 ont été recensées plusieurs priorités absolues, en matière de lutte contre les menaces chimiques, devant faire l'objet d'une coopération accrue. Poursuivant sur cette lancée, la Commission collaborera avec les États membres afin de **mener à bien les actions suivantes** avant la fin de l'année 2018:

- Élaborer une liste commune des substances chimiques représentant une menace particulière, qui servira de base à toute action opérationnelle ultérieure visant à réduire leur accessibilité et à renforcer les capacités à les détecter. Ces travaux seront réalisés au sein d'un groupe d'experts ad hoc sur la détection des menaces chimiques, créé en mai 2018, qui exploitera les travaux de recherche actuellement menés dans les États membres et au Centre commun de recherche de la Commission.
- Instaurer un dialogue avec les acteurs privés de la chaîne d'approvisionnement pour collaborer à des mesures visant à contrer les menaces grandissantes et en évolution que constituent les produits chimiques pouvant être utilisés comme précurseurs. Ces travaux suivent l'exemple[13] des mesures prises au niveau de l'UE pour restreindre l'accès aux précurseurs d'explosifs; un premier échange de vues a déjà eu lieu au sein du comité permanent sur les précurseurs.
- Accélérer le passage en revue des scénarios de menace et l'analyse des méthodes de détection existantes afin d'améliorer la détection des menaces chimiques, dans le but d'élaborer des orientations opérationnelles pour aider les États membres à renforcer leurs capacités de détection. C'est à cette fin que le groupe d'experts ad hoc susmentionné a été créé pour lutter contre les menaces chimiques émergentes. À plus

---

formation en ligne au domaine CBRN») (numéro de référence - HOME/2013/ISEC/AG/CBRN/4000005269) et a obtenu un financement au titre du programme «Prévenir et combattre la criminalité».

[13] Dans le cadre des travaux relevant de l'union de la sécurité et visant à restreindre le périmètre d'action des terroristes et des criminels, la Commission a agi avec fermeté pour réduire l'accès aux précurseurs d'explosifs dont l'utilisation peut être détournée pour la fabrication d'explosifs artisanaux. En octobre 2017, elle a présenté une recommandation définissant des mesures à prendre sans délai pour prévenir toute utilisation détournée des précurseurs d'explosifs fondées sur les règles existantes [recommandation C(2017) 6950 final du 18.10.2017]. Poursuivant sur cette lancée, la Commission a, en avril 2018, adopté une proposition visant à réviser et à renforcer le règlement (UE) n° 98/2013 relatif à la commercialisation et à l'utilisation de précurseurs d'explosifs [COM(2018) 209 final du 17.4.2018]. Pour de plus amples informations, voir le quatorzième rapport sur les progrès accomplis dans la mise en place d'une union de la sécurité réelle et effective [COM(2018) 211 final du 17.4.2018].

long terme, les travaux de ce groupe peuvent poser les jalons de la normalisation des équipements de détection.

- Mener un travail de sensibilisation auprès du personnel de première intervention, en particulier celui des services répressifs et de la protection civile, afin de lui permettre de reconnaître les premiers signes d'une attaque chimique et de réagir de manière appropriée.

III. LUTTER CONTRE LA RADICALISATION

1. Lutte contre les contenus à caractère terroriste en ligne

La lutte contre les contenus à caractère terroriste en ligne demeure une problématique d'envergure dans la prévention de la radicalisation. À la suite de l'adoption de la recommandation de la Commission du 1er mars 2018[14] **sur les mesures destinées à lutter contre les contenus illicites en ligne**, un exercice d'établissement de rapports, préconisé par cette recommandation, a été ultérieurement lancé afin de permettre le suivi des efforts déployés par le secteur et par les États membres ainsi que par d'autres partenaires de premier plan, tels qu'Europol, dans la réduction de l'accessibilité aux contenus à caractère terroriste en ligne.

Les premières conclusions de ce premier exercice d'établissement de rapports fondé sur des indicateurs adoptés d'un commun accord et définis au sein du forum de l'UE sur l'internet – exercice qui concerne 13 entreprises au total, dont les grandes entreprises du secteur des médias sociaux[15], 20 États membres et Europol – font état de quelques progrès en matière de transparence, étant donné qu'un plus grand nombre d'entreprises, notamment des entreprises qui n'avaient pas antérieurement participé au forum de l'UE sur l'internet, ont communiqué davantage d'informations.

De surcroît, les sociétés sont plus nombreuses à adopter des mesures proactives pour détecter les contenus à caractère terroriste, parallèlement au retrait d'un volume supérieur de ces contenus. Les entreprises ayant développé des outils automatisés pour circonscrire les contenus à caractère terroriste (y compris les contenus précédemment retirés) sont parvenues à accroître la rapidité avec laquelle elles retirent ces contenus de leur plateforme, tout en circonscrivant et en retirant d'importants volumes de documents archivés. La base de données d'empreintes numériques («Database of Hashes»), outil créé par un consortium de sociétés afin de faciliter la coopération, de manière à empêcher la diffusion de contenus à caractère terroriste sur l'ensemble des plateformes, continue à s'étendre, sur le plan tant du nombre de membres que du volume de contenus à caractère terroriste consignés dans la base de données. 13 sociétés sont à présent connectées à la base de données, qui comprend désormais 80 000 empreintes d'images numériques et 8 000 empreintes de vidéos numériques. Pour la première fois, certaines sociétés ont fourni un retour d'information sur les effets de la base de données d'empreintes numériques sous l'angle des contenus retirés, mais ce retour d'information doit se développer et être plus détaillé et systématique, toutes plateformes confondues.

Les signalements effectués par les États membres demeurent également un volet important de la réaction. Le nombre d'États membres signalant des contenus à caractère terroriste aux

[14] Il en est fait état dans le quatorzième rapport sur les progrès accomplis dans la mise en place d'une union de la sécurité [COM(2018) 211 final du 17.4.2018].

[15] Sur 33 entreprises contactées par la Commission.

entreprises de l'internet continue d'augmenter tandis que l'unité chargée du signalement des contenus sur internet au sein d'Europol continue de chercher des moyens d'améliorer les signalements au niveau de l'UE, notamment sur le plan de la coordination et de la rationalisation du processus. L'unité de l'UE chargée du signalement des contenus sur internet est à l'origine de 8 103 décisions de signalement de contenu au quatrième trimestre de 2017, lesquelles ont donné lieu au retrait du contenu dans 89 % des cas. Sur les 5 708 décisions de signalement arrêtées au premier trimestre de 2018 à l'intention notamment d'un nombre accru de sociétés de taille plus modeste, et moins connues, 61 % de ces décisions ont abouti au retrait d'un contenu. Les taux de retrait effectif pour les sociétés qui collaborent depuis longtemps avec les unités chargées du signalement des contenus sur internet demeurent stables, oscillant dans la plupart des cas entre 90 % et 100 %. La vitesse de réaction des sociétés aux signalements varie d'une plateforme à l'autre et est comprise entre moins d'une heure et plusieurs jours; les sociétés de grande ou de petite taille doivent continuer à réagir encore plus rapidement pour donner convenablement suite à la recommandation selon laquelle il conviendrait de retirer les contenus à caractère terroriste dans l'heure qui suit la réception du signalement.

Il n'existe pas encore de mécanismes de retour d'information systématique complet sur les signalements, bien que les États membres reconnaissent effectivement recevoir, de la part de plusieurs entreprises, des accusés de réception et la confirmation de prise de mesures. Seule une société communique des informations complètes sur la réception, le délai de réaction et la prise de mesures. Afin d'améliorer la coopération et la coordination entre les services répressifs et les entreprises, l'unité de l'UE chargée du signalement des contenus sur internet a créé en 2016 l'application de gestion des signalements sur internet. À ce jour, trois États membres sont reliés à la plateforme, tandis que d'autres ont manifesté leur intérêt en ce sens.

La Commission a également lancé une analyse d'impact pour déterminer si l'approche actuelle est suffisante ou si de nouvelles mesures sont nécessaires afin d'assurer la détection et le retrait rapides et proactifs des contenus illicites en ligne, y compris d'éventuelles mesures législatives destinées à compléter le cadre réglementaire en vigueur. Les rapports établis au titre de la recommandation seront intégrés dans cette analyse d'impact.

L'unité de l'UE chargée du signalement des contenus sur internet au sein d'Europol a dirigé une collaboration coordonnée et multinationale, associant six États membres ainsi que les États-Unis et le Canada, afin de cibler la machine de propagande de Daech. Cet effort de collaboration, qui marque l'aboutissement de l'équivalent de plus de deux ans de travail impliquant 29 pays, s'est traduit non seulement par une forte perturbation des activités et de l'infrastructure de propagande de Daech, mais aussi par la saisie d'un volume considérable de preuves numériques.

2. Suites données aux travaux du groupe d'experts à haut niveau sur la radicalisation

Parallèlement aux efforts déployés pour lutter contre les contenus à caractère terroriste en ligne, les travaux menés à l'échelle de l'Union continuent de soutenir la prévention de la radicalisation dans les États membres et dans leurs communautés locales. Le groupe d'experts à haut niveau sur la radicalisation, institué[16] en juillet 2017 pour formuler des recommandations sur les moyens d'améliorer la coordination et la collaboration entre tous les

16 http://ec.europa.eu/transparency/regexpert/index.cfm?do=groupDetail.groupDetail&groupID=3552&NewSearch=1&NewSearch=1.

acteurs concernés, a présenté son **rapport final**[17] **le 18 mai 2018**. Ce rapport comprend toute une série de recommandations d'action concrète visant à remédier aux problématiques qui se posent dans des domaines prioritaires tels que la radicalisation en milieu carcéral (y compris le suivi après la libération d'un détenu et la gestion des peines), la communication et la propagande en ligne, la coopération multipartite au niveau local, l'éducation et l'inclusion sociale, l'aide aux groupes qui nécessitent une attention particulière (notamment en ce qui concerne la radicalisation des jeunes et le retour des enfants de zones de conflit) ainsi que la dimension extérieure. Reconnaissant la valeur ajoutée d'initiatives de l'UE, telles que le réseau de sensibilisation à la radicalisation (RSR), le réseau européen des communications stratégiques (SCN) et le forum de l'UE sur l'internet, et les résultats qu'elles ont produits, le rapport appelle à renforcer ces initiatives et à les coordonner davantage, tout en resserrant les liens entre l'ensemble des parties prenantes associées, dont les professionnels de première ligne, les responsables politiques et les chercheurs. Le rapport insiste sur l'importance que les actions au niveau de l'UE soient mieux adaptées aux besoins des États membres.

La Commission accueille favorablement le rapport final dans la mesure où il recense les domaines dans lesquels une action urgente s'impose au sein des États membres et au niveau de l'UE. En particulier, la Commission donnera suite à la recommandation consistant à mettre en place un mécanisme de coopération de l'UE afin d'assurer une participation plus étroite des États membres aux travaux sur la lutte contre la radicalisation. Ce mécanisme de coopération de l'UE comprendra un nouveau comité directeur composé des États membres et une structure de coordination et de soutien en matière de radicalisation qui devront être créés au sein de la Commission.

La Commission va prendre **sans délai des mesures** pour donner suite aux recommandations formulées par le groupe d'experts:

- Premièrement, en adoptant une décision portant création du comité directeur, composé des États membres (le coordinateur de l'UE pour la lutte contre le terrorisme et le Service européen pour l'action extérieure siégeant en tant qu'observateurs), pour veiller à ce que les actions de l'UE dans ce domaine soient davantage orientées vers les besoins et les priorités d'action au sein des États membres, et offrir à ces derniers la possibilité d'être plus étroitement associés à la définition des orientations stratégiques. Une première réunion du comité directeur est prévue au plus tard en novembre 2018.
- Deuxièmement, en créant une structure de coordination et de soutien renforcée au sein de la Commission, dans le respect des ressources limitées actuellement disponibles. Les contributions des États membres au développement de l'expertise requise revêtiraient une importance particulière pour la réalisation des objectifs énoncés dans le rapport final. À cette fin, la Commission invite les États membres à présenter des propositions de détachements sans frais auprès de la structure de coordination et de soutien. Avec le comité directeur, cette structure formera le mécanisme de coopération de l'UE en matière de lutte contre la radicalisation.
- Troisièmement, en organisant une réunion du réseau de responsables nationaux des politiques de prévention avant octobre 2018 afin de faciliter davantage les échanges entre les États membres et de discuter des actions de suivi concrètes.

La Commission prend note de la recommandation du groupe d'experts que le mécanisme de coopération de l'UE en matière de lutte contre la radicalisation soit apprécié et évalué au

[17] http://ec.europa.eu/transparency/regexpert/index.cfm?do=groupDetail.groupDetail&groupID=3552.

cours de l'année 2019, et elle tâchera de présenter les résultats de cette évaluation d'ici décembre 2019, reconnaissant que d'ici là, les mesures proposées n'auront probablement pas encore été intégralement mises en œuvre.

Dans le domaine de l'éducation, le Conseil «Éducation, jeunesse, culture et sport» a, le 22 mai 2018, adopté une recommandation[18] sur la promotion de valeurs communes dans les écoles afin de consolider un plus grand sentiment d'appartenance au niveau local et national, ainsi que la Commission l'avait proposée[19]. Cette recommandation invite les États membres à prendre des mesures supplémentaires pour **renforcer l'esprit critique et l'éducation aux médias dans les écoles**.

IV. MESURES CONCRÈTES À COURT TERME VISANT À AMÉLIORER LA SÛRETÉ DU TRANSPORT FERROVIAIRE DE VOYAGEURS

Les plateformes de transport, ainsi que les voies ferrées et les trains représentent une cible à haut risque puisque leur infrastructure est, par nature, ouverte[20]. À l'heure actuelle en Europe, 26 millions de voyageurs prennent le train chaque jour tandis que le transport ferroviaire devrait connaître une croissance d'environ 80 % d'ici à 2050. La protection des usagers, des travailleurs et des infrastructures du transport ferroviaire contre les menaces en constante évolution qui pèsent sur la sûreté constitue un défi majeur et permanent. Le transport ferroviaire européen doit rester sûr et sécurisé.

L'Europe a besoin d'un **système de sûreté ferroviaire moderne** qui se fonde sur une évaluation des risques et qui permette une réaction rapide et proportionnée aux menaces émergentes tout en maintenant les services ferroviaires accessibles. Afin d'obtenir un niveau accru de sûreté, tout en maintenant les services ferroviaires accessibles et ouverts aux voyageurs et en évitant les obstacles inutiles au marché intérieur, les États membres devraient améliorer l'échange d'informations et augmenter le niveau de sensibilisation, de préparation et de capacité de réaction aux actes terroristes. Les mesures introduites par les États membres de manière individuelle sans coordination en amont sont susceptibles de créer des obstacles et d'engendrer des coûts liés à l'allongement du temps de voyage, aux annulations et à la congestion des centres ferroviaires.

Il est nécessaire que **les niveaux de sûreté soient équivalents pour les voyageurs ferroviaires dans toute l'UE et quel que soit l'opérateur de transport.** Une action prise au niveau de l'UE pour assurer la coordination transfrontière de tous les acteurs concernés peut contribuer à une protection cohérente de la sûreté dans l'ensemble de l'UE.

La Commission propose par conséquent de prendre une série de **mesures concrètes à court terme pour améliorer la sûreté des voyageurs ferroviaires dans l'UE** (voir annexe I). Le train de mesures européen de lutte contre le terrorisme adopté le 18 octobre 2017 annonçait des actions pour mieux protéger les espaces publics[21]; les mesures proposées se fondent sur ces actions et sur des études spécialisées qui montrent qu'il convient d'agir pour améliorer la

---

18 Recommandation du Conseil relative à la promotion de valeurs communes, à l'éducation inclusive et à la dimension européenne de l'enseignement: http://data.consilium.europa.eu/doc/document/ST-8015-2018-INIT/fr/pdf.

19 Treizième rapport sur les progrès accomplis dans la mise en place d'une Union de la sécurité réelle et effective [COM(2018) 46 final du 18.10.2017].

20 Onzième rapport sur les progrès accomplis dans la mise en place d'une union de la sécurité réelle et effective [COM(2017) 608 final du 18.10.2017].

21 COM(2017) 612 final du 18.10.2017.

résilience du secteur ferroviaire européen en matière de sûreté, notamment pour les services internationaux[22]. Ces mesures reflètent également les résultats d'une évaluation des risques réalisée par la Commission, les États membres et le Centre de situation et du renseignement de l'UE (EU INTCEN).

Les mesures **visant à renforcer la sûreté ferroviaire** qui ont été recensées se situent **tant au niveau de l'UE que des États membres**. Au niveau de l'UE, la Commission propose d'établir une plateforme de l'UE en matière de sûreté des voyageurs ferroviaires afin de créer un cadre effectif de coopération et de proposer des recommandations pour aider les États membres à coordonner efficacement leurs actions dans le domaine de la sûreté ferroviaire. Cette plateforme permettra de recueillir et d'échanger des informations essentielles sur la sûreté ferroviaire, d'optimiser la sûreté des services ferroviaires transfrontières et de définir un mécanisme de coordination afin d'éviter les décisions unilatérales au niveau national. Elle aidera également les États membres et les parties prenantes du secteur ferroviaire à évaluer conjointement les nouvelles menaces et les nouveaux incidents liés à la sûreté et à réagir de manière coordonnée et appropriée. En outre, la Commission, en étroite collaboration avec les États membres, le Service européen pour l'action extérieure et les agences concernées, élaborera une méthodologie commune d'évaluation des risques liés à la sûreté ferroviaire au niveau de l'UE.

Les mesures proposées seront testées en pratique. La Commission mènera des activités annuelles qui permettront de tester l'efficacité de ce mécanisme dans différents scénarios. Ces activités pourraient être mises en relation avec les exercices existants soutenus par l'UE et effectués par les forces de police ferroviaire. La Commission fera rapport sur la mise en œuvre de ces mesures et pourra envisager toutes les dispositions appropriées conformément aux principes pour une meilleure réglementation afin d'améliorer ces mesures ou de corriger les faiblesses constatées.

V. MISE EN ŒUVRE DES AUTRES DOSSIERS PRIORITAIRES EN MATIÈRE DE SÉCURITÉ

1. Vers l'interopérabilité des systèmes d'information

En vue d'élaborer des systèmes d'information plus robustes et plus intelligents aux fins de la gestion de la sécurité, des frontières et des flux migratoires, l'Union européenne cherche à remédier de toute urgence et en priorité aux lacunes que présentent la gestion et le partage des informations au niveau de l'Union. Les propositions présentées par la Commission en décembre 2017[23] sur l'interopérabilité des systèmes d'information, dont le Parlement européen et le Conseil poursuivent l'examen, sont essentielles à cet égard. Dans la déclaration commune sur les priorités législatives de l'UE, les trois institutions se sont fixé comme objectif commun de trouver un accord sur ces propositions avant la fin de 2018. C'est pourquoi, comme annoncé précédemment[24], la **Commission a présenté en même temps que**

---

22 *Study on options for the security of European high-speed and international rail services conducted at the request of the services of the EC* (Étude sur les options envisageables en ce qui concerne la sûreté des services ferroviaires européens à grande vitesse et internationaux, menée à la demande des services de la CE), Steer Davies & Gleave, décembre 2016: http://europa.eu/!mM86yp.

23 COM(2017) 793 final et COM(2017) 794 final du 12.12.2017.

24 Voir le quatorzième rapport sur les progrès accomplis dans la mise en place d'une union de la sécurité réelle et effective, COM(2018) 211 final du 17.4.2018. Les propositions législatives de décembre 2017 sur l'interopérabilité des systèmes d'information contiennent déjà les modifications nécessaires à apporter aux instruments juridiques relatifs au code frontières Schengen, au futur système d'entrée/de sortie et au système d'information sur les visas. Par contre, elles ne prévoient pas les modifications qu'il convient

le présent rapport deux propositions modifiées sur l'interopérabilité qui intègrent les modifications nécessaires des propositions sur l'interopérabilité de décembre 2017 concernant les instruments juridiques qui étaient encore en cours de négociation à ce moment-là. La Commission invite les colégislateurs à inclure les propositions modifiées dans leur examen en cours des propositions sur l'interopérabilité afin d'entamer des trilogues sans tarder.

Les propositions modifiées reflètent les progrès enregistrés récemment par le Parlement européen et le Conseil sur les propositions législatives relatives aux systèmes d'information de l'UE appliqués à la gestion de la sécurité, des frontières et des flux migratoires. Les colégislateurs ont dégagé un accord politique final le 25 avril 2018 sur la création du **système européen d'information et d'autorisation concernant les voyages (ETIAS)**[25] qui permettra de soumettre les voyageurs exemptés de l'obligation de visa et se rendant dans l'UE à des vérifications préalables en matière d'immigration irrégulière et de sécurité. Le 12 juin 2018, les colégislateurs sont également parvenus à un accord politique sur les trois propositions législatives[26] visant à renforcer le **système d'information Schengen**, système de partage d'informations le plus largement utilisé pour la gestion de la sécurité et des frontières en Europe. Ce renforcement augmentera la sécurité des citoyens européens en consolidant les capacités du système à lutter contre le terrorisme et la criminalité transfrontière, à améliorer la gestion des frontières et des migrations et à garantir un échange d'informations efficace entre les États membres. De plus, les colégislateurs ont conclu un accord politique le 24 mai 2018 sur la proposition législative[27] visant à renforcer **eu-LISA, l'agence européenne pour la gestion opérationnelle des systèmes d'information à grande échelle** au sein de l'espace de liberté, de sécurité et de justice. Le mandat renforcé conféré à cette agence permettra à celle-ci de développer et de déployer les solutions techniques qui rendront les systèmes d'information concernés interopérables. L'accord intervenu sur ces trois initiatives, ainsi que les progrès réalisés lors des discussions sur la proposition législative[28] visant à étendre le **système européen d'information sur les casiers judiciaires** aux ressortissants de pays tiers, ont permis à la Commission de présenter les propositions modifiées précitées sur l'interopérabilité, qui intègrent les modifications nécessaires concernant ces instruments juridiques dans les propositions sur l'interopérabilité de décembre 2017.

Les propositions modifiées sur l'interopérabilité ne contiennent pas les modifications relatives à **Eurodac**, la base de données européenne utilisée dans le domaine de l'asile et de la migration irrégulière, étant donné que les discussions au sujet de la proposition législative[29] de mai 2016 visant à renforcer Eurodac n'ont pas abouti. L'architecture actuelle du système Eurodac existant empêche celui-ci, du point de vue technique, de participer à l'interopérabilité des systèmes d'information puisqu'il ne stocke que des données biométriques et un numéro de référence, mais pas d'autres données à caractère personnel (comme les noms, l'âge, la date de naissance) qui permettraient de détecter d'éventuelles identités multiples liées au même ensemble de données biométriques. La proposition législative de mai 2016 vise à étendre la portée d'Eurodac à l'identification des ressortissants de pays tiers en séjour irrégulier et de

---

d'apporter à d'autres instruments (règlements sur le système européen d'information et d'autorisation concernant les voyages, Eurodac, le système d'information Schengen, le système européen d'information sur les casiers judiciaires pour les ressortissants de pays tiers et l'Agence européenne pour la gestion opérationnelle des systèmes d'information à grande échelle) qui étaient en cours de négociation au Parlement européen et au Conseil lorsque les propositions sur l'interopérabilité ont été présentées.

25 COM(2016) 731 final du 16.11.2016.

26 COM(2016) 881 final, 882 final et 883 final du 21.12.2016.

27 COM(2017) 352 final du 29.6.2017.

28 COM(2017) 344 final du 29.6.2017.

29 COM(2016) 272 final du 4.5.2016.

ceux qui sont entrés dans l'UE dans des conditions irrégulières. En particulier, elle prévoit l'enregistrement de données à caractère personnel telles que les nom(s), âge, date de naissance, nationalité et références de documents d'identité. Ces données d'identité sont essentielles pour qu'Eurodac soit en mesure de contribuer aux objectifs d'interopérabilité et de fonctionner dans son cadre technique. Pour ce faire, il est indispensable que les colégislateurs parviennent de toute urgence à un accord sur cette proposition législative. Dans l'attente d'un accord sur la proposition législative visant à renforcer Eurodac, les données des ressortissants de pays tiers en séjour irrégulier et de ceux qui sont entrés dans l'UE dans des conditions irrégulières ne peuvent pas faire partie de l'interopérabilité des systèmes d'information européens. Dès que les colégislateurs auront trouvé un accord sur la proposition législative visant à renforcer Eurodac, ou qu'ils auront accompli des progrès suffisants, la Commission présentera les modifications afférentes aux propositions sur l'interopérabilité dans un délai de deux semaines.

Le 16 mai 2018, la Commission a présenté une proposition législative[30] visant à renforcer le **système d'information sur les visas (VIS)** afin de mieux faire face à l'évolution des enjeux en matière de sécurité et de migration et d'améliorer la gestion des frontières extérieures de l'UE. Tandis que le système d'information sur les visas existant est déjà couvert par les propositions sur l'interopérabilité de décembre 2017, la proposition législative de mai 2018 visant à renforcer le système d'information sur les visas permettrait à celui-ci de recourir pleinement aux solutions d'interopérabilité proposées. Cette proposition prévoit d'intensifier les vérifications entre les bases de données pour prévenir les risques de migration irrégulière et les risques pour la sécurité lors de la délivrance des visas et de renforcer les capacités de prévention de la criminalité, contribuant dès lors à accroître la sécurité et à combler les lacunes d'information.

2. Transposition et mise en œuvre de la directive sur les données des dossiers passagers

La **directive sur les données des dossiers passagers**[31] est cruciale pour permettre à l'Union d'organiser sa réponse commune à la menace que représentent le terrorisme et la criminalité organisée. Les États membres avaient jusqu'au 25 mai 2018 pour la transposer. À la date du 7 juin 2018, 14 États membres avaient communiqué à la Commission les mesures adoptées pour transposer la directive[32]. Les 13 autres États membres n'ont pas encore communiqué leurs mesures nationales de transposition[33]. Dans neuf États membres, la législation nécessaire a été déposée au parlement pour adoption tandis que dans un autre État membre, la législation primaire transposant la directive a déjà été adoptée mais la législation secondaire permettant d'en assurer la transposition complète est toujours en attente d'adoption. Parmi les États membres qui n'ont pas encore communiqué leurs mesures de transposition à la Commission, cinq disposent d'une législation en vigueur qui leur permet de recueillir des données PNR en vertu du droit national. Toutefois, leur cadre législatif doit encore être modifié afin d'être pleinement conforme à la directive.

---

30 COM(2018) 302 final du 16.5.2018.

31 Directive (UE) 2016/681 du Parlement européen et du Conseil du 27 avril 2016 relative à l'utilisation des données des dossiers passagers (PNR) pour la prévention et la détection des infractions terroristes et des formes graves de criminalité, ainsi que pour les enquêtes et les poursuites en la matière, JO L 119 du 4.5.2016, p. 132.

32 La Belgique, la Croatie, l'Estonie, l'Allemagne, la Hongrie, l'Irlande, l'Italie, la Lettonie, la Lituanie, le Luxembourg, Malte, la Pologne, la Slovaquie et le Royaume-Uni. Les informations concernant les mesures nationales de transposition communiquées par les États membres sont accessibles au public sur Eur-Lex: https://eur-lex.europa.eu/legal-content/FR/NIM/?uri=CELEX:32016L0681.

33 Le Danemark ne participe pas à la directive PNR.

Outre la communication des mesures nationales de transposition au titre de l'article 18, la directive PNR prévoit des notifications spécifiques concernant son application aux vols intra-UE (article 2); la création d'unités d'informations passagers (UIP) (article 4) et la liste des autorités compétentes habilitées à demander aux UIP ou à recevoir de celles-ci des données PNR (article 7). Les 27 États membres[34] ont tous transmis à la Commission la liste de leurs autorités compétentes habilitées à demander ou à recevoir des données PNR ou le résultat du traitement de telles données, conformément aux dispositions de l'article 7, paragraphe 3, de la directive PNR. 19 États membres ont informé la Commission de leur intention d'appliquer la directive aux vols intra-UE conformément à l'article 2, paragraphe 1, et 21 États membres lui ont notifié la mise en place de leur UIP conformément à l'article 4, paragraphe 5.

Outre les mesures qu'ils ont prises pour transposer la directive en droit interne et pour parachever les dispositions institutionnelles requises, les États membres ont effectué des progrès dans la mise en place des solutions techniques permettant de stocker, traiter et analyser les données PNR. 24 États membres disposent d'une solution technique PNR alors que les trois autres se situent à divers stades de déploiement des infrastructures nécessaires. Dans 12 États membres, le processus visant à établir la connectivité avec les transporteurs aériens afin de permettre la transmission des données PNR aux UIP est en bonne voie, alors que dans 11 autres États membres, au moins un transporteur aérien transmet déjà des données PNR en temps réel à l'UIP.

Dans l'ensemble, la Commission constate donc que des progrès importants ont été accomplis dans la transposition et la mise en œuvre de la directive PNR au cours des deux dernières années. Toutefois, étant donné l'importance capitale de cet instrument pour permettre à l'UE d'organiser sa réponse commune au terrorisme et aux formes graves de criminalité, la Commission aura recours à toutes les mesures dont elle dispose pour faire respecter le droit de l'Union, y compris la procédure d'infraction s'il y a lieu. Le défaut de transposition nuit à l'efficacité du mécanisme européen PNR dans son ensemble, réduit la sécurité juridique pour les transporteurs aériens en retardant la création d'un régime européen unique de fourniture des données PNR et entrave la protection effective des données à caractère personnel dans l'UE. La Commission continuera d'apporter son soutien à tous les États membres dans l'élaboration de leur système PNR, y compris en facilitant l'échange d'informations et de bonnes pratiques après l'expiration du délai de transposition. À cet égard, une première réunion avec les États membres a eu lieu le 7 juin 2018 pour discuter des questions liées à l'application de la directive PNR.

3. Cybersécurité et menaces liées au cyberespace

La Commission poursuit, en coopération avec le Service européen pour l'action extérieure, la mise en œuvre des actions prévues dans la communication conjointe de septembre 2017[35] intitulée «Résilience, dissuasion et défense: doter l'UE d'une cybersécurité solide».

Le 9 mai 2018 était la date limite impartie à tous les États membres de l'UE pour transposer la **directive sur la sécurité des réseaux et des systèmes d'information** en droit national. Il s'agit du premier ensemble de règles juridiquement contraignantes en matière de cybersécurité à l'échelle de l'UE qui assure un niveau élevé commun de sécurité des réseaux et des systèmes d'information dans l'UE.

[34] Le Danemark ne participe pas à la directive PNR.
[35] JOIN (2017) 450 final du 13.9.2017.

Les 6 et 7 juin 2018, le 5e **exercice paneuropéen en matière de crises cybernétiques Cyber Europe 2018** a eu lieu sous la coordination de l'Agence de l'UE chargée de la sécurité des réseaux et de l'information (ENISA)[36]. Cet exercice, destiné à des équipes de sécurité informatique, de continuité des activités et de gestion des crises provenant d'États membres de l'UE et de l'AELE, a rassemblé plus de 1 000 participants. Le scénario avait pour thème l'aviation et il impliquait les autorités de l'aviation civile, les prestataires de services de navigation aérienne, les compagnies aériennes, les transporteurs aériens, avec des répercussions potentielles sur d'autres secteurs.

L'exposition des citoyens à la désinformation à grande échelle, y compris à des informations trompeuses ou absolument fausses, constitue un autre type grave de menace liée au cyberespace, ainsi qu'un défi majeur pour l'Europe. Dans sa communication du 26 avril 2018 intitulée «**Lutter contre la désinformation en ligne: une approche européenne**»[37], la Commission a présenté un plan d'action et des instruments d'autorégulation pour lutter contre la propagation et l'incidence de la désinformation en ligne en Europe, et pour assurer la protection des valeurs européennes et des systèmes démocratiques. Les mesures spécifiques exposées comprennent un code de bonnes pratiques pour combattre la désinformation à l'échelle de l'UE, adressé aux plateformes en ligne et aux annonceurs, doublé d'un soutien à un réseau indépendant de vérificateurs de faits, et une série de mesures visant à encourager le journalisme de qualité et à promouvoir l'éducation aux médias. Le 29 mai 2018, le forum plurilatéral sur la désinformation s'est réuni pour la première fois et s'est engagé à suivre une feuille de route ambitieuse en vue d'assurer l'adoption du code le 17 juillet 2018.

La Société pour l'attribution des noms de domaine et des numéros sur Internet (ICANN) joue un rôle majeur dans le soutien aux objectifs de politique publique du système de noms de domaine. La Commission rappelle[38] que l'ICANN devrait intensifier ses efforts pour s'assurer qu'elle respecte pleinement le règlement général sur la protection des données à la suite de la réforme en cours du **service WHOIS** tout en instituant un modèle WHOIS qui préserve les missions essentielles d'intérêt public, allant de la répression à la cybersécurité et à la protection des droits de propriété intellectuelle. Compte tenu de cet objectif, la Commission continue de faciliter les discussions entre l'ICANN et le comité européen de la protection des données[39] (CEPD) en vue d'établir un nouveau modèle qui réponde aux deux objectifs. À cet égard, la Commission invite l'ICANN à assumer la responsabilité de la résolution des questions en suspens. Le 17 mai 2018, le conseil d'administration de l'ICANN a adopté un cahier des charges temporaire pour les données d'enregistrement de domaines de premier niveau générique (gTLD) qui s'applique à partir du 25 mai 2018 dans le but de garantir le respect des dispositions du RGPD. Bien que le cahier des charges temporaire laisse un certain nombre de questions ouvertes, notamment l'accès aux données de WHOIS à des fins légitimes comme les enquêtes des services répressifs, le conseil d'administration de l'ICANN s'est engagé à poursuivre la collaboration avec la communauté afin d'élaborer et de mettre en œuvre une solution globale et permanente[40]. Le 27 mai 2018, le comité européen de la protection des données a approuvé une déclaration reconnaissant les efforts consentis par

---

36 Pour de plus amples détails, voir: http://www.cyber-europe.eu/.

37 COM(2018) 236 final du 26.4.2018.

38 Dans le quatorzième rapport sur les progrès accomplis dans la mise en place d'une union de la sécurité réelle et effective [COM(2018) 211 final du 17.4.2018], la Commission décrit les évolutions en cours concernant le service WHOIS, notamment dans la perspective de l'application du règlement général sur la protection des données à partir du 25 mai 2018.

39 Remplace le groupe de travail «article 29».

40 Le conseil d'administration de l'ICANN a confirmé cette approche dans une lettre adressée à la Commission le 23 mai 2018: https://www.icann.org/resources/pages/correspondence.

l'ICANN pour garantir que le système WHOIS respecte le RGPD, même si les progrès ultérieurs de l'ICANN pour dûment se conformer aux obligations juridiques continueront à faire l'objet d'un suivi[41]. Étant donné que l'absence d'un modèle global pour le service WHOIS peut fortement entraver la capacité des autorités répressives à enquêter sur des infractions, notamment dans le domaine de la cybercriminalité, la Commission veillera également à ce que l'ICANN réalise dans les délais un modèle approprié qui donne accès aux données WHOIS à des fins légitimes.

4. Lutte contre le blanchiment de capitaux et le financement du terrorisme

Les criminels et les terroristes déployant leurs activités dans plusieurs États membres et étant capables de transférer des fonds en l'espace de quelques heures d'un compte bancaire à un autre pour préparer leurs actes ou pour déplacer et blanchir les produits de leurs activités criminelles, la lutte contre le blanchiment de capitaux et contre le financement du terrorisme constitue un aspect important des travaux en vue de la mise en place d'une union de la sécurité effective. Le 14 mai 2018, le Conseil a adopté une directive qui renforce les règles de l'UE afin de prévenir le blanchiment de capitaux et le financement du terrorisme. La **cinquième directive anti-blanchiment** augmentera la transparence en ce qui concerne la propriété des sociétés et des fiducies/trusts pour prévenir le blanchiment de capitaux et le financement du terrorisme à travers des structures opaques. Elle permettra d'améliorer le travail des cellules de renseignement financier qui bénéficieront d'un meilleur accès aux informations au moyen de registres centraux de comptes bancaires. Elle constituera aussi une réponse aux risques de financement du terrorisme liés à l'utilisation anonyme de monnaies virtuelles et d'instruments prépayés. Enfin, cette directive fournira un niveau commun élevé de garanties pour les flux financiers en provenance de pays tiers à haut risque.

Le 30 mai 2018, le Parlement européen et le Conseil sont parvenus à un accord politique sur la proposition législative[42] de directive **visant à lutter contre le blanchiment de capitaux au moyen du droit pénal** qui permettra d'harmoniser les infractions pénales liées au blanchiment de capitaux.

Dans le contexte du plan d'action[43] destiné à renforcer la lutte contre le financement du terrorisme, le Conseil a invité la Commission en février 2016 «à examiner la nécessité d'appliquer des restrictions appropriées aux paiements en espèces dépassant certains seuils». À la suite de cela, la Commission a consulté les États membres de manière informelle, elle a commandé une étude à un contractant externe et elle a mené une consultation publique de mars à mai 2017. Elle a publié un **rapport sur les restrictions concernant les paiements en espèces** parallèlement au présent rapport sur les progrès accomplis dans la mise en place d'une union de la sécurité. Sur la base des résultats obtenus, la Commission a conclu que les restrictions aux paiements en espèces ne freineraient pas de manière significative le financement du terrorisme mais que ces restrictions pourraient être utiles pour lutter contre le blanchiment de capitaux. À ce stade, elle n'entend pas prendre d'autres mesures législatives en la matière.

5. Dimension extérieure

---

41 https://edpb.europa.eu/news/news/2018/european-data-protection-board-endorsed-statement-wp29-icannwhois_fr.

42 COM(2016) 826 final du 21.12.2016.

43 COM (2016) 50 du 2.2.2016.

Les armes légères et de petit calibre (ALPC) et les armes à feu illicites continuent de contribuer à l'instabilité et à la violence à la fois dans l'Union européenne, dans son voisinage immédiat et au-delà. La Commission et la haute représentante proposent donc au Conseil une révision de la stratégie sur les armes légères et de petit calibre de 2005, qui tient compte du nouveau contexte de sécurité, des initiatives prises par l'UE et des évolutions en matière de contrôle des armes conventionnelles depuis 2005, à savoir: l'entrée en vigueur du traité sur le commerce des armes, la conclusion du protocole des Nations unies relatif aux armes à feu, la révision de la législation de l'UE sur les armes à feu, les activités avec les pays voisins à travers le plan d'action de la Commission de 2015[44] et les travaux réalisés dans le contexte du cycle politique de l'UE. La mise à jour de cette stratégie vise à guider l'action européenne, collective et coordonnée afin de prévenir et d'enrayer l'acquisition illicite d'armes à feu et d'armes légères et de petit calibre, ainsi que de leurs munitions par des terroristes, des criminels et d'autres acteurs non autorisés. La stratégie favorise le renforcement des normes internationales et européennes, l'amélioration des contrôles et la traçabilité des armes à feu, des armes légères et de petit calibre ainsi que des munitions durant leur cycle de vie.

Les 23 et 24 avril 2018, les **ministres du G7 chargés de la sécurité** se sont réunis à **Toronto** afin de discuter de la coopération en matière de sécurité au sein du G7, y compris d'une action commune contre les menaces terroristes grandissantes. Les engagements pris par les ministres de la sécurité à Toronto[45] insistent sur la protection des espaces publics, la préparation aux risques CBRN, les efforts déployés pour lutter contre les contenus à caractère terroriste en ligne, renforcer la cybersécurité et lutter contre la traite des êtres humains. Une session conjointe des ministres de la sécurité et des ministres des affaires étrangères a débouché sur l'adoption d'engagements communs sur la gestion des combattants terroristes étrangers et des voyageurs associés[46] et sur la défense de la démocratie et le fait de s'attaquer aux menaces étrangères[47].

Le 14 mai 2018, le Conseil a adopté une décision autorisant l'EUNAVFOR MED Opération Sophia à mettre en œuvre le projet pilote de **«cellule d'information en matière criminelle»** (CIC). La cellule sera installée sur le navire qui accueille les quartiers généraux de la force de l'Opération Sophia et fonctionnera comme une plateforme au sein de l'Opération, où tous les acteurs concernés peuvent collaborer afin de faciliter la réception, la collecte et les échanges réciproques et en temps utile d'informations à des fins d'analyse et de réutilisation opérationnelle entre l'EUNAVFOR MED Opération Sophia, les agences relevant du domaine «Justice et Affaires intérieures» et les autorités répressives des États membres, sur des questions liées au mandat de l'Opération, à savoir le trafic de migrants, la traite des êtres humains, le trafic d'armes et le trafic d'exportations illicites de pétrole, et à la protection des forces de l'Opération.

Le sommet des **dirigeants des Balkans occidentaux** s'est tenu à Sofia le 17 mai 2018. Ce sommet a été l'occasion de confirmer la perspective européenne de la région et de définir une série d'actions concrètes pour renforcer la coopération, y compris, et c'est important, dans les

---

44 COM(2015) 624 final du 2.12.2015.

45 https://g7.gc.ca/fr/presidence-g7/themes/construire-monde-pacifique-sur/reunion-ministerielle-g7/declaration-president-rencontre-ministres-securite/document-dengagement-ministres-securite-g7/.

46 https://g7.gc.ca/fr/presidence-g7/themes/construire-monde-pacifique-sur/reunion-ministerielle-g7/gestion-combattants-terroristes-etrangers-voyageurs-associes/.

47 https://g7.gc.ca/fr/presidence-g7/themes/construire-monde-pacifique-sur/reunion-ministerielle-g7/defendre-democratie-sattaquer-aux-menaces-etrangeres/.

domaines de la sécurité et de l'état de droit, conformément à l'initiative phare concernant la sécurité et la migration de la stratégie pour les Balkans occidentaux[48].

Les 22 et 23 mai 2018, la **réunion ministérielle «Justice et affaires intérieures» entre l'UE et les États-Unis** s'est tenue sous la présidence bulgare du Conseil à Sofia. L'Union et les États-Unis ont abordé les efforts à déployer pour lutter contre le terrorisme, en se concentrant sur les échanges d'informations efficaces, la prévention de la radicalisation, l'utilisation d'internet à des fins terroristes et la vigilance face aux menaces chimiques, biologiques, radiologiques et nucléaires, surtout en ce qui concerne l'évolution des menaces chimiques qui pèsent sur la sûreté de l'aviation et sur les espaces publics.

Le 25 mai 2018, le premier dialogue à haut niveau Union européenne-Nations unies sur la lutte contre le terrorisme a eu lieu à Bruxelles. L'UE et les Nations unies ont discuté des efforts à déployer pour coopérer sur la prévention du terrorisme et la lutte contre celui-ci dans un nombre défini de priorités thématiques et géographiques, en mettant l'accent sur les combattants terroristes étrangers et les victimes du terrorisme.

Le 29 mai 2018, des représentants de l'**UE** et de l'**OTAN** ont tenu un premier **dialogue sur la lutte contre le terrorisme** à Bruxelles dans le cadre de la mise en œuvre de la déclaration commune de 2016 de ces deux institutions. Ils ont abordé les défis que constituent le retour et la relocalisation des combattants terroristes étrangers et les efforts portant sur le renforcement des capacités antiterroristes en Irak, en Afghanistan, en Bosnie-Herzégovine et en Tunisie.

Le 4 juin 2018, le Conseil «Justice et affaires intérieures» a adopté huit décisions autorisant la Commission à ouvrir des négociations en vue d'accords entre l'Union européenne et **l'Algérie, l'Égypte, Israël, la Jordanie, le Liban, le Maroc, la Tunisie et la Turquie, respectivement, sur l'échange de données à caractère personnel entre Europol et les autorités de ces pays** compétentes pour lutter contre les formes graves de criminalité et le terrorisme.

Après l'adoption récente d'un mandat de négociation par le Canada à la fin du mois de mai 2018 en vue d'un **accord révisé sur les données des dossiers passagers (PNR) entre l'UE et le Canada**, la Commission et le Canada ont immédiatement pris des mesures pour lancer les négociations formelles à cette fin; leur ouverture est prévue pour le 20 juin 2018.

VI. CONCLUSION

Le présent rapport illustre les progrès continus accomplis dans la mise en place d'une union de la sécurité réelle et effective, qui soutienne les États membres dans la lutte contre le terrorisme, contre les formes graves de criminalité et contre les menaces liées au cyberespace, et qui contribue à un niveau élevé de sécurité pour les citoyens. La Commission invite les colégislateurs à dégager rapidement un accord sur toutes les propositions législatives actuellement en discussion qui visent à renforcer davantage la sécurité des citoyens, conformément à la déclaration commune sur les priorités législatives de l'UE pour 2018-2019.

[48] COM(2018) 65 final du 6.2.2018. Cette initiative phare comprend: l'intensification des efforts communs déployés dans la lutte contre le terrorisme et la prévention de la radicalisation, le renforcement de la coopération dans la lutte contre la criminalité organisée dans des domaines prioritaires ciblant notamment les armes à feu, les stupéfiants, le trafic de migrants et la traite des êtres humains, et la préparation d'un plan d'action renouvelé en matière de coopération contre le trafic d'armes à feu illicites.

La Commission poursuivra en priorité les travaux en la matière, notamment en vue de la réunion informelle des chefs d'État ou de gouvernement consacrée à la sécurité intérieure qui se tiendra le 20 septembre 2018 à Salzbourg dans le cadre du programme des dirigeants.