COMMISSION
EUROPÉENNE

Bruxelles, le 9.12.2020
COM(2020) 797 final

COMMUNICATION DE LA COMMISSION AU PARLEMENT EUROPÉEN ET AU CONSEIL

Premier rapport sur l'état d'avancement de la stratégie de l'UE sur l'union de la sécurité

I INTRODUCTION

La sécurité constitue pour les citoyens un sujet de préoccupation majeure et la récente vague d'attentats terroristes sur le sol européen a encore souligné la nécessité d'une action de l'UE. Le 24 juillet 2020, la Commission a adopté une **stratégie de l'UE pour l'union de la sécurité pour la période 2020-2025**[1] afin de mettre l'accent sur les domaines prioritaires dans lesquels l'UE peut apporter une valeur ajoutée aux efforts nationaux. Cette stratégie s'appuie sur les avancées déjà réalisées dans le cadre du programme européen en matière de sécurité pour la période 2015-2020[2] et recentre la politique de sécurité de l'UE sur de nouveaux éléments, pour garantir qu'elle tienne compte de l'évolution de la nature de la menace; qu'elle développe une résilience durable à long terme; qu'elle associe les institutions et agences de l'UE, les gouvernements, le secteur privé et les particuliers à une approche englobant l'ensemble de la société; et qu'elle regroupe les nombreux domaines d'action ayant une incidence directe sur la sécurité. Le plein respect des droits fondamentaux est au cœur de ce travail, car la sécurité de l'Union ne peut être assurée que lorsque chaque individu a la certitude que ses droits fondamentaux sont pleinement respectés.

La menace que représentent les réseaux terroristes transnationaux est un douloureux rappel de l'absolue nécessité d'une action coordonnée de l'UE pour assurer efficacement la protection des Européens, en défendant nos valeurs communes et notre mode de vie européen. Cette situation illustre parfaitement l'émergence de menaces transfrontières et transsectorielles de plus en plus complexes pour la sécurité, qui rendent de plus en plus essentielle une coopération plus étroite en matière de sécurité à tous les niveaux. C'est le cas pour la criminalité organisée ou le trafic de stupéfiants – c'est également le cas pour le monde numérique, les cyberattaques et la cybercriminalité ne cessant d'augmenter. Tous ces défis s'appliquent également au-delà de nos frontières, avec une interconnexion claire entre sécurité intérieure et sécurité extérieure. La crise de la COVID-19 a également mis en lumière la sécurité européenne, mettant à l'épreuve la résilience des infrastructures critiques de l'Europe ainsi que des systèmes de préparation aux crises, des chaînes de valeur stratégiques et des systèmes de gestion des crises, ainsi que la résilience de nos sociétés face aux interférences manipulatrices et à la désinformation.

La stratégie pour l'union de la sécurité définit quatre priorités stratégiques d'action au niveau de l'UE: un environnement de sécurité à l'épreuve du temps, faire face à l'évolution des menaces, protéger l'Europe contre le terrorisme et la criminalité organisée, et un solide écosystème européen de la sécurité. La mise en œuvre est cruciale pour la stratégie, et elle constitue le thème central du présent rapport - une mise en œuvre qui requiert l'engagement total des autorités nationales en première ligne en matière de sécurité dans l'UE. Le présent rapport est le premier rapport de mise en œuvre de la stratégie, qui respecte l'engagement pris par la Commission de rendre compte régulièrement des progrès accomplis[3]. Il couvre la période écoulée depuis le 31 octobre 2019, date à laquelle le dernier rapport sur l'état d'avancement de l'union de la sécurité a été publié dans le cadre du mandat précédent de la Commission[4].

---

1 COM(2020) 605.
2 COM(2016) 230.
3 Lors de l'audition du vice-président Schinas devant le Parlement européen, le 3.10.2019.
4 COM(2019) 552.

II UN ENVIRONNEMENT DE SÉCURITÉ À L'ÉPREUVE DU TEMPS

1. *Protection et résilience des infrastructures critiques*

La vie quotidienne des citoyens repose sur des infrastructures physiques et numériques de plus en plus interconnectées et interdépendantes. Ces infrastructures sont vitales pour le fonctionnement de l'économie et de la société. Sans un approvisionnement fiable en énergie, des transports prévisibles, des systèmes de santé complets ou un réseau financier fondé sur le numérique, notre mode de vie actuel ne serait pas possible. La pandémie de COVID-19 a montré encore plus clairement l'importance de **garantir la résilience des secteurs et des opérateurs critiques**. L'UE a reconnu l'intérêt commun de protéger les infrastructures critiques contre les menaces, qu'il s'agisse de catastrophes naturelles ou d'origine humaine, ou d'attentats terroristes. Le tableau actuel des menaces auxquelles sont confrontées les infrastructures critiques est vaste. Il comprend: le terrorisme, les actions hybrides, les cyberattaques, les délits d'initiés; les menaces liées aux technologies nouvelles et émergentes (telles que les drones, la 5G, l'intelligence artificielle); les défis liés au changement climatique; la perturbation des chaînes d'approvisionnement; et l'ingérence électorale. Nos règles actuelles doivent être modernisées et étendues[5]. Elles doivent mettre l'accent non plus sur la protection, mais sur la résilience, en apportant une meilleure cohérence et une plus grande uniformité dans la couverture sectorielle et en mettant l'accent sur les entités critiques fournissant des services essentiels.

Tel sera l'objectif des propositions à venir visant à promouvoir la résilience des **infrastructures physiques et numériques**. L'objectif général est d'améliorer la préparation aux niveaux national et de l'UE en mettant en place des capacités solides de prévention, de détection, de réaction et d'atténuation des menaces, et d'être prêts à agir en cas de crise. La législation existante a permis d'accroître et d'améliorer la gestion des risques dans les secteurs critiques; il convient d'intensifier ce processus. L'un des principaux objectifs de la directive révisée sur les infrastructures critiques sera de promouvoir un niveau commun élevé de résilience dans un nombre suffisant de secteurs clés. De même, la mise à jour de la directive sur la sécurité des réseaux et des systèmes d'information (SRI) visera une plus grande cohérence dans l'identification par les États membres des «opérateurs de services essentiels»[6]. Plus généralement, malgré des progrès considérables, les capacités en matière de cybersécurité dans les États membres restent inégales, de sorte que la révision visera à renforcer la cybersécurité en général[7]. Il en résultera des approches plus nombreuses et plus cohérentes en matière de résilience des infrastructures physiques et numériques.

Alors que les travaux progressent en vue de réaliser ce cadre plus cohérent, des **initiatives sectorielles** complètent ces travaux et ciblent des vulnérabilités spécifiques. Les défis spécifiques de la cybersécurité pour le secteur de l'énergie sont à présent approfondis sur la base de la recommandation de la Commission de 2019[8], en tenant compte des caractéristiques du secteur, telles que les exigences en temps réel, le risque d'effets en cascade et la combinaison des systèmes existants avec les nouvelles technologies. Des travaux sont en cours sur un code de réseau spécifique sur la cybersécurité pour les flux

---

5 Directive 2008/114/CE et directive (UE) 2016/1148.

6 COM(2019) 546. La Commission a également procédé à une consultation publique (du 7 juillet au 2 octobre 2020) et à des visites dans tous les États membres afin de vérifier la conformité de la mise en œuvre de la directive grâce à des réunions avec les opérateurs et les autorités nationales.

7 COM(2019) 546.

8 C(2019) 2400.

transfrontaliers d'électricité, ainsi que sur la protection, la résilience et la cybersécurité des infrastructures énergétiques critiques. Le réseau thématique pour la protection des infrastructures énergétiques critiques a également été relancé, avec une attention et des objectifs renouvelés, et s'est réuni pour la première fois en juin 2020, avec plus de 100 participants en ligne. Ce réseau constitue une plateforme pour encourager la collaboration transfrontière entre les gestionnaires et les propriétaires d'infrastructures critiques dans le secteur de l'énergie.

Afin de fournir un point de départ commun à la collaboration des États membres en matière de **préparation aux risques dans le secteur de l'électricité**, le Réseau européen des gestionnaires de réseaux de transport d'électricité a défini, en septembre 2020, le scénario régional de crise de l'électricité le plus pertinent, comme le prévoit le règlement sur la préparation aux risques[9]. Ces risques comprennent les cyberattaques ainsi que les pandémies et les phénomènes météorologiques extrêmes. Les États membres élaboreront des scénarios nationaux de crise et des plans de préparation aux risques afin de prévenir et d'atténuer les crises de l'électricité (les premiers projets doivent être présentés en avril 2021). Pour contribuer à ce processus, un ensemble de bonnes pratiques a été publié en juin 2020[10], sur la base d'un suivi étroit de l'impact de la COVID-19 sur le secteur de l'énergie par l'intermédiaire des groupes de coordination pour l'électricité, le gaz et le pétrole, ainsi que du groupe des régulateurs européens dans le domaine de la sûreté nucléaire et du groupe des autorités du pétrole et du gaz en mer de l'Union européenne.

Le recours accru et sophistiqué aux processus numériques dans la fourniture de services financiers exige également d'accroître le niveau de cybersécurité dans le **secteur financier**. S'il est reconnu que la sécurité des systèmes TIC fait partie intégrante de la gestion des risques pour les entités financières, cela n'a pas encore été pleinement pris en compte dans le paysage réglementaire des services financiers de l'UE. Le 24 septembre 2020, la Commission a adopté son train de mesures sur la stratégie en matière de finance numérique[11], dont l'objectif est clairement de relever les défis et les risques liés à la transformation numérique, de promouvoir la résilience, la protection des données et une surveillance prudentielle appropriée. Ce paquet comprenait notamment une proposition législative sur la résilience opérationnelle numérique[12], afin de veiller à ce que des garanties soient mises en place pour atténuer les cyberattaques et d'autres risques[13]. Cette initiative contribue à un secteur financier numérique européen fort et dynamique et augmente ainsi la capacité de l'Europe à renforcer son autonomie stratégique ouverte en matière de services financiers et, par extension, sa capacité à réglementer et surveiller le système financier pour protéger la stabilité financière de l'Europe.

Dans les situations d'urgence de grande ampleur, le degré élevé d'interdépendance entre les secteurs et les pays nécessite une action coordonnée pour garantir une réaction rapide et efficace, ainsi qu'une meilleure prévention et une meilleure préparation à des situations similaires à l'avenir. Dans le cadre de la révision de la décision relative au mécanisme de

---

9 JO L 158 du 14.6.2019, p. 1.

10 Sécurité énergétique: bonnes pratiques pour faire face aux risques de pandémie [SWD(2020) 104].

11 https://ec.europa.eu/info/publications/200924-digital-finance-proposals_fr

12 COM(2020) 595.

13 La proposition établit une base de référence cohérente pour les exigences en matière de gestion des risques liés aux TIC, la notification aux autorités de surveillance financière des incidents liés aux TIC, les essais numériques et le partage d'informations. En outre, la proposition soumet les tiers prestataires essentiels de services informatiques à un cadre de surveillance à l'échelle européenne.

protection civile de l'Union[14], la Commission a proposé[15] de définir des **objectifs en matière de résilience face aux catastrophes** et de **planifier la résilience**, en mettant davantage l'accent sur le renforcement de la résilience intersectorielle à long terme face aux catastrophes transfrontières. La nouvelle approche proposée en matière de renforcement de la résilience complète les travaux de gestion des risques de catastrophes au niveau national. Le 26 novembre, le Conseil est parvenu à un accord sur un mandat de négociation visant à renforcer la prévention, la préparation et la réaction aux catastrophes, sur la base de la proposition de la Commission du 2 juin 2020[16].

La pandémie de COVID-19 a démontré l'impact de la crise sanitaire sur la sécurité au niveau de l'UE et au niveau mondial et mis en évidence la nécessité de renforcer la planification de la préparation et de la réaction face aux épidémies et à d'autres menaces transfrontières graves pour la santé. Le train de mesures de la Commission du 11 novembre 2020 intitulé «**Construire une Union européenne de la santé**: renforcer la résilience de l'UE» expose les prochaines étapes pour lutter contre les menaces sanitaires transfrontières. Il prévoit un cadre renforcé de coopération transfrontalière contre toutes les menaces pour la santé et comprend trois propositions législatives: améliorer la législation relative aux menaces transfrontières graves pour la santé et renforcer le Centre européen de prévention et de contrôle des maladies (ECDC) et l'Agence européenne des médicaments (EMA). Ensemble, ces propositions mettront en place un cadre solide présentant un bon rapport coût-efficacité afin de permettre à l'UE et aux États membres d'affronter de futures crises sanitaires sur une base plus sûre.

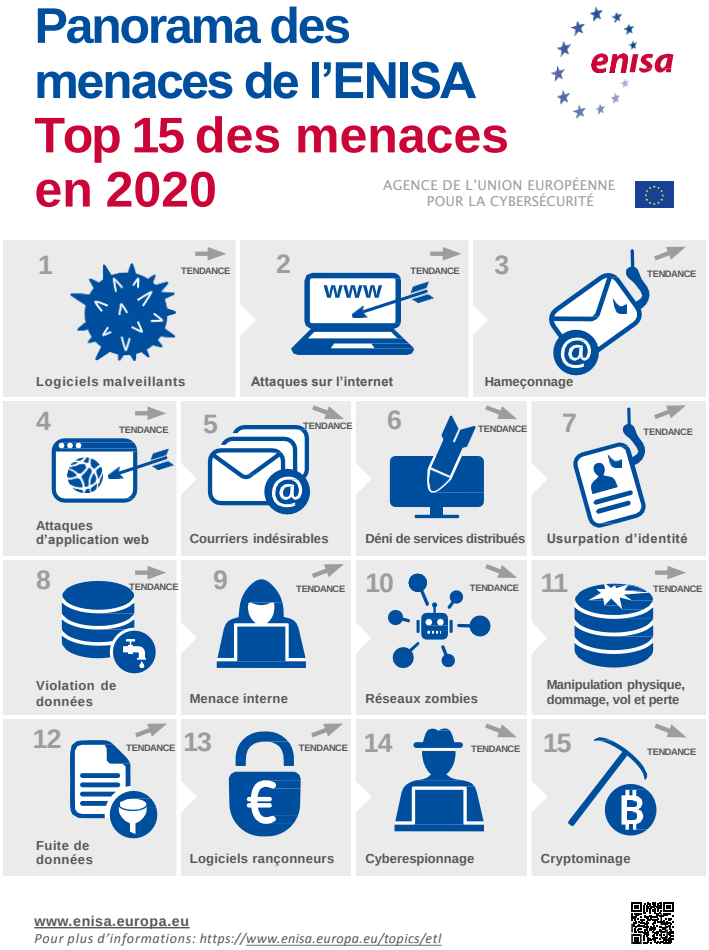
Pour protéger les actifs numériques clés de l'UE et des États membres, il est primordial d'équiper les infrastructures critiques d'un canal de **communication sécurisé**. Cela est soutenu par le développement d'une infrastructure de réseau pour des télécommunications gouvernementales par satellite sécurisées et résilientes dans le cadre du programme spatial de l'UE.

[14] Décision nº 1313/2013/UE du 17 décembre 2013 relative au mécanisme de protection civile de l'Union.
[15] COM(2020) 220.
[16] Proposition de modification de la décision nº 1313/2013/UE relative au mécanisme de protection civile de l'Union - Mandat de négociation avec le Parlement européen.

2. ***Cybersécurité***

Les avantages de la transformation numérique sont évidents, tout comme le fait qu'elle s'accompagne inévitablement d'une augmentation des vulnérabilités potentielles[17]. Les infrastructures critiques sont souvent la cible de cyberattaques de plus en plus sophistiquées[18]. La **cybersécurité** doit donc être la préoccupation non seulement des décideurs politiques, mais aussi de tous ceux qui travaillent ou communiquent en ligne.

Afin de renforcer la confiance dans les produits, processus et services numériques ainsi que leur sécurité, le règlement sur la cybersécurité de juin 2019 a créé un **cadre européen de certification de cybersécurité**. La Commission a demandé à l'Agence de l'Union européenne pour la cybersécurité, l'ENISA, d'élaborer deux schémas de certification de cybersécurité, dont la préparation est en bonne voie. Les autorités nationales de certification de cybersécurité, les entreprises, les consommateurs, les organismes d'accréditation, de normalisation et de certification, ainsi que le comité européen de la protection des données sont également associés à ces travaux.



L'un de ces dispositifs est un système de **services en nuage** destiné à soutenir un marché des services informatiques en nuage sûr et fiable. Il s'agit d'un élément clé de la **stratégie européenne pour les données** adoptée en février 2020[19]. Ce système créerait une base de sécurité commune pour les services en nuage dans tous les secteurs, en s'appuyant sur le plus grand dénominateur commun des normes, systèmes et pratiques existants (européens et internationaux). Il s'agira d'un élément clé du libre flux des données dans l'ensemble de l'UE[20]. Le système encouragera également l'adoption des technologies en nuage en offrant aux utilisateurs, en particulier aux petites et moyennes entreprises et au secteur public, des garanties compréhensibles quant au niveau de sécurité offert lorsqu'ils utilisent l'informatique en nuage.

---

17 ENISA Threat Landscape 2020: Cyber Attacks Becoming More Sophisticated, Targeted, Widespread and Undetected.

18 Depuis le début de la pandémie, les agences de l'UE et les États membres ont détecté une augmentation significative des cyberattaques, y compris à l'encontre du secteur des soins de santé.

19 COM(2020) 66.

20 Règlement (UE) 2018/1807.

Ainsi que cela a été souligné dans la stratégie pour l'union de la sécurité, compte tenu du déploiement en cours des infrastructures liées à la 5G dans l'ensemble de l'UE et de la dépendance potentielle de nombreux services critiques à l'égard des réseaux 5G, les conséquences de perturbations systémiques et généralisées pourraient être particulièrement graves. Un effort commun a donc été réalisé par les États membres pour élaborer et mettre en place des mesures de sécurité adéquates. À la suite de la recommandation de la Commission de mars 2019 sur la **cybersécurité des réseaux 5G**[21], les États membres ont mené à bien leur évaluation nationale des risques qui s'est traduite par un rapport d'évaluation coordonnée des risques au niveau de l'UE[22] recensant les défis en matière de sécurité liés aux réseaux 5G. C'est sur cette base que le groupe de coopération SRI[23] a présenté, le 29 janvier 2020, la **boîte à outils de l'UE prévoyant des mesures destinées à atténuer les risques**[24], définissant les mesures stratégiques et techniques nécessaires. La boîte à outils comprend des mesures visant à renforcer les exigences de sécurité pour les opérateurs de réseaux mobiles (ORM), à garantir la diversité des fournisseurs pour les différents ORM, à évaluer le profil de risque des fournisseurs et à appliquer des restrictions aux fournisseurs considérés comme présentant un risque élevé. La Commission soutiendra la mise en œuvre de la boîte à outils, en faisant pleinement usage des compétences et des moyens dont elle dispose[25], notamment les règles en matière de télécommunications et de cybersécurité; la coordination en matière de normalisation et de certification à l'échelle de l'UE; ainsi que le cadre de l'UE pour les investissements directs étrangers[26].

Le groupe de coopération SRI a publié un rapport sur l'état d'avancement de la mise en œuvre des mesures relevant de la boîte à outils en juillet 2020[27]. Il constatait qu'une grande majorité d'États membres ont déjà adopté ou sont en train de mettre en œuvre les mesures recommandées dans la boîte à outils. Parmi les mesures dont la mise en œuvre était moins avancée figuraient l'atténuation du risque de dépendance à l'égard de fournisseurs à haut risque et l'élaboration de stratégies multifournisseurs tant au niveau des entreprises qu'au niveau national.

Au cours des derniers mois, les institutions et les États membres de l'UE ont réagi à l'augmentation des risques liés à la cybersécurité découlant de la **crise de la COVID-19** en intensifiant l'échange d'informations et en améliorant le niveau de préparation à une crise informatique potentielle. La coopération de l'UE a été renforcée dans les enceintes clés [groupe de coopération SRI et réseau des centres de réponse aux incidents de sécurité informatique (CSIRT)], ainsi que grâce à de nouvelles formes de coordination et à de nouveaux outils de partage d'informations[28]. En septembre 2020, un deuxième exercice de

---

21 COM(2019) 2335.

22 Rapport sur l'évaluation coordonnée au niveau de l'UE des risques liés à la cybersécurité des réseaux 5G.

23 Le groupe de coopération SRI a été créé pour assurer la coopération stratégique et l'échange d'informations entre les États membres de l'UE en matière de cybersécurité.

24 https://ec.europa.eu/digital-single-market/en/news/cybersecurity-5g-networks-eu-toolbox-risk-mitigating-measures.

25 COM(2020) 50.

26 Règlement (UE) 2019/452. Ce règlement contient également des références explicites aux «infrastructures critiques» (ainsi qu'aux «technologies critiques») plus largement en tant que «facteurs susceptibles d'être pris en considération par les États membres ou la Commission» lors de l'évaluation de l'impact potentiel d'un investissement.

27 Rapport sur l'état d'avancement de la mise en œuvre par les États membres de la boîte à outils de l'UE pour la cybersécurité de la 5G.

28 Les institutions et organes de l'UE se sont réunis au sein d'une task force cybersécurité COVID-19 et ont lancé un rapport hebdomadaire sur la connaissance et l'analyse de la situation sectorielle. L'ENISA et Europol ont lancé des campagnes sur la manière de préserver la cybersécurité pendant la pandémie de

simulation Blue OLEx («Blueprint Operational Level Exercise»)[29] a été organisé, dans le cadre duquel le réseau CyCLONe («Cyber Crisis Liaison Organisation Network») des États membres a également été créé, qui poursuivra la mise en œuvre du plan de réaction rapide d'urgence en cas de cyberincidents ou de crises transfrontières de grande ampleur[30].

Dans le cyberespace mondial, les cyberattaques et les menaces informatiques proviennent souvent de pays tiers. Pour relever ces défis de manière efficace, l'UE et les États membres coopèrent en vue de faire progresser la sécurité et la stabilité internationales dans le cyberespace, de promouvoir un comportement responsable des États, d'accroître la résilience mondiale et de sensibiliser aux cybermenaces et aux actes de cybermalveillance, y compris avec les partenaires internationaux[31]. Le 30 avril 2020, le haut représentant a publié une déclaration au nom de l'UE condamnant les actes de malveillance commis dans le cyberespace et exprimant sa solidarité avec les victimes[32].

Le 30 juillet 2020, le Conseil a adopté les **toutes premières sanctions de l'UE à la suite de cyberattaques** à l'encontre de six personnes et de trois entités responsables ou impliquées dans des cyberattaques. Il s'agit notamment de la tentative de cyberattaque contre l'OIAC (Organisation pour l'interdiction des armes chimiques) et de celles connues sous les noms de «WannaCry», «NotPetya» et «Operation Cloud Hopper». Le 22 octobre 2020, le Conseil a appliqué des sanctions à l'encontre de deux autres personnes et d'une entité responsables de la cyberattaque contre le parlement fédéral allemand ou impliquées dans cette attaque. Ces décisions font suite à la mise en garde permanente par l'UE et les États membres rappelant la nécessité d'empêcher, de décourager et de prévenir les actes de cybermalveillance et d'y faire face, notamment en utilisant son régime de sanctions en matière de cyberattaques dans le cadre de sa boîte à outils cyberdiplomatique de 2017[33].

Les négociations entre les colégislateurs sur de nouvelles règles de contrôle des exportations qui limitent la vente de technologies de cybersurveillance à des régimes mondiaux réprimant les droits de l'homme[34] ont également progressé. Une fois adoptées, ces règles conduiront à un commerce plus responsable, plus compétitif et plus transparent

---

COVID-19. La CERT-UE a publié des orientations sur la manière de mettre en place des réseaux privés virtuels (VPN) sécurisés. Au cours de l'été 2019, le groupe de coopération a mis en place un nouveau volet de travail consacré à la cybersécurité dans le domaine de la santé et la Commission et l'ENISA ont lancé un centre européen de partage et d'analyse des informations en matière de santé.

29 https://www.enisa.europa.eu/news/enisa-news/blue-olex-2020-the-european-union-member-states-launch-the-cyber-crisis-liaison-organisation-network-cyclone.

30 C(2017) 6100.

31 L'UE promeut le cadre stratégique pour la prévention des conflits, la stabilité et la coopération dans le cyberespace, notamment en participant aux discussions des Nations unies sur les questions liées au cyberespace. Deux processus importants sont le groupe de travail à composition non limitée sur les progrès de l'informatique et des télécommunications dans le contexte de la sécurité internationale et le groupe d'experts gouvernementaux chargé de favoriser le comportement responsable des États dans le cyberespace. Parmi les domaines abordés figurent notamment l'incidence du droit international, la mise en œuvre de normes volontaires non contraignantes en matière de comportement responsable des États et de mesures visant à instaurer la confiance, ainsi que l'élaboration d'une mise en œuvre par un renforcement ciblé des capacités.

32 https://www.consilium.europa.eu/fr/press/press-releases/2020/04/30/declaration-by-the-high-representative-josep-borrell-on-behalf-of-the-european-union-on-malicious-cyber-activities-exploiting-the-coronavirus-pandemic/.

33 Décisions (PESC) 2020/1127, 2020/1537 et 2020/651 du Conseil dans le cadre du document 9916/17.

34 COM(2016) 616. La proposition de la Commission vise à modifier et à refondre le règlement (CE) nº 428/2009 instituant un régime communautaire de contrôle des exportations, des transferts, du courtage et du transit de biens à double usage.

des biens à double usage[35]. Les modifications proposées, rendues nécessaires par les évolutions technologiques et les risques croissants en matière de sécurité, comprennent de nouveaux critères d'octroi ou de refus des licences d'exportation pour certains biens.

3. Protection des espaces publics

Comme le reconnaît le programme de l'UE en matière de lutte antiterroriste[36], la protection des espaces publics, par le renforcement de la résilience face aux menaces pesant sur la sécurité, demeure un élément essentiel des travaux en vue de la mise en place d'une union de la sécurité réelle et effective. La Commission travaille avec un large éventail d'acteurs publics et privés pour élaborer des orientations et fournir un soutien financier et pratique[37], conformément au **plan d'action de 2017 en faveur de la protection des espaces publics**[38] et au recueil de bonnes pratiques de 2019 en faveur de la protection des espaces publics[39]. Comme indiqué dans le programme de l'UE en matière de lutte antiterroriste, la Commission intensifiera son soutien aux autorités régionales et locales, qui jouent un rôle essentiel dans la protection des espaces publics et la prévention de la radicalisation. Il s'agira notamment d'élaborer un protocole de l'UE sur la sécurité et la résilience urbaines, qui définira les principes et objectifs fondamentaux pour les collectivités locales dans ces domaines.

Étant donné que les attentats terroristes ciblent de plus en plus des **lieux de culte**, un accent particulier est mis sur la coopération entre les pouvoirs publics et les dirigeants religieux et les congrégations confessionnelles, afin d'améliorer le niveau de sensibilisation à la sécurité et de contribuer à la mise en œuvre des bonnes pratiques et de la formation dans les lieux de culte. Des mesures simples peuvent faire la différence entre la vie et la mort. En octobre 2019, une synagogue à Halle a fait l'objet d'un attentat terroriste. Une porte renforcée, un bouton d'alerte et des caméras de sécurité sont autant d'éléments qui ont contribué à sauver des vies.

Afin de continuer à soutenir le renforcement de la sécurité dans les espaces publics, en particulier dans les lieux de culte, la Commission a débloqué en 2020 20 000 000 EUR en faveur de projets menés par les parties prenantes.

La Commission s'emploie également à réagir aux **risques émergents pour les espaces publics**, y compris les **systèmes d'aéronef sans équipage à bord** (UAS). Si les drones offrent d'importantes perspectives économiques et d'emploi, ils représentent également un risque important pour les espaces publics, les infrastructures critiques et d'autres sites sensibles, tels que les prisons. Les règles récentes de l'UE[40] dans ce domaine atténuent ce risque en renforçant la sécurité des opérations liées aux drones. À partir de janvier 2021, les utilisateurs de drones seront également tenus de s'enregistrer auprès des autorités nationales. Ce régime peut être complété par un **cadre réglementaire relatif à l'«U-**

---

35 Il s'agit d'un vaste groupe de biens, de matériaux, de logiciels et de technologies susceptibles d'avoir une utilisation tant civile que militaire.

36 COM(2020) 795.

37 L'appel à propositions «Protect» lancé en 2019 au titre du FSI incluait «Secu4All», l'élaboration d'un cycle de formation complet permettant aux autorités locales d'offrir aux citoyens un environnement urbain sûr, et «DroneWISE» pour renforcer la préparation des premiers intervenants à lutter contre les aéronefs sans pilote hostiles. En 2020, un nouvel appel de 12 000 000 EUR sera consacré à la protection des espaces publics.

38 COM(2017) 612.

39 SWD(2019) 140.

40 Règlement d'exécution (UE) 2019/947 de la Commission.

Space», le système européen de gestion du trafic sans pilote[41], afin de garantir des opérations utilisant des drones plus sûres et mieux sécurisées. Il sera plus difficile pour des individus de faire voler des drones dans des zones à accès réglementé grâce à ces mesures combinées qui permettront en outre d'identifier et de poursuivre les auteurs d'infractions.

La Commission s'emploie également à aider les services répressifs, les exploitants d'infrastructures critiques, les organisateurs d'événements de masse et d'autres parties prenantes à lutter contre l'utilisation non coopérative des drones, par exemple en collaborant avec l'Agence de l'Union européenne pour la sécurité aérienne afin d'élaborer de **bonnes pratiques pour aider les parties prenantes des aéroports** à réagir aux incidents concernant des drones non autorisés, en facilitant une **expérimentation** plus harmonisée **de mesures visant à lutter contre les drones** dans l'ensemble de l'UE et en élaborant un manuel pratique à l'intention des parties prenantes, axé sur le contexte urbain.

Une **école d'automne numérique de l'UE pour la protection des espaces publics**, organisée par le Centre commun de recherche de la Commission en octobre 2020, a réuni plus de 200 urbanistes et exploitants publics et privés d'espaces publics. Les sessions ont porté sur un large éventail de sujets, tels que la protection contre les explosions ou les attaques à la voiture-bélier, l'atténuation des menaces que représentent les drones hostiles en milieu urbain et l'utilisation de technologies de surveillance et de détection.

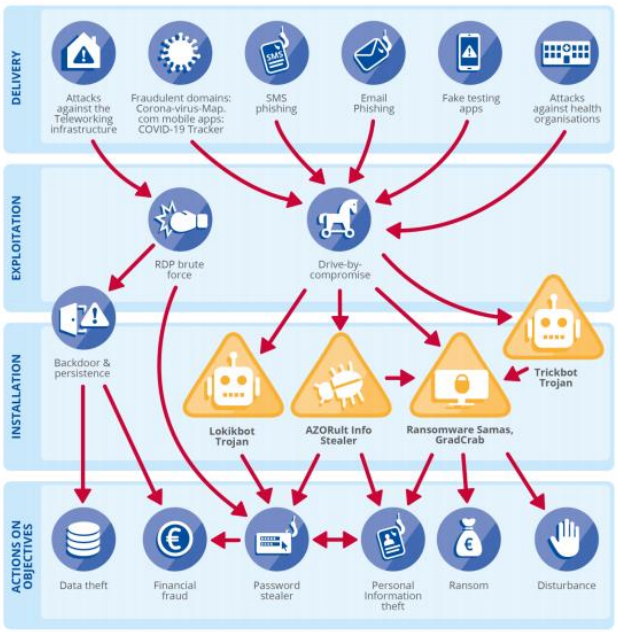
La Commission a également continué de soutenir activement le **partenariat autour de la sécurité dans les espaces publics**, lancé en janvier 2019 dans le cadre du programme urbain pour l'UE, qui a publié son nouveau plan d'action[42] pour relever les enjeux en matière de sécurité urbaine à différents niveaux de gouvernance. Les actions portent notamment sur la création d'un cadre pour un outil d'autoévaluation, des recommandations pour l'élaboration des politiques, la gouvernance et le financement à plusieurs niveaux, l'innovation au moyen de solutions et de technologies intelligentes, incluant le principe de la sécurité dès la conception, la prévention et l'inclusion sociale. Le partenariat va maintenant entrer dans la phase de mise en œuvre.

Le renforcement de la sécurité dans les espaces publics au niveau local a également bénéficié d'un soutien grâce au 4^{e} appel à projets lancé dans le cadre des actions innovatrices urbaines. Trois villes ont été sélectionnées et testent actuellement de nouvelles solutions en matière de sécurité urbaine (le Pirée en Grèce, Tampere en Finlande et Turin en Italie), grâce au financement du Fonds européen de développement régional.

[41] La Commission peut présenter à cet effet un règlement d'exécution qui serait adopté dans le cadre d'une procédure d'examen impliquant le comité de la sécurité aérienne.

[42] Le plan d'action a été adopté et est disponible sur Futurium: https://ec.europa.eu/futurium/en/security-public-spaces/security-public-spaces-partnership-final-action-plan-0.

En termes de réaction, la Commission a également élaboré un cadre européen visant à améliorer la préparation et la réaction face aux catastrophes entraînant un grand nombre de brûlés, en exploitant la capacité européenne globale en matière de soins aux brûlés pour traiter les patients grâce à une coopération au niveau de l'UE. Il peut être fait appel au mécanisme de protection civile de l'Union pour apporter une aide à un grand nombre de patients souffrant de brûlures graves, en donnant accès à des lits pour grands brûlés dans des centres de traitement spécialisés, à des experts en évaluation des brûlures et à des capacités d'évacuation médicale.



III FAIRE FACE À L'ÉVOLUTION DES MENACES

1. Cybercriminalité

Les failles en matière de cybersécurité sont souvent exploitées par les criminels. Cela a été plus clair que jamais au cours de la crise de la COVID-19. On a observé une augmentation de la cybercriminalité «classique» utilisant des logiciels malveillants et des rançongiciels (c'est-à-dire pour voler des données à caractère personnel et des données de paiement ou pour exercer un chantage sur des victimes), ainsi que la prolifération de nouveaux sites web qui incitent les utilisateurs à installer des logiciels malveillants. Des cyberattaques ont été perpétrées contre des infrastructures de soins de santé et de recherche, bloquant des systèmes informatiques qui ne peuvent être débloqués que contre le paiement d'une rançon ou donnant accès à des informations sur la mise au point de vaccins[43]. Une augmentation significative des abus sexuels concernant des enfants et du matériel à caractère pédopornographique a également été observée[44].

Une réponse efficace à la cybercriminalité nécessite un cadre solide pour les enquêtes et les poursuites pénales, et une première étape essentielle est la transposition et la mise en œuvre intégrales de la directive relative aux **attaques contre les systèmes d'information**[45]. La Commission suit les actions de la Bulgarie, de l'Italie, du Portugal et de la Slovénie à la suite de l'ouverture de procédures d'infraction en 2019. Des progrès sont également nécessaires en ce qui concerne la mise en œuvre de la **directive** de 2011 **relative à la lutte contre les abus sexuels concernant des enfants**[46]. Les domaines dans lesquels des efforts restent nécessaires sont notamment la prévention, le droit pénal

[43] Évaluation de la menace que représente la criminalité organisée sur l'internet (IOCTA) 2020, octobre 2020.

[44] Rapport d'Europol: Exploiting isolation: Offenders and victims of online child sexual abuse during the COVID-19 pandemic (Exploiter l'isolement: les prédateurs sexuels ciblent de plus en plus les enfants pendant la pandémie de COVID-19), 19.6.2020

[45] Directive 2013/40/UE.

[46] Directive 2011/93/UE.

matériel, l'assistance, le soutien et les mesures de protection en faveur des enfants victimes. Depuis 2018, la Commission a ouvert des procédures d'infraction à l'encontre de 25 États membres[47].

Le 24 juillet 2020, la Commission a adopté une **stratégie de l'UE en faveur d'une lutte plus efficace contre les abus sexuels commis contre des enfants**[48], qui vise à apporter une réponse efficace de l'UE aux crimes que constituent les abus sexuels commis contre des enfants. Un défi spécifique est également apparu, dans la mesure où, à partir du 21 décembre 2020, certains services de communication en ligne, tels que les services de courrier électronique web ou de messagerie, relèveront du champ d'application de la directive vie privée et communications électroniques et qu'ils sont couverts par les définitions révisées du code des communications électroniques européen. En conséquence, il existe un risque évident que les prestataires de ces services qui entreprennent actuellement certaines activités volontaires importantes aux fins de détecter, de combattre et de signaler les abus sexuels commis contre des enfants en ligne se voient contraints de cesser leurs activités. La Commission a donc fait une proposition de **règlement**[49] autorisant la poursuite de ces activités volontaires dans certaines conditions, en attendant une solution législative à long terme. La Commission travaille actuellement à une proposition en vue d'une solution de ce type, dont l'adoption est prévue en 2021.

Le réseau ECHO (réseau européen des centres de cybersécurité et pôle de compétences en matière d'innovation et d'opérations) a mis en place une **alliance de cyberdéfense COVID-19** en vue d'élaborer des approches innovantes en matière de lutte contre la criminalité liée à la COVID-19. En avril 2020, une plateforme du CEI dédiée à la COVID[50] a été mise en place pour mettre en relation la société civile, les innovateurs, les partenaires et les investisseurs dans toute l'Europe en vue de mettre au point des solutions innovantes.

Afin de garantir une efficacité accrue des poursuites pénales et compte tenu de l'importance des informations et preuves électroniques dans les enquêtes pénales, les autorités répressives et judiciaires devraient obtenir rapidement l'accès à ces informations et éléments de preuve pour accomplir leur travail. Cela a été reconnu par les ministres de l'intérieur de l'UE dans leur déclaration commune du 13 novembre 2020[51]. Europol, Eurojust et le Réseau judiciaire européen ont publié, le 1er décembre 2020, leur deuxième rapport intitulé «SIRIUS EU Digital Evidence Situation Report». Ce rapport souligne l'importance croissante des preuves électroniques dans le cadre des enquêtes pénales[52]. En ce qui concerne les propositions de la Commission relatives à l'**accès transfrontière aux**

---

47 Espagne, Portugal, Italie, Pays-Bas, Suède, Malte, Lituanie, Slovaquie, Bulgarie, Roumanie, Allemagne, Autriche, Belgique, Tchéquie, Estonie, Grèce, Finlande, France, Croatie, Hongrie, Irlande, Luxembourg, Lettonie, Pologne, Slovénie.

48 COM(2020) 607.

49 COM(2020) 568.

50 La Commission, en collaboration avec le Conseil européen de l'innovation et les États membres, a organisé un hackathon + un matchathon EU vsVirus paneuropéen https://covid-eic.easme-web.eu/.

51 Déclaration commune des ministres de l'intérieur de l'UE sur les attentats terroristes perpétrés récemment en Europe, 13 novembre 2020, 12634/20.

52 Selon le rapport, le volume des demandes transfrontières présentées par les autorités de l'UE aux fournisseurs de services en ligne a considérablement augmenté en 2019, la grande majorité d'entre elles ayant été émises par l'Allemagne (37,7 % des demandes), la France (17,9 %) et le Royaume-Uni (16,4 %). Les demandes d'accès aux données électroniques ont doublé en Pologne et presque triplé en Finlande. En outre, les demandes de divulgation d'urgence ont augmenté de près de la moitié en un an.

preuves électroniques[53] d'avril 2018, le Parlement européen n'a pas encore arrêté sa position, de sorte que les négociations entre les colégislateurs doivent encore commencer. Les retards dans l'adoption de ces propositions freinent le travail des autorités répressives et judiciaires et compliquent les efforts en cours visant à établir des règles compatibles pour l'accès transfrontière aux preuves électroniques dans le cadre de négociations internationales[54].

Au niveau international, la Commission participe, au nom de l'Union, aux négociations en cours sur le deuxième protocole additionnel à la **convention de Budapest sur la cybercriminalité** du Conseil de l'Europe. Ce protocole fournirait aux services répressifs compétents des outils renforcés et de grande envergure pour la coopération transfrontière aux fins des enquêtes et des poursuites en matière de cybercriminalité et d'autres formes graves de criminalité, y compris une coopération directe avec les prestataires de services. Étant donné que la plupart de ces modes de coopération améliorés et renforcés s'appuieront sur l'échange de données à caractère personnel, il est essentiel que le futur protocole prévoie des garanties appropriées en matière de protection des données, non seulement du point de vue des droits fondamentaux, mais aussi pour garantir la sécurité juridique, la confiance mutuelle et l'efficacité de la coopération opérationnelle en matière d'application des lois.

Les négociations devraient être conclues en 2021. Parallèlement, à la suite du mandat reçu l'an dernier par le Conseil JAI, la Commission négocie actuellement un **accord entre l'Union européenne et les États-Unis sur l'accès transfrontière aux preuves électroniques**. Cela viendrait compléter les règles internes de l'UE proposées pour la coopération transfrontière directe avec les prestataires de services, en supprimant les conflits de lois et en prévoyant des règles et des garanties communes. Des négociations formelles ont débuté le 25 septembre 2019 et plusieurs cycles de négociation ont déjà eu lieu. Toutefois, le résultat des négociations dépend dans une large mesure des progrès réalisés en ce qui concerne les règles internes sur les preuves électroniques.

Pour ce qui est de la **conservation et de l'utilisation de données à des fins répressives**, l'arrêt Tele2/Watson[55] de 2016 a été suivi par la Commission au moyen de consultations d'experts avec les fournisseurs de services concernés, les autorités policières et judiciaires, la société civile, les autorités chargées de la protection des données, le monde universitaire et les agences de l'UE. Les réflexions ont également été alimentées par une étude sur les pratiques de conservation des données des fournisseurs de services de communications électroniques et les besoins et pratiques des services répressifs en matière d'accès aux données, l'identification des défis technologiques pertinents et une vue d'ensemble des cadres juridiques nationaux[56]. Ces travaux ont mis en évidence la nécessité pour les

---

53 COM(2018) 226 et COM(2018) 225.

54 Par exemple, l'Assemblée générale des Nations unies a adopté le 27 décembre 2019 la résolution 74/247 sur la lutte contre l'utilisation des technologies de l'information et des communications à des fins criminelles, instituant un comité intergouvernemental spécial d'experts à composition non limitée ayant pour mission d'élaborer une convention internationale générale sur la cybercriminalité. L'UE n'est pas favorable à la création d'un nouvel instrument juridique international sur la cybercriminalité, étant donné que la convention de Budapest sur la cybercriminalité fournit déjà un cadre juridique multilatéral complet. En juillet 2020, les États membres des Nations unies sont convenus de reporter les premières étapes: l'UE a contribué au processus sur la base d'une position commune (doc. 7677/2/20).

55 Arrêt du 21 décembre 2016 dans les affaires jointes C-203/15 et C-698/15, Tele2 Sverige AB et Watson e.a.

56 https://data.europa.eu/doi10.2837/26288

services répressifs d'avoir accès aux données pour s'acquitter plus efficacement de leurs tâches.

Le 6 octobre 2020, la Cour de justice a rendu des arrêts[57] concernant la législation nationale de la Belgique, de la France et du Royaume-Uni relative à la conservation et à la transmission de données de communication non relatives au contenu et à l'accès à ces données à des fins répressives et de sécurité nationale. La Commission évaluera les options disponibles pour faire en sorte que les terroristes et autres criminels puissent être identifiés et retrouvés, tout en respectant le droit de l'UE tel qu'interprété par la Cour de justice, compte tenu également des autres affaires pendantes devant la Cour à ce sujet.

Un autre élément important de la lutte contre la cybercriminalité a été le travail visant à garantir la disponibilité et l'exactitude des données d'enregistrement des noms de domaine internet («**données WHOIS**»), conformément aux efforts déployés par l'ICANN (société pour l'attribution des noms de domaines et des numéros sur Internet). Les discussions visent à garantir que les personnes qui souhaitent y accéder légitimement, y compris les opérateurs des services répressifs et de cybersécurité, puissent se voir accorder un accès efficient aux données génériques d'enregistrement de domaine de premier niveau, dans le plein respect des règles applicables en matière de protection des données. Les recommandations finales pour une nouvelle politique en matière de données WHOIS ont été publiées le 10 août 2020 et font actuellement l'objet d'un réexamen, avant qu'une décision ne soit prise par le conseil d'administration de l'ICANN. La Commission examinera les conclusions du réexamen et évaluera dans quelle mesure elles tiennent suffisamment compte de la protection des données et des considérations d'intérêt public liées à la fourniture d'un accès effectif aux services répressifs et aux opérateurs de cybersécurité.

2. Des services répressifs modernes

Tandis que la technologie continue de refaçonner presque tous les secteurs de la société, y compris la sécurité, les services répressifs et les juges doivent pouvoir suivre le rythme. L'intégration de l'intelligence artificielle, des mégadonnées et du calcul à haute performance dans la politique de sécurité, sans pour autant affaiblir la protection effective des droits fondamentaux, est essentielle pour renforcer la sûreté et la sécurité.

La Commission articule ses travaux autour de plusieurs grands axes[58]. Le 25 novembre 2020, la Commission a proposé[59] l'acte sur la gouvernance des données, un cadre destiné à faciliter le partage et la réutilisation des données à caractère personnel et non personnel à des fins d'innovation et de développement. Ce cadre couvre l'industrie et les organismes publics, et ce par l'intermédiaire d'espaces de données sectoriels virtuels ou physiques. Les services répressifs nationaux seraient ainsi en mesure d'accéder aux données hébergées dans d'autres espaces de données pour leurs propres objectifs en matière d'innovation. Dans le même temps, l'accès aux données détenues par les services répressifs et les autorités de sécurité des États ne serait pas autorisé, à moins que le droit de l'Union ou la législation nationale ne le prévoient. Les autorités de sécurité et les services répressifs nationaux peuvent également tirer parti de la mise à disposition, à titre volontaire, des

[57] Arrêts dans les affaires C-623/17, Privacy International, et dans les affaires jointes C-511/18, La Quadrature du Net e.a., C-512/18, French Data Network e.a., et C-520/18, Ordre des barreaux francophones et germanophone e.a.

[58] Y compris la stratégie européenne pour les données (voir ci-dessus).

[59] COM(2020) 767 final.

données à caractère personnel par les personnes concernées pour le bien commun, aux seules fins de la recherche scientifique.

Les travaux de préparation d'une nouvelle initiative sur **l'intelligence artificielle (IA)** sont également en cours, à la suite de la publication du livre blanc sur l'IA[60]. Tout en reconnaissant les possibilités qu'offre la technologie de l'IA pour renforcer la sécurité et le bien-être des citoyens et de la société dans son ensemble, le livre blanc a également mis en évidence un certain nombre de risques, tels que les menaces informatiques, les risques pour la sécurité des personnes ou la perte de connectivité. Lors de la consultation publique, les principales préoccupations exprimées par les participants portaient sur le risque que l'IA porte atteinte aux droits fondamentaux et conduise à des résultats discriminatoires[61]. Dans sa communication intitulée «Renforcer la confiance dans l'intelligence artificielle axée sur le facteur humain»[62], la Commission a souligné la nécessité de faire en sorte que les systèmes d'IA puissent résister à la fois aux attaques directes et aux tentatives plus subtiles de manipulation des données ou des algorithmes, et de prendre des mesures pour atténuer ce risque.

Le **chiffrement** joue un rôle fondamental quand il s'agit d'assurer une cybersécurité solide et la protection effective des droits fondamentaux, tels que le droit au respect de la vie privée, notamment la confidentialité des communications, et la protection des données à caractère personnel, et de garantir la confiance dans les services et produits fondés sur les technologies de chiffrement, comme les solutions fondées sur l'identité numérique. Parallèlement, les auteurs d'infractions peuvent eux aussi s'en servir pour dissimuler leurs faits aux services répressifs et au pouvoir judiciaire, ce qui complique la recherche, la détection et la poursuite desdites infractions. Au sein du Conseil, les États membres ont plaidé en faveur de solutions permettant aux services répressifs et aux autorités judiciaires d'accéder légalement aux preuves numériques, dans le respect absolu de la vie privée, de la protection des données et des garanties d'un procès équitable[63]. La Commission collaborera avec les États membres pour trouver des solutions juridiques, opérationnelles et techniques aux fins de l'accès licite aux informations électroniques dans des environnements chiffrés, qui soient à même de préserver la sécurité des communications.

Parmi les mesures pratiques en cours figure une **plateforme de déchiffrement** au sein d'Europol, qui a pour but d'aider les services répressifs à obtenir un accès licite aux informations chiffrées sur les dispositifs saisis dans le cadre d'enquêtes pénales[64]. Le groupe européen de formation et d'enseignement sur la cybercriminalité a élaboré des modules de formation pilotes qui alimenteront le travail de l'Agence pour la formation des services répressifs (CEPOL). Un réseau de points d'expertise des États membres en matière de chiffrement a été mis en place aux fins de l'échange de bonnes pratiques et d'expertise et du soutien à l'élaboration d'une boîte à outils de nature technique et pratique.

---

[60] COM(2020) 65 final.

[61] Respectivement 90 % et 87 % des personnes interrogées estiment que ces préoccupations sont importantes, voire très importantes.

[62] COM(2019) 168 final.

[63] ST 13084 2020 — Résolution du Conseil sur le chiffrement - La sécurité grâce au chiffrement et malgré le chiffrement

[64] Ce projet, d'un montant de 6 000 000 EUR, bénéficie également du soutien du Centre commun de recherche de la Commission.

Le **système d'échange de preuves numériques (eEDES)** permettra d'échanger de manière sécurisée, rapide et efficace, par-delà les frontières, des décisions d'enquête européennes, des demandes d'assistance mutuelle et des preuves au format numérique. Il devrait être progressivement enrichi et étendu à d'autres instruments de coopération judiciaire en matière pénale et son champ d'application futur sera défini dans une proposition législative sur la numérisation des procédures de coopération judiciaire prévue pour 2021[65].

3. Lutte contre les contenus illicites en ligne

La radicalisation conduisant à l'extrémisme violent et au terrorisme est un phénomène pluridimensionnel et transfrontière, qui a su tirer parti de la rapide croissance de l'internet. L'internet reste un canal utilisé pour radicaliser et recruter les personnes vulnérables. En juillet, l'unité d'Europol chargée du signalement des contenus sur l'internet a retiré 2 000 liens renvoyant vers des contenus à caractère terroriste, dont des manuels et des tutoriels sur la manière de commettre un attentat. Le rôle avéré de l'internet dans la radicalisation et la promotion des crimes commis par les auteurs des attentats en France et en Autriche met également en lumière la nécessité d'instaurer un cadre législatif clair pour prévenir la diffusion de contenus à caractère terroriste en ligne, tout en maintenant des garde-fous efficaces pour la protection des droits fondamentaux. Les négociations entre le Parlement européen et le Conseil sur la proposition de **règlement sur les contenus à caractère terroriste en ligne**[66] se sont intensifiées au cours des dernières semaines. Il est essentiel, aux fins de la gestion de la problématique des contenus à caractère terroriste, notamment des contenus contribuant à la radicalisation, que les négociations se soldent par la mise en place, en particulier, du nouvel instrument constitué par les injonctions de suppression en vue de l'élimination transfrontière des contenus à caractère terroriste dans un délai d'une heure au maximum à compter de la réception de ces injonctions, et que cet instrument soit effectif et opérationnel.

Dans l'intervalle, le **forum de l'UE sur l'internet** continue de jouer un rôle de catalyseur d'actions, en fournissant une plateforme indispensable réunissant les États membres et les entreprises afin de prévenir la diffusion de contenus à caractère terroriste en ligne et de contrer les messages de radicalisation. Le forum œuvre à l'élaboration d'une liste de référence des symboles et groupes interdits dans les États membres, qui pourrait servir de base aux politiques de la plateforme en matière de modération des contenus.

Le forum de l'UE sur l'internet a élargi son champ d'activités afin de couvrir également **l'exploitation sexuelle de mineurs en ligne**. Il offrira un espace commun de partage des bonnes pratiques et de recensement des obstacles rencontrés par les acteurs tant privés que publics, afin d'améliorer la compréhension mutuelle et de trouver des solutions collectivement. Il permet également une coordination politique de haut niveau afin de maximiser l'efficience et l'efficacité de l'action. Un processus d'experts techniques a été créé dans le cadre du forum de l'UE sur l'internet, composé de représentants du monde universitaire, d'entreprises, d'autorités publiques et d'organisations de la société civile, afin de répertorier et d'évaluer à titre préliminaire les solutions techniques possibles pour détecter, dans les communications électroniques chiffrées de bout en bout, les abus sexuels commis sur des enfants et les signaler. Ces solutions techniques ne devraient pas affaiblir

[65] Communication sur la numérisation de la justice au sein de l'Union européenne, COM(2020) 710 final du 2 décembre 2020.

[66] COM(2018) 640 final.

le chiffrement. Cette approche complète d'autres éléments de la lutte contre les abus sexuels concernant des enfants, tant en ligne que hors ligne, comme décrit ci-dessus.

La Commission a également continué de partager l'expertise et l'expérience de l'UE dans le cadre du comité consultatif indépendant du **Forum mondial de l'internet contre le terrorisme**, récemment créé, et en tant que chef de file, conjointement avec Microsoft, du groupe de travail sur la réaction aux crises. La Commission a continué, aux côtés d'Europol, de soutenir les États membres dans la mise en œuvre du **protocole européen de crise**. Le 23 novembre 2020, l'unité de l'UE chargée du signalement des contenus sur l'internet a organisé un deuxième exercice de simulation dans le but d'élaborer des lignes directrices visant à améliorer les réactions opérationnelles et la coordination en temps réel entre les États membres et les fournisseurs de services en ligne.

En juin 2020, la Commission a publié les résultats du dernier exercice de suivi de la mise en œuvre du **code de conduite visant à combattre les discours de haine illégaux en ligne**[67]. Il en est ressorti qu'en moyenne, les entreprises informatiques examinent 90 % des contenus signalés en l'espace de 24 heures et retirent 71 % des contenus considérés comme des discours de haine illégaux. Toutefois, cet exercice a également permis de relever des lacunes en matière de transparence et de retour d'information aux utilisateurs. La mise en œuvre du code de conduite au cours des quatre dernières années a également alimenté les réflexions sur la manière de traiter, dans la future proposition législative relative aux services numériques, la question des contenus illicites en ligne tout en protégeant la liberté d'expression. Dans son discours sur l'état de l'Union de 2020, la présidente von der Leyen a également annoncé que, d'ici la fin de 2021, la Commission proposerait d'étendre la liste des «infractions pénales de l'UE» au titre de l'article 83, paragraphe 1, du TFUE aux crimes de haine et aux discours haineux[68].

4. *Menaces hybrides*

Prenant acte du caractère évolutif des menaces hybrides, le Conseil a créé, en juillet 2019, un **groupe horizontal «Renforcement de la résilience et lutte contre les menaces hybrides»**, lequel vise principalement à soutenir la coordination stratégique et horizontale entre les États membres dans le domaine de la résilience des États et de la société, en améliorant la communication stratégique et en luttant contre la désinformation. Ses travaux ont également consisté, entre autres, à suivre les études sur les risques hybrides[69], ainsi qu'à examiner, de manière spécifique, les menaces hybrides et la désinformation dans les pays partenaires du voisinage. Les activités du groupe horizontal ont été présentées dans un rapport annuel adopté le 14 septembre 2020.

En décembre 2019, le Conseil a adopté des conclusions intitulées «Des efforts complémentaires pour renforcer la résilience et lutter contre les menaces hybrides»[70], dans lesquelles il demande l'élaboration d'une approche globale en matière de sécurité et de lutte contre les menaces hybrides, en travaillant de manière plus stratégique, coordonnée et cohérente dans l'ensemble des domaines d'action pertinents. Deux mesures essentielles de suivi ont été prises en juillet 2020. Premièrement, les services de la Commission et le

---

67 https://ec.europa.eu/info/policies/justice-and-fundamental-rights/combatting-discrimination/racism-and-xenophobia/eu-code-conduct-countering-illegal-hate-speech-online_en

68 Voir également, pour plus de détails, la stratégie en faveur de l'égalité de traitement à l'égard des personnes LGBTIQ pour la période 2020-2025 [COM(2020) 698].

69 Action 1 du cadre commun de 2016 en matière de lutte contre les menaces hybrides, voir JOIN/2016/018.

70 Conclusions 14972/19 du Conseil.

SEAE ont préparé une **cartographie des mesures et documents relatifs à la réaction de l'UE face aux menaces hybrides**[71]. Celle-ci dresse l'inventaire complet des mesures de lutte contre les menaces hybrides au niveau de l'UE et des documents stratégiques correspondants, et sert de point de départ à la création d'une plateforme en ligne à accès restreint, qui fera office de guichet unique regroupant tous les documents stratégiques et législatifs et mesures liés aux menaces hybrides, ainsi que les études pertinentes. Deuxièmement, le dernier **rapport** annuel **sur la lutte contre les menaces hybrides**[72] a permis d'examiner l'état d'avancement du point de vue de l'appréciation de la situation, du renforcement de la résilience, de la préparation et de la réaction aux crises, ainsi que de la coopération internationale et, en particulier, de la coopération entre l'UE et l'OTAN dans le domaine de la lutte contre les menaces hybrides. S'il est pris bonne note, dans le rapport, de certains progrès en matière de coordination au niveau de l'UE, l'ampleur et la diversité sans précédent des menaces hybrides nécessitent aujourd'hui de nouvelles mesures au niveau de l'approche de l'UE afin d'intégrer la dimension extérieure et intérieure dans un flux continu et de soutenir les efforts déployés par les États membres pour lutter contre les menaces hybrides et renforcer leur résilience.

Parallèlement, des travaux sont en cours au sujet de la mise en œuvre des mesures prévues dans la nouvelle stratégie de sécurité afin d'intégrer les aspects hybrides dans l'élaboration des politiques, de mettre en place une plateforme en ligne à accès restreint, d'établir des exigences de base sectorielles de l'UE en matière de résilience et de rationaliser les flux d'informations afin de poursuivre l'amélioration de la connaissance de la situation[73]. Ces travaux s'appuient sur la **cellule de fusion de l'UE contre les menaces hybrides** établie au sein du Centre de situation et du renseignement de l'UE (INTCEN), qui demeure le principal point focal de l'UE pour l'évaluation des menaces hybrides. À ce jour, elle a produit plus de 180 rapports écrits sur les menaces hybrides et informatiques. L'un des projets de la cellule de fusion de l'UE contre les menaces hybrides est l'**analyse des tendances hybrides**[74], qui fournit des données sur les sujets suivants, entre autres: analyse récurrente des activités hybrides des acteurs émergents; activités de renseignement extérieur contre les États membres, les institutions, les partenaires et les intérêts de l'UE; et exploitation de la pandémie de COVID-19 par des acteurs étatiques et non étatiques hybrides.

La **coopération UE-OTAN** (dans le cadre global établi par les déclarations communes de Varsovie et de Bruxelles de 2016 et 2018) s'est encore intensifiée, comme l'a souligné le cinquième rapport sur l'état d'avancement de la mise en œuvre de juin 2020, des interactions étant observées entre les services des deux organisations et des résultats concrets étant constatés dans les domaines des menaces hybrides, de la cyberdéfense et du

---

[71] SWD(2020) 152, document de travail conjoint des services, Cartographie des mesures destinées à renforcer la résilience et à lutter contre les menaces hybrides (Mapping of measures related to enhancing resilience and countering hybrid threats).

[72] SWD(2020) 153, document de travail conjoint des services, Rapport sur la mise en œuvre du cadre commun de 2016 en matière de lutte contre les menaces hybrides (Report on the implementation of the 2016 Joint Framework on countering hybrid threats) et communication conjointe de 2018 intitulée «Accroître la résilience et renforcer la capacité à répondre aux menaces hybrides».

[73] Par exemple, le 26 novembre 2020, le Centre commun de recherche a proposé un nouveau cadre de sensibilisation aux menaces: https://ec.europa.eu/jrc/en/news/jrc-framework-against-hybrid-threats

[74] L'analyse des tendances hybrides est un outil à utiliser parallèlement aux systèmes nationaux pour surveiller l'ampleur et l'intensité des menaces hybrides dans les domaines de la politique/diplomatie, de l'armée, de l'économie, de l'information, du renseignement, du cyberespace, de l'énergie et des infrastructures, ainsi que dans le domaine social.

renforcement des capacités[75]. Il est essentiel de mettre au point une méthodologie unique à travers l'ensemble des secteurs pour les travaux sur les exigences de base sectorielles en matière de résilience face aux menaces hybrides, afin de faire face au risque de fragmentation et de chevauchement des politiques, des outils et des actions. Le Centre européen d'excellence pour la lutte contre les menaces hybrides, situé à Helsinki, a également été associé à cette coopération. La coopération avec l'OTAN a été renforcée dans le contexte de la crise de la COVID-19, notamment en ce qui concerne la désinformation liée à la pandémie et la lutte contre les activités d'information hostiles.

De manière générale, la pandémie de COVID-19 a mis en évidence les risques - à évolution rapide - de **désinformation** et le risque réel pour la vie des citoyens[76]. Le 10 juin 2020, la Commission et le haut représentant ont adopté une **communication conjointe sur la COVID-19 et la désinformation[77]** afin de souligner les risques spécifiques de la désinformation concernant la COVID-19 et le type de mesures à prendre. Cette approche a nécessité la mise en place, par les principales plateformes en ligne, de politiques de lutte contre la menace, un suivi renforcé de l'action des plateformes ainsi qu'une coopération spécifique dans le cadre du système d'alerte rapide géré par le SEAE. La pandémie a incité à redoubler d'efforts pour lutter contre la désinformation, et a provoqué une plus grande sensibilisation du public. Au cours du premier semestre de 2020, **EUvsDisinfo**, une base de données publique sur les cas de désinformation, a ajouté 1 963 nouveaux cas de désinformation pro-Kremlin, dont près d'un tiers étaient liés à l'infodémie concernant la COVID-19. Entre la mi-mars et la fin du mois d'avril 2020, le site internet a enregistré plus de 10 000 visites quotidiennes, et le nombre total de visiteurs a augmenté de 400 % par rapport à la même période en 2019. La réaction de l'UE a comporté des campagnes de communication ciblées[78] et des informations factuelles sur la pandémie.

Les enseignements tirés ont été pris en compte dans l'élaboration du **plan d'action pour la démocratie européenne** adopté le 2 décembre 2020[79]. Celui-ci définit les mesures clés à prendre pour renforcer la résilience du tissu démocratique de l'UE en promouvant des élections libres et régulières, en s'attaquant aux tensions que subissent les médias libres et indépendants et en luttant contre la désinformation. Ce dernier aspect se fondera sur le plan d'action de 2018 contre la désinformation[80], qui servira de base à une action renforcée de l'UE pour lutter contre la désinformation et aux moyens à mettre en œuvre pour associer les principales parties prenantes de la société civile et du secteur privé. Il pourra aussi s'appuyer sur la prochaine étape que constitue le **code de bonnes pratiques contre la désinformation**, après l'évaluation de l'efficacité du code en septembre 2020[81]. Le code a

---

[75] La coopération entre les deux organisations dans le domaine de la cybersécurité et de la cyberdéfense s'est encore intensifiée dans le cadre des travaux sur des concepts et doctrines cohérents, des exercices, des échanges d'informations et des sessions d'information mutuelle.

[76] Figuraient parmi les conséquences concrètes sur le terrain l'incendie volontaire d'infrastructures de télécommunications et la diffusion d'informations trompeuses dans le domaine de la santé, avec des conséquences directes.

[77] JOIN (2020) 8, communication conjointe intitulée «Lutter contre la désinformation concernant la COVID-19 – Démêler le vrai du faux».

[78] Par exemple, la campagne «Réfléchissez avant de partager», lancée pour fournir des conseils sur la manière de limiter la propagation de fausses informations auprès des jeunes et des multiplicateurs d'opinion dans les pays du partenariat oriental de l'UE, a obtenu plus de 500 000 vues sur les plateformes de médias sociaux.

[79] COM(2020) 790 final.

[80] JOIN (2018) 36, communication conjointe intitulée «Plan d'action contre la désinformation».

[81] SWD(2020) 180.

constitué une étape importante et nécessaire en vue de la création d'un écosystème de plateformes en ligne plus transparent et plus responsable, mais il serait plus efficace si ses définitions étaient uniformisées, si sa mise en œuvre était plus cohérente et s'il était associé à davantage d'actions dans des domaines spécifiques tels que le microciblage. Un autre outil essentiel désormais à la disposition de l'UE est l'**Observatoire européen des médias numériques**, opérationnel depuis juin 2020. Il réunit les principales parties prenantes travaillant dans le domaine de la désinformation, y compris les vérificateurs de faits et les chercheurs universitaires.

IV PROTÉGER LES EUROPÉENS CONTRE LE TERRORISME ET LA CRIMINALITÉ ORGANISÉE

1. *Terrorisme et radicalisation*

Les attentats perpétrés récemment ont montré une fois de plus que la menace terroriste dans l'UE reste élevée. L'assassinat d'un enseignant à Conflans-Sainte-Honorine le 16 octobre 2020 a été suivi du meurtre de trois personnes dans l'église de Notre-Dame de Nice le 29 octobre. Le 2 novembre, un attentat terroriste à Vienne a fait quatre morts et 23 blessés. Le 13 novembre, le Conseil a adopté une déclaration commune des ministres de l'intérieur de l'UE sur les récents attentats terroristes perpétrés en France et en Autriche[82]. Ces récentes attaques d'inspiration djihadiste viennent s'ajouter à la menace croissante que représentent l'extrémisme de droite violent et d'autres formes de terrorisme.

Afin de continuer de soutenir les États membres dans leurs efforts de lutte contre le terrorisme et la radicalisation, la Commission adopte aujourd'hui un **programme de lutte contre le terrorisme pour l'UE**[83]. Ce programme, qui s'appuie sur les politiques et instruments existants, renforcera le cadre de l'UE afin de continuer d'améliorer l'anticipation des menaces et des risques, la prévention de la radicalisation et de l'extrémisme violent, la protection des personnes et des infrastructures, y compris par la sécurité des frontières extérieures, et un suivi efficace post-attentats. Il expose aussi la voie à suivre afin de mieux faire appliquer la loi et d'améliorer la coopération judiciaire, ainsi que l'utilisation des technologies et le partage d'informations pertinentes dans l'ensemble de l'UE, y compris pour les acteurs qui effectuent des contrôles aux frontières extérieures. Il est essentiel de mettre en œuvre la législation et de veiller à ce qu'elle soit effectivement appliquée.

La prévention est l'un des éléments clés de la lutte contre le terrorisme. Les efforts déployés par l'UE dans le domaine de la **prévention de la radicalisation** s'appuient sur la solide expérience acquise à ce jour en matière de soutien aux intervenants de première ligne et aux décideurs. Le 24 novembre, la Commission a adopté un nouveau **plan d'action en faveur de l'intégration et de l'inclusion**[84]. Il importe, dans le cadre de la lutte contre la radicalisation, de redoubler d'efforts pour rapprocher les communautés. Une société plus solidaire et plus inclusive peut contribuer à prévenir la propagation d'idéologies extrémistes susceptibles de conduire au terrorisme et à l'extrémisme violent. Le soutien au **réseau de sensibilisation à la radicalisation** comprend, depuis

[82] Déclaration commune des ministres de l'intérieur de l'UE sur les récents attentats terroristes perpétrés en France et en Autriche, 13 novembre 2020, 12634/20.

[83] COM(2020) 795 final.

[84] COM(2020) 758 final.

janvier 2020, un nouveau contrat de 30 000 000 euros pour les quatre prochaines années dans le but de venir en aide aux acteurs de terrain, ainsi que d'apporter un soutien supplémentaire aux responsables politiques et aux chercheurs. Ces instruments, ainsi que d'autres, tels que le **forum de l'UE sur l'internet**, permettront à la Commission d'aborder les actions prioritaires mises en évidence dans les orientations stratégiques sur une approche coordonnée de l'UE en matière de prévention de la radicalisation pour 2021, élaborées conjointement avec les États membres. Ils sont complétés par des actions entreprises dans le cadre du programme de lutte contre le terrorisme visant à lutter contre les idéologies extrémistes en ligne, à intensifier les efforts dans les prisons et dans les domaines de la réhabilitation et de la réintégration, y compris pour les combattants terroristes étrangers, et à renforcer le soutien aux acteurs locaux et la résilience des communautés.

La **directive relative à la lutte contre le terrorisme**[85], adoptée en mars 2017, est le principal instrument de justice pénale au niveau de l'UE pour lutter contre le terrorisme. Elle fixe des normes minimales pour la définition des infractions terroristes et des infractions liées au terrorisme, ainsi que pour les sanctions, tout en conférant aux victimes du terrorisme des droits en matière de protection, de soutien et d'assistance. Le 30 septembre 2020, la Commission a adopté un rapport[86] évaluant les mesures prises par les États membres pour se conformer à la directive. Dans ce rapport, elle a conclu que bien que la transposition de la directive en droit national ait contribué à renforcer l'approche des États membres en matière de justice pénale à l'égard du terrorisme et les droits accordés aux victimes du terrorisme, des lacunes subsistent. Par exemple, tous les États membres n'érigent pas en infraction pénale, dans leur droit national, toutes les infractions énumérées dans la directive en tant qu'infractions terroristes, et ne tiennent pas non plus compte, dans leur droit national, des dispositions visant à ériger en infraction pénale les voyages à des fins terroristes et à lutter contre le financement du terrorisme, ni des dispositions en matière de soutien aux victimes. Un rapport d'évaluation de la directive sera adopté dans le courant de l'année 2021.

L'UE s'emploie sans relâche à aider les États membres à priver les terroristes des moyens de passer à l'acte et à les soutenir dans la mise en œuvre des règles. Le règlement sur la commercialisation et l'utilisation de **précurseurs d'explosifs**, adopté en juin 2019,[87] commencera à s'appliquer à partir du 1er février 2021. Afin d'aider les autorités nationales et le secteur privé à mettre en œuvre le règlement, la Commission a publié en juin 2020 un ensemble de lignes directrices[88]. En outre, la Commission a mis en place, en juin 2020[89], un programme de suivi des réalisations, des résultats et de l'incidence du règlement.

En novembre 2019, la Commission a invité les États membres à évaluer la mise en œuvre du plan d'action de 2017 visant à améliorer la préparation aux risques en matière de sécurité **chimique, biologique, radiologique et nucléaire (CBRN)**[90]. La conclusion générale était qu'une majorité d'actions avaient été mises en œuvre. Au début de l'année 2020, la Commission a établi, en coopération avec des experts nationaux, une liste de

[85] Directive (UE) 2017/541.
[86] COM(2020) 619 final.
[87] Règlement (UE) 2019/1148.
[88] Communication de la Commission- Lignes directrices concernant la mise en œuvre du règlement (UE) 2019/1148 relatif à la commercialisation et à l'utilisation de précurseurs d'explosifs, JO C 210 du 24.6.2020, p. 1.
[89] SDW(2020) 114 final.
[90] COM(2017) 610 final.

substances chimiques à haut risque suscitant des inquiétudes. C'est sur cette base que le dialogue a été engagé avec les fabricants d'équipements en vue d'améliorer les capacités de détection. Récemment, la Commission a lancé une étude sur la possibilité de restreindre l'accès à certaines de ces substances chimiques. Des travaux sont également en cours dans le cadre du mécanisme de protection civile de l'Union, et le renforcement des capacités de réaction dans le domaine CBRN fait actuellement l'objet de discussions avec les États membres dans les domaines de la décontamination, de la détection, de la surveillance et du suivi, ainsi que de la constitution de stocks.

Le 12 octobre 2020, le Conseil a décidé de prolonger d'un an le régime de sanctions contre la prolifération et l'utilisation d'armes chimiques[91], permettant ainsi à l'UE d'imposer des mesures restrictives aux personnes et entités impliquées dans le développement et l'utilisation d'armes chimiques. Le 14 octobre 2020, le Conseil a adopté des mesures restrictives à l'encontre de six personnes et d'une entité impliquées dans la tentative d'assassinat d'Alexei Navalny, empoisonné par un agent neurotoxique du groupe «Novitchok» le 20 août 2020 en Russie[92].

Les **informations financières** jouent également un rôle fondamental dans l'identification des réseaux terroristes, étant donné que les terroristes ont besoin de financements pour se déplacer, se former et s'équiper, et les **efforts de lutte contre le financement du terrorisme** sont primordiaux dans le cadre des enquêtes antiterroristes. Il convient notamment d'exploiter pleinement les outils et les renseignements existants, de mettre correctement en œuvre les normes convenues au niveau international et de relever les défis, sans cesse changeants, que représentent les technologies émergentes et les plateformes de médias sociaux[93] (voir ci-dessous).

Le réseau de **transport** a été et reste une cible du terrorisme. Les efforts de l'UE comprennent une approche fondée sur l'évaluation des risques afin de protéger le secteur de l'aviation[94]. Les zones de conflit présentent un risque considérable pour l'aviation civile, et l'atténuation des risques requiert de partager les informations et les évaluations des risques[95]. Le système de l'UE en matière d'alerte, d'information et d'**évaluation des risques émanant des zones de conflit** a été érigé au rang de bonne pratique, et des normes internationales en matière de partage d'informations ont été intégrées dans la législation de l'UE[96]. Sur la base de l'expérience acquise dans le domaine de l'aviation civile, la Commission a élargi à d'autres modes de transport l'approche fondée sur l'évaluation des risques. La mise en œuvre du **plan d'action de l'UE en matière de sûreté ferroviaire**[97] est bien avancée et bénéficie de l'expertise de la plateforme de l'UE des passagers ferroviaires, un groupe d'experts ad hoc instauré par la Commission. Dans le domaine

[91] Décision (PESC) 2020/1466 du Conseil du 12 octobre 2020 modifiant la décision (PESC) 2018/1544.

[92] Décision (PESC) 2020/1482 du Conseil du 14 octobre 2020 et règlement d'exécution (UE) 2020/1480 du Conseil.

[93] Ainsi que l'UE l'a indiqué en novembre 2019 lors de la conférence ministérielle «*No money for terror*» sur le financement de la lutte contre le terrorisme, qui s'est tenue en Australie.

[94] Le processus intégré d'évaluation des risques liés à la sûreté aérienne de l'UE soutient le processus décisionnel dans le domaine de la sûreté du fret aérien, des normes de sûreté aérienne et des risques pour l'aviation civile qui émanent des zones de conflit.

[95] La destruction tragique du vol 752 d'Ukraine International Airlines le 8 janvier 2020 a démontré une fois encore l'importance du partage d'informations et de l'évaluation des risques pour la sûreté de l'aviation civile.

[96] https://eur-lex.europa.eu/legal-content/FR/TXT/PDF/?uri=CELEX:32019R1583

[97] COM(2018) 470 final.

maritime, l'approche fondée sur l'évaluation des risques est bien connue et appliquée, et la Commission collabore avec les États membres et les parties prenantes pour renforcer la sécurité des passagers. Cet aspect est intégré dans la **stratégie de sûreté maritime de l'UE** et dans son **plan d'action**, révisé en 2018, qui comprend également une dimension en matière de sûreté et de défense. Ce point est présenté dans le dernier rapport de mise en œuvre, adopté et publié le 23 octobre 2020[98].

Europol apporte son aide aux États membres dans les enquêtes liées au terrorisme par l'intermédiaire du **Centre européen de lutte contre le terrorisme (ECTC)**. Les demandes de soutien opérationnel adressées par les États membres à l'ECTC ont continué d'augmenter, et l'ECTC est désormais associé à presque toutes les enquêtes majeures en matière de lutte contre le terrorisme. En 2019, Europol a soutenu au total 632 opérations différentes dans le domaine de la lutte contre le terrorisme. Les enquêteurs des États membres ont également fait part d'une satisfaction croissante à l'égard de ce travail, affichant un niveau de satisfaction de 9,1/10 en 2019, contre 8/10 en 2018. Au total, l'ECTC a coordonné 18 journées d'action en 2019[99].

Eurojust a également apporté son aide dans le cadre de 116 enquêtes sur le terrorisme en 2019 et 2020. Les travaux en cours déboucheront sur une proposition législative relative à l'échange d'informations numériques sur les affaires de terrorisme transfrontières en vue de développer le registre antiterroriste lancé en 2019[100], ainsi que sur l'extension des travaux portant sur les groupes extrémistes de droite et de gauche.

Le 30 juillet 2020, le Conseil a procédé au dernier renouvellement en date de la liste de l'UE des personnes, groupes et entités faisant l'objet des mesures restrictives dans le cadre de la lutte contre le terrorisme. Cette liste renouvelée comprend 14 personnes et 21 entités. Le même jour, le Conseil a imposé des mesures restrictives à l'encontre d'une personne dans le cadre du régime de sanctions en matière de terrorisme à l'encontre de l'EIIL (Daech) et d'Al-Qaida. À l'heure actuelle, cinq personnes sont inscrites de manière isolée sur la liste au titre de ce régime, lequel a été renouvelé pour une durée d'un an le 19 octobre 2020[101].

Un élément important de la politique de lutte contre le terrorisme concerne les menaces que représentent les **combattants terroristes étrangers (CTE)** actuellement stationnés en Syrie et en Iraq. Tout en tenant pleinement compte de ce que la responsabilité première dans ces domaines incombe aux États membres, l'UE aide ceux-ci, par son soutien et la coopération mise en place, à relever des défis communs: poursuites à l'encontre des auteurs d'infractions terroristes, prévention de l'entrée non détectée dans l'espace Schengen et réintégration et réhabilitation des combattants terroristes étrangers de retour dans leur pays d'origine. Par exemple, la Commission travaille en étroite collaboration avec les États membres et les principaux pays partenaires pour veiller à ce que les éléments de preuve recueillis sur le théâtre des opérations soient partagés et utilisés efficacement à des fins d'identification, de détection aux frontières de l'UE et de poursuites. Le

[98] Rapport des services de la Commission, du Service européen pour l'action extérieure et de l'Agence européenne de défense sur la mise en œuvre du plan d'action révisé pour la stratégie de sûreté maritime de l'UE, SWD(2020) 252.

[99] Rapport annuel d'activités consolidé 2019, Europol, 9 juin 2020.

[100] Le registre antiterroriste est géré par Eurojust, 24 heures sur 24, et apporte un soutien proactif aux autorités judiciaires nationales. Ces informations centralisées devraient aider les procureurs à se coordonner plus activement et à identifier les suspects ou les réseaux faisant l'objet d'une enquête dans des affaires données susceptibles d'avoir des incidences transfrontières.

[101] Décisions (PESC) 2020/1132, 2020/1126 et 2020/1516 du Conseil.

mémorandum de 2020 sur les preuves recueillies sur le théâtre des opérations[102] publié par Eurojust montre que, si les difficultés rencontrées pour obtenir ces données et s'assurer qu'elles remplissent les critères d'admissibilité des preuves sont nombreuses, ces preuves peuvent aider à traduire en justice les terroristes présumés.

La Commission facilite également le dialogue avec les États membres et les acteurs humanitaires afin de fournir une vue d'ensemble complète et factuelle de la situation dans les camps du nord-est de la Syrie où se trouvent des membres de la famille de CTE européens. Une attention particulière est accordée à la situation des enfants se trouvant dans les camps syriens. La Commission aide également les États membres à partager leurs expériences sur les mesures et mécanismes nationaux visant à mieux gérer **la réhabilitation et la réintégration** des CTE de retour dans leur pays d'origine, ainsi que des enfants. Le réseau de sensibilisation à la radicalisation organise également des visites d'étude et fournit des conseils sur mesure afin de mieux gérer les difficultés associées aux combattants étrangers de retour dans leur pays d'origine qui ont fait l'objet d'une condamnation, en particulier après leur sortie de prison, ainsi que sur le rôle des familles et des communautés locales dans les efforts de réintégration.

Les **partenariats et la coopération avec les pays tiers** et les pays partenaires du voisinage de l'UE dans le domaine de la lutte contre le terrorisme sont également essentiels pour améliorer la sécurité au sein de l'UE, et pour mieux relier les dimensions intérieure et extérieure de la politique de sécurité de l'UE. Le Conseil a appelé à poursuivre le renforcement de l'engagement extérieur de l'UE en matière de lutte contre le terrorisme[103], en mettant l'accent sur les Balkans occidentaux, l'Afrique du Nord et le Moyen-Orient, la région du Sahel, la Corne de l'Afrique et l'Asie. À cet effet, les instruments de l'action extérieure sont pleinement utilisés, notamment les dialogues de haut niveau sur la lutte contre le terrorisme et le réseau de 17 **experts en matière de lutte contre le terrorisme/de sécurité**[104] déployés dans les délégations de l'UE, qui ont continué d'apporter leur soutien, de faciliter la coopération et de promouvoir le renforcement des capacités. Une réflexion sur la possibilité de renforcer et d'étendre ce réseau est actuellement menée.

Le plan d'action conjoint de 2018 relatif à la lutte contre le terrorisme dans les **Balkans occidentaux** et les accords bilatéraux qui l'accompagnent, signés en 2019 avec chaque partenaire[105], mettent l'accent sur une région revêtant une importance capitale pour les objectifs de sécurité communs et pour la protection des personnes vivant dans l'UE. Lors du forum ministériel UE-Balkans occidentaux sur la justice et les affaires intérieures du 22 octobre 2020, l'UE et les partenaires des Balkans occidentaux ont réaffirmé leur volonté de mettre en œuvre les objectifs du plan d'action conjoint au-delà de 2020[106]. La coopération avec les Balkans occidentaux comprend la gestion des retours en cours des combattants

[102] https://www.eurojust.europa.eu/eurojust-memorandum-battlefield-evidence-0

[103] Conclusions du Conseil (8868/20) sur l'action extérieure de l'UE concernant la prévention du terrorisme et de l'extrémisme violent et la lutte contre ces phénomènes (16 juin 2020).

[104] Algérie, Bosnie-Herzégovine (pour les Balkans occidentaux), Tchad (pour le Sahel), Éthiopie (en liaison avec l'Union africaine), Indonésie (pour l'Asie du Sud-Est et en liaison avec l'ASEAN/FRA), Iraq, Jordanie, Kenya (pour la Corne de l'Afrique), Kirghizstan (pour l'Asie centrale), Liban, Libye, Maroc, Nigeria, Pakistan, Arabie saoudite, Tunisie et Turquie.

[105] Serbie, Macédoine du Nord, Bosnie-Herzégovine, Kosovo*, Albanie et Monténégro.

[106] Communiqué de presse conjoint: https://www.consilium.europa.eu/en/press/press-releases/2020/10/23/joint-press-statement-eu-western-balkans-ministerial-forum-on-justice-and-home-affairs/pdf

terroristes étrangers et des membres de leur famille, ainsi qu'une intégration plus poussée dans les activités de lutte contre la radicalisation. L'UE maintient également un dialogue régulier en matière de lutte contre le terrorisme avec **le Moyen-Orient, l'Afrique du Nord et l'Asie centrale**[107]. Les travaux menés avec l'**Asie centrale** se sont concentrés sur la lutte contre les menaces chimiques, biologiques, radiologiques et nucléaires. Le comité mixte de coopération **UE-Conseil de coopération du Golfe** s'est réuni le 25 juin 2020 et a abordé des questions telles que la lutte contre la radicalisation, le financement du terrorisme et le blanchiment de capitaux, ainsi que la cybersécurité et la coopération avec Europol. L'UE a travaillé avec l'OTAN au tout premier audit sur les menaces chimiques, biologiques, radiologiques et nucléaires dans l'un des pays du Golfe à la fin de 2019. Dans l'ensemble, à la fin de l'année 2019, quelque 465 000 000 EUR avaient été consacrés à des projets en cours dans le domaine de la lutte contre le terrorisme et de la prévention de l'extrémisme violent en dehors de l'UE, soit un montant en hausse de 15 % par rapport à l'année précédente.

L'UE a également continué d'approfondir sa coopération avec les **Nations unies** en matière de lutte contre le terrorisme[108], notamment avec le Bureau de lutte contre le terrorisme des Nations unies et la Direction exécutive du Comité contre le terrorisme (DECT) des Nations unies, y compris au moyen de dialogues annuels de haut niveau et, plus récemment, d'une participation active à la semaine virtuelle de lutte contre le terrorisme organisée par les Nations unies pendant l'été 2020. La Commission a également suivi de près les délibérations relatives à la révision de la définition des infractions terroristes figurant dans la convention du **Conseil de l'Europe** pour la prévention du terrorisme, encourageant un alignement étroit sur les définitions du droit de l'Union. Le climat de coopération fructueuse dans le domaine de la lutte contre le terrorisme et des matières chimiques, biologiques, radiologiques et nucléaires s'est maintenu entre l'**OTAN** et l'UE, ces dernières échangeant des informations sur le renforcement des capacités afin d'éviter les doubles emplois et d'assurer la complémentarité.

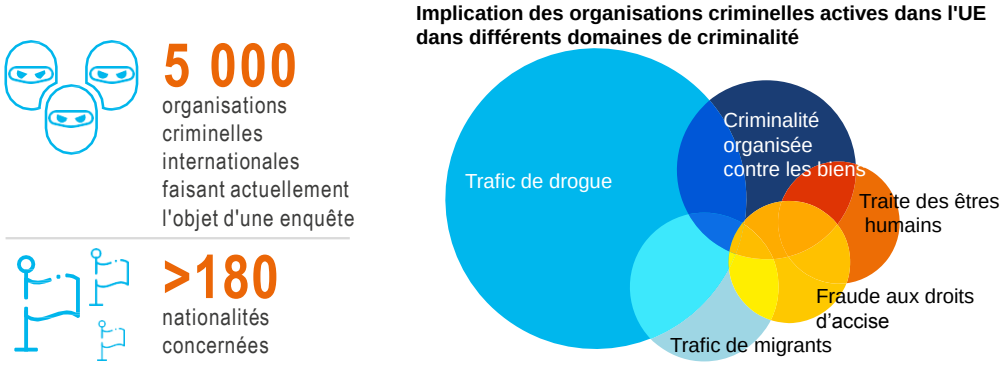
2. Lutte contre la criminalité organisée

Phénomène en expansion, la criminalité organisée devient de plus en plus transfrontière et se déplace vers la sphère en ligne.

---

[107] La lutte contre le terrorisme a par exemple été mise en avant dans la nouvelle stratégie de l'UE pour l'Asie centrale.
*Cette désignation est sans préjudice des positions sur le statut et est conforme à la résolution 1244 (1999) du Conseil de sécurité des Nations unies ainsi qu'à l'avis de la CIJ sur la déclaration d'indépendance du Kosovo.

[108] En 2019, l'UE et les Nations unies ont signé un cadre de coopération dans le domaine de la lutte contre le terrorisme https://eeas.europa.eu/sites/eeas/files/2019042019_un-eu_framework_on_counter-terrorism.pdf



Europol, évaluation de la menace que représente la grande criminalité organisée (SOCTA, 2017)

Dans le cadre de son action, la Commission s'emploie notamment à lutter contre la drogue, les armes à feu illégales, la criminalité financière, l'importation illégale de biens culturels, la traite des êtres humains ou la criminalité environnementale, en soutenant les autorités répressives et judiciaires des États membres et des partenaires du voisinage. La coopération avec les pays tiers, en particulier les pays du voisinage tels que les Balkans occidentaux, et avec les organisations internationales, notamment l'Office des Nations unies contre la drogue et le crime[109], a également joué un rôle fondamental[110].

En 2019, le **centre d'Europol sur la grande criminalité organisée** a reçu et traité près de 55 000 contributions opérationnelles, ce qui représente une hausse de 12 % par rapport à 2018. En ce qui concerne le nombre d'opérations bénéficiant d'un soutien, le centre a apporté son aide à divers pays dans 726 dossiers[111]. Il est également primordial que le cadre législatif de l'UE en matière de criminalité organisée[112], qui vise à harmoniser les législations des États membres pour ce qui est de l'incrimination des infractions liées à la participation à une organisation criminelle et prévoit des sanctions pour lesdites infractions, soit pleinement transposé dans tous les États membres. La Commission a lancé une étude visant à analyser les moyens de renforcer cette législation. De nouvelles mesures visant à intensifier la lutte contre la criminalité organisée dans l'UE seront élaborées dans le cadre du programme de l'UE destiné à lutter contre la criminalité organisée, qui doit être adopté au cours du premier trimestre de 2021.

Le gel et la confiscation des produits du crime comptent parmi les moyens les plus efficaces de lutter contre la criminalité organisée. Le nouveau **Centre européen sur la criminalité financière et économique** (EFECC), créé en juin 2020 au sein d'Europol, renforcera le soutien opérationnel apporté aux États membres et aux organes de l'UE dans le domaine de la criminalité financière et économique et encouragera le recours systématique aux enquêtes financières. Apportant son soutien aux efforts de l'UE visant à améliorer l'efficacité de l'identification, du gel et de la confiscation des avoirs d'origine criminelle, le Conseil a, en juin 2020, adopté des conclusions sur le renforcement des

[109] Un dialogue de haut niveau entre l'UE et l'ONUDC a eu lieu le 8 décembre 2020.
[110] À la fin de l'année 2019, quelque 830 000 000 EUR avaient été consacrés à des actions en cours dans le domaine de la criminalité organisée en dehors de l'UE.
[111] Rapport annuel d'activités consolidé 2019, Europol, juin 2020.
[112] Décision-cadre 2008/841/JAI.

enquêtes financières en vue de lutter contre la grande criminalité organisée[113]. En 2021, la Commission réexaminera la législation relative au gel et à la confiscation des produits du crime[114] et aux bureaux de recouvrement des avoirs[115].

La lutte contre la criminalité organisée a besoin de garde-fous pour faire en sorte que le travail des services répressifs puisse se dérouler de manière efficace dans le respect de limites essentielles, telles que la protection des données à caractère personnel. La directive de 2016 en matière de protection des données dans le domaine répressif, relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel en rapport avec des infractions pénales[116], protège le droit fondamental à la protection des données chaque fois que des données à caractère personnel sont utilisées par les autorités répressives en matière pénale à des fins de répression. Elle garantit la protection des données à caractère personnel des victimes, des témoins et des personnes soupçonnées d'infractions pénales et facilite la coopération transfrontière dans la lutte contre la criminalité et le terrorisme. Le délai de transposition de la directive relative à la protection des données dans le domaine répressif a expiré le 6 mai 2018. À ce jour, la plupart des États membres ont adopté des dispositions législatives transposant la directive. Toutefois, des procédures d'infraction sont toujours en cours[117]. La Commission évalue en ce moment la conformité avec la directive des mesures législatives de transposition adoptées par les États membres.

Lutte contre les drogues illicites

En juillet 2020, la Commission a adopté un nouveau **programme et plan d'action antidrogue de l'UE (2021-2025)**[118], dans le prolongement des stratégies antidrogue actuelles de l'UE[119]. Y sont définis le cadre politique et les priorités d'action pour les cinq prochaines années. Le programme mettra principalement l'accent sur les points suivants: 1) mesures de sécurité renforcées contre le trafic illicite de drogue, depuis les organisations criminelles jusqu'à la gestion des frontières extérieures, en passant par la distribution et la production illicites; 2) amélioration de la prévention, y compris la sensibilisation aux effets nocifs des drogues, notamment lien entre la consommation de drogue et les actes violents et d'autres formes de criminalité; et 3) lutte contre les dommages connexes de la drogue grâce à l'accès au traitement, à la réduction des risques et des dommages et à une approche équilibrée de la lutte contre la drogue dans les prisons. Le 30 novembre 2020, la Commission a également adopté une évaluation de la politique de l'UE en matière de précurseurs de drogues, dont la conclusion est que des mesures supplémentaires sont

[113] Conclusions 8927/20 du Conseil.

[114] Directive 2014/42/UE.

[115] Décision 2007/845/JAI du Conseil.

[116] Directive (UE) 2016/680 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les autorités compétentes à des fins de prévention et de détection des infractions pénales, d'enquêtes et de poursuites en la matière ou d'exécution de sanctions pénales, et à la libre circulation de ces données.

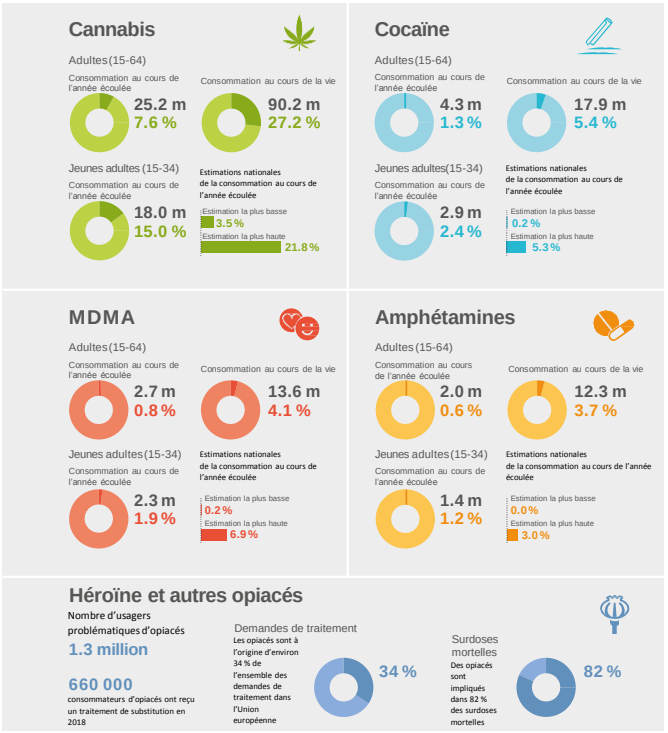
[117] Trois États membres (Allemagne, Slovénie et Espagne) n'ont toujours pas notifié l'intégralité des mesures de transposition malgré les procédures d'infraction ouvertes à leur encontre. Pour l'un d'entre eux, la Commission a saisi la Cour de justice de l'Union européenne d'un recours pour non-transposition de la directive et, en mai 2020, a adressé des avis motivés complémentaires aux deux autres États membres pour transposition incomplète de la directive.

[118] COM(2020) 606 final.

[119] Stratégie antidrogue de l'UE (2013-2020) et plan d'action antidrogue de l'UE (2017-2020).

nécessaires pour empêcher les groupes criminels organisés dans l'UE d'accéder aux substances chimiques dont ils ont besoin pour produire des drogues de synthèse illicites[120].

L'UE a également financé des projets concrets visant à renforcer la lutte contre la drogue, tels que le Forum de la société civile sur la drogue. Le rapport européen sur les drogues de 2020 établi par l'Observatoire européen des drogues et des toxicomanies, publié le 22 septembre 2020[121], montre les toutes dernières tendances en ce qui concerne la consommation de drogue et le marché de la drogue dans l'UE, en Turquie et en Norvège. On observe une résurgence de la cocaïne, dont les saisies ont atteint un niveau record de 181 tonnes, un quasi-doublement des saisies d'héroïne, soit 9,7 tonnes, et une grande disponibilité des drogues d'une grande pureté dans l'UE. Ledit rapport analyse également l'apparition de nouveaux opioïdes synthétiques, suscitant des préoccupations sanitaires particulières, et s'attaque aux défis posés par la pandémie de COVID-19.



Les travaux visant à lutter contre la drogue se poursuivent à plusieurs niveaux. Le **train de mesures législatives relatif aux nouvelles substances psychoactives** (NSP) a été adopté à l'automne 2017[122] et est entré pleinement en vigueur en novembre 2018. Cinq États membres font toujours l'objet d'une procédure d'infraction[123]. Le premier acte délégué visant à inclure une nouvelle substance psychoactive (isotonitazène) dans la définition du terme «drogue» vient d'être adopté[124].

Sur la **scène internationale**, l'UE a joué un rôle actif au sein de la Commission des stupéfiants des Nations unies[125], notamment pour mettre à jour l'inscription de nouvelles substances psychoactives[126] ainsi que pour la réinscription du cannabis et des substances apparentées[127]. Deux nouveaux dialogues sur la drogue avec la Chine et l'Iran ont été approuvés par le Conseil[128], et l'Observatoire

[120] COM(2020) 768 final du 30 novembre 2020.
[121] Rapport européen sur les drogues de 2020: tendances et évolutions, EMCDDA, 22 septembre 2020.
[122] Règlement (UE) 2017/2101 et directive (UE) 2017/2103,
[123] Autriche, Finlande, Irlande, Portugal et Slovénie.
[124] C(2020) 5897; JO L 379 du 13.11.2020, p. 55.
[125] Un organe directeur de l'Office des Nations unies contre la drogue et le crime (ONUDC).
[126] COM(2019) 631 final.
[127] COM(2019) 624 final et COM(2020) 659 final.
[128] Le sommet UE-Chine qui s'est tenu les 16 et 17 juillet 2018 à Pékin a débouché sur un accord visant à lancer un dialogue annuel UE-Chine sur les drogues. Les modalités du futur dialogue ont été confirmées par le Coreper le 30 octobre 2019. Le Conseil a approuvé le lancement d'un nouveau dialogue UE-Iran sur les drogues le 5 mars 2020.

européen des drogues et des toxicomanies a progressé dans la définition d'arrangements de travail avec les pays tiers[129].

Lutte contre la criminalité financière

De nouvelles mesures législatives ont été adoptées pour renforcer la lutte contre la criminalité financière et le blanchiment de capitaux. La directive facilitant l'utilisation d'informations financières et d'une autre nature aux fins de la prévention ou de la détection de certaines infractions pénales, ou des enquêtes ou des poursuites en la matière a été adoptée en 2019. Elle accorde aux services répressifs et aux bureaux de recouvrement des avoirs l'accès aux registres nationaux centralisés des comptes bancaires aux fins de la lutte contre les formes graves de criminalité. La directive vise également à améliorer la coopération entre les services répressifs et les cellules de renseignement financier (CRF) et à faciliter l'échange d'informations entre ces cellules. En juin 2020, la Commission a publié un rapport intitulé «Recouvrement et confiscation d'avoirs: garantir que le crime ne paie pas»[130], lequel a permis de mettre en évidence la possibilité d'harmoniser davantage les régimes de recouvrement des avoirs[131] afin de moderniser la législation de l'UE relative au recouvrement des avoirs et de renforcer les capacités des autorités nationales dans la lutte contre la criminalité organisée. Une analyse plus approfondie du recouvrement des avoirs a été lancée dans le cadre d'une étude externe. Le règlement concernant la reconnaissance mutuelle des décisions de gel et des décisions de confiscation[132], qui entrera en vigueur le 19 décembre 2020, renforcera considérablement la coopération entre les États membres.

En mai 2020, la Commission a adopté **un plan d'action pour une politique globale de l'Union en matière de prévention du blanchiment de capitaux et du financement du terrorisme**[133] afin de renforcer le cadre de l'UE. Le 5 novembre, le Conseil a adopté des conclusions concernant la lutte contre le blanchiment de capitaux et le financement du terrorisme[134], demandant notamment à la Commission d'œuvrer à l'adoption d'un corpus de règles unique, à la mise en place d'une surveillance indépendante et à la coordination des cellules de renseignement financier. Conformément aux conclusions du Conseil sur le renforcement des enquêtes financières[135], la Commission évalue également la nécessité de l'interconnexion des registres centralisés des comptes bancaires, ce qui accélérerait considérablement l'accès des cellules de renseignement financier et des autorités répressives aux informations relatives aux comptes bancaires. Parallèlement, les efforts se poursuivent pour veiller à ce que les normes les plus récentes de l'UE soient effectivement mises en œuvre par les États membres. Les règles prévues par la 5e directive sur la lutte contre le blanchiment de capitaux visent à garantir un niveau accru de transparence pour ce qui est de la structure de propriété des sociétés. Le délai de transposition a expiré le 1er janvier 2020 et la Commission a engagé des procédures d'infraction à l'encontre de

[129] Avis de la Commission concernant le projet d'arrangement de travail avec le Kosovo adopté le 14 avril 2020, et avis de la Commission concernant le projet d'arrangement de travail avec la Serbie adopté le 16 décembre 2019.
[130] COM(2020) 217 final.
[131] Y compris l'évaluation de la directive 2014/42/UE et de la décision 2007/845/JAI du Conseil.
[132] Règlement (UE) 2018/1805.
[133] C(2020) 2800 final.
[134] Conclusions 12608/20 du Conseil.
[135] Conclusions 8927/20 du Conseil.

16 États membres[136]. Une autre mesure importante est le nouveau règlement relatif au contrôle des mouvements d'argent liquide[137] adopté en octobre 2018 et applicable à partir du 3 juin 2021. Il améliorera le système existant de contrôles de l'argent liquide entrant dans l'UE ou sortant de l'UE, et des dispositions d'application sont en cours d'élaboration.

Sur le plan extérieur, les efforts se poursuivent pour aider les pays partenaires à lutter contre le blanchiment de capitaux et le financement du terrorisme. Dans ce contexte, le SEAE et les délégations de l'UE jouent un rôle clé pour ce qui est d'encourager et de soutenir le dialogue politique avec les pays tiers et les organisations internationales telles que le Groupe d'action financière (GAFI).

Pour compléter ces travaux, la Commission a lancé un mécanisme mondial visant à aider les pays partenaires en dehors de l'UE à mettre en place des cadres efficaces de lutte contre le blanchiment de capitaux et le financement du terrorisme, conformément aux normes internationales. Cette action, dotée d'une enveloppe de 20 000 000 EUR, vise également à encourager la coopération entre les acteurs financiers et judiciaires aux niveaux national, régional et international.

Lutte contre la corruption

La corruption constitue une forme de criminalité, ainsi qu'un élément clé favorisant la criminalité organisée. La prévention de la corruption et la lutte contre ce phénomène donneront lieu à une évaluation et à un suivi réguliers du cadre juridique des États membres au titre du nouveau **mécanisme de protection de l'état de droit[138]**. Le premier rapport à l'échelle de l'UE sur l'état de droit a été adopté le 30 septembre 2020[139]. Il en est ressorti que, même si de nombreux États membres appliquent des normes sévères en matière d'état de droit, d'importants défis restent à relever. Le rapport présente une évaluation annuelle factuelle et objective pour chaque État membre, dans le but d'améliorer la connaissance et la compréhension de l'évolution de la situation dans les différents États membres, afin d'être en mesure d'identifier les risques, d'élaborer des solutions possibles et de cibler le soutien à un stade précoce. Le **Parquet européen** s'attaquera aux infractions portant atteinte au budget de l'UE, et ce dans les 22 États membres de l'Union qui y participent à ce stade. Il sera compétent pour mener des enquêtes, engager des poursuites et faire juger des infractions portant atteinte au budget de l'UE, telles que la fraude, la corruption ou la fraude transfrontière grave à la TVA. Le Parquet européen devrait être opérationnel au premier trimestre de 2021[140].

La Commission évalue en ce moment la transposition en droit national des règles établies dans la **directive relative à la lutte contre la fraude portant atteinte aux intérêts financiers de l'Union au moyen du droit pénal**[141] et a engagé des procédures d'infraction

[136] Autriche, Belgique, Chypre, Espagne, Estonie, Grèce, Hongrie, Irlande, Luxembourg, Pays-Bas, Pologne, Portugal, Roumanie, Slovaquie, Slovénie, Tchéquie, ainsi que le Royaume-Uni.

[137] Règlement (UE) 2018/1672.

[138] Le mécanisme européen de protection de l'état de droit prévoit un processus de dialogue sur l'état de droit entre la Commission et les États membres, ainsi qu'avec le Conseil et le Parlement européen, et les parlements nationaux, la société civile et d'autres parties prenantes. Les rapports sur l'état de droit sont au cœur de ce nouveau processus.

[139] COM(2020) 580 final.

[140] La décision d'exécution du Conseil portant nomination des procureurs européens est entrée en vigueur le 29 juillet 2020. Le collège des procureurs européens s'est réuni pour la première fois le 28 septembre 2020. Le Parquet européen conclura bientôt des arrangements de travail avec Europol, Eurojust et l'OLAF.

[141] Directive (UE) 2017/1371.

à l'encontre des États membres qui ont omis de notifier l'ensemble des mesures qu'ils ont prises aux fins de sa transposition[142]. En 2021, la Commission adoptera un rapport qui évaluera la mesure dans laquelle les États membres ont pris les dispositions nécessaires pour se conformer à la directive.

Lutte contre le trafic de biens culturels

Le principal objectif du **règlement concernant l'introduction et l'importation de biens culturels[143]**, adopté en juin 2019, est de mettre un terme aux importations, dans l'Union, de biens culturels exportés illicitement depuis leur pays d'origine. Afin de garantir sa bonne mise en œuvre, la Commission prépare actuellement l'adoption de dispositions d'application, notamment en ce qui concerne un système électronique centralisé pour l'importation de biens culturels, qui permettra le stockage et l'échange d'informations entre les États membres, ainsi que les formalités nécessaires relatives aux importations[144]. La règle de l'interdiction générale entrera en vigueur d'ici la fin de 2020, dotant les autorités douanières des États membres des moyens légaux pour contrôler les envois susceptibles de contenir des biens culturels exportés illicitement à partir de leur pays d'origine et prendre des mesures, le cas échéant.

Lutte contre le trafic d'armes à feu illégales

Le 24 juillet 2020, la Commission a publié **un nouveau plan d'action de l'UE en matière de lutte contre le trafic d'armes à feu pour la période 2020-2025[145]**. Une conférence ministérielle à haut niveau, qui avait rassemblé les ministères des affaires étrangères et des affaires intérieures de l'UE et des Balkans occidentaux le 31 janvier 2020, avait souligné la nécessité de prendre davantage de mesures pour lutter contre le trafic d'armes à feu illégales. Le plan comprend des actions spécifiques visant à améliorer le contrôle légal des armes à feu, la connaissance de la menace liée aux armes à feu, la coopération en matière répressive et la coopération internationale, une attention particulière étant accordée à l'Europe du Sud-Est. La Commission a pris des mesures pour faire en sorte que la directive relative au contrôle de l'acquisition et de la détention d'armes, adoptée en mai 2017[146], soit transposée intégralement par les États membres. Toutefois, dix États membres doivent encore notifier la transposition complète de la directive[147] et une grande majorité d'États membres n'ont pas transposé les dispositions d'exécution qui ont suivi. Par conséquent, la Commission a ouvert des procédures d'infraction[148]. La Commission procède également à

[142] Des procédures d'infraction sont actuellement en cours contre l'Autriche, l'Irlande et la Roumanie.

[143] Règlement (UE) 2019/880.

[144] Le système ICG doit être mis en place pour le 28 juin 2025 au plus tard. La Commission a adopté un premier rapport sur l'état d'avancement de la mise en œuvre du système ICG. [COM(2020) 342].

[145] COM(2020) 608: ce nouveau plan d'action intègre l'initiative franco-allemande pour les Balkans occidentaux intitulée «Feuille de route pour un règlement durable du problème de la détention illicite, de l'utilisation abusive et du trafic des ALPC et de leurs munitions d'ici à 2024».

[146] Directive (UE) 2017/853. Deux directives d'exécution du 16 janvier 2019 établissant des spécifications techniques relatives au marquage et aux armes de signalisation et d'alarme sont également à signaler.

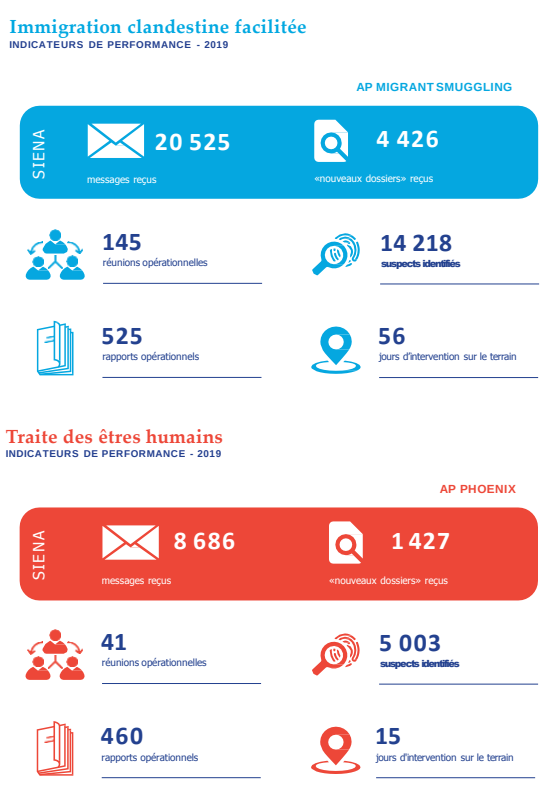
[147] Il s'agit de la Tchéquie, du Danemark, de l'Espagne, de Chypre, du Luxembourg, de la Hongrie, de la Pologne, de la Slovénie, de la Slovaquie et de la Suède.

[148] On dénombre 25 procédures d'infraction en cours concernant cette directive (contre l'Autriche, la Belgique, la Bulgarie, Chypre, la Tchéquie, le Danemark, l'Allemagne, l'Estonie, la Grèce, l'Espagne, la Finlande, la France, la Hongrie, l'Irlande, la Lituanie, le Luxembourg, la Lettonie, Malte, les Pays-Bas, la Pologne, le Portugal, la Roumanie, la Suède, la Slovénie et la Slovaquie, ainsi que le Royaume-Uni) et 34 concernant les directives d'exécution (la directive 2019/68 – contre l'Autriche, la Belgique, la Bulgarie, Chypre, la Tchéquie, l'Allemagne, la Grèce, l'Espagne, la Finlande, la Croatie, la Hongrie, l'Irlande, l'Italie, le Luxembourg, la Pologne, la Roumanie, la Suède, la Slovénie, ainsi que le Royaume-Uni; et la

une évaluation détaillée des mesures de transposition notifiées et fera rapport sur la mise en œuvre de la directive au cours du premier semestre de 2021. Elle a aussi commencé à étudier la possibilité de moderniser le cadre juridique relatif à l'importation, à l'exportation et au transit d'armes à feu[149].

Lutte contre la traite des êtres humains

La stratégie pour l'union de la sécurité a souligné la nécessité de définir une nouvelle approche stratégique en vue d'éradiquer la traite des êtres humains dans le cadre du programme de lutte contre la criminalité organisée. En outre, conformément à l'article 20 de la directive relative à la lutte contre la traite des êtres humains[150], la Commission a publié en octobre 2020 son troisième rapport sur les progrès réalisés dans la lutte contre la traite des êtres humains[151]. Ce rapport fait état d'avancées pour ce qui est de la coopération transnationale, des actions opérationnelles transfrontières répressives et judiciaires, de la mise en place de mécanismes nationaux et transnationaux d'orientation pour les victimes et du développement de la base de connaissances sur la traite des êtres humains. Les États membres recourent de plus en plus aux agences de l'UE pour échanger des informations, mener des actions conjointes et constituer des équipes communes d'enquête pour lutter contre la traite des êtres humains, tant à l'intérieur qu'à l'extérieur de l'UE[152]. La coopération opérationnelle a produit des résultats tangibles, notamment dans le cadre de la plateforme pluridisciplinaire européenne contre les menaces criminelles: en 2019, ces actions se sont traduites par 825 arrestations et par l'identification de 8 824 suspects et de 1 307 victimes potentielles, dont 69 enfants. Elles ont aussi conduit à l'identification ou au démantèlement de 94 groupes criminels organisés et au gel de 1 500 000 EUR d'avoirs sous forme de comptes bancaires, d'entreprises et de domaines internet. À l'occasion de la Journée européenne de lutte contre la traite des êtres humains,



directive 2019/69 – contre la Bulgarie, Chypre, la Tchéquie, la Grèce, l'Espagne, la Finlande, la Croatie, la Hongrie, l'Irlande, l'Italie, le Luxembourg, les Pays-Bas, la Pologne, la Roumanie, la Suède et la Slovénie, ainsi que le Royaume-Uni).

149 Régi par le règlement (UE) nº 258/2012.

150 JO L 101 du 15.4.2011, p. 1.

151 COM(2020) 661 final, complété par une étude relative à la collecte de données sur la traite des êtres humains dans l'UE (2017-2018).

152 Par exemple, l'Autorité européenne du travail a coopéré avec Europol pour lutter contre la traite des êtres humains dans l'UE pour toutes les formes d'exploitation, notamment l'exploitation sexuelle et par le travail, ainsi que toutes les formes de traite des enfants. La coopération s'inscrit également dans le cadre du protocole sur le travail forcé (P29) de l'Organisation internationale du travail. Ce protocole est une norme fondamentale du travail qui définit le travail forcé comme une infraction et traite de la prévention, de la protection des victimes, de l'indemnisation et de la coopération internationale concernant les formes actuelles de travail forcé, y compris en lien avec la traite des êtres humains.

le 18 octobre 2020, la Commission a publié une étude sur le coût de la traite des êtres humains et une autre sur les mécanismes nationaux et transnationaux d'orientation[153].

Trafic de migrants

Le centre européen chargé de lutter contre le trafic de migrants a fait état d'une augmentation constante des activités de **trafic de migrants**, principalement dans les Balkans occidentaux et les pays voisins, ainsi que, dans le cadre des mouvements secondaires, dans toute l'UE. En 2019, Europol a contribué à l'identification de 14 218 personnes soupçonnées de trafic de migrants[154]. En mai 2020, Eurojust a lancé le groupe de réflexion des procureurs sur le trafic de migrants, qui constitue une plateforme importante pour établir des relations régulières entre les principaux acteurs judiciaires au niveau national dans les États membres de l'UE et soutenir leur action opérationnelle commune[155].

Lutte contre la criminalité environnementale

La criminalité environnementale désigne les actes qui enfreignent la législation en matière d'environnement et entraînent ou peuvent entraîner un préjudice ou un risque significatif pour l'environnement et la santé humaine[156]. Parmi les domaines les plus importants de la **criminalité environnementale** figurent l'émission ou le rejet illégal de substances dans l'atmosphère, les eaux ou le sol, le commerce illégal d'espèces de faune ou de flore sauvages, le commerce illégal de substances appauvrissant la couche d'ozone et le transfert ou le déversement illégal de déchets. La récente évaluation de la directive relative à la protection de l'environnement par le droit pénal[157] a montré que les progrès accomplis dans l'élaboration d'un cadre européen ne se sont pas accompagnés d'effets significatifs sur le terrain, notamment en ce qui concerne l'amélioration de la coopération transfrontière et l'harmonisation des sanctions dans les différents États membres. En particulier, ils n'ont pas donné lieu à davantage de condamnations ni à l'imposition de sanctions plus dissuasives dans les États membres. Il a donc été décidé de réviser la directive avant la fin 2021.

Les 29 et 30 octobre 2019, Eurojust a organisé, avec le Réseau européen des procureurs pour l'environnement (REPE), une conférence sur la collaboration et la coopération internationales en matière de lutte contre la criminalité environnementale, afin de sensibiliser à cette question et de promouvoir la coopération transfrontière entre les procureurs et les autres praticiens au sein et en dehors de l'UE dans le domaine de la criminalité environnementale.

Le plan d'action contre le trafic d'espèces sauvages adopté en 2016 est en cours d'évaluation. L'une des actions spécifiques menées à cet égard est un projet qui court jusqu'en janvier 2021 et qui cible le trafic d'espèces sauvages dans et via l'UE au moyen de l'internet et des services de livraison de colis, dans le but de perturber et de démanteler les réseaux de cybercriminalité liée aux espèces sauvages[158].

---

[153] Études sur le coût économique, social et humain de la traite des êtres humains et sur le réexamen du fonctionnement des mécanismes nationaux et transnationaux d'orientation des États membres, disponibles à l'adresse suivante: https://ec.europa.eu/anti-trafficking.

[154] Centre européen chargé de lutter contre le trafic de migrants, quatrième rapport annuel, 15.5.2020.

[155] http://www.eurojust.europa.eu/press/PressReleases/Pages/2020/2020-05-29.aspx.

[156] Directive 2008/99/CE relative à la protection de l'environnement par le droit pénal.

[157] SDW(2020) 259 final.

[158] https://wwf.be/fr/wildlife-cybercrime/.

V. UN SOLIDE ÉCOSYSTÈME EUROPÉEN DE LA SÉCURITÉ

La mise en place d'une union de la sécurité réelle et effective doit être un combat commun à toutes les composantes de la société. Les gouvernements, les services répressifs, le secteur privé, le secteur de l'éducation et les citoyens eux-mêmes doivent s'y investir et être équipés et bien connectés pour renforcer la préparation et la résilience pour tous, en particulier les plus vulnérables, les victimes ainsi que les témoins.

1. Coopération et échange d'informations

L'une des contributions les plus importantes que l'UE peut apporter en matière de protection des citoyens consiste à aider les responsables de la sécurité à collaborer de manière efficace. La coopération et le partage d'informations sont des outils puissants pour lutter contre la criminalité et le terrorisme, s'attaquer aux menaces telles que celles pesant sur la cybersécurité et rendre la justice. Un certain nombre d'outils ont été mis en place pour soutenir l'échange d'informations entre les services répressifs et les autorités judiciaires.

La Commission adopte aujourd'hui un mandat révisé pour **Europol**[159] afin d'apporter un certain nombre d'améliorations ciblées à ses activités. Ce mandat révisé permettra à Europol de mieux faire face au caractère évolutif des infractions commises au moyen de l'internet ainsi qu'à la criminalité financière. Il renforcera la coopération avec le secteur privé et alignera les dispositions relatives à la protection des données sur les règles existantes de l'UE.

Europol, et d'autres agences de l'UE comme Frontex, le CEPOL et Eurojust, ont, avec l'appui de la Commission, continué à développer le cycle politique de l'UE pour lutter contre la grande criminalité internationale organisée, dans le cadre de la «**plateforme pluridisciplinaire européenne contre les menaces criminelles**» (EMPACT)[160]. La coopération dans le cadre d'EMPACT a continué de montrer son efficacité pour lutter contre la criminalité organisée dans toute l'Europe, par exemple lors des «journées d'action commune» qui ont eu lieu en septembre, en octobre et en novembre 2020[161]. Les résultats obtenus démontrent clairement la valeur de la coopération. Elle a aussi contribué à des objectifs moins quantifiables: l'amélioration de l'état du renseignement, la formation et le renforcement des capacités, la prévention, la coopération avec des partenaires extérieurs à l'UE et la lutte contre la criminalité en ligne[162]. L'évaluation indépendante du cycle

[159] COM(2020) 796.

[160] EMPACT est l'outil de coopération policière de l'UE, qui vise à faire face aux principales menaces pesant sur la sécurité de l'UE en renforçant la coopération entre les services compétents des États membres, des institutions et agences de l'UE, ainsi que des pays tiers et des organisations. EMPACT associe différentes parties prenantes (approche pluridisciplinaire) afin d'améliorer et de renforcer la coopération entre les États membres, les institutions et agences de l'UE, ainsi que les pays tiers et les organisations, y compris le secteur privé.

[161] Journées d'action commune EMPACT: opération BOSPHORE – 1 776 armes à feu saisies (2-11 novembre), JAC mobile 3 – plus de 350 voitures volées et plus de 1 000 pièces de voitures volées récupérées (12-13 octobre), JAC contre la traite des êtres humains à des fins d'exploitation par le travail – 715 victimes potentielles d'exploitation par le travail identifiées (14-20 septembre), JAC contre la criminalité en Europe du Sud-Est – 51 armes de différents types et 47 kilogrammes de drogues diverses saisis (septembre).

[162] Toutes les fiches d'information détaillées présentant les résultats chiffrés par priorité de l'UE en matière de criminalité dans le cadre d'EMPACT peuvent être consultées à l'adresse suivante: https://data.consilium.europa.eu/doc/document/ST-7623-2020-INIT/en/pdf, document 7623/20 du 5 mai 2020.

politique de l'UE 2018-2021/EMPACT réalisée en 2020[163] a permis de conclure que la plateforme était de plus en plus pertinente et efficace pour faire face aux menaces les plus pressantes des organisations criminelles. La valeur ajoutée réside dans la mise à disposition d'une plateforme de coopération qui permet aux États membres d'obtenir, en matière de lutte contre la grande criminalité organisée, de meilleurs résultats que s'ils avaient agi seuls. L'évaluation a également donné lieu au recensement de possibilités et à la formulation de recommandations en vue de continuer à développer cet outil de coopération très utile pour le prochain cycle (2022-2025).

La Commission lancera en 2021 une initiative tendant à établir **un code de coopération policière de l'UE**, afin de rationaliser, d'améliorer, de développer, de moderniser et de faciliter la coopération en matière répressive entre les agences nationales compétentes. Ce code aidera beaucoup les États membres à lutter contre la grande criminalité organisée et le terrorisme.

Une coopération est également nécessaire entre **la police et d'autres services répressifs clés**, ainsi qu'avec des agences telles que les douanes. Les **douanes** de l'UE jouent un rôle essentiel dans la sécurité des frontières extérieures et de la chaîne d'approvisionnement et contribuent ainsi à la sécurité intérieure de l'Union européenne. Des menaces nouvelles et en évolution touchent aux principaux liens entre les douanes et les services répressifs, ce qui souligne tout particulièrement la valeur des contrôles douaniers sur les plans de la détection et de la prévention et le rôle moteur des douanes en ce qui concerne les marchandises. La Commission soutient et encourage la coopération entre les douanes et Europol[164], qui a une incidence directe sur l'action dans des domaines tels que les armes à feu, la criminalité environnementale, le financement lié à des activités criminelles et le cyberespace. Les autorités douanières participent actuellement à plusieurs actions menées par Europol contre la grande criminalité internationale organisée[165], ainsi qu'à des formations du CEPOL. Ces activités contribuent à promouvoir et à développer plus avant la coopération interservices et à renforcer l'interaction entre les principaux acteurs.

Il est indispensable de disposer de **systèmes d'information solides et efficaces** pour améliorer l'échange d'informations entre les autorités judiciaires et les services répressifs dans l'ensemble de l'UE. Le **système d'information Schengen (SIS)** a également été renforcé au moyen de règles actualisées qui comblent des lacunes potentielles en établissant des catégories de signalements supplémentaires, en allongeant la liste d'objets pour lesquels des signalements peuvent être introduits et en permettant l'introduction de nouveaux types de données[166]. Les nouvelles règles sont entrées en vigueur le 28 décembre 2018 et devraient être pleinement opérationnelles d'ici décembre 2021[167].

---

[163] Une évaluation indépendante était prévue dans les conclusions du Conseil du 27 mars 2017 sur la poursuite du cycle politique de l'UE pour lutter contre la grande criminalité internationale organisée pour la période 2018-2021 (document 7704/17).

[164] Voir par exemple le plan d'action du groupe «Coopération douanière» (GCD). Les domaines clés pour 2020-2021 sont notamment les suivants: présence accrue de fonctionnaires des douanes dans les bureaux de liaison au sein d'Europol, accès direct des autorités douanières à l'application du réseau d'échange sécurisé d'informations d'Europol (SIENA), meilleure représentation des fonctionnaires des douanes au sein des unités nationales Europol et participation des chefs des services de police et de douane à la convention des chefs des services de police européens.

[165] Fraude aux droits d'accise/à la TVA, trafic d'armes à feu, criminalité environnementale, fonds d'origine criminelle, abus sexuels commis sur des enfants.

[166] Règlements (UE) 2018/1860, 2018/1861 et 2018/1862.

[167] Le SIS sera également mis à jour pour tenir compte des modifications qu'il est proposé d'apporter au règlement Europol [COM(2020) XXX].

De même, en 2019, le **système européen d'information sur les casiers judiciaires (ECRIS)** a été complété par un système supplémentaire permettant d'échanger efficacement des informations sur les casiers judiciaires des ressortissants de pays tiers condamnés dans l'UE (ECRIS-TCN). Les travaux de développement technique et de mise en œuvre de ce nouveau système centralisé sont en cours; l'entrée en vigueur devrait avoir lieu en 2023.

Le 24 juillet 2020, la Commission a adopté le rapport sur le réexamen de la directive relative aux dossiers passagers (PNR)[168], qui porte sur les deux premières années d'application de la directive PNR[169]. Celui-ci montre que le développement du système PNR à l'échelle de l'UE est bien avancé. L'utilisation des données PNR est essentielle pour lutter contre le terrorisme, la grande criminalité et la criminalité organisée et elle a déjà produit des résultats tangibles. Seul un État membre n'a pas encore notifié une transposition complète à la Commission[170]. Le 3 décembre 2020, la Commission lui a adressé un avis motivé pour défaut de notification de la transposition complète de la directive.

Le 9 septembre 2020, la Commission a publié l'évaluation de la **directive** de 2004 **concernant l'information préalable sur les passagers**[171]. Cette évaluation met en lumière un certain nombre de lacunes et d'incohérences qui seront prises en considération lors de la révision prochaine du cadre législatif actuel. Un autre instrument essentiel fait l'objet d'un réexamen: les **décisions Prüm**[172], sur lesquelles il convient de se pencher en tenant compte des évolutions intervenues sur les plans opérationnel, technologique, médico-légal et de la protection des données.

La coopération doit également aller au-delà de l'UE et s'étendre à des **pays tiers clés pour lutter contre le terrorisme et la criminalité organisée**. Le 13 mai 2020, le Conseil a autorisé l'ouverture de négociations avec la Nouvelle-Zélande concernant l'échange de données à caractère personnel entre Europol et ce pays. Des négociations sont en cours avec la Turquie; en revanche, aucun progrès n'a été accompli en ce qui concerne les négociations avec l'Algérie, l'Égypte, Israël, la Jordanie, le Liban, le Maroc et la Tunisie sur l'échange de données à caractère personnel pour lutter contre la grande criminalité et le terrorisme. En outre, le 19 novembre 2020, la Commission a adopté une recommandation de décision du Conseil autorisant l'ouverture de négociations en vue d'accords entre l'Union européenne et dix pays tiers sur la coopération entre Eurojust et ces pays tiers en ce qui concerne l'échange de données à caractère personnel[173].

Pour ce qui est de la **coopération internationale relative à l'échange de données PNR** aux fins de la lutte contre le terrorisme et la grande criminalité, le Conseil a autorisé l'ouverture de négociations avec le Japon en vue de la signature d'un accord PNR[174]. Entre-temps, les **évaluations conjointes des accords existants entre l'UE et les États-Unis et entre l'UE et l'Australie** *sont en cours de finalisation.* La Commission a également

[168] COM(2020) 305.
[169] Directive (UE) 2016/681.
[170] La Slovénie.
[171] SWD(2020) 174.
[172] Le cadre Prüm permet l'échange automatisé de données relatives à l'ADN, aux empreintes digitales et à l'immatriculation des véhicules entre les services répressifs. Une analyse d'impact initiale a été publiée.
[173] Les pays tiers proposés sont les suivants: l'Algérie, l'Arménie, la Bosnie-Herzégovine, l'Égypte, Israël, la Jordanie, le Liban, le Maroc, la Tunisie et la Turquie. COM(2020) 743 final.
[174] Le 18 février 2020.

engagé un processus visant à revoir son approche globale actuelle en matière de transfert de données PNR vers des pays tiers[175].

La Commission collabore également avec les Nations unies afin d'accroître la capacité des pays partenaires à prévenir et à détecter les infractions terroristes et les autres formes graves de criminalité, ainsi qu'à enquêter sur celles-ci et à engager des poursuites en la matière, en collectant et en analysant les données relatives aux passagers, qu'il s'agisse des informations préalables sur les passagers ou des données des dossiers passagers.

La Commission s'est engagée dans le processus visant à faciliter les transferts de données PNR en conformité avec les exigences juridiques de l'UE dans le cadre des nouvelles normes PNR[176] adoptées par l'Organisation de l'aviation civile internationale (OACI)[177]. Le 23 juin 2020, le Conseil de l'OACI a adopté les nouvelles normes et pratiques recommandées (SARP) en matière de données PNR[178] et ses parties contractantes ont jusqu'au 30 janvier 2021 pour informer l'OACI de toute différence entre leurs pratiques réglementaires nationales et les nouvelles SARP relatives aux données PNR.

2. La contribution de frontières extérieures solides

Une gestion moderne et efficace des frontières extérieures est essentielle pour garantir la sécurité des citoyens de l'UE. Mobiliser l'ensemble des acteurs concernés pour tirer le meilleur parti de la sécurité aux frontières et les doter des outils adéquats peut avoir une réelle incidence sur la prévention de la criminalité et du terrorisme transfrontières. Le nouveau pacte sur la migration et l'asile[179] a également souligné la nécessité d'une gestion rigoureuse et équitable des frontières extérieures, y compris de contrôles d'identité, sanitaires et de sécurité. Il s'inscrit dans une approche globale, qui montre que les politiques dans les domaines de la migration, de l'asile, de l'intégration et de la gestion des frontières dépendent des progrès réalisés sur tous les fronts.

Le nouveau pacte a mis en exergue le caractère indispensable d'un espace Schengen effectif aux fins de la politique migratoire, et il a également de profondes implications en matière de sécurité. Ces aspects ont été examinés lors du premier forum Schengen, qui s'est tenu le 30 novembre 2020. Les représentants des États membres et du Parlement européen se sont accordés sur l'importance d'un espace Schengen effectif apportant aux citoyens des avantages sur le plan de la libre circulation, mais aussi de la sécurité. Ce processus alimentera une nouvelle stratégie Schengen qui sera présentée en 2021. Le mécanisme d'évaluation et de contrôle de Schengen est un outil essentiel pour assurer la confiance mutuelle et garantir une mise en œuvre améliorée et cohérente de l'acquis de Schengen, y compris sous l'angle de la sécurité. Il s'agissait là d'un thème important du rapport adopté le 25 novembre[180], qui dresse un état des lieux de la mise en œuvre de l'acquis de Schengen et fait le bilan du fonctionnement du mécanisme d'évaluation et de contrôle de Schengen.

---

[175] Feuille de route sur la dimension extérieure de la politique de l'UE relative aux données des dossiers passagers, disponible à l'adresse suivante: https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/12531-External-dimension-of-the-EU-policy-on-Passenger-Name-Records-

[176] Décision (UE) 2019/2107 du Conseil.

[177] Résolution 2396 (2017) du Conseil de sécurité.

[178] Amendement 28 de l'annexe 9 (Facilitation) de la convention relative à l'aviation civile internationale (la «convention de Chicago»).

[179] COM(2020) 609.

[180] SWD(2020) 327 final.

Les **règlements relatifs à l'interopérabilité**[181] visent à faire en sorte que les systèmes d'information de l'UE dans les domaines de la sécurité, des frontières et de la gestion des migrations, qu'ils soient existants, nouveaux ou améliorés, fonctionnent ensemble de manière plus intelligente et plus efficiente. L'interopérabilité des systèmes d'information de l'UE améliorera l'efficacité et l'efficience des vérifications aux frontières extérieures et contribuera à la prévention de l'immigration illégale ainsi qu'à l'établissement d'un niveau élevé de sécurité. Elle constituera un outil supplémentaire précieux pour les services répressifs et les autorités frontalières[182]. Les États membres, les pays associés à l'espace Schengen et les agences de l'Union concernées (l'eu-LISA, l'Agence européenne de garde-frontières et de garde-côtes et Europol) doivent être prêts et la Commission suit les préparatifs pour veiller à une mise en œuvre intégrale d'ici la fin 2023.

Un accord provisoire a été trouvé le 8 décembre 2020 entre les colégislateurs sur la proposition d'**actualisation du système d'information sur les visas**[183].

Toutefois, **certains actes législatifs clés doivent encore être adoptés**. Le Parlement européen doit concrétiser sa volonté de coopérer avec le Conseil au sujet des modifications[184] à apporter au système européen d'information et d'autorisation concernant les voyages (ETIAS)[185].

Les liens entre les systèmes d'information pertinents aux fins de l'analyse des risques en matière de sécurité sont cruciaux pour renforcer notre sécurité. L'amélioration de la **coopération entre les services douaniers et les autorités chargées de la gestion des frontières** et le renforcement des synergies entre leurs **systèmes d'information**, dans le respect de l'équilibre des pouvoirs, y compris de la législation relative à la protection des données à caractère personnel et de la vie privée, constituent une priorité du plan d'action du 28 septembre 2020 intitulé «Faire passer l'union douanière à l'étape supérieure»[186]. Une évaluation préliminaire réalisée par la Commission avec des experts des services de police et de douane des États membres recommande en particulier d'établir un lien entre le système d'information Schengen (SIS) et les données d'Europol, d'une part, et le système douanier de contrôle des importations (ICS2)[187], d'autre part; une étude de faisabilité va à présent débuter.

Le **règlement relatif au corps européen de garde-frontières et de garde-côtes**[188] est entré en vigueur en décembre 2019 et représente une réorganisation majeure des capacités et des outils dont dispose l'UE pour renforcer ses frontières extérieures. Il permettra d'améliorer sensiblement la contribution des frontières à la sécurité. Le nouveau mandat accroît la capacité de Frontex à soutenir les États membres dans la gestion des frontières extérieures et des retours et étend les possibilités de coopération avec des pays tiers. Des travaux sont en cours pour faire en sorte que le contingent permanent du corps européen de

[181] Règlements (UE) 2019/817 et 2019/818.
[182] Systèmes existants: système d'information Schengen (SIS), système d'information sur les visas (VIS), Eurodac. Systèmes futurs: système d'entrée/de sortie, système européen d'information et d'autorisation concernant les voyages (ETIAS), système européen d'information sur les casiers judiciaires pour les ressortissants de pays tiers (ECRIS-TCN).
[183] COM(2019) 12.
[184] COM (2019) 3 final et COM (2019) 4 final.
[185] Règlements (UE) 2018/1240 et 2018/1241.
[186] COM(2020) 581.
[187] Système d'information préalable sur le fret utilisé pour l'évaluation anticipée des risques en matière de sécurité de tous les mouvements de marchandises franchissant les frontières extérieures.
[188] Règlement (UE) 2019/1896.

garde-frontières et de garde-côtes soit prêt pour son premier déploiement à partir du 1er janvier 2021.

En juin 2019, l'UE a introduit des **normes de sécurité plus strictes pour les cartes d'identité** afin de faciliter la libre circulation des citoyens de l'UE tout en réduisant la fraude à l'identité[189]. Les États membres sont tenus de commencer à délivrer des cartes d'identité et des documents de séjour répondant aux nouvelles normes de sécurité à partir du mois d'août 2021. La plupart d'entre eux sont en train d'aligner leurs modèles de documents sur les exigences du règlement.

3. Renforcement de la recherche et de l'innovation en matière de sécurité

La recherche en matière de sécurité et la promotion de l'innovation sous-tendent une action coordonnée de l'UE face à des défis complexes et permettent de prendre des mesures concrètes pour atténuer les risques. L'union de la sécurité est l'un des quatre domaines prioritaires du programme de travail 2018-2020 d'**Horizon 2020**[190], qui représente 50 % du financement public global de la recherche en matière de sécurité dans l'UE. Les appels relatifs à la recherche en matière de sécurité lancés en 2019 dans le cadre d'Horizon 2020 ont abouti à la sélection de 42 projets, qui bénéficieront d'un financement total de l'UE de 253 000 000°EUR. Les travaux porteront notamment sur la protection des infrastructures, le renforcement de la résilience face aux catastrophes, la lutte contre la criminalité et le terrorisme, la sécurisation des frontières extérieures et l'amélioration de la sécurité numérique. Le budget indicatif disponible pour les projets en 2020 est de 265 000 000 EUR. Sur ce montant, 20 000 000 EUR seront consacrés à un appel à propositions concernant l'intelligence artificielle, qui aidera les services répressifs européens à accroître leurs capacités en la matière, à combler leur déficit de compétences dans ce domaine et à stimuler la coopération. Les travaux en préparation au titre du nouveau programme-cadre de recherche «Horizon Europe» soutiendront la mise en œuvre de la stratégie de l'UE pour l'union de la sécurité, ainsi que de la dimension «gestion des frontières et sécurité» du nouveau pacte sur la migration et l'asile, des politiques de l'UE en matière de réduction des risques de catastrophe et de la stratégie de sûreté maritime de l'UE[191].

La recherche en matière de sécurité financée par l'UE s'est aussi avérée efficace pour favoriser la coopération et soutenir les praticiens de la sécurité durant la pandémie de COVID-19[192]. Bénéficient notamment d'un soutien des outils d'évaluation et d'enquête communes concernant les menaces et les risques épidémiologiques et criminels.

Pour faire en sorte que les **projets innovants** soient utilisés dans la pratique, les agences de l'UE doivent être intégrées dans le paysage existant de la recherche et de l'innovation en matière de sécurité. À la suite du Conseil «Justice et affaires intérieures» d'octobre 2019, les agences de l'UE et le Centre commun de recherche de la Commission mettent actuellement sur pied, sur la base de leurs mandats juridiques existants, le **pôle**

[189] Règlement (UE) 2019/1157.

[190] L'UE a alloué un financement d'environ 91 000 000 EUR à des projets renforçant la protection des infrastructures, y compris contre les menaces informatiques et physiques combinées, par une réaction améliorée et rapide aux incidents et un meilleur partage des informations.

[191] Dans le cadre d'Horizon Europe, le troisième pôle soutiendra en particulier le domaine d'action prioritaire de la Commission consistant à «promouvoir notre mode de vie européen», ainsi que ceux liés au «pacte vert pour l'Europe» et à «une Europe adaptée à l'ère du numérique».

[192] Les actions menées au titre d'Horizon 2020 pour soutenir la réaction à la pandémie peuvent être consultées à l'adresse suivante: https://www.researchgate.net/publication/341287556.

d'innovation de l'UE pour la sécurité intérieure, qui doit servir de réseau de collaboration entre leurs laboratoires d'innovation. Ce pôle constituera un mécanisme de coordination destiné à aider les entités participantes à partager informations et connaissances, à établir des projets communs et à diffuser les résultats et les solutions technologiques mises au point présentant un intérêt pour la sécurité intérieure[193].

Pour soutenir l'innovation et la politique industrielle dans le domaine de la cybersécurité, l'Europe compte sur **le Centre européen de compétences industrielles, technologiques et de recherche en matière de cybersécurité et le Réseau de centres nationaux de coordination**. Ceux-ci visent à renforcer les capacités européennes en matière de cybersécurité, à protéger notre économie et notre société contre les cyberattaques, à maintenir l'excellence de la recherche et à accroître la compétitivité de l'UE. Des trilogues sont en cours.

4. Compétences et sensibilisation

La sensibilisation aux aspects sécuritaires et l'acquisition des compétences nécessaires pour faire face aux menaces potentielles sont essentielles pour bâtir une société plus résiliente caractérisée par des entreprises, des administrations et des citoyens mieux préparés. L'accès des victimes à leurs droits est tout aussi important.

Professionnels des services répressifs et de la justice

Les restrictions liées à la COVID-19 ont durement touché le CEPOL, qui a été contraint d'annuler toutes les activités en présentiel prévues à partir de mars 2020. Ces circonstances particulières ont également entraîné une demande croissante de services en ligne; au cours des quatre premiers mois de l'année, l'Agence a enregistré une augmentation de 30 % des activités virtuelles et une hausse de 100 % des utilisateurs en ligne. Les domaines de formation prioritaires pour la période 2019-2021[194] comprennent entre autres la lutte contre l'immigration clandestine, le terrorisme, la traite des êtres humains et la cybercriminalité, ainsi que les abus sexuels commis sur des enfants. La Commission prépare actuellement l'évaluation du CEPOL, qui devrait être achevée d'ici juillet 2021.

Grand public

La **campagne #SaferInternet4EU** a été lancée en 2018, lors de la Journée pour un internet plus sûr. Les activités ont touché près de 63 millions de personnes dans l'UE au cours des deux dernières années et comprennent des récompenses, un appui aux enseignants et des mesures d'hygiène informatique. Le réseau des centres pour un internet plus sûr a fourni plus de 1 800 nouvelles ressources couvrant des sujets tels que les fausses informations, le cyberharcèlement, les problèmes de respect de la vie privée, le pédopiégeage et l'hygiène informatique.

En octobre 2020 s'est tenu le huitième **Mois** européen **de la cybersécurité**, visant à promouvoir la sécurité en ligne dans l'UE. La campagne de cette année a mis l'accent sur les problèmes de sécurité qui se posent alors que la transformation numérique gagne notre quotidien et que le phénomène s'est accéléré avec la pandémie de COVID-19. En encourageant à «réfléchir avant de cliquer», elle a braqué les projecteurs sur différents

[193] Le 21 février 2020, le comité permanent de coopération opérationnelle en matière de sécurité intérieure a confirmé la déclaration de mission, les principales caractéristiques, les tâches et la gouvernance du pôle d'innovation de l'UE pour la sécurité intérieure.

[194] Rapport sur l'évaluation des besoins stratégiques de formation dans l'Union européenne pour la période 2018-2021, CEPOL.

thèmes pertinents en matière de cybersécurité pour aider les utilisateurs à identifier les cybermenaces et à s'y préparer. L'édition 2021 du Défi européen de la cybersécurité, qui se tiendra à Prague, est en préparation.

Un outil essentiel pour aider les victimes de la cybercriminalité est «No More Ransom»[195], un répertoire gratuit d'outils de déchiffrement qui aide les victimes à se défendre sans payer les pirates informatiques. Soutenu par le Centre de lutte contre la cybercriminalité d'Europol, il a célébré son quatrième anniversaire en juillet 2020 et, depuis son lancement, il a attiré plus de 4,2 millions de visiteurs provenant de 188 pays, ce qui a empêché, selon les estimations, 632 000 000 USD de demandes de rançon de se retrouver dans les poches de criminels.

Le 1er juillet 2020, la Commission a présenté la **stratégie européenne en matière de compétences**[196] en faveur de la compétitivité durable, de l'équité sociale et de la résilience. Celle-ci fixe des objectifs quantitatifs ambitieux en vue d'améliorer les compétences existantes et la formation à des compétences nouvelles, à atteindre au cours des cinq prochaines années. Elle comprend des actions spécifiques visant à augmenter le nombre de diplômés en sciences, technologies, ingénierie, arts et mathématiques dans des domaines de pointe tels que la cybersécurité. Le 10 novembre 2020, la Commission a lancé le pacte pour les compétences lors de la cinquième édition de la Semaine européenne des compétences professionnelles. Celui-ci encourage une action commune pour maximiser les effets des investissements dans l'amélioration des compétences existantes et la formation à des compétences nouvelles. En même temps que le pacte, les premiers partenariats européens en matière de compétences ont également été annoncés, dans trois domaines: la construction automobile, la microélectronique et l'industrie de l'aérospatial et de la défense.

Le 30 septembre 2020, la Commission a adopté une série de stratégies qui auront des effets importants sur le développement des capacités à long terme de l'UE pour ce qui est des compétences en matière de sécurité. Le **plan d'action en matière d'éducation numérique 2021-2027**[197] favorisera la mise en place d'un écosystème d'éducation numérique hautement performant, assorti de compétences renforcées pour la transformation numérique[198]. Une communication relative à la réalisation d'un **espace européen de l'éducation** d'ici à 2025[199], mettant l'accent sur les compétences de base et les compétences numériques, a été adoptée le même jour. Une communication sur un nouvel **espace européen de la recherche pour la recherche et l'innovation**[200] définit la voie à suivre pour améliorer le paysage européen de la recherche et de l'innovation et accélérer la transition de l'UE vers le leadership numérique tout en luttant contre la violence fondée sur le genre, sous toutes ses formes, dans les organismes de recherche et d'innovation.

Le **programme Erasmus+** contribue également à la lutte contre la radicalisation par des projets visant à combattre la radicalisation, l'extrémisme violent, l'exclusion sociale, la désinformation et les fausses informations[201]. Par exemple, le projet de prévention de la

[195] https://www.nomoreransom.org/.
[196] COM(2020) 274.
[197] COM(2020) 624.
[198] https://ec.europa.eu/education/sites/education/files/document-library-docs/deap-communication-sept2020_en.pdf.
[199] COM(2020) 625.
[200] COM(2020) 628.
[201] À ce jour, quelque 80 projets portant sur des questions liées à la radicalisation ont été financés, tout comme plus de 100 projets sur la manière de prévenir et de combattre le cyberharcèlement et plus de

radicalisation dans les prisons a pour objectif de renforcer les compétences du personnel de première ligne pour lui permettre de repérer les signes de radicalisation, de les interpréter, de les signaler et d'y réagir de manière appropriée[202]. Le projet «No Hate BootCamp» a aidé des animateurs de jeunesse à devenir des «ambassadeurs de la lutte contre les discours de haine» dans leur quartier.

La Commission elle-même s'efforce de faire participer les citoyens à la réflexion sur la politique de sécurité de l'UE. Les actions menées au niveau de l'UE ont été rendues plus visibles et plus accessibles aux citoyens grâce au nouveau **site web consacré à la stratégie de sécurité de l'UE**[203]. Plusieurs **consultations publiques** ont été lancées, donnant aux citoyens la possibilité d'influencer directement l'élaboration des politiques.

Toutes les victimes de la criminalité ont le droit de bénéficier d'un soutien et d'une protection, mais les victimes des infractions les plus graves, comme le terrorisme ou l'exploitation sexuelle des enfants, doivent faire l'objet d'une attention particulière. Le 24 juin 2020, la Commission a adopté la toute première **stratégie de l'UE relative au droit des victimes (2020-2025)**[204]. Cette stratégie concerne les victimes de toutes les formes de criminalité, mais met particulièrement l'accent sur les plus vulnérables d'entre elles, y compris les victimes du terrorisme, les enfants victimes d'exploitation sexuelle et les victimes de la traite des êtres humains. Le 22 septembre 2020, la Commission a organisé une conférence à haut niveau sur les droits des victimes, au cours de laquelle elle a inauguré la **plateforme des droits des victimes**, afin de promouvoir une approche plus horizontale de ces droits[205]. La Commission a également nommé son tout premier **coordinateur pour les droits des victimes**, dans le but de favoriser la cohérence et l'efficacité de la politique en la matière.

En ce qui concerne les **victimes du terrorisme**, le centre d'expertise de l'UE pour les victimes du terrorisme a été créé en janvier 2020 afin de fournir expertise, orientation et soutien aux autorités nationales et aux organisations d'aide aux victimes. Il encourage l'échange de bonnes pratiques et le partage d'expertise entre les praticiens et les spécialistes par-delà les frontières. Il n'est pas destiné à offrir un appui direct à certaines victimes du terrorisme, mais bien à aider les structures nationales à fournir une assistance et un soutien professionnels, y compris au moyen de lignes directrices qui seront publiées en 2020. Le centre de l'UE est un projet pilote qui durera deux ans. La présidence du Conseil s'emploie à soutenir ce projet par un réseau de points de contact nationaux uniques concernant les victimes du terrorisme.

---

100 projets concernant l'éducation à une utilisation critique et éthique de l'internet en vue de lutter contre la désinformation en ligne.

[202] http://www.r2pris.org/.

[203] https://ec.europa.eu/info/strategy/priorities-2019-2024/promoting-our-european-way-life/european-security-union-strategy_fr.

[204] COM(2020) 258.

[205] La plateforme réunira pour la première fois les principaux acteurs au niveau de l'UE, dont le réseau européen s'occupant de questions liées aux droits des victimes, le réseau de l'UE des points de contact nationaux en matière d'indemnisation, le coordinateur de l'UE pour la lutte contre le terrorisme, les agences concernées telles qu'Eurojust, l'Agence des droits fondamentaux, l'Agence de l'Union européenne pour la formation des services répressifs, l'Institut européen pour l'égalité entre les hommes et les femmes et la société civile.

VI CONCLUSION

La stratégie pour l'union de la sécurité a été établie afin de fournir une approche globale et dynamique. Les attentats terroristes perpétrés récemment ont montré une nouvelle fois que l'UE doit être en mesure de réagir, en renforçant sa résilience et sa réactivité par la modernisation et le déploiement effectif des outils essentiels dont elle dispose. Ils ont également mis en évidence la nécessité d'associer pleinement l'ensemble des acteurs à une approche commune, de sorte que les États membres, les institutions de l'UE, le secteur privé, les ONG et les citoyens eux-mêmes puissent tous jouer un rôle dans la mise en place d'une base de sécurité suffisamment solide et flexible pour produire des résultats. Cette approche cohérente et uniforme constitue également le meilleur moyen de s'assurer que nos droits fondamentaux sont protégés dans le cadre de la promotion de notre mode de vie européen.

Le présent rapport expose les nombreux axes de travail au titre desquels des activités sont en cours, mais indique aussi la façon dont cette dynamique doit être maintenue. L'objectif du programme de l'UE contre le terrorisme présenté aujourd'hui est de renforcer le cadre européen de lutte contre le terrorisme en définissant les prochaines étapes nécessaires: anticiper et prévenir le terrorisme, protéger les citoyens et les infrastructures, et être prêts à réagir, en gardant à l'esprit le lien entre sécurité intérieure et extérieure. La coopération a déjà été renforcée, tout comme les efforts visant à s'attaquer à la radicalisation et les outils destinés à priver les terroristes des moyens de commettre des attentats. Il faut maintenant aller plus loin. Dans ce contexte, il convient avant tout de veiller à l'adoption de nouvelles règles pour lutter contre les contenus à caractère terroriste en ligne, l'obtention d'un accord à ce sujet cette année constituant une priorité majeure. La Commission invite également instamment les États membres à accélérer la mise en œuvre de l'ensemble des actes législatifs adoptés. Il est de notre responsabilité partagée de garantir la sécurité des citoyens de l'UE et notre ambition collective doit être de faire progresser notre action commune afin de créer une Europe plus sûre.