COMMISSION
EUROPÉENNE

Bruxelles, le 23.6.2021
COM(2021) 440 final

COMMUNICATION DE LA COMMISSION AU PARLEMENT EUROPÉEN ET AU CONSEIL

relative au deuxième rapport sur l'état d'avancement de la mise en œuvre de la stratégie de l'UE pour l'union de la sécurité

I. Introduction

En juillet dernier, 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. Si cette stratégie s'appuie sur le programme européen en matière de sécurité pour la période 2015-2020, elle lui a donné une nouvelle orientation et a introduit une nouvelle approche coordonnée pour les différents volets de la politique de sécurité, afin que l'UE puisse réagir à des menaces évoluant rapidement. Le but de cette stratégie est de faire en sorte que l'UE joue pleinement son rôle de garant de la sécurité des citoyens et de leurs droits fondamentaux, à la fois en s'attaquant aux risques actuels et en s'adaptant aux nouveaux défis, et en promouvant les valeurs qui définissent le mode de vie européen.

La pandémie de COVID-19 est venue s'ajouter à ce contexte de changement dynamique, en créant de nouvelles possibilités pour la criminalité en ligne, en stimulant la cybercriminalité et en ouvrant la voie à une augmentation de la contrefaçon et de la distribution de biens non conformes aux normes, de la criminalité organisée contre les biens et de divers types de fraude[2]. Certaines de ces formes de criminalité ont directement compromis les systèmes de santé et la fourniture de services de santé. Tandis que certaines activités criminelles retrouveront leur état antérieur à la pandémie, d'autres en sortiront fondamentalement changées[3].

La stratégie définit des actions à mener sur une période de cinq ans. Au cours de cette première année de mise en œuvre, de nombreuses initiatives ont été lancées[4]. La Commission a adopté un programme de lutte antiterroriste pour l'UE et des initiatives visant à lutter contre la criminalité organisée, la traite des êtres humains, le trafic de drogue, les abus sexuels commis contre des enfants et le trafic d'armes à feu, ainsi qu'une nouvelle stratégie de cybersécurité de l'UE. La Commission a présenté de nouvelles propositions législatives importantes pour renforcer Europol, protéger les infrastructures critiques physiques et numériques et lutter contre le matériel pédopornographique. Le Parlement européen et le Conseil ont fait avancer ce programme et ont mené à leur terme des dossiers clés, notamment en ce qui concerne les contenus à caractère terroriste en ligne et la lutte contre les abus sexuels commis contre des enfants en ligne. Les travaux sur la législation exposée dans la stratégie devraient progresser rapidement, mais le niveau d'ambition doit rester élevé.

En juin, la Commission a adopté une nouvelle stratégie pour un espace Schengen pleinement opérationnel et résilient[5], qui prévoit des mesures efficaces dans le domaine de la sécurité et de la coopération policière et judiciaire pour le fonctionnement de l'espace de liberté, de sécurité et de justice, afin que l'UE reste forte face aux menaces qui pèsent sur la sécurité, même sans contrôles aux frontières intérieures. Pendant la période visée par le présent rapport, les colégislateurs ont trouvé un accord sur les fonds à mobiliser pour soutenir de nombreuses actions au titre de l'union de la sécurité, en particulier le Fonds pour la sécurité

[1] Communication de la Commission relative à la stratégie de l'UE pour l'union de la sécurité [COM(2020) 605].

[2] Y compris dans le domaine des médicaments vitaux, des dispositifs médicaux et des vaccins.

[3] Rapport 2021 sur l'évaluation de la menace que représente la grande criminalité organisée dans l'Union européenne (SOCTA), Europol.

[4] Voir annexe II — Feuille de route pour la mise en œuvre.

[5] COM(2021) 277.

intérieure (FSI) renforcé et l'instrument relatif à la gestion des frontières et aux visas (IGFV) dans le cadre du Fonds pour la gestion intégrée des frontières (FGIF).

Le succès de la stratégie pour l'union de la sécurité dépendra de la qualité de sa mise en œuvre[6]. À cette fin, il faudra compter sur un engagement total des autorités nationales et sur une coopération continue entre tous les acteurs concernés par la sécurité intérieure et extérieure de l'Europe, y compris les agences de l'UE. Une approche inclusive et axée sur la société dans son ensemble sera possible grâce à une coopération renforcée entre les acteurs de la sécurité.

Le présent deuxième rapport sur l'état d'avancement de la stratégie pour l'union de la sécurité, qui couvre la période écoulée depuis le premier rapport[7], paru le 9 décembre 2020, présente les progrès accomplis dans les quatre piliers de la stratégie: 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. Il expose la manière dont les activités dans ces domaines sont menées, en présentant notamment la contribution spécifique des agences de l'UE.

II. Un environnement de sécurité à l'épreuve du temps

1. Protection et résilience des infrastructures critiques

La protection et la résilience des infrastructures critiques, tant physiques que numériques, revêtent une importance capitale pour le fonctionnement des sociétés modernes et le mode de vie européen. Cela n'a jamais été plus vrai qu'en cette période d'urgence de santé publique. Les menaces, les incidents et les attaques impliquant des infrastructures critiques peuvent avoir des conséquences très perturbatrices.

La résilience est plus essentielle que jamais dans le contexte de la pandémie

Alors que les infrastructures sanitaires sont déjà sous pression, les cyberincidents visant des hôpitaux, des structures médicales et d'autres services prodiguant des soins de santé complets peuvent avoir des conséquences particulièrement dramatiques.

L'Irlande a récemment été frappée par une série de cyberattaques graves qui ont perturbé son système de soins de santé, au cours desquelles les pirates s'en sont pris à la fois au ministère de la santé et au système de santé publique.

Les bases de données nationales du système d'alerte précoce et de réaction (SAPR)[8] qui sous-tendent les réactions au niveau du secteur de la santé ont été la cible de tentatives d'intrusions et d'attaques par rançongiciel[9].

La cyberattaque commise contre l'Agence européenne des médicaments, au cours de laquelle

[6] L'annexe I donne un aperçu de l'état d'avancement de la mise en œuvre de la législation en matière de sécurité.

[7] Premier rapport sur l'état d'avancement de la stratégie de l'UE sur l'union de la sécurité [COM(2020) 797].

[8] Le SAPR est un système d'alerte rapide permettant de notifier, au niveau de l'UE, des alertes liées à des menaces transfrontières graves sur la santé; il a été mis en place en vertu de la décision nº 1082/2013/UE (https://ec.europa.eu/health/security/surveillance_early-warning_fr).

[9] La sécurité des données du SAPR, gérée par le Centre européen de prévention et de contrôle des maladies (ECDC), n'a pas été compromise. Elle sera néanmoins renforcée.

les pirates ont accédé illégalement à des documents concernant les médicaments et vaccins contre la COVID-19, a révélé que la divulgation sur l'internet de ces documents peut avoir des effets dramatiques.

En dehors du domaine de la santé, mais toujours dans un domaine proche de la vie quotidienne des citoyens, la cyberattaque par rançongiciel visant le Colonial Pipeline aux États-Unis a mis en évidence le défi de la protection des infrastructures critiques physiques et son lien avec la cybersécurité[10].

L'ampleur des risques potentiels montre qu'il est urgent de renforcer la préparation au niveau national et au niveau de l'UE, en mettant en place des capacités solides pour prévenir, détecter et atténuer ces menaces et pour gérer les crises hors ligne et en ligne.
Grâce à la législation de l'UE dans ce domaine, en particulier la directive sur la sécurité des réseaux et des systèmes d'information[11] (directive SRI) et la directive sur les infrastructures critiques européennes[12] (directive ICE), il existait une base solide pour réagir aux incidents récents. Dans le cas de l'attaque par rançongiciel qui a visé le service de santé irlandais, les experts de la cybersécurité nationaux ont utilisé les espaces de coopération[13] mis en place par la directive SRI pour s'échanger des informations, tant au niveau technique qu'au niveau stratégique, ce qui a permis aux autorités irlandaises de recevoir une aide et aux autres États membres de renforcer leur préparation face à de telles attaques.

Dans le même temps, l'augmentation de l'incidence et de l'intensité des menaces montre que le cadre législatif actuel n'est pas adapté à l'objectif poursuivi. Il ressort de l'évaluation[14] de la mise en œuvre de la directive SRI que son champ d'application ne reflète pas le niveau actuel de numérisation et d'interconnexion, ni l'interdépendance des principaux secteurs économiques et sociétaux. En outre, certaines entités publiques et privées appartenant à des secteurs essentiels ne sont pas couvertes par cette directive ou sont soumises à des obligations non harmonisées en matière de cybersécurité et de signalement des incidents. Il ressort de l'évaluation[15] de la mise en œuvre de la directive ICE que celle-ci se concentre uniquement sur la protection des actifs dans un nombre très limité de secteurs, et non sur la résilience des opérateurs. Les deux évaluations ont mis en évidence des approches divergentes et des lacunes au niveau national.

En décembre 2020, la Commission a donc proposé deux textes législatifs essentiels: une directive sur la **résilience des entités critiques**[16] et une directive révisée concernant des mesures destinées à assurer un **niveau élevé commun de cybersécurité dans l'ensemble de**

[10] Le Colonial Pipeline, un oléoduc critique qui transporte 45 % du pétrole consommé sur la côte est des États-Unis, a été la cible en mai 2021 d'une cyberattaque par rançongiciel qui a perturbé l'approvisionnement en pétrole pendant plusieurs jours.

[11] Directive (UE) 2016/1148 du Parlement européen et du Conseil du 6 juillet 2016 concernant des mesures destinées à assurer un niveau élevé commun de sécurité des réseaux et des systèmes d'information dans l'Union.

[12] Directive 2008/114/CE du Conseil du 8 décembre 2008 concernant le recensement et la désignation des infrastructures critiques européennes ainsi que l'évaluation de la nécessité d'améliorer leur protection.

[13] Le réseau des centres de réponse aux incidents de sécurité informatique (CSIRT) et le groupe de coopération.

[14] SWD(2020) 345, partie II.

[15] SWD(2019) 310.

[16] Proposition de directive sur la résilience des entités critiques [COM(2020) 829].

l'Union (directive SRI révisée)[17]. Ces deux directives ont un vaste champ d'application et couvrent les mêmes dix secteurs essentiels: les transports, l'énergie, le secteur bancaire, les infrastructures des marchés financiers, la santé, l'eau potable, les eaux usées, les infrastructures numériques, l'administration publique et l'espace. Pour ces secteurs, la directive sur la résilience des entités critiques prévoit des mesures destinées à mettre en place un cadre de résilience physique assorti de normes minimales, en permettant une certaine souplesse pour tenir compte des spécificités nationales. La proposition de directive SRI révisée vise à établir une norme horizontale pour les exigences de cybersécurité dans le marché intérieur, en mettant davantage l'accent sur la sécurité de la chaîne d'approvisionnement. Elle instaurerait de nouveaux outils permettant de coordonner le traitement et la divulgation des vulnérabilités, ainsi que d'améliorer l'efficacité de la réaction aux incidents et de la gestion des crises. Elle permettrait également de rationaliser les obligations en matière de signalement des incidents, en prévoyant des dispositions plus précises sur le processus, le contenu et le délai des signalements.

Compte tenu de l'évolution constante des menaces pesant sur nos infrastructures critiques, la Commission invite les colégislateurs à faire preuve d'un niveau d'ambition élevé et à garantir l'adoption sans heurts de ces deux propositions, tout en préservant leur cohérence et leur complémentarité. Les progrès accomplis en vue de l'adoption de ces propositions doivent également assurer la cohérence avec la proposition de la Commission de 2020 sur la résilience opérationnelle numérique du secteur financier[18], qui vise à renforcer la capacité de l'Europe à consolider son autonomie stratégique dans le domaine des services financiers et, par extension, sa capacité à réglementer et à superviser le système financier dans l'intérêt de la stabilité financière.

Initiatives dans le secteur de l'énergie

Pour cibler des vulnérabilités plus spécifiques, il convient d'adopter des initiatives sectorielles. À cet égard, il y a lieu de mettre en avant les évolutions importantes dans le secteur de l'énergie. Dans le cadre du suivi des incidences de la crise de la COVID-19 dans le secteur de l'énergie, une étude, achevée en mai 2021, a recensé les chaînes d'approvisionnement en technologies énergétiques qui sont critiques pour la sécurité énergétique et la transition vers une énergie propre et a proposé des mesures destinées à améliorer la résilience face aux pandémies et à d'autres scénarios de menace. Ses conclusions alimenteront d'autres axes de travail pertinents, dont les travaux du groupe de coopération dans le secteur de l'énergie mis en place par la directive SRI. Le réseau thématique sur la protection des infrastructures énergétiques critiques a poursuivi ses travaux sur les défis liés à la protection des infrastructures énergétiques critiques, en examinant des questions telles que l'évaluation des risques, l'échange d'informations et le financement des mesures de sécurité[19].

En janvier 2021, la Commission a lancé avec l'Agence pour la coopération des régulateurs de l'énergie (ACER) la procédure formelle visant à établir un code de réseau spécifique sur la **cybersécurité des flux transfrontaliers d'électricité**. Ce code de réseau contiendra des

[17] Proposition de directive concernant des mesures destinées à assurer un niveau élevé commun de cybersécurité dans l'ensemble de l'Union, abrogeant la directive (UE) 2016/1148 [COM(2020) 823].

[18] Proposition de règlement sur la résilience opérationnelle numérique du secteur financier et modifiant les règlements (CE) nº 1060/2009, (UE) nº 648/2012, (UE) nº 600/2014 et (UE) nº 909/2014 [COM(2020) 595].

[19] La discussion avec les opérateurs a été étendue aux États membres et un cycle technique de discussions bilatérales a eu lieu entre mars et juin 2021.

exigences minimales communes en matière de planification, de surveillance, d'établissement des rapports et de gestion de crise, conformément au cadre horizontal établi par la directive SRI. En ce qui concerne la **préparation aux risques dans le secteur de l'électricité**, les États membres ont lancé en avril 2021 une consultation sur la cohérence de leurs projets de plans de préparation aux risques. Ces plans comportent des mesures visant à prévenir et à atténuer les crises électriques sur la base des scénarios nationaux de crise électrique définis par chaque État membre, ainsi que sur la base des scénarios régionaux de crise électrique définis par le réseau européen des gestionnaires de réseau de transport en septembre 2020, qui envisagent des cyberattaques, ainsi que des pandémies et des phénomènes météorologiques extrêmes.

2. Cybersécurité

La transformation numérique de la société, intensifiée par la crise de la COVID-19, crée de nouveaux défis, qui requièrent des réponses innovantes. Au cours des derniers mois, le nombre de cyberattaques a continué d'augmenter et les attaques, provenant d'un large éventail de sources, tant à l'intérieur qu'à l'extérieur de l'UE, sont devenues de plus en plus sophistiquées. Les violations de données majeures et les cyberattaques récentes, telles que la cyberopération à grande échelle ayant visé SolarWinds[20], montrent l'ampleur des risques pour la société si nous ne parvenons pas à changer radicalement la cybersécurité. L'UE doit s'efforcer de protéger ses gouvernements, ses citoyens et ses entreprises contre les cybermenaces, tout en garantissant un internet ouvert et mondial. Des mesures importantes ont été prises pour concrétiser la vision selon laquelle tout citoyen de l'UE devrait pouvoir vivre sa vie numérique en toute sécurité en utilisant l'internet ouvert et mondial.

En décembre 2020, la Commission et le haut représentant ont présenté une nouvelle stratégie de cybersécurité de l'UE[21]. Cette stratégie, qui constitue un élément clé de la stratégie «Façonner l'avenir numérique de l'Europe», du plan de relance pour l'Europe et de la stratégie pour l'union de la sécurité, vise à renforcer la résilience collective de l'Europe face aux cybermenaces et à permettre de faire en sorte que tous les citoyens et toutes les entreprises puissent bénéficier pleinement de services et d'outils numériques sûrs et fiables. Le cyberespace doit rester mondial, ouvert, stable et sûr. Cette stratégie s'articule autour de trois grands piliers: 1) résilience, souveraineté technologique et leadership; 2) renforcement des capacités opérationnelles de prévention, de dissuasion et de réaction; 3) promouvoir un cyberespace ouvert et mondial grâce à une coopération accrue. Elle traite pour la première fois de la cybersécurité des institutions, organes et organismes de l'UE. Le Conseil a adopté des conclusions sur la stratégie[22], dans lesquelles il approuve les principales initiatives stratégiques qu'elle prévoit pour sa mise en œuvre. La mise en œuvre de cette stratégie est en cours et un rapport de mise en œuvre spécifique[23] donne un aperçu détaillé de son état d'avancement.

---

[20] Solarwinds, une grande société américaine active dans le secteur des technologies de l'information, a été la cible d'une cyberattaque qui s'est propagée à ses clients et n'a pas été détectée pendant plusieurs mois. Durant tout ce temps, les pirates ont eu accès à des milliers d'entreprises et de services publics qui utilisaient les produits de cette entreprise.

[21] Communication conjointe au Parlement européen et au Conseil intitulée «La stratégie de cybersécurité de l'UE pour la décennie numérique» [JOIN(2020) 18].

[22] Cybersécurité: le Conseil adopte des conclusions sur la stratégie de cybersécurité de l'UE — Consilium (europa.eu)

[23] JOIN(2021) 14.

Une initiative majeure annoncée dans les orientations politiques de la Commission et à laquelle il a été donné suite dans le cadre de la stratégie de cybersécurité est la création d'une **unité conjointe de cybersécurité**. Après avoir consulté les États membres, la Commission a adopté, en même temps que le présent rapport, une recommandation visant à mieux définir le processus, les étapes et le calendrier de la mise en place de cette unité conjointe[24]. L'unité conjointe de cybersécurité va fédérer toutes les communautés du domaine de la cybersécurité, à savoir les communautés civile, répressive, diplomatique et militaire. L'unité conjointe de cybersécurité s'appuiera sur des structures, des ressources et des capacités existantes et leur apportera une valeur ajoutée, constituant ainsi une plateforme pour une coopération opérationnelle et technique sécurisée et rapide entre les entités de l'Union et les autorités des États membres. L'unité conjointe de cybersécurité va également fédérer toutes les communautés du domaine de la cybersécurité, à savoir les communautés civile, répressive, diplomatique et militaire. L'unité conjointe de cybersécurité sera mise en place selon un processus en quatre étapes comprenant le recensement des capacités opérationnelles de l'Union disponibles, la préparation des plans de réaction aux incidents et aux crises au niveau national et au niveau de l'UE et l'extension des activités aux fins d'une coopération avec des entités du secteur privé. L'unité conjointe de cybersécurité devrait être pleinement opérationnelle pour le 30 juin 2023.

Dans le but de renforcer davantage les **capacités de détection** et de mobiliser des outils fondés sur l'IA pour protéger l'Union contre les cyberattaques, les États membres sont actuellement en train d'augmenter leurs investissements dans les **centres des opérations de sécurité** (COS), au moyen de fonds mis à disposition au titre de la facilité pour la reprise et la résilience. La Commission complétera les efforts des États membres par des fonds relevant du programme pour une Europe numérique.

Cybersécurité des réseaux 5G

Dans le cadre de la stratégie de cybersécurité, la Commission a défini trois objectifs clés pour les futurs travaux sur la cybersécurité des réseaux 5G, compte tenu de leur rôle central dans la réalisation de la transformation numérique de l'économie et de la société de l'UE: i) assurer une plus grande convergence des approches en matière d'atténuation des risques dans l'ensemble de l'UE, ii) soutenir l'échange continu de connaissances et le renforcement des capacités, et iii) promouvoir la résilience de la chaîne d'approvisionnement et d'autres objectifs de sécurité stratégique de l'UE. Ces objectifs reposent sur un rapport sur la cybersécurité de la 5G[25] qui, au terme d'un examen des travaux intenses menés conjointement par les États membres et la Commission, avec le soutien de l'ENISA (l'Agence de l'UE pour la cybersécurité), a confirmé que des progrès considérables avaient été accomplis depuis l'adoption de la boîte à outils de l'UE relative aux mesures d'atténuation des risques[26]. De plus amples informations sur l'état d'avancement de la mise en œuvre de la boîte à outils de l'UE figurent dans le rapport sur la mise en œuvre de la stratégie de cybersécurité[27].

Un écosystème de la cybersécurité

---

[24] C(2021) 4520.
[25] SWD(2020) 357.
[26] https://digital-strategy.ec.europa.eu/en/library/cybersecurity-5g-networks-eu-toolbox-risk-mitigating-measures
[27] JOIN(2021) 14.

Afin de contribuer à la création d'un écosystème de la cybersécurité européen et interconnecté rassemblant les communautés de la recherche et l'industrie, le règlement établissant le **Centre de compétences en matière de cybersécurité** et le **Réseau de centres nationaux de coordination**[28] a été adopté en mai 2021. Il vise à renforcer les capacités européennes en matière de cybersécurité, à promouvoir l'excellence dans la recherche et à renforcer la compétitivité de l'industrie de l'Union dans ce domaine[29]. La Commission coopère déjà avec les autorités roumaines pour préparer l'implantation du Centre à Bucarest. Dans le cadre du plan d'action sur les synergies entre les industries civile, spatiale et de la défense[30], la Commission s'efforcera de renforcer l'enrichissement mutuel entre les activités du Centre, du Fonds européen de la défense et du programme spatial de l'UE en matière de cybersécurité et de cyberdéfense.

Le règlement sur la cybersécurité[31] a introduit un **cadre de certification de cybersécurité à l'échelle de l'UE pour les produits, services et processus TIC**. Les entreprises qui opèrent dans l'Union bénéficieront de la possibilité de ne faire certifier qu'une seule fois leurs produits, processus et services TIC, la certification ainsi obtenue étant ensuite reconnue dans toute l'Union européenne. La Commission a déjà demandé à l'ENISA de préparer trois systèmes de certification de cybersécurité: le système européen de critères communs, le système européen pour les services d'informatique en nuage et le système européen pour les réseaux 5G[32].

Dimension internationale

La stratégie de cybersécurité comprenait des propositions visant à mieux prévenir les actes de cybermalveillance, à mieux les décourager et à mieux y réagir, en favorisant le comportement responsable des États chez les partenaires internationaux de l'UE dans le cyberespace[33]; en renforçant le cadre pour une réponse diplomatique commune de l'UE face aux actes de cybermalveillance (la boîte à outils cyberdiplomatique)[34]; en intensifiant la coordination et la coopération dans l'UE dans le domaine de la cyberdéfense; et en renforçant les capacités de cyberdéfense au moyen du cadre stratégique de cyberdéfense[35]. Le haut représentant prépare actuellement un réexamen de ces cadres, en consultation avec la Commission et conformément à l'ambition de la boussole stratégique. En mai, le Service européen pour l'action extérieure (SEAE) a organisé une discussion fondée sur des scénarios avec les États membres et les partenaires internationaux afin d'améliorer la compréhension mutuelle des options diplomatiques permettant de prévenir, décourager et empêcher les actes de cybermalveillance et y faire face, et afin de recenser les possibilités de renforcer encore la coopération internationale.

---

28 RÈGLEMENT (UE) 2021/887.

29 Cela passera notamment par l'affectation et la gestion des fonds consacrés à la cybersécurité provenant du programme pour une Europe numérique et du programme Horizon Europe, ainsi que des États membres.

30 COM(2021) 70 du 22.2.2021.

31 Règlement (UE) 2019/881 du 17 avril 2019 relatif à l'ENISA (Agence de l'Union européenne pour la cybersécurité) et à la certification de cybersécurité des technologies de l'information et des communications.

32 Le statut de ces programmes sera décrit dans le programme de travail glissant de l'Union.

33 Notamment en faisant progresser la proposition de programme d'action visant à mettre en place une infrastructure permanente pour des actions concrètes visant à favoriser le comportement responsable des États dans le cyberespace.

34 Décisions (PESC) 2020/1127, 2020/1537 et 2020/651 du Conseil dans le cadre des conclusions 9916/17.

35 Décision 14413/18 du Conseil.

Au-delà de l'Europe, un soutien à la cybersécurité est apporté dans les pays du voisinage oriental, en Afrique, en Asie, en Amérique latine et dans les Caraïbes, au moyen de projets de coopération bien définis visant à mobiliser le savoir-faire européen dans le but de renforcer les capacités en matière de cybersécurité et d'accroître la sécurité et la résilience des infrastructures et réseaux critiques[36]. Avec le pacte en matière de PSDC civile[37], la cybersécurité a également été ajoutée en tant que domaine prioritaire des missions de PSDC civiles.

Afin d'empêcher que les technologies de cybersurveillance ne soient utilisées en violation des droits de l'homme en dehors de l'UE, le nouveau règlement sur les exportations[38] sous-tend une modernisation complète des règles de l'UE relatives aux exportations de biens à double usage[39]. En adoptant ce nouveau règlement, l'UE s'est dotée d'une base pour mettre en œuvre des contrôles efficaces des exportations de technologies de cybersurveillance et pour se prémunir face aux risques en matière de sécurité liés au commerce mondial de technologies émergentes.

3. Protéger les espaces publics

Ces dernières années, les espaces publics de l'UE ont été le théâtre d'attentats terroristes sans précédent contre la population. La propagation des **drones** fait partie des risques émergents pour les espaces publics. Les acteurs malveillants peuvent utiliser ces systèmes d'aéronefs sans équipage à bord pour effectuer une surveillance, interrompre les opérations d'infrastructures critiques ou attaquer des cibles de grande valeur. En avril, la Commission a adopté un **cadre pour le concept européen de gestion du trafic sans pilote** (l'U-space)[40], afin de permettre aux autorités d'opérer plus aisément la distinction entre les drones coopératifs et les drones non coopératifs, potentiellement malveillants. En outre, la Commission facilite l'élaboration de documents d'orientation par l'Agence de l'Union européenne pour la sécurité aérienne, en finançant des projets et des études innovants en matière de lutte contre les drones et en jetant des ponts entre les différents secteurs concernés (services répressifs, aviation, infrastructures critiques, prisons, douanes/frontières, protection individuelle, organisateurs d'événements de masse) et d'autres parties intéressées. Un programme européen a été lancé pour faciliter une approche plus coordonnée des essais de différentes technologies de lutte contre les drones.

Des lignes directrices visant à permettre de recenser et d'atténuer les vulnérabilités des espaces publics et à garantir la sécurité dès la conception sont en cours d'élaboration. Un programme de 20 millions d'euros est actuellement mené dans le cadre du Fonds pour la sécurité intérieure — Police afin de renforcer la **protection des lieux de culte et autres espaces publics contre les menaces terroristes**, en mettant l'accent sur les grands lieux sportifs. En mars, la Commission a organisé une conférence sur les nouveaux projets à mener en 2021. Par ailleurs, la Commission apporte son concours aux autorités nationales, régionales et urbaines et aux exploitants d'espaces publics pour leur permettre de s'échanger

[36] Citons par exemple les projets «Cyber4Dev», «EU4Digital» et «EU CyberNet».
[37] Document 14305/18 du 19 novembre 2018.
[38] Règlement instituant un régime de l'Union de contrôle des exportations, du courtage, de l'assistance technique, du transit et des transferts en ce qui concerne les biens à double usage (refonte) (19 mai 2021).
[39] À savoir les biens, logiciels et technologies susceptibles d'avoir une utilisation tant civile que militaire.
[40] Règlements d'exécution de la Commission C(2021) 2671, C(2021) 2672 et C(2021) 2673.

de bonnes pratiques, de créer des réseaux et de coopérer dans l'ensemble de l'UE[41], dans le cadre du programme urbain de l'UE et des activités menées dans le cadre du Fonds européen de développement régional[42].

Le plan d'action sur la **sûreté ferroviaire** adopté en 2018[43], qui prévoyait des actions concrètes pour améliorer la sûreté du transport ferroviaire de voyageurs, est à présent pleinement mis en œuvre. La plateforme de l'UE en matière de sûreté des voyageurs ferroviaires[44] a adopté plusieurs documents présentant des bonnes pratiques concernant l'évaluation des risques, les menaces intérieures et les technologies de détection, favorisant ainsi une plus grande coopération entre les États membres et l'obtention de meilleurs résultats dans le domaine de la sûreté ferroviaire.

III. Faire face à l'évolution des menaces

1. Cybercriminalité

Les effets de la pandémie sur la cybercriminalité[45]

Les criminels ont rapidement exploité les changements induits par le télétravail et le recours accru aux services en ligne pour adapter leurs activités illicites au contexte de crise. Le nombre d'escroqueries facilitées par l'internet et liées à la pandémie, commises au moyen de logiciels malveillants, de rançongiciels et d'attaques par hameçonnage ciblant des particuliers, des entreprises et le secteur de la santé en particulier, a augmenté au cours de la pandémie.

Les circonstances de la pandémie ont offert de nouvelles possibilités de fraude: les pénuries ont été exploitées par de fausses boutiques en ligne faisant de la publicité pour des biens inexistants, y compris des équipements de protection individuelle et des kits d'autodiagnostic, et vendant de tels biens. Du fait du passage du marché physique au marché en ligne pour la distribution de produits pharmaceutiques, des offres frauduleuses de vaccins contre la COVID ont même été trouvées sur l'internet clandestin.

L'augmentation des pertes économiques mondiales liées à la cybercriminalité (qui devraient atteindre 5 400 milliards d'euros par an d'ici à 2021) révèle la nécessité de mettre en place des applications et des infrastructures sécurisées pour pouvoir anticiper les menaces sans cesse croissantes et y réagir rapidement. Le registre judiciaire relatif à la cybercriminalité

[41] Par exemple, dans le cadre du programme urbain de l'UE, la Commission a fourni des orientations et un soutien sous la forme d'un savoir-faire thématique et technique au partenariat sur la sécurité dans les espaces publics afin de contribuer à la mise en œuvre de son plan d'action. Les programmes de coopération transfrontière Interreg cofinancés par le Fonds européen de développement régional aident les acteurs de la sécurité dans les régions frontalières voisines à coopérer plus efficacement.

[42] https://ec.europa.eu/jrc/en/protection-public-spaces-from-terrorist-attacks/newsletter-protection-public-spaces

[43] COM(2018) 470.

[44] La plateforme de l'UE en matière de sûreté des voyageurs ferroviaires rassemble les autorités des États membres compétentes dans le domaine de la sûreté ferroviaire et des parties intéressées. Le mandat de cette plateforme ayant expiré en juin 2021, la mise en œuvre des résultats du plan d'action sur la sûreté ferroviaire se poursuivra par l'intermédiaire d'un groupe de travail consacré à la sûreté ferroviaire au sein du groupe d'experts en matière de sûreté des transports terrestres (LANDSEC).

[45] Rapport 2021 sur l'évaluation de la menace que représente la grande criminalité organisée dans l'Union européenne (SOCTA), Europol.

publié par Eurojust en mai donne un aperçu de l'évolution de la législation et de la jurisprudence dans l'UE dans le domaine de la cybercriminalité et de la criminalité facilitée par l'internet[46].

Étant donné qu'une cybersécurité forte est essentielle pour endiguer la vague de cybercriminalité, il est impératif que les États membres mettent pleinement en œuvre la législation existante. La Commission évalue en permanence la conformité de la transposition de la **directive relative aux attaques contre les systèmes d'information**[47]. Outre les procédures d'infraction engagées précédemment[48], la Commission a ouvert de nouvelles procédures d'infraction (voir annexe I du présent rapport) pour des manquements dans la transposition de cette directive. Si nécessaire, la Commission engagera de nouvelles procédures. Parallèlement, la Commission a aidé les États membres à mettre en œuvre cette directive en organisant, le 23 février 2021, un atelier sur les bonnes pratiques en matière d'enregistrement, de production et de publication de données statistiques sur les signalements, les poursuites et les condamnations face à des cyberattaques telles que définies dans la directive. Pour démanteler les réseaux criminels et mettre fin à des phénomènes tels que l'augmentation actuellement observée des attaques par rançongiciel, il est nécessaire que la directive relative aux attaques contre les systèmes d'information soit pleinement transposée. L'engagement de l'UE dans ce domaine a été publiquement souligné lors de réunions de l'OTAN[49] et du G7[50] qui se sont tenues en juin, au cours desquelles l'Union s'est dite disposée à coopérer avec les pays partageant sa vision pour faire face à l'aggravation de la menace commune que représentent les réseaux criminels de rançongiciels.

Lutte contre les abus sexuels commis contre des enfants

La question des abus sexuels commis contre des enfants est de plus en plus inquiétante; pour cette forme de criminalité, les crimes perpétrés en ligne et hors ligne sont souvent liés.

La pandémie de COVID-19 et les abus sexuels commis contre des enfants

D'après de nombreux rapports, la pandémie a exacerbé les abus, en particulier ceux qui sont commis contre des enfants qui vivent avec leur agresseur[51]. La pandémie a également induit une nette augmentation du matériel visuel «autoproduit», en partie en conséquence d'abus commis en ligne dans le cadre desquels des enfants sont incités par tromperie à produire ce matériel ou subissent des pressions en ce sens[52].

[46] Eurojust, Registre judiciaire relatif à la cybercriminalité, sixième édition, mai 2021, consulté le 7 juin 2021.

[47] Directive 2013/40/UE relative aux attaques contre les systèmes d'information et remplaçant la décision-cadre 2005/222/JAI du Conseil.

[48] Des procédures d'infraction contre la Bulgarie, l'Italie, le Portugal et la Slovénie ont été ouvertes en 2019.

[49] Communiqué du sommet de l'OTAN à Bruxelles, 14 juin 2021.

[50] Communiqué du sommet du G7, Our Shared Agenda for Global Action to Build Back Better [Notre programme commun d'action mondiale pour reconstruire en mieux], 13 juin 2021.

[51] Voir rapport d'Europol du 19 juin 2020 et NetClean (14 avril 2021). Selon des informations communiquées par le US National Center for Missing and Exploited Children (Centre national américain pour les enfants disparus et exploités), le nombre de signalements d'abus sexuels commis contre des enfants dans le monde en avril 2020 était quatre fois supérieur à celui d'avril 2019. Voir, également, Alliance mondiale WePROTECT, World Childhood Foundation, Unicef, ONUDC, OMS, UIT, End Violence Against Children et Unesco, avril 2020.

[52] Voir rapports de l'Internet Watch Foundation, 12 janvier 2021; et Europol, Évaluation de la menace que représente la grande criminalité organisée, 12 avril 2021.

Conformément à la **stratégie de l'UE en faveur d'une lutte plus efficace contre les abus sexuels commis contre des enfants**[53] et à la **stratégie globale de l'UE sur les droits de l'enfant**[54], la Commission s'efforce actuellement de concrétiser les initiatives spécifiques prévues pour favoriser une action proactive et multipartite dans tous les domaines concernés, couvrant la prévention, le soutien à l'application de la législation et l'assistance aux victimes.

En avril, le Parlement européen et le Conseil sont parvenus à un accord politique provisoire sur la proposition de la Commission relative à une **législation temporaire** visant à permettre aux fournisseurs de services en ligne de maintenir leurs pratiques volontaires de détection et de signalement des abus sexuels commis contre des enfants en ligne ainsi que de suppression du matériel pédopornographique de leurs systèmes, pour autant que ces pratiques soient licites. Ces règles provisoires seront remplacées en temps utile par une législation à plus long terme, qui prévoira des garanties détaillées pour lutter plus efficacement contre les abus sexuels commis contre des enfants. Cette initiative a fait l'objet d'une consultation publique ouverte et d'une analyse d'impact.

La Commission observe actuellement la mise en œuvre de la **directive relative à la lutte contre les abus sexuels et l'exploitation sexuelle des enfants, ainsi que la pédopornographie**[55]. À la suite des procédures d'infraction lancées en 2019 contre 23 États membres, la Commission poursuit son évaluation et pourrait engager des actions supplémentaires au cours du second semestre de 2021. La Commission prévoit par ailleurs de clore plusieurs procédures au cours des mois à venir, étant donné que plusieurs États membres ont pleinement aligné leur législation nationale sur cette directive.

Pour soutenir les services répressifs et favoriser la coordination multipartite, la Commission a entamé des travaux devant déboucher sur la mise en place d'un **réseau de prévention** rassemblant des praticiens et des chercheurs, afin d'intensifier la coopération et l'échange de bonnes pratiques entre tous les acteurs concernés. Ce réseau contribuera à l'établissement de normes mondiales plus élevées en matière de protection des enfants contre les abus sexuels, en encourageant la coopération par l'intermédiaire de l'Alliance mondiale WePROTECT visant à mettre fin à l'exploitation sexuelle des enfants en ligne et en apportant un financement spécifique.

Enquêtes en ligne et données électroniques

Pour traduire les cybercriminels en justice, il est essentiel de garantir l'accès aux preuves numériques qui peuvent donner des pistes aux enquêteurs. Si certains États membres ont mis en place des cadres de **conservation des données** pour la conservation et l'utilisation des métadonnées des communications électroniques à des fins répressives, ces mesures soulèvent des questions importantes en ce qui concerne leur éventuelle ingérence dans les droits fondamentaux, dont le droit au respect de la vie privée et à la protection des données à caractère personnel. La Cour de justice de l'Union européenne a formulé des précisions et

[53] Communication de la Commission intitulée «Stratégie de l'UE en faveur d'une lutte plus efficace contre les abus sexuels commis contre des enfants» [COM(2020) 607].

[54] COM(2021) 142.

[55] Directive 2011/93/UE relative à la lutte contre les abus sexuels et l'exploitation sexuelle des enfants, ainsi que la pédopornographie.

orientations importantes[56]. En mars, dans un arrêt concernant la législation nationale estonienne[57], la Cour a confirmé sa jurisprudence antérieure. Toujours en mars, le Conseil européen[58] a appelé à prendre des mesures pour «mieux exploiter le potentiel que recèlent les données et les technologies numériques, dans l'intérêt de la société, de l'environnement et de l'économie, tout en veillant au respect des droits pertinents en matière de protection des données et de vie privée et des autres droits fondamentaux et en assurant la conservation des données nécessaire pour permettre aux services répressifs et aux autorités judiciaires d'exercer leurs pouvoirs légaux pour lutter contre les formes graves de criminalité». En réponse à ces récents développements, la Commission a annoncé dans la stratégie de l'UE visant à lutter contre la criminalité organisée[59] qu'elle analyserait et définirait les approches et solutions envisageables, conformément aux arrêts de la Cour, qui répondent aux besoins des services répressifs et judiciaires d'une manière qui soit utile sur le plan opérationnel, techniquement possible et juridiquement solide, notamment en respectant pleinement les droits fondamentaux. Elle consulte à présent les États membres afin de définir la voie à suivre.

La législation sur l'**accès transfrontière aux preuves électroniques** représente un autre moyen essentiel de lutter plus efficacement contre la cybercriminalité et de garantir des poursuites plus efficaces. Depuis le premier rapport sur l'état d'avancement de la stratégie pour l'union de la sécurité, un nouvel élan a été insufflé aux négociations avec les colégislateurs sur la proposition de la Commission[60], le Parlement européen ayant adopté sa position en décembre 2020. Sur cette base, le Parlement européen et le Conseil ont entamé des discussions en trilogue. L'adoption rapide de mesures efficaces qui soient conformes à l'objectif des propositions aidera les services répressifs et les autorités judiciaires à accéder rapidement aux preuves électroniques nécessaires aux enquêtes pénales.

Pour juguler l'augmentation de la cybercriminalité et permettre la sécurisation des transactions transfrontières sur l'internet, les services de confiance et l'identification électronique sont indispensables. La proposition de **cadre européen relatif à une identité numérique**, adoptée le 3 juin, vise à fournir des identités numériques de confiance à tous les citoyens, résidents et entreprises de l'UE. Ce cadre établira les normes de sécurité les plus élevées pour lutter contre les menaces de fraude et d'usurpation d'identité et permettra aux citoyens et autres détenteurs d'identités numériques de confiance de contrôler pleinement et facilement la quantité de données les concernant qui sont fournies pour une transaction donnée. Il reposera sur une architecture technique commune et fondée sur les normes les plus récentes.

La date limite d'application du règlement relatif au renforcement de **la sécurité des cartes d'identité et des documents de séjour** est fixée au 2 août 2021. La plupart des États

[56] Dans ses arrêts du 6 octobre 2020 dans l'affaire C-623/17, Privacy International, et dans les affaires jointes C-511/18, C-512/18 et C-520/18, La Quadrature du Net e.a., la Cour a confirmé sa jurisprudence antérieure, selon laquelle les données relatives aux communications électroniques sont confidentielles et, en principe, les données de trafic et de localisation ne peuvent pas faire l'objet d'une conservation généralisée et indifférenciée. Dans le même temps, elle a recensé certaines situations dans lesquelles la conservation est autorisée, sur la base d'obligations claires et proportionnées prévues par la loi et sous réserve de garanties matérielles et procédurales strictes.

[57] Arrêt dans l'affaire C-746/18, Prokuratuur.

[58] Déclaration des membres du Conseil européen, SN 18/21 du 25 mars 2021.

[59] Stratégie de l'UE visant à lutter contre la criminalité organisée (2021-2025) [COM(2021) 170 du 14.4.2021].

[60] COM(2018) 226 et COM(2018) 225.

membres sont sur la bonne voie et délivreront des cartes d'identité et des documents de séjour dans le nouveau format[61].

Dimension internationale
Compte tenu de la nature mondiale de la cybercriminalité, il est essentiel de déployer des efforts au niveau international pour trouver des solutions plus efficaces.

Les négociations relatives au deuxième protocole additionnel à la **convention de Budapest du Conseil de l'Europe sur la cybercriminalité** visent à renforcer les règles existantes en matière d'accès transfrontière aux preuves électroniques dans le cadre d'enquêtes pénales. En mai 2021, les parties à cette convention ont achevé leurs discussions et le projet de protocole sera à présent examiné par les comités compétents du Conseil de l'Europe. La conclusion formelle de ce processus est toujours attendue pour cette année, à la suite de quoi le protocole pourra être signé et ratifié. La Commission collaborera avec le Parlement européen et le Conseil pour permettre aux États membres de signer et de ratifier le protocole dans les meilleurs délais.

Le protocole contient également des dispositions qui faciliteront l'accès des autorités aux données d'enregistrement des noms de domaine (également appelées «**informations WHOIS**») dans le cadre d'enquêtes pénales. À cet égard, la Commission participe également à l'élaboration et à la mise en œuvre, au niveau de l'Internet Corporation for Assigned Names and Numbers (ICANN, Société pour l'attribution des noms de domaine et des numéros sur l'internet), de politiques multipartites en matière de collecte des données d'enregistrement des noms de domaine et d'accès à ces données. Il y a lieu de veiller à la cohérence de ces processus avec les dispositions pertinentes de la proposition de directive SRI révisée, telles que les dispositions visant à garantir la collecte et la divulgation de données d'enregistrement des noms de domaine qui soient fiables pour les demandeurs d'accès légitimes, dont les services répressifs.

L'Action globale sur la cybercriminalité élargie (GLACY+) est une initiative importante dans le domaine de la coopération internationale. Cette initiative vise à renforcer la capacité des pays du monde entier à appliquer la législation relative à la cybercriminalité et aux preuves électroniques, sur la base de la convention de Budapest, et à améliorer leur capacité à coopérer efficacement dans le respect des normes internationales en matière de droits de l'homme et de l'état de droit. Ce projet soutient 16 pays prioritaires[62]. Il permettra également de mettre en relation les praticiens de la justice pénale avec les décideurs politiques et les législateurs, afin de renforcer le soutien politique à la convention de Budapest.

---

[61] Si des retards sont à déplorer dans un nombre limité d'États membres, principalement en raison de la pandémie, d'autres retards importants résultent notamment de la contestation des procédures d'appel d'offres devant la Cour.

[62] Par exemple, le Conseil de l'Europe bénéficie du soutien de l'instrument européen de voisinage pour la mise en œuvre du projet CyberSouth, qui vise à renforcer la législation et les capacités institutionnelles en matière de cybercriminalité et de preuves électroniques dans les pays du voisinage méridional, dans le respect des droits de l'homme et de l'état de droit. Un projet similaire (CyberEast) est mené par le Conseil de l'Europe dans la région du partenariat oriental. Un autre projet du Conseil de l'Europe, financé au titre de l'instrument d'aide de préadhésion, est en cours dans les Balkans occidentaux et en Turquie pour renforcer davantage la capacité des autorités des Balkans occidentaux et de la Turquie à rechercher, saisir et confisquer les produits de la cybercriminalité, à prévenir le blanchiment de capitaux sur l'internet et à obtenir des preuves électroniques.

2. Des services répressifs modernes

Les nouvelles technologies offrent d'importantes possibilités dans le domaine de la sécurité. 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.

L'**intelligence artificielle** peut offrir des outils pour soutenir les services répressifs dans leur lutte contre la criminalité et le terrorisme, en suivant le rythme effréné de l'évolution des technologies utilisées par les criminels pour leurs activités transfrontières. La récente communication de la Commission intitulée «Fostering a European approach to Artificial Intelligence» [Promouvoir une approche européenne de l'intelligence artificielle][63] expose comment l'IA peut apporter une contribution majeure à la stratégie pour l'union de la sécurité, en tant qu'outil stratégique permettant à la fois de contrer les menaces actuelles et d'anticiper les risques et opportunités futurs. En avril, la Commission a présenté une proposition de règles harmonisées (la «législation sur l'IA»)[64] pour faire de l'Europe le centre mondial de l'IA digne de confiance. Une partie importante de ces propositions est axée sur les systèmes d'IA à haut risque qui présentent des risques importants pour la santé et la sécurité ou pour les droits fondamentaux des personnes. La législation sur l'IA interdirait en principe, sauf exceptions strictement encadrées, l'identification biométrique à distance en temps réel dans des espaces accessibles au public à des fins répressives. Ces types de systèmes à haut risque doivent respecter un ensemble d'exigences horizontales obligatoires pour une IA digne de confiance, notamment en matière de traçabilité, de transparence, de contrôle humain et d'exactitude. La législation sur l'intelligence artificielle aurait des retombées considérables dans le domaine de la répression et des contrôles aux frontières. Elle vise à créer un cadre de contrôle équilibré tout au long du cycle de vie des systèmes à haut risque utilisés par les services répressifs et instaure une série de garanties visant à protéger les droits fondamentaux.

L'espace européen des données de sécurité pour l'innovation qui relève du **programme pour une Europe numérique** vise à renforcer la confiance dans l'utilisation de l'IA par les services répressifs, en créant, en rendant accessibles et en partageant des jeux de données de haute qualité pour former, tester et valider des algorithmes en tant que condition préalable essentielle à la création d'écosystèmes d'excellence et de confiance pour l'IA. L'importance de la création des espaces communs des données a été reconnue par le Conseil européen en mars.

Le **calcul à haute performance** est une fonctionnalité essentielle pour permettre à des technologies clés telles que l'IA et l'analyse des données d'exploiter l'énorme potentiel des mégadonnées. Les simulations par supercalcul sont indispensables pour améliorer la sécurité des produits et des services (notamment par la modélisation), ainsi que pour renforcer la sécurité nationale, la défense et l'autonomie technologique. Les supercalculateurs sont critiques dans de nombreux domaines, de la cybersécurité à la simulation nucléaire, et la combinaison du calcul à haute performance et de l'IA changera radicalement le paysage de la défense et de la sécurité. L'inauguration en mai du siège de l'entreprise commune pour le

[63] Communication intitulée «Fostering a European approach to Artificial Intelligence» [COM(2021) 205].
[64] COM(2021) 206.

calcul à haute performance européen[65] a constitué une étape majeure pour la fourniture d'un accès rapide aux ressources de supercalcul de cette entreprise en cas de besoin à des fins de sécurité et de défense.

Le rôle du cryptage

Le **cryptage** est une technologie essentielle dans le domaine de la sécurité et joue un rôle fondamental dans la sécurisation des systèmes et transactions numériques et dans la protection des droits fondamentaux, notamment la liberté d'expression, la protection de la vie privée et la protection des données. Comme l'ont montré les récentes opérations Encrochat[66] et Sky ECC[67], les criminels utilisent des communications cryptées et les services répressifs de l'UE doivent constamment améliorer leur capacité à traiter les informations cryptées lors de leurs enquêtes pénales, tout en respectant la législation applicable. En décembre 2020, la nouvelle plateforme de décryptage d'Europol a été lancée. Cette plateforme, qui a été créée pour garantir le respect des droits fondamentaux et pour éviter de limiter ou d'affaiblir le cryptage, est mise à la disposition des services répressifs nationaux de tous les États membres, qui peuvent ainsi veiller à la sûreté et à la sécurité des citoyens et de la société.

En décembre 2020, le Conseil a appelé à engager une discussion active avec le secteur des technologies et à mettre en place un cadre réglementaire qui permettrait aux autorités nationales de s'acquitter efficacement de leurs tâches opérationnelles tout en protégeant la vie privée, les droits fondamentaux et la sécurité des communications[68]. Dans la stratégie de l'UE visant à lutter contre la criminalité organisée[69], la Commission a fait part de son intention de proposer, en 2022, une voie à suivre pour permettre un accès légal et ciblé aux informations cryptées dans le cadre d'enquêtes et de poursuites pénales, sans affaiblir le chiffrement ni conduire à une surveillance aveugle. Une première étape consiste à dresser une cartographie détaillée de la manière dont les États membres traitent le cryptage, ainsi qu'à mener un processus multipartite visant à explorer et à évaluer les options juridiques, éthiques et techniques.

Coopération judiciaire

Pour relever de manière adéquate les défis en matière de sécurité, il faut également **moderniser la coopération judiciaire** entre les pays de l'UE au moyen des technologies numériques. L'élaboration d'une proposition législative sur la numérisation de la coopération judiciaire transfrontière dans l'UE est en cours. Cette proposition mettra en place un canal de

---

[65] L'entreprise commune EuroHPC a été créée en 2018 pour permettre à l'UE de devenir un acteur mondial de premier rang dans le domaine du supercalcul. Un nouveau règlement est actuellement examiné au niveau de l'UE; il devrait entrer en vigueur au cours des prochains mois.

[66] En 2020, une enquête menée à l'échelle européenne a permis de démanteler un service téléphonique crypté utilisé par la criminalité organisée.

[67] Le 10 mars 2021, Eurojust a apporté son soutien à des opérations conjointes menées par les services répressifs et les autorités judiciaires de Belgique, de France et des Pays-Bas pour bloquer l'utilisation de communications cryptées par des groupes de la grande criminalité organisée. Les enquêteurs ont réussi à surveiller l'utilisation criminelle de l'outil de communication Sky ECC, ce qui a permis de recueillir de précieux renseignements sur des centaines de millions de messages échangés par des criminels, d'accéder à des informations cruciales sur plus d'une centaine d'opérations criminelles planifiées à grande échelle, de prévenir des situations dans lesquelles des vies seraient menacées et de sauver des futures victimes potentielles.

[68] Résolution du Conseil sur le chiffrement — La sécurité grâce au chiffrement et malgré le chiffrement, 13084/1/20 REV 1.

[69] Communication de la Commission relative à la stratégie de l'UE visant à lutter contre la criminalité organisée (2021-2025) [COM(2021) 170].

communication numérique entre les autorités compétentes des États membres et, le cas échéant, les agences de l'UE. L'objectif est d'abandonner la communication sur support papier entre les autorités et de veiller à ce que les échanges de données aient lieu rapidement et de manière sûre et efficace. Lors d'une consultation publique[70], les citoyens et les parties intéressées se sont dits favorables à cette approche.

3. Lutte contre les contenus illicites en ligne

Dans la stratégie pour l'union de la sécurité, la Commission souligne que la sécurité des environnements tant numériques que physiques requiert des efforts constants de lutte contre les contenus illicites en ligne, et des progrès décisifs ont été accomplis au cours de la période visée par le présent rapport. Le règlement longtemps attendu pour lutter contre la **diffusion des contenus à caractère terroriste en ligne** a été adopté par le Parlement européen et le Conseil[71] et sera pleinement applicable à partir de juin 2022. Il permettra aux États membres d'émettre des injonctions de retrait à l'intention de certains fournisseurs de services d'hébergement proposant des services dans l'UE et de retirer, dans un délai d'une heure, les contenus qui incitent à commettre des infractions terroristes ou prônent la commission de tels actes, promeuvent les activités d'un groupe terroriste ou contiennent des instructions ou présentent des techniques permettant de commettre des infractions terroristes. Ce règlement prévoit également des garanties visant à renforcer la responsabilité et la transparence en ce qui concerne les mesures prises pour retirer les contenus à caractère terroriste, et à éviter les retraits erronés de discours licites en ligne.

La **législation sur les services numériques** proposée par la Commission en décembre 2020 comporte des mesures visant à lutter contre la distribution en ligne de biens, services et contenus illicites. Cette législation permettrait aux utilisateurs de signaler les contenus illicites en ligne et créerait un canal privilégié permettant à des signaleurs de confiance de signaler les contenus illicites en priorité. En outre, elle obligerait les plateformes en ligne qui soupçonneraient l'existence de certaines infractions pénales graves à en informer les services répressifs compétents et elle prévoit aussi des règles en vertu desquelles les très grandes plateformes en ligne devraient procéder à des évaluations annuelles des risques et prendre des mesures d'atténuation face aux risques systématiques importants de diffusion de contenus illicites. La proposition de législation sur les services numériques est fondée sur des initiatives volontaires telles que le **code de conduite visant à combattre les discours de haine illégaux en ligne**, qui constituent des outils précieux pour lutter contre des formes spécifiques de contenus illicites.

Les défis posés par la lutte contre les contenus illicites en ligne, y compris les contenus pédopornographiques, ont été au cœur des discussions menées lors de la réunion ministérielle du Forum de l'UE sur l'internet de janvier 2021, qui a réuni les États membres de l'UE et des entreprises du secteur des technologies. Dans le cadre du Forum de l'UE sur l'internet, la Commission a lancé un processus associant des experts du monde des entreprises, de la recherche, des pouvoirs publics et des organisations de la société civile pour trouver des solutions techniques permettant aux entreprises de détecter les abus sexuels commis contre des enfants en ligne dans les communications électroniques cryptées de bout en bout tout en

[70] https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/12547-Digitalisation-of-justice-in-the-European-Union-_en

[71] Règlement (UE) 2021/784 du 29 avril 2021 relatif à la lutte contre la diffusion des contenus à caractère terroriste en ligne.

préservant les droits fondamentaux, y compris la protection de la vie privée et la confidentialité des communications. Par ailleurs, l'élaboration d'une liste de l'UE recensant les symboles et groupes violents d'extrême droite est en cours afin d'aider les entreprises du secteur des technologies dans leurs décisions de modération des contenus, à la lumière des problèmes concernant l'identification des contenus extrémistes qui ont été soulevés lors de ces discussions.

4. Menaces hybrides

Les tensions géopolitiques, qui sévissent également sur les nouvelles technologies, entraînent une augmentation des menaces pesant sur la sécurité mondiale, une fragmentation des efforts et une lutte permanente entre discours et contre-discours. Les acteurs étatiques et non étatiques détournent de plus en plus les technologies pour atteindre leurs objectifs, menaçant ainsi nos sociétés, notre économie et notre sécurité et portant atteinte aux droits de l'homme et aux libertés fondamentales. La pandémie a rendu l'UE et ses États membres plus vulnérables face aux menaces hybrides, notamment en intensifiant la propagation de la désinformation et des ingérences manipulatrices.

Santé et résilience face aux menaces hybrides

La pandémie a mis en lumière la faiblesse des mécanismes de préparation et de réaction aux situations d'urgence au niveau de l'UE. Les capacités des acteurs tant publics que privés dans le domaine de la préparation et de la gestion de crise, en particulier en ce qui concerne les contre-mesures médicales, sont fragmentées, dispersées et perfectibles par rapport à celles d'autres acteurs mondiaux (tels que les États-Unis ou la Chine). Cette fragmentation représente un terreau fertile pour les menaces hybrides émanant d'acteurs étatiques et non étatiques. Comme indiqué dans les communications intitulées «Construire une Union européenne de la santé: renforcer la résilience de l'UE face aux menaces transfrontières pour la santé»[72] et «Premiers enseignements tirés de la pandémie de COVID-19»[73], la future Autorité européenne de préparation et de réaction en cas d'urgence sanitaire (HERA) jouerait un rôle essentiel dans le renforcement de la résilience globale, en garantissant un cadre solide de l'UE pour la préparation, la surveillance, l'évaluation des risques, l'alerte précoce et la réaction face à toutes les menaces transfrontières graves pour la santé.

Un réexamen des mécanismes de gestion de crise de l'UE, étroitement lié au réexamen du **protocole opérationnel de l'UE pour la lutte contre les menaces hybrides (EU Playbook)**, est en cours. Une première étape de ce processus a consisté à renforcer et à élargir le réseau de points de contact sur les menaces hybrides parmi les services de la Commission, le Service européen pour l'action extérieure et l'Agence européenne de défense. Un autre élément, qui permet d'intégrer les considérations hybrides dans l'élaboration des politiques, est l'inclusion de l'évaluation des menaces hybrides dans les initiatives au titre de la politique «Mieux légiférer».

La mise en œuvre du cadre commun de 2016 en matière de lutte contre les menaces hybrides et de la communication conjointe de 2018 intitulée «Accroître la résilience et renforcer la capacité à répondre aux menaces hybrides» se poursuit, et l'état d'avancement de la mise en

[72] COM(2020) 724.
[73] COM(2021) 380.

œuvre est examiné dans le cinquième rapport annuel[74] sur la lutte contre les menaces hybrides. Ce rapport décrit les progrès enregistrés vers la création d'une plateforme en ligne restreinte devant permettre aux États membres et aux institutions de l'UE de consulter facilement les outils et mesures de lutte contre les menaces hybrides au niveau de l'UE, de prendre des mesures pour mieux connaître la situation, en particulier au travers de la cellule de fusion de l'UE contre les menaces hybrides, et de définir des bases de référence sectorielles en matière de résilience.

La lutte contre les menaces hybrides et les cybermenaces, de plus en plus complexes et destructrices, est un domaine dans lequel la **coopération entre l'UE et l'OTAN** reste essentielle. C'est ce qui ressort également du récent communiqué du sommet de l'OTAN tenu à Bruxelles[75]. Cette coopération s'est poursuivie à un rythme soutenu, en s'appuyant sur les résultats déjà obtenus et en maintenant la dynamique qui caractérisait les périodes précédentes. Les principaux résultats ont été présentés dans le sixième rapport d'étape conjoint UE-OTAN[76]. Le nombre de membres du Centre européen d'excellence pour la lutte contre les menaces hybrides à Helsinki (CdE hybride) a continué de croître, 30 États membres de l'UE et alliés de l'OTAN ayant désormais rejoint ce centre. Au cours de la période visée par le présent rapport, le CdE hybride a facilité plusieurs discussions, ateliers et exercices fondés sur des scénarios.

Avec le pacte en matière de PSDC civile[77], les menaces hybrides ont également été ajoutées en tant que domaine prioritaire des missions de PSDC civiles. Un mini-concept correspondant sur le soutien de la PSDC civile à la lutte contre les menaces hybrides[78] a été élaboré. Ce document propose 1) d'accorder la priorité à la protection des missions contre les attaques hybrides et 2) le cas échéant, d'aider l'État hôte à renforcer sa résilience face aux menaces hybrides.

La **désinformation** est un élément important des menaces hybrides. Le plan d'action pour la démocratie européenne[79] a défini plusieurs actions pour renforcer la réponse aux opérations étrangères de manipulation de l'information et d'ingérence[80]. Le Conseil européen s'est félicité de l'approche prévue par ce plan d'action et le Conseil a par ailleurs appelé à renforcer l'action de l'UE[81]. Le SEAE collabore étroitement avec la Commission à cet égard et utilise le système d'alerte rapide de l'UE pour mobiliser la communauté des experts en vue de la mise en place d'un cadre solide, robuste, souple et global de lutte contre les opérations étrangères de manipulation de l'information et d'ingérence. L'action de l'UE est aussi fondée sur le code de bonnes pratiques contre la désinformation en ligne, qui, en mai, a été renforcé par des orientations sur la manière dont les fournisseurs de services en ligne participants et

---

74 SWD(2021) 729.

75 Communiqué du sommet de Bruxelles de l'OTAN, Bruxelles, 14 juin 2021.

76 Sixième rapport d'étape sur les suites données aux propositions communes entérinées le 6 décembre 2016 et le 5 décembre 2017 par le Conseil de l'Union européenne et le Conseil de l'Atlantique Nord, 3 juin 2021.

77 Document 14305/18 du 19 novembre 2018.

78 Document 8077/20 du 20 mai 2020.

79 COM(2020) 790.

80 Des actions sont ainsi prévues dans trois domaines clés: 1) affiner davantage la terminologie qui décrit ce phénomène; 2) élaborer une méthode et un cadre communs pour la collecte de preuves systématiques en cas d'opérations étrangères de manipulation de l'information et d'ingérence; et 3) étoffer la panoplie d'outils dont l'UE dispose pour contrer les opérations étrangères de manipulation de l'information et d'ingérence afin qu'elle soit mieux adaptée à l'objectif consistant à imposer des sanctions financières aux auteurs.

81 Déclaration du Conseil européen de mars 2021; conclusions du Conseil de décembre 2020.

les autres parties prenantes concernées devraient renforcer leurs mesures visant à combler les lacunes et les insuffisances du code et créer un environnement en ligne plus transparent, plus sûr et plus fiable[82].

IV. Protéger les Européens contre le terrorisme et la criminalité organisée

1. Terrorisme et radicalisation

Les attentats de fin 2020 ont montré que, plus que jamais, il faut s'attaquer au terrorisme et à ses causes profondes. Le nouveau **programme de lutte antiterroriste pour l'UE**[83] adopté en décembre 2020 définit des mesures visant à renforcer la lutte contre le terrorisme et l'extrémisme violent et à améliorer la résilience de l'UE face aux menaces terroristes. La mise en œuvre de ce programme est en bonne voie. En outre, la directive (UE) 2017/541 relative à la lutte contre le terrorisme, qui établit des règles minimales concernant la définition des infractions et sanctions pénales dans le domaine des infractions terroristes et des infractions liées, ainsi que des mesures pour la protection, le soutien et l'assistance à apporter aux victimes du terrorisme, est actuellement évaluée par la Commission.

À la fin de 2020, la Commission a attribué un nouveau contrat-cadre à un consortium pour le soutien stratégique à apporter dans le cadre du **réseau de sensibilisation à la radicalisation** (Radicalisation Awareness Network, RAN), pour compléter les travaux des praticiens du RAN et continuer à soutenir les décideurs politiques dans le domaine de la prévention en général. L'objectif consiste à renforcer les connaissances et les capacités des États membres en matière de communication stratégique, ainsi que la base de données probantes sous-tendant l'élaboration des politiques et les approches et mesures concrètes.

De plus, la Commission collabore avec les États membres pour lutter contre les idéologies extrémistes susceptibles de conduire à l'extrémisme violent. En 2021, les activités dans ce domaine sont concentrées sur les liens entre tous les types d'idéologies extrémistes violentes (y compris l'extrémisme de gauche, l'extrémisme de droite et l'extrémisme islamiste) et sur la radicalisation conduisant à l'autoségrégation. Plusieurs initiatives de sensibilisation ont été menées dans ce domaine ces derniers mois. Les activités du RAN ont été étendues aux Balkans occidentaux au moyen d'un contrat spécifique qui a débuté en janvier 2021.

Une autre priorité consiste à empêcher les terroristes d'acquérir du matériel pouvant servir d'armement. Le plan d'action de 2017 visant à améliorer la préparation aux **risques en matière de sécurité chimique, biologique, radiologique et nucléaire (risques CBRN)** a fait l'objet d'une étude portant sur la faisabilité d'une restriction d'accès à certains produits chimiques à haut risque, qui s'est achevée en juin 2021. La Commission a par ailleurs lancé des travaux préparatoires en vue de la tenue d'exercices et d'ateliers transfrontières sur la sécurité des sources radioactives et biologiques dans les hôpitaux et les laboratoires, prévus pour 2022. La mise en œuvre du plan d'action en matière de risques CBRN est soutenue par des projets cofinancés par le Fonds pour la sécurité intérieure, qui a sélectionné des initiatives

[82] COM(2021) 262. Ces orientations abordent également la question spécifique de l'infodémie liée à la COVID-19.

[83] Communication de la Commission intitulée «Programme de lutte antiterroriste pour l'UE: anticiper, prévenir, protéger et réagir» [COM(2020) 795].

telles que le projet Safe Stadium[84], qui porte sur la protection et la préparation face aux risques CBRN dans les grands espaces sportifs tels que les stades de football. Une nouvelle législation sur la commercialisation et l'utilisation de précurseurs d'explosifs est entrée en vigueur le 1er février 2021. Sa mise en œuvre est en bonne voie et la Commission continue d'aider toutes les parties prenantes à s'acquitter de leurs obligations.

La coopération face aux menaces telles que les risques CBRN fait partie intégrante du lien intrinsèque entre la sécurité extérieure et la sécurité intérieure de l'Union. Les instruments de financement extérieur de l'UE soutiennent les efforts visant à renforcer la gouvernance et la coopération mondiales et régionales en matière de détection et d'atténuation des risques CBRN, sur la base de l'expérience positive acquise, par exemple, dans le cadre de l'initiative relative aux centres d'excellence de l'UE pour l'atténuation des risques CBRN et du programme de contrôle des exportations de biens à double usage. À ce jour, un plan d'action national de gestion des risques CBRN a été préparé dans 34 pays et a été officiellement adopté dans 10 pays.

Santé et terrorisme

Le programme «L'UE pour la santé»[85] soutient les actions visant à prévenir les menaces transfrontières pour la santé, à s'y préparer et à y faire face.

Le troisième programme de l'UE dans le domaine de la santé cofinance l'action de **préparation du secteur de la santé face aux attentats terroristes**[86], une action lancée en mai 2021 et menée conjointement avec les autorités sanitaires de l'UE. Elle vise à protéger les citoyens de l'UE contre les crises sanitaires intentionnelles, en comblant les lacunes en matière de préparation du secteur de la santé et en renforçant la coopération intersectorielle (santé, sécurité et protection civile) en cas d'attentat terroriste biologique et/ou chimique.

Le programme dans le domaine de la santé pour la période 2017-2021 a permis de renforcer les capacités de préparation et de réaction du secteur de la santé face aux menaces chimiques et biologiques. L'action conjointe de **renforcement de la mise en œuvre du règlement sanitaire international et de la préparation dans l'UE**[87] couvre un réseau de 41 laboratoires de référence pour les agents hautement pathogènes.

La lutte contre la menace que représentent les **combattants terroristes étrangers** de retour en Syrie et en Iraq demeure un élément important de la lutte contre le terrorisme et une priorité dans la prévention de la radicalisation. Comme convenu dans les orientations stratégiques sur une approche coordonnée de l'UE en matière de prévention de la radicalisation pour 2021, la Commission s'est attelée à quatre grandes priorités: les enfants de retour dans leur pays d'origine; le renforcement et la sécurisation du processus de retour (rapatriement, poursuites et réintégration); les compétences des professionnels participant à la réintégration des enfants de retour dans leur pays d'origine; et les femmes de retour dans leur

[84] https://ec.europa.eu/info/funding-tenders/opportunities/portal/screen/opportunities/projects-details/31077817/101034226/ISFP

[85] Établi par le règlement (UE) 2021/522.

[86] Action conjointe de préparation du secteur de la santé face aux attentats terroristes (https://ec.europa.eu/chafea/health/funding/joint-actions/documents/ja-2019-presentation-03_en.pdf).

[87] Strengthened International Health Regulations and Preparedness in the EU — SHARP JA (https://sharpja.eu/wp7/).

pays d'origine. En ce qui concerne les prisons et les camps de personnes déplacées dans le nord-est de la Syrie, et en accord avec les États membres, le SEAE et la Commission étudient de nouveaux moyens de renforcer l'assistance dans la région afin de contribuer à améliorer les conditions de vie et de tenter de mettre un terme à la radicalisation.

La Commission a récemment achevé la mise à jour de l'analyse des données relatives à la lutte contre le terrorisme et à la lutte contre l'extrémisme violent/la prévention de ce phénomène. La cartographie révèle que l'ampleur et la rapidité du financement consacré à ces activités au titre des instruments de financement extérieur de l'UE ont été impressionnantes[88]. Au 1er janvier 2021, un total de 99 actions d'anticipation, de prévention, de réaction et de protection dans le domaine de la lutte contre le terrorisme étaient en cours dans des pays tiers pour un total de 501 millions d'euros (soit une augmentation de 8 % par rapport à l'année précédente) pour mettre en œuvre les priorités du programme de lutte antiterroriste pour l'UE et des conclusions du Conseil sur la lutte contre le terrorisme.

D'autres mesures ont été prises pour favoriser et renforcer les partenariats et la coopération en matière de lutte contre le terrorisme avec les pays de notre voisinage et au-delà, en tirant parti du savoir-faire du réseau des experts de l'UE en matière de sécurité et de lutte contre le terrorisme. Au cours des derniers mois, la mise en œuvre du plan d'action conjoint relatif à la lutte contre le terrorisme avec les partenaires des Balkans occidentaux a progressé, malgré certains retards dus à la pandémie et à la dynamique politique interne des partenaires.

L'UE a continué à utiliser son cadre de sanctions contre le terrorisme durant la période visée par le présent rapport. En février 2021, le Conseil a achevé le réexamen de la liste de l'UE en matière de terrorisme[89] et une nouvelle désignation a été adoptée en avril 2021 dans le cadre du régime de sanctions autonomes de l'UE à l'encontre de l'EIIL (Daech) et d'Al-Qaida[90].

Enfin, en mai 2021, Eurojust et le réseau européen ont coorganisé la 6e Journée européenne de lutte contre l'impunité, l'accent étant mis sur les grands crimes internationaux commis en Syrie par des organisations terroristes et par le régime syrien. Les coorganisateurs de cette journée se sont appuyés sur les travaux entrepris depuis l'année dernière pour soutenir les poursuites cumulées à l'encontre des combattants terroristes étrangers pour des infractions liées au terrorisme et pour des crimes internationaux. Cette journée a également démontré qu'il est essentiel de renforcer la coopération judiciaire entre les États membres pour identifier et poursuivre les criminels de guerre présents dans l'UE.

2. Lutte contre la criminalité organisée

[88] L'UE apporte un soutien considérable à toutes les initiatives du Forum mondial de lutte contre le terrorisme, dont l'Institut pour la justice et l'état de droit, et au Fonds mondial pour la mobilisation et la résilience communautaire afin de soutenir les activités de lutte contre l'extrémisme violent et de prévention de ce phénomène dans plusieurs pays revêtant une importance stratégique pour l'UE.

[89] Décision (PESC) 2021/142 du Conseil du 5 février 2021 portant mise à jour de la liste des personnes, groupes et entités auxquels s'appliquent les articles 2, 3 et 4 de la position commune 2001/931/PESC.

[90] Décision (PESC) 2021/613 du Conseil du 15 avril 2021 concernant des mesures restrictives à l'encontre de l'EIIL (Daech) et d'Al-Qaida et de personnes, groupes, entreprises et entités associés et règlement d'exécution (UE) 2021/612 du Conseil du 15 avril 2021.

Le rapport 2021 sur l'évaluation de la menace que représente la grande criminalité organisée dans l'Union européenne (SOCTA)[91] a mis en lumière la menace persistante que représente la criminalité organisée et sa complexité croissante. La criminalité organisée est transnationale: 65 % des groupes criminels organisés sont composés de membres de diverses nationalités et sept sur dix sont actifs dans plus de trois pays. Le paysage de la criminalité organisée dans l'UE se caractérise par un environnement en réseau dans lequel différents groupes coopèrent entre eux et avec des fournisseurs de services criminels. Tandis que 60 % des réseaux criminels recourent à la violence dans le cadre de leurs activités criminelles, pratiquement toutes les activités criminelles comportent désormais une composante en ligne. Le risque d'infiltration de l'économie légale par la criminalité organisée est également en augmentation: selon les estimations, plus de 80 % des groupes criminels organisés utilisent des structures commerciales légales pour mener des activités criminelles.

Les criminels exploitent les vulnérabilités économiques créées par la pandémie

À la lumière des enseignements tirés des crises précédentes, on peut s'attendre à ce qu'une situation économique instable, caractérisée par une augmentation de la pauvreté et des inégalités sociales, représente un terreau fertile pour la grande criminalité organisée.

Les entreprises opérant dans des secteurs confrontés à des pressions économiques particulièrement négatives, tels que les secteurs de l'hôtellerie, de la restauration et du tourisme, sont de plus en plus vulnérables à l'infiltration par la criminalité[92].

En 2020, le centre d'Europol sur la grande criminalité organisée (ESOCC) a reçu et traité plus de 35 183 messages opérationnels dans les sept domaines qu'il couvre[93], soit plus de la moitié (57 %) des messages opérationnels d'Europol. L'ESOCC a assisté les États membres dans 837 opérations, soit une augmentation de 41 % comparativement à 2019. Ces chiffres reflètent l'intensification des activités des groupes criminels organisés et l'augmentation des demandes introduites par les États membres pour qu'Europol leur apporte une aide dans ce domaine. L'ESOCC a organisé et coordonné 11 cellules opérationnelles coordonnant des efforts de renseignement et d'enquête à l'encontre de 60 cibles de grande importance, des membres présumés d'organisations criminelles présentant un risque particulièrement élevé, et 21 de ces personnes ont été arrêtées.

Pour aider à faire face aux défis de plus en plus nombreux, la Commission a adopté en avril la **stratégie de l'UE visant à lutter contre la criminalité organisée** (2021-2025)[94]. Cette stratégie définit des actions prioritaires pour renforcer l'application du droit et la coopération judiciaire, garantir l'efficacité des enquêtes en vue de désorganiser les structures de la criminalité organisée et lutter contre les formes de criminalité hautement prioritaires, cibler les profits générés par la criminalité organisée et adapter les services répressifs et l'appareil judiciaire à l'ère numérique. La Commission a également publié la «plateforme

[91] https://www.europol.europa.eu/activities-services/main-reports/european-union-serious-and-organised-crime-threat-assessment

[92] D'après la contribution du groupe de travail sur les menaces criminelles liées à la COVID-19 et les réponses apportées par les services répressifs lors de sa 1re réunion; Europol 2020, Enterprising criminals: Europe's fight against the global networks of financial and economic crime.

[93] Le trafic de migrants, les groupes criminels organisés à haut risque, la criminalité environnementale, la criminalité organisée contre les biens, le trafic de drogue, la traite des êtres humains, et le trafic d'armes et d'explosifs.

[94] COM(2021) 170.

pluridisciplinaire européenne contre les menaces criminelles» (EMPACT)[95]. Elle explique comment tirer le meilleur parti du potentiel d'EMPACT et en faire un instrument phare pour la coopération opérationnelle pluridisciplinaire et interservices dans le cadre de la lutte contre la criminalité organisée. En outre, la Commission est étroitement associée à la préparation en cours du prochain cycle EMPACT, qui couvrira la période 2022-2025.

Lutte contre la traite des êtres humains

La traite des êtres humains est une forme de criminalité très lucrative qui génère d'énormes profits pour les criminels au détriment des victimes et de la société dans son ensemble. En avril, la Commission a adopté la stratégie de l'UE visant à lutter contre la traite des êtres humains (2021-2025)[96]. Étant donné que la traite des êtres humains est souvent le fait de groupes organisés, cette stratégie est étroitement liée à la stratégie de l'UE visant à lutter contre la criminalité organisée. La stratégie de lutte contre la traite des êtres humains propose des initiatives en termes de législation, de politiques et de cadre opérationnel afin de lutter contre la traite des êtres humains depuis la prévention jusqu'à la condamnation des criminels, en faisant de la protection des victimes une priorité à tous les stades, ainsi qu'en accordant une attention particulière aux femmes et enfants victimes et à la traite des êtres humains à des fins d'exploitation sexuelle. Les priorités consistent à réduire la demande qui alimente la traite des êtres humains; briser le modèle criminel pour mettre fin à l'exploitation des victimes; protéger et soutenir les victimes et leur donner des moyens d'agir; et aborder la dimension internationale de cette forme de criminalité. Cette stratégie a fait suite à un rapport d'Eurojust présentant 18 recommandations visant à soutenir les États membres non seulement dans les enquêtes, les poursuites et la coopération judiciaire dans les affaires de traite des êtres humains, mais également dans l'identification, le sauvetage et la protection des victimes[97].

Lutte contre les drogues illicites

À la suite de l'adoption de la stratégie antidrogue de l'UE pour la période 2021-2025, les discussions sur le plan d'action y afférent se poursuivent, dans l'optique de leur adoption par le Conseil d'ici à la fin de la présidence portugaise. La législation sur les nouvelles **substances psychoactives**, qui est pleinement entrée en vigueur en novembre 2018, a été suivie d'un acte délégué visant à inclure deux nouvelles substances psychoactives dans la définition des drogues[98].

Le rapport d'Eurojust sur le trafic de drogue publié en avril 2021[99] met en lumière l'augmentation de la production de drogues de synthèse et de l'utilisation de l'internet

---

[95] 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 réunit différentes parties prenantes afin d'améliorer et de renforcer le cas échéant 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 [SWD(2021) 74].

[96] Communication de la Commission relative à la stratégie de l'UE visant à lutter contre la traite des êtres humains 2021-2025 [COM(2021) 171].

[97] Ce rapport est disponible à l'adresse suivante: https://www.eurojust.europa.eu/eurojust-report-trafficking-human-beings

[98] C(2021) 1570; la période de contrôle du Parlement européen et du Conseil prendra fin à la mi-mai.

[99] Ce rapport est disponible à l'adresse suivante: https://www.eurojust.europa.eu/eurojust-report-drug-trafficking.

clandestin pour leur vente, ce qui pose des problèmes juridiques aux procureurs de l'UE. Ce rapport formule des recommandations en matière de renforcement des enquêtes financières, de recouvrement des avoirs et de coopération judiciaire, y compris avec les pays tiers. En mars 2021, à l'occasion du dialogue annuel UE - États-Unis sur la lutte contre le trafic de drogue, Eurojust a présenté des problèmes clés et des exemples de coopération judiciaire fructueuse entre les États membres et les États-Unis dans des affaires de trafic de drogue. La première réunion du dialogue UE-Chine sur la lutte contre le trafic de drogue a eu lieu le 22 janvier 2021 et a porté sur la coopération dans ce domaine. L'UE a participé à la 64e session de la Commission des stupéfiants des Nations unies et a réitéré son appel à l'accélération de la mise en œuvre de l'ensemble des engagements pris par la communauté internationale pour remédier à la situation mondiale en matière de drogues.

Lutte contre le trafic d'armes à feu illégales

La directive codifiée sur les armes à feu[100] est entrée en vigueur en avril 2021 et la Commission y a donné suite en adoptant des règles sur l'échange systématique, par voie électronique, d'informations relatives au refus d'octroyer des autorisations d'acquérir ou de posséder certaines armes à feu[101]. Celles-ci devraient s'appliquer à partir du 31 janvier 2022 et permettront aux autorités nationales compétentes de savoir si un demandeur d'une autorisation de détention d'une arme à feu s'est vu refuser une autorisation similaire dans un autre État membre. Ces règles empêcheront ainsi les demandeurs de rechercher le territoire qui leur est le plus favorable dans le but de contourner les interdictions de détention d'armes à feu.

La Commission soutient par ailleurs un projet pilote visant à établir un suivi en temps réel des incidents liés aux armes à feu dans l'ensemble de l'UE afin de dresser un tableau actualisé en permanence. Pour faciliter les missions des services répressifs, la Commission guide l'action relative à la mise en place et au développement de points focaux sur les armes à feu au niveau national.

En ce qui concerne la coopération internationale, la Commission a activement soutenu la participation constructive de la Turquie aux activités opérationnelles d'EMPACT liées à la menace que représentent les armes d'alarme et de signalisation convertibles. Elle a également contribué à ce que la question du trafic d'armes à feu soit remise à l'ordre du jour de la coopération avec les pays du Moyen-Orient et d'Afrique du Nord. En outre, la Commission a joué un rôle très actif dans la coopération opérationnelle avec l'Europe du Sud-Est, notamment en préparant une opération conjointe entre les États membres et les partenaires des Balkans occidentaux et en organisant des réunions régionales des commissions sur les armes légères et de petit calibre.

Le programme de l'UE sur les flux illicites mondiaux[102] a continué d'être un mécanisme efficace pour la coordination de l'action transrégionale de lutte contre la criminalité organisée et pour le renforcement des capacités de plus de 80 pays partenaires dans le monde à démanteler le trafic de marchandises illicites, en mettant l'accent sur les stupéfiants et les

[100] Directive (UE) 2017/853 relative au contrôle de l'acquisition et de la détention d'armes.

[101] Directive déléguée C(2021) 3400 du 21 mai 2021 établissant les modalités détaillées de l'échange systématique, par voie électronique, d'informations relatives au refus d'octroyer des autorisations d'acquérir ou de posséder certaines armes à feu.

[102] https://illicitflows.eu/

armes à feu. Il a également aidé les agences et les États membres de l'UE à avoir une portée plus large en matière répressive.

Lutte contre la criminalité financière

Dans le cadre de la lutte contre le risque d'infiltration de l'économie légale par la criminalité organisée, les États membres sont tenus de transposer d'ici à août 2021 la directive de 2019 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[103]. La Commission suivra de près la transposition et l'application effective de cette directive.

En mai et juin 2021, deux réunions de consultation ont eu lieu avec les États membres sur la révision de la décision du Conseil relative aux bureaux de recouvrement des avoirs[104] et de la directive sur la confiscation[105]. Ces discussions ont souligné la valeur ajoutée de ces instruments pour l'amélioration du recouvrement des avoirs dans l'Union et l'importance d'une gestion efficace des avoirs confisqués, dans le plein respect des droits fondamentaux, ainsi que la nécessité d'améliorer la coopération tout au long du processus de recouvrement des avoirs.

Une nouvelle législation relative aux contrôles de l'argent liquide entrant dans l'UE ou sortant de l'UE s'applique depuis le 3 juin 2021[106] et une législation d'exécution essentielle qui établit des procédures et des règles techniques est en place depuis mai[107]. Une autre législation d'exécution visant à établir des critères pour le cadre commun de gestion des risques en matière de mouvements d'argent liquide est en cours d'élaboration.

Le Parquet européen a pris ses fonctions d'enquête et de poursuites le 1er juin 2021. Désormais, le Parquet européen enquête sur les infractions portant atteinte aux intérêts financiers de l'Union et engage des poursuites en la matière. Les infractions qu'il recherche et poursuit incluent la fraude à la TVA liée au territoire de deux États membres ou plus, ayant entraîné un préjudice total d'au moins 10 millions d'euros. Chaque année, la fraude fait perdre des milliards d'euros de recettes de TVA aux États membres.

Lutte contre la criminalité environnementale

La **directive 2008/99/CE relative à la criminalité environnementale** est le principal instrument juridique de l'UE pour protéger l'environnement par le droit pénal. Des consultations approfondies sont en cours pour la révision du texte de la directive afin d'en améliorer la mise en œuvre et de renforcer le fonctionnement de la chaîne répressive

[103] Directive (UE) 2019/1153 du 20 juin 2019 fixant les règles 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.

[104] Décision 2007/845/JAI du Conseil du 6 décembre 2007 relative à la coopération entre les bureaux de recouvrement des avoirs des États membres en matière de dépistage et d'identification des produits du crime ou des autres biens en rapport avec le crime.

[105] Directive 2014/42/UE du 3 avril 2014 concernant le gel et la confiscation des instruments et des produits du crime dans l'Union européenne.

[106] Règlement (UE) 2018/1672 relatif aux contrôles de l'argent liquide entrant dans l'Union ou sortant de l'Union.

[107] Règlement d'exécution (UE) 2021/776 de la Commission du 11 mai 2021 établissant des modèles pour certains formulaires ainsi que des règles techniques pour l'échange effectif d'informations.

(détection, enquête, poursuites, procédure pénale). La lutte contre la criminalité environnementale est également menée dans le cadre du forum sur le respect de la législation environnementale et la gouvernance environnementale[108], dont les réunions de janvier et juin 2021 ont porté sur la révision de la directive et sur la lutte contre la criminalité environnementale en général.

Lutte contre le trafic de biens culturels

La législation de l'UE relative à l'importation de biens culturels vise à mettre un terme aux importations de biens culturels exportés illicitement depuis leur pays d'origine. Des dispositions d'application sont en cours d'adoption pour la mise en place d'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 l'accomplissement des formalités d'importation. La règle de l'interdiction générale prévue par le règlement[109] est entrée en vigueur le 28 décembre 2020, permettant aux autorités douanières des États membres de contrôler les envois susceptibles de contenir des biens culturels exportés illicitement à partir de leur pays d'origine et de prendre des mesures le cas échéant.

V. Un solide écosystème européen de la sécurité

1. Coopération et échange d'informations

La stratégie pour l'union de la sécurité définit la manière dont l'action de l'UE peut contribuer de manière substantielle à la réponse aux menaces transfrontières et transsectorielles de plus en plus complexes pour la sécurité, en fournissant aux acteurs de la sécurité dans les États membres les outils et les informations dont ils ont besoin.

Europol joue un rôle central à cet égard. La proposition de la Commission adoptée en décembre dernier en vue de moderniser et de renforcer le **mandat d'Europol**[110] répond aux contraintes spécifiques auxquelles Europol est confronté aujourd'hui, telles que ses relations avec le secteur privé. En outre, la Commission propose d'habiliter Europol à introduire dans le système d'information Schengen des signalements concernant des terroristes et d'autres criminels sur la base d'informations provenant de pays tiers. Cette proposition renforcera la capacité d'Europol à aider les États membres à lutter contre les formes graves de criminalité et le terrorisme. La Commission espère l'adoption rapide, par le Parlement européen et le Conseil, de leurs positions afin que les trilogues puissent être entamés sous la présidence slovène.

L'**UE et Interpol** entretiennent déjà depuis longtemps une coopération étroite. Interpol est un partenaire essentiel de l'UE en matière de sécurité intérieure et extérieure, qui inclut la lutte contre le terrorisme et la criminalité organisée, ainsi qu'en matière de gestion intégrée des frontières. La Commission a proposé des négociations en vue de renforcer davantage la coopération opérationnelle et stratégique au moyen d'un accord de coopération[111].

[108] Assurance de la conformité — Législation — Environnement — Commission européenne (europa.eu)
[109] Règlement (UE) 2019/880 du 17 avril 2019 concernant l'introduction et l'importation de biens culturels.
[110] COM(2020) 769 et COM(2020) 791.
[111] COM(2021) 177.

Sur le plan opérationnel, les préparatifs en vue de la pleine mise en œuvre de la révision du **système d'information Schengen** (SIS) sont en cours, l'objectif étant de mener à bien toutes les activités d'essai requises d'ici à la fin de 2021. En mars 2021, Europol a été connecté au relais de messagerie Sirene[112]. À la fin de 2020, la plupart des États membres avaient déployé la nouvelle fonctionnalité de recherche d'empreintes digitales dans le SIS[113].

Une modification de la législation est en cours pour améliorer la capacité d'**Eurojust** à établir des liens entre des procédures parallèles dans les affaires de terrorisme transfrontières[114]. En parallèle, Eurojust a continué ses activités de suivi opérationnel et de coordination sur la base des informations transmises par l'intermédiaire du registre judiciaire européen antiterroriste, qui a été mis en place dans le but de trouver des liens dans les procédures judiciaires visant des infractions terroristes dans les États membres. Jusqu'à présent, l'expérience acquise au moyen de ce registre révèle une nette augmentation du volume d'informations transmises à Eurojust, et certains liens entre des procédures précédemment inconnus des autorités nationales ont déjà été détectés. Le registre judiciaire antiterroriste a également apporté d'importantes améliorations au niveau de l'échange d'informations dans les procédures antiterroristes.

Les travaux préparatoires en vue de la mise en place de la **plateforme collaborative pour les équipes communes d'enquête (ECE)** ont commencé. Des consultations sur la conception de cette plateforme sont en cours avec les États membres, le secrétariat du réseau des ECE, Eurojust, Europol et l'OLAF. Depuis avril 2021, Eurojust apporte aussi une assistance financière aux ECE pour des actions urgentes et/ou imprévues ne relevant pas du champ d'application du régime de financement ordinaire[115].

Les **données des dossiers passagers** (PNR) constituent une source importante d'informations pour l'identification des personnes présentant des risques pour la sécurité. Sur la base des informations qu'elle a recueillies pour préparer un réexamen de la législation[116], la Commission aide les États membres à améliorer l'utilisation des données PNR et à approfondir la coopération[117]. La majorité des unités nationales de renseignements passagers sont désormais pleinement opérationnelles et le traitement des données PNR est un outil important pour les services répressifs nationaux dans leur lutte contre le terrorisme et les formes graves de criminalité, malgré la diminution du nombre de passagers aériens pendant la pandémie.

Les travaux se sont également intensifiés sur le front international. L'accord de commerce et de coopération entre l'UE et le Royaume-Uni[118] a été signé le 30 décembre 2020 et est entré en vigueur au mois de mai. Cet accord couvre l'échange de données PNR et leur utilisation aux fins de la lutte contre le terrorisme et les formes graves de criminalité. La Commission a

[112] Supplément d'information requis à l'entrée nationale. Chaque pays de l'UE exploitant le SIS a mis en place un bureau Sirene national chargé des échanges de suppléments d'information et de la coordination des activités liées aux signalements SIS.
[113] Système automatisé de reconnaissance d'empreintes digitales.
[114] Décision 2005/671/JAI du Conseil et règlement (UE) 2018/1727.
[115] https://www.eurojust.europa.eu/eurojust-launches-new-scheme-urgent-jit-funding
[116] COM(2020) 305 concernant la directive (UE) 2016/681.
[117] La Slovénie est le dernier État membre dont les mesures nationales de transposition de la directive sur les données PNR sont examinées par la Commission, tous les autres États membres ayant pleinement transposé cette directive.
[118] JO L 444 du 31.12.2020, p. 309.

adopté des rapports[119] sur l'évaluation conjointe des accords internationaux existants en matière de données PNR conclus avec les États-Unis et avec l'Australie, ainsi que sur l'examen conjoint de l'accord UE-Australie. Dans l'ensemble, ces rapports ont confirmé les avantages de l'utilisation des données PNR, leur efficacité dans la réalisation des objectifs poursuivis et le caractère unique des informations fournies par les données PNR. En janvier 2021, le Conseil a adopté la position de l'Union[120] favorable à l'adoption, par l'Organisation de l'aviation civile internationale (OACI), d'un nouvel ensemble de normes et de pratiques recommandées en matière de traitement et de protection des données PNR. Le 28 février 2021, la décision de l'OACI est devenue opérationnelle et contraignante pour tous ses membres[121]; elle constitue désormais une base solide pour le traitement des données PNR dans le monde entier, dans le plein respect des droits fondamentaux.

Des négociations relatives à l'échange de données à caractère personnel entre Europol et certains pays tiers aux fins de la lutte contre les formes graves de criminalité et le terrorisme sont en cours. Les deux premiers cycles de négociations avec la Nouvelle-Zélande se sont déroulés dans une atmosphère constructive. Des progrès sont également à signaler dans les négociations avec la Turquie et des discussions constructives ont eu lieu avec la Tunisie. Des discussions exploratoires sont en cours au niveau technique avec plusieurs autres pays.

En mars 2021, le Conseil a adopté le mandat autorisant la Commission à entamer des négociations en vue de la conclusion d'accords entre l'UE et treize pays tiers[122] sur la coopération entre Eurojust et les autorités compétentes dans le domaine de la coopération judiciaire en matière pénale. Ces accords internationaux deviendront une pierre angulaire de la législation de l'UE en matière de sécurité et contribueront, à l'échelle mondiale, à une meilleure lutte contre la criminalité organisée.

Depuis 2012, avec plus de 4 millions de messages échangés chaque année, le **système européen d'information sur les casiers judiciaires (ECRIS)** garantit un échange électronique efficace d'informations sur les casiers judiciaires entre les États membres. La Commission a adopté un rapport sur le fonctionnement de l'ECRIS[123] et procède actuellement au suivi de ses conclusions avec les États membres. Les travaux relatifs à l'élaboration et à la mise en œuvre d'un système centralisé permettant d'identifier les États membres détenant des informations relatives aux condamnations concernant des ressortissants de pays tiers (ECRIS-TCN) sont en cours, l'objectif étant de faire en sorte que ce système soit opérationnel en 2023. Ce nouveau système complétera l'ECRIS en ce qui concerne l'échange d'informations sur les ressortissants de pays tiers condamnés dans l'UE.

2. *La contribution de frontières extérieures solides*

Une gestion efficace des frontières extérieures de l'UE est essentielle pour garantir la sécurité des citoyens. La stratégie de la Commission pour l'espace Schengen[124] prévoit dans ce domaine des actions visant à protéger l'intégrité de l'espace Schengen et à améliorer encore

[119] COM(2021) 17 final, COM(2021) 18 final et COM(2021) 19 final.
[120] JO L 37 du 3.2.2021, p. 6.
[121] Les États membres ont introduit une différence pour une partie des normes et pratiques recommandées (SARP) concernées.
[122] Algérie, Argentine, Arménie, Bosnie-Herzégovine, Brésil, Colombie, Égypte, Israël, Jordanie, Liban, Maroc, Tunisie et Turquie.
[123] COM(2020) 778 et SWD(2020) 378, 21 décembre 2020.
[124] COM(2021) 277.

son fonctionnement. La nouvelle architecture des systèmes d'information de l'UE pour la gestion de la sécurité, des frontières et des migrations, qui devrait soutenir les autorités nationales, est en développement. Il est essentiel que les États membres prennent sans tarder les mesures nécessaires pour respecter le calendrier de mise en œuvre convenu afin de réaliser ce projet ambitieux.

Les travaux relatifs à la mise en œuvre des **règlements sur l'interopérabilité** progressent et devraient déboucher sur une mise en œuvre complète d'ici à la fin de 2023. L'eu-LISA est en train de conclure la passation de marchés publics pour les différents composants de l'interopérabilité et la Commission coopère avec des experts pour élaborer un guide à ce sujet. Les préparatifs en vue de la mise en service du **système d'entrée/de sortie** (EES) sont en cours, l'objectif étant de terminer les essais et les formations au début de l'année 2022 pour une mise en service en mai 2022. Des préparatifs sont également en cours pour le **système européen d'information et d'autorisation concernant les voyages** (ETIAS), dont la mise en service est prévue pour la fin de 2022. Le Parlement européen et le Conseil viennent d'approuver la proposition visant à assurer la connexion entre ETIAS et les bases de données pertinentes de l'UE.

En décembre 2020, le Parlement européen et le Conseil sont parvenus à un accord provisoire sur la proposition de la Commission visant à réviser et à moderniser le **système d'information sur les visas** (VIS). Parmi les principaux avantages des modifications convenues figurent la réalisation de vérifications plus approfondies des antécédents des demandeurs de visa, la réduction des lacunes des informations en matière de sécurité au moyen d'un meilleur échange d'informations entre les États membres, l'élargissement du VIS pour qu'y soient inclus les visas de long séjour et les titres de séjour, et la lutte contre la traite des êtres humains par un abaissement de l'âge du relevé des empreintes digitales pour les mineurs. Le nouveau VIS devrait être opérationnel et pleinement interopérable avec les autres systèmes d'information nouveaux et améliorés d'ici à la fin de 2023.

Les premières équipes du **corps européen de garde-frontières et de garde-côtes** ont été déployées avec succès depuis le 1er janvier. Le contingent permanent, composé de 10 000 agents de Frontex et des autorités nationales, renforcera considérablement la sécurité des frontières, à mesure qu'il sera mis en place au cours des prochaines années pour atteindre sa pleine capacité. Le règlement d'exécution relatif au système européen de surveillance des frontières (Eurosur)[125], qui a été récemment adopté, améliorera davantage encore la connaissance de la situation et renforcera la capacité de réaction aux frontières extérieures afin de détecter, de prévenir et de combattre l'immigration illégale et la criminalité transfrontière,

Contrôles douaniers

La Commission œuvre actuellement à une nouvelle stratégie de gestion des risques en matière douanière, qui devrait renforcer l'approche structurée de la gestion des risques en matière douanière, améliorer l'efficacité des contrôles et réduire les risques pour l'UE et ses citoyens, tout en garantissant la compétitivité des entreprises légitimes de l'UE.

Dans le cadre de la stratégie et du plan d'action de l'UE pour le renforcement de la gestion des risques en matière douanière, la Commission œuvre aussi à un nouveau système de

[125] Règlement d'exécution (UE) 2021/581 de la Commission.

gestion anticipée des risques en matière douanière liés aux marchandises, qui permettra une analyse collaborative des risques en matière de sûreté et de sécurité avant l'arrivée des marchandises dans l'UE ou leur chargement en vue de leur transport vers l'UE[126].

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

L'innovation devrait être considérée comme un outil stratégique pour l'UE: elle a des effets horizontaux sur presque tous les aspects de la communauté de la sécurité et offre de nouveaux moyens de relever les défis posés par les technologies, de réduire la dépendance stratégique et de renforcer les chaînes d'approvisionnement. C'est pourquoi l'UE construit ses principaux projets de recherche en tenant compte de la dimension sécuritaire, de ses besoins et du rôle du secteur privé.

La création du **pôle d'innovation européen pour la sécurité intérieure** est en cours. Le programme **Horizon Europe** soutient les réponses de l'UE aux défis en matière de sécurité grâce à un financement de 1,6 milliard d'euros pour la période 2021-2027. En mars 2021, la Commission a adopté le premier plan stratégique pour Horizon Europe, qui définit des orientations stratégiques pour les quatre premières années: la recherche en matière de sécurité servira d'outil pour passer d'une approche réactive dans le domaine de la sécurité à une approche proactive, fondée sur la prospective et la prévention. Un nouveau programme de travail pour 2021-2022 a été adopté: celui-ci soutiendra la mise en œuvre de la dimension «sécurité intérieure» de la stratégie pour l'union de la sécurité, les dimensions «gestion des frontières» et «sécurité» des politiques en matière de migration et d'asile, ainsi que les politiques de l'UE en matière de réduction des risques de catastrophes.

Le financement de l'UE offre de nouvelles possibilités de renforcer l'innovation européenne à l'interface entre les utilisations civiles, spatiales et de la défense. En février 2021, la Commission a lancé le plan d'action sur les synergies entre les **industries civile, spatiale et de la défense**[127]. Trois projets phares ont été définis (sur les technologies des drones, la connectivité spatiale sécurisée et la gestion du trafic spatial). Ce plan d'action soutiendra les industries de la sécurité de l'UE au moyen de solutions innovantes et de pointe découlant de l'enrichissement mutuel et des synergies efficaces entre les industries civile, spatiale et de la défense.

Les technologies, données et services spatiaux sont devenus indispensables pour assurer la sécurité des Européens et contribuent de manière essentielle à la sauvegarde de nombreux intérêts stratégiques. Le **règlement relatif au programme spatial**[128], adopté en avril et doté d'un budget de 14,6 milliards d'euros, introduit une nouvelle composante pour les télécommunications gouvernementales par satellite, qui servira de tremplin pour la connectivité spatiale sécurisée de l'UE.

4. Compétences et sensibilisation

[126] La version 1, qui couvre les transports express aériens et les transports postaux, est entrée en service en mars. La version 2, qui couvrira le fret aérien général, est prévue pour mars 2023. La version 3, qui couvrira les transports maritimes, routiers et ferroviaires, est prévue pour 2024.

[127] COM(2021) 70.

[128] Règlement (UE) 2021/696 du 28 avril 2021 établissant le programme spatial de l'Union et l'Agence de l'Union européenne pour le programme spatial.

La connaissance des menaces qui pèsent sur la sécurité et les compétences pour y faire face sont essentielles pour bâtir une société plus résiliente caractérisée par des entreprises, des administrations et des citoyens mieux préparés. Le 9 février 2021, la 18e Journée pour un internet plus sûr s'est déroulée en ligne dans 170 pays, avec la présence virtuelle de jeunes ambassadeurs du programme Better Internet for Kids et de représentants de l'Alliance pour une meilleure protection des mineurs en ligne. Le plan d'action de l'UE en matière d'éducation numérique (2021-2027) comprend une action visant à aider les enseignants et le personnel de l'éducation à favoriser la culture numérique et à lutter contre la désinformation. Des lignes directrices seront élaborées et mises en œuvre dans l'UE en septembre 2022.

Une bonne connaissance de l'environnement numérique et le renforcement des compétences connexes dans les secteurs privé et public sont essentiels à une société résiliente et compétitive. Dans le cadre du programme pour une Europe numérique, un premier appel pour les pôles d'innovation numérique (PIN) européens[129] a été publié en mai, l'objectif étant de faire en sorte que les premiers pôles soient opérationnels dès le début de l'année 2022. Les PIN européens aideront les acteurs des secteurs privé et public en leur donnant accès à un savoir-faire technique et en leur permettant d'expérimenter, en stimulant l'adoption généralisée de l'intelligence artificielle, du calcul à haute performance et de la cybersécurité ainsi que d'autres technologies numériques par l'industrie (en particulier les PME et les entreprises à capitalisation moyenne) et par les organisations du secteur public en Europe.

Face à une situation en matière de sécurité qui ne cesse d'évoluer, les compétences des agents des services répressifs et des professionnels de la justice devraient être constamment mises à jour. Une évaluation du **CEPOL** s'achèvera au cours du second semestre de 2021. À la fin de 2020, la Commission a adopté la stratégie européenne de formation judiciaire pour la période 2021-2024[130] et a organisé une conférence des parties prenantes avec la présidence portugaise en mai 2021 afin de renforcer la formation des juges et des procureurs.

La sensibilisation est également au cœur de la stratégie de l'UE relative au **droit des victimes** (2020-2025), adoptée en juin 2020, qui vise à faire en sorte que toutes les victimes de la criminalité quels que soient l'endroit de l'UE où l'infraction a eu lieu et les circonstances dans lesquelles elle a été commise puissent pleinement se prévaloir de leurs droits. La première réunion plénière de la plateforme des droits des victimes a eu lieu en février 2021. Par ailleurs, la Commission évalue actuellement la directive concernant les droits des victimes et, si nécessaire, elle pourrait proposer des modifications législatives en 2022.

5. Le rôle des agences de l'UE

La stratégie pour l'union de la sécurité est fondée sur une approche qui englobe l'ensemble de la société et qui rassemble toutes les institutions, organisations et autorités jouant un rôle dans la protection de nos concitoyens. Au-delà du soutien et du savoir-faire qu'elles apportent aux États membres, les agences de l'UE jouent un rôle central dans la promotion de la coopération et de l'échange d'informations entre les autorités nationales des États membres au niveau opérationnel. Compte tenu de la multiplicité des menaces nouvelles et émergentes dans le paysage actuel, il convient d'encourager davantage les synergies entre les activités des agences de l'UE et leur coordination.

[129] https://digital-strategy.ec.europa.eu/en/activities/edihs
[130] COM(2020) 713.

Europol

Les rapports annuels d'Europol sur la criminalité organisée (SOCTA), le terrorisme (TE-SAT) et la criminalité organisée sur l'internet (IOCTA) fournissent des données et des analyses clés pour soutenir les activités stratégiques et opérationnelles dans le domaine de la sécurité. Europol contribue en outre au renforcement de l'efficacité opérationnelle globale des services répressifs en élargissant sa coopération avec des pays tiers aux fins de la lutte contre la criminalité et le terrorisme, de manière cohérente avec d'autres politiques et outils extérieurs de l'UE.

Le Centre opérationnel et d'analyse est le centre d'information d'Europol. Il suit de manière continue les opérations et l'évolution de la situation, assure la coopération avec les pays tiers et les organisations et déploie des experts sur le terrain. Il fournit également des analyses aux autres centres d'Europol et à d'autres organisations. Le Centre européen de lutte contre la grande criminalité organisée d'Europol aide les pays de l'UE à lutter contre les réseaux criminels internationaux impliqués dans le trafic de drogue, d'armes et d'explosifs, dans la criminalité contre les biens et dans la criminalité environnementale. Il héberge également le Centre européen chargé de lutter contre le trafic de migrants, qui cible et démantèle les réseaux criminels complexes et sophistiqués impliqués dans le trafic de migrants. Quant au Centre européen de lutte contre la criminalité financière et économique d'Europol, il est chargé d'apporter un soutien dans les affaires très sophistiquées de blanchiment de capitaux, d'escroquerie et de fraude menées contre des particuliers, des entreprises et le secteur public.

La contribution d'Europol est également fondamentale pour la coordination de l'approche de l'UE en matière de lutte contre le terrorisme. Europol a continué à apporter son aide aux États membres dans les enquêtes liées au terrorisme par l'intermédiaire du Centre européen de lutte contre le terrorisme (ECTC). Malgré les restrictions causées par la pandémie, l'ECTC a soutenu 776 opérations de lutte contre le terrorisme en 2020 (contre 632 en 2019). L'unité de signalement des contenus sur l'internet de l'UE à Europol a elle aussi continué à jouer un rôle crucial dans la surveillance des activités des groupes terroristes en ligne et des mesures prises par les plateformes, ainsi que dans la poursuite de l'élaboration du protocole européen de crise. Europol reste déterminé à aider les États membres à renforcer leurs capacités nationales de prévention des contenus à caractère terroriste en ligne, par l'organisation de journées d'action ciblées sur le signalement des contenus.

Eurojust

Au cours des premiers mois de 2021, Eurojust a soutenu plusieurs enquêtes et poursuites transfrontières contre des groupes criminels organisés spécialisés dans la fraude. Eurojust a également permis de saisir des actifs d'entreprises ou de contraindre à la fermeture administrative des entreprises impliquées dans un système de fraude[131].

Eurojust a soutenu d'importantes opérations internationales conjointes visant à démanteler des réseaux de cybercriminalité, notamment en ciblant les groupes criminels exploitant une application mobile interplateforme appelée Mobdro, qui facilitait la diffusion en continu

[131] https://www.eurojust.europa.eu/action-counter-italian-fuel-tax-fraud-worth-almost-eur-1-billion

d'œuvres audiovisuelles obtenues illégalement, dont des matches de football[132], ou l'un des logiciels malveillants les plus dangereux (Emotet), déployé pour compromettre les ordinateurs des victimes en vue d'infections par des tiers[133]. Eurojust a également dialogué avec des praticiens de la justice pour aider à recenser les défis juridiques et opérationnels liés aux enquêtes et poursuites concernant les infractions commises par des extrémistes de droite, des groupes terroristes et des acteurs isolés, ainsi que pour faciliter l'échange d'expériences[134].

Coopération entre agences

Au niveau opérationnel, Europol et Eurojust ont signé, le 23 décembre 2020, un accord de contribution[135] qui étendra leur partenariat en vue d'aider les services répressifs et les autorités judiciaires à avoir un accès transfrontière aux preuves électroniques. Eurojust et Europol ont également signé des accords de coopération bilatéraux avec le **Parquet européen** afin de réglementer leurs relations futures dans le but d'une coopération étroite pour mieux protéger les intérêts financiers de l'Union à l'intérieur et à l'extérieur des frontières de l'UE. Grâce à une étroite coopération entre Europol, Eurojust et le Réseau judiciaire européen, le projet Sirius[136] soutient les services répressifs et la communauté judiciaire de l'UE en proposant des formations et des lignes directrices pour améliorer la coopération (principalement entre l'UE et les États-Unis) en matière d'accès transfrontière aux informations électroniques. En mars, Eurojust et l'Office de l'Union européenne pour la propriété intellectuelle (EUIPO) ont convenu de renforcer leur coopération afin de contribuer à la lutte contre la contrefaçon et le piratage en ligne[137]. Ce nouvel accord, qui permettra de soutenir efficacement les affaires tout au long de leur cycle de vie, de la plainte pénale à une décision de justice, marque le début d'une nouvelle ère de coopération entre Eurojust, Europol et l'EUIPO.

ENISA

L'ENISA met en œuvre le cadre de **coopération structurée avec la CERT-UE**[138] afin d'exploiter les synergies et d'éviter les chevauchements des efforts dans l'exécution de sa mission dans le domaine de la coopération opérationnelle, sur la base d'un protocole d'accord signé en mars. Il s'ensuivra une augmentation de l'efficacité et de l'efficience du mécanisme de réaction de l'UE et un renforcement des capacités à long terme, et ce par l'intermédiaire d'un bureau local de l'agence à Bruxelles, chargé de favoriser la coopération avec d'autres institutions, organes et organismes de l'UE[139]. L'ENISA contribue aux mesures concrètes de mise en œuvre des nouvelles politiques en matière de cybersécurité. En mai, l'ENISA a transmis la proposition de premier système de certification de cybersécurité fondé sur des

[132] https://www.eurojust.europa.eu/eurojust-supports-spanish-action-against-illegal-streaming-football-matches
[133] https://www.eurojust.europa.eu/worlds-most-dangerous-malware-emotet-disrupted-through-global-action.
[134] https://www.eurojust.europa.eu/eurojust-expert-workshops-violent-right-wing-extremism-and-terrorism
[135] Europol coopère avec Eurojust dans le cadre du projet Sirius, qui comprend une plateforme interactive de partage des connaissances, accessible aux services répressifs et aux autorités judiciaires, et qui vise à élaborer et à diffuser des formations et des lignes directrices pour améliorer la coopération (principalement) entre l'UE et les États-Unis en matière d'accès transfrontière aux informations électroniques.
[136] https://www.europol.europa.eu/activities-services/sirius-project
[137] https://www.eurojust.europa.eu/stepping-cooperation-tackle-intellectual-property-crime
[138] L'équipe d'intervention en cas d'urgence informatique pour les institutions, organes et organismes de l'UE (CERT-UE) est composée d'experts en sécurité informatique des principales institutions de l'UE.
[139] C(2021) 4626.

critères communs[140] et, en juin, elle a lancé le processus de création d'un groupe de travail ad hoc sur la certification de cybersécurité des réseaux 5G[141].

Agence européenne de garde-frontières et de garde-côtes (Frontex)
Frontex joue un rôle crucial en aidant les États membres à gérer les frontières extérieures et les retours, contribuant ainsi à la sécurité de l'U. Le nouveau règlement[142] a fait de Frontex la plus grande agence de l'UE, sur le plan tant du personnel que des ressources financières.

Observatoire européen des drogues et des toxicomanies
L'Observatoire européen des drogues et des toxicomanies (OEDT) joue un rôle important en surveillant en permanence la situation des drogues dans l'UE afin de fournir aux institutions et aux États membres de l'UE les informations les plus récentes. Ses travaux récents ont porté en particulier sur les conséquences de la pandémie sur les marchés des stupéfiants, sur la consommation de drogue et sur les dommages et les services liés à la drogue[143].

VI. Conclusion

L'UE dispose d'une capacité unique pour faire face aux menaces et aux défis actuels en matière de sécurité, et elle se dote progressivement de moyens pour renforcer sa réaction. Avec son approche globale et dynamique, la stratégie pour l'union de la sécurité se veut de portée générale pour faire en sorte que chaque risque soit compris dans le contexte plus large des menaces, que le savoir-faire de toutes les parties prenantes contribue à la mise en place d'une UE plus sûre et plus résiliente et que tous les outils à notre disposition soient déployés efficacement et dans le respect des valeurs européennes et des droits fondamentaux.

La Commission aidera le Parlement européen et le Conseil à mener à bien les processus législatifs importants qui sont encore en cours dans le domaine de la sécurité, en veillant à ce que le niveau d'ambition corresponde aux défis auxquels l'UE est confrontée aujourd'hui et sera confrontée à l'avenir.

Afin de relever les défis mondiaux en matière de sécurité et de renforcer les liens avec les pays partageant sa vision, l'UE intensifiera également sa coopération avec les partenaires internationaux dans des domaines tels que la lutte contre le terrorisme et l'extrémisme, les actes de cybermalveillance, les menaces hybrides et d'autres risques communs en matière de sécurité. C'est ce qui ressort également de la déclaration adoptée lors du récent sommet UE - États-Unis[144].

Bien que l'UE continue à progresser selon un rythme régulier pour moderniser et adapter son cadre législatif afin de tenir compte des différentes dimensions de la sécurité, les règles doivent être correctement mises en œuvre. Dans le cadre de cette responsabilité commune, chaque État membre a son rôle à jouer pour assurer la sécurité de l'Europe dans son ensemble.

---

[140] Crossing a bridge: the first EU cybersecurity certification scheme is availed to the Commission — ENISA (europa.eu)
[141] Calling on you, 5G Experts! Join us on 5G Cybersecurity Certification — ENISA (europa.eu)
[142] Règlement (UE) 2019/1896.
[143] Rapport européen sur les drogues 2021 de l'OEDT, 9 juin 2021.
[144] Déclaration du sommet UE - États-Unis: Vers un partenariat transatlantique renouvelé, 15 juin 2021.