COMMISSION
EUROPÉENNE

Strasbourg, le 1.4.2025
COM(2025) 148 final

COMMUNICATION DE LA COMMISSION AU PARLEMENT EUROPÉEN, AU CONSEIL, AU COMITÉ ÉCONOMIQUE ET SOCIAL EUROPÉEN ET AU COMITÉ DES RÉGIONS

ProtectEU: une stratégie européenne de sécurité intérieure

1. ProtectEU: une stratégie européenne de sécurité intérieure

La sécurité est le socle sur lequel se construisent toutes nos libertés. La démocratie, l'état de droit, les droits fondamentaux, le bien-être des Européens, la compétitivité et la prospérité reposent tous sur notre capacité à garantir un niveau de sécurité élémentaire. En cette nouvelle ère marquée par les menaces sécuritaires, la capacité des États membres de l'UE à garantir la sécurité de leurs citoyens dépend plus que jamais de la mise en place d'une **approche européenne unifiée pour protéger notre sécurité intérieure**. Dans un paysage géopolitique changeant, l'Europe doit continuer de tenir sa promesse de paix durable.

Les premières mesures en vue de la mise en place d'un dispositif de sécurité européen ont déjà été prises. Ces dix dernières années, nous avons doté l'Union de mécanismes d'action collective plus performants dans les domaines de la coopération des services répressifs et judiciaires, de la sécurité aux frontières, de la lutte contre la grande criminalité organisée, de la lutte contre le terrorisme et l'extrémisme violent et de la protection des infrastructures critiques, physiques et numériques de l'UE. La bonne mise en œuvre des actes législatifs et des politiques antérieurs demeure essentielle.

La nature des menaces actuelles et le lien intrinsèque entre la sécurité intérieure et extérieure de l'UE nous obligent à aller plus loin.

L'état de la menace est inquiétant. La frontière entre les **menaces hybrides** et la guerre ouverte est floue. La Russie mène une campagne hybride, en ligne et hors ligne, contre l'UE et ses partenaires, dans le but d'ébranler et de fragiliser la cohésion sociale et les processus démocratiques, et de mettre à l'épreuve la solidarité de l'UE avec l'Ukraine. Des États étrangers hostiles et des acteurs soutenus par des États cherchent à infiltrer et à perturber nos infrastructures critiques et nos chaînes d'approvisionnement, à voler des données sensibles et à se positionner en vue de provoquer ultérieurement une désorganisation maximale. Ils utilisent la criminalité comme un service et les criminels comme des agents à leur solde. En outre, notre dépendance à l'égard des pays tiers concernant les chaînes d'approvisionnement nous rend plus vulnérables aux campagnes hybrides menées par des États hostiles.

De puissants **réseaux de criminalité organisée** prolifèrent en Europe. Alimentés en ligne, ils se propagent dans notre économie et nuisent à notre société, comme Europol l'a récemment souligné lors de la présentation de l'évaluation de la menace que représente la grande criminalité organisée dans l'UE (SOCTA)[1]. Une fois que la criminalité organisée s'est implantée dans une communauté ou un secteur économique, l'éradiquer devient un véritable parcours du combattant: un tiers des réseaux criminels les plus menaçants/dangereux sont actifs pendant plus de dix ans. Les cryptomonnaies et les systèmes financiers parallèles les aident à blanchir et à dissimuler leurs produits du crime.

Le **niveau de menace terroriste en Europe reste élevé.** Les crises régionales à l'extérieur de l'UE ont un effet d'entraînement et donnent aux acteurs terroristes, quelle que soit leur idéologie, de nouvelles raisons de recruter, de mobiliser ou de renforcer leurs capacités. Ils ciblent leurs efforts de radicalisation et de recrutement spécifiquement sur les groupes les plus vulnérables de nos sociétés, et en particulier sur certains jeunes. Ils poussent des acteurs isolés à commettre des attentats et provoquent une augmentation de l'extrémisme anti-système, dont l'objectif est de perturber l'ordre juridique démocratique.

Les **progrès technologiques** fulgurants nous permettent certes de nous doter d'outils essentiels pour renforcer notre dispositif de sécurité, mais les cyberattaques et la manipulation de l'information depuis l'étranger sont de plus en plus fréquentes, au moyen de nouvelles

[1] https://www.europol.europa.eu/cms/sites/default/files/documents/EU-SOCTA-2025.pdf

technologies telles que l'intelligence artificielle. Les enfants, les jeunes et les personnes âgées sont particulièrement vulnérables en ligne et la propagation de la haine sur le web constitue une menace pour la liberté d'expression et la cohésion sociale.

Nos vies sont devenues moins sûres, comme le ressentent de plus en plus d'Européens, dont la **perception de la sûreté et de la sécurité dans l'UE** s'est érodée au point que, lorsqu'on les interroge sur l'avenir, 64 % d'entre eux se déclarent inquiets pour la sécurité de l'UE.[2] Dans les entreprises aussi, l'inquiétude augmente; la mésinformation et la désinformation, la criminalité et les activités illicites, ainsi que le cyberespionnage figurent tous parmi les dix principaux risques recensés dans le Global Risks Report 2025[3] (Rapport sur les risques mondiaux 2025) publié par le Forum économique mondial.

Les Européens devraient **pouvoir vivre sans avoir peur**, que ce soit dans la rue, chez eux, dans les lieux publics, dans le métro ou sur l'internet. La protection des personnes – en particulier celle des plus vulnérables aux attentats qui ont tendance à toucher de manière disproportionnée les enfants, les femmes et les minorités, notamment les communautés juive et musulmane – est au cœur de l'action de l'UE en matière de sécurité. C'est essentiel pour construire des sociétés résilientes et cohésives.

La Commission met actuellement en place une **stratégie européenne de sécurité intérieure** afin de mieux contrer les menaces dans les années à venir. Grâce à des outils juridiques plus affûtés, une coopération plus approfondie et un partage accru des informations, nous renforcerons notre résilience et notre capacité collective à anticiper, prévenir et détecter les menaces pour la sécurité et à y répondre de manière efficace. Une approche unifiée de la sécurité intérieure peut aider les États membres à exploiter la puissance de la technologie pour renforcer, et non affaiblir, la sécurité, tout en promouvant un espace numérique sécurisé pour tous. En outre, elle permet une réaction commune des États membres aux changements politiques et économiques mondiaux qui ont des incidences sur la sécurité intérieure de l'Union.

Cette stratégie est guidée par **trois principes** et intègre au cœur de son action le respect de l'état de droit et des droits fondamentaux.

Premièrement, elle fixe pour ambition un changement de culture en matière de sécurité. Nous avons besoin d'**une approche englobant l'ensemble de la société**, qui associe tous les citoyens et tous les acteurs, y compris la société civile, le monde de la recherche, le monde universitaire et les entités privées. Les actions prévues dans la stratégie adoptent donc, dans la mesure du possible, une approche intégrée et multipartite.

Deuxièmement, **les considérations de sécurité doivent être intégrées et prises en compte dans l'ensemble des actes législatifs, des politiques et des programmes de l'UE**, y compris l'action extérieure de l'UE. Les actes législatifs, les politiques et les programmes devront être préparés, examinés et mis en œuvre dans une perspective de sécurité, en veillant à ce que les considérations de sécurité nécessaires soient prises en compte, afin de favoriser une approche cohérente et globale en matière de sécurité.

Enfin, pour que l'Europe soit sûre, sécurisée et résiliente, des **investissements importants de la part de l'UE, de ses États membres et du secteur privé** sont indispensables. Les priorités et les actions définies dans la présente stratégie nécessitent des ressources humaines et financières suffisantes pour assurer leur mise en œuvre. Comme le prévoit la communication intitulée «La voie vers le prochain cadre financier pluriannuel»[4], l'Europe devra augmenter les

[2] Flash Eurobarometer FL550: EU Challenges and Priorities.
[3] https://reports.weforum.org/docs/WEF_Global_Risks_Report_2025.pdf, p.17.
[4] COM(2025) 46 final.

dépenses publiques consacrées à la sécurité et promouvoir la recherche et l'investissement dans ce domaine, ce qui lui permettra de renforcer son autonomie stratégique.

La présente stratégie complète la **stratégie pour une union de la préparation**[5], qui définit une approche «tous risques» intégrée de la préparation aux conflits, aux catastrophes naturelles et d'origine humaine et aux crises, ainsi que le **livre blanc «Préparation de la défense européenne à l'horizon 2030»**[6], qui encourage le développement et l'acquisition de capacités de défense dans toute l'UE afin de dissuader les adversaires étrangers. La Commission proposera également un **bouclier européen de la démocratie**, destiné à renforcer la résilience démocratique dans l'Union. Ensemble, ces initiatives définissent une vision pour une UE sûre, sécurisée et résiliente.

Une nouvelle gouvernance européenne de la sécurité intérieure

La Commission travaillera en étroite collaboration avec les États membres et les organismes de l'UE pour perfectionner l'approche de l'UE en matière de sécurité intérieure, tant au niveau stratégique qu'opérationnel.

Pour y parvenir, il faut:

- **identifier systématiquement, d'emblée et tout long du processus de négociation, les potentielles implications que les initiatives nouvelles ou révisées de la Commission auront en termes de sécurité et de préparation;**
- **convoquer des réunions régulières du groupe de projet «sécurité intérieure de l'UE» de la Commission, assorties d'une collaboration stratégique intersectorielle au sein de la Commission;**
- **présenter des analyses des menaces pesant sur la sécurité intérieure, afin de soutenir les travaux du collège Sécurité;**
- **discuter, avec les États membres au sein du Conseil, de l'évolution des défis en matière de sécurité intérieure, sur la base de l'analyse des menaces, et échanger sur les principales priorités d'action;**
- **rendre compte régulièrement au Parlement européen et au Conseil de la mise en œuvre systématique des initiatives clés, afin de soutenir celle-ci et d'en permettre le suivi.**

2. Connaissance de la situation et analyse de la menace intégrées

Nous doterons l'UE de nouveaux moyens pour partager et combiner les informations et fournirons une analyse régulière des menaces pour la sécurité intérieure de l'UE, ce qui permettra de réaliser une évaluation globale des risques et des menaces.

La sécurité suppose d'abord une **anticipation efficace**. L'UE doit disposer d'une connaissance de la situation et d'une analyse de la menace qui soient complètes, suffisamment autonomes et actualisées. Le renseignement exploitable, que les États membres sont encouragés à compléter par la capacité unique d'analyse du renseignement (SIAC), qui est le point d'entrée unique pour le renseignement dans les États membres, est essentiel pour évaluer et contrer les menaces et, en définitive, guider l'action des pouvoirs publics et du législateur[7]. Nous devons exploiter l'**analyse fondée sur le renseignement** et l'**évaluation des menaces**, réalisées au niveau de l'UE, de manière plus efficace et dans un esprit de collaboration.

[5] JOIN(2025) 130 final.
[6] JOIN(2025) 120 final.
[7] Safer Together – Strengthening Europe's Civilian and Military Preparedness and Readiness, p. 23.

S'inspirant des diverses évaluations des risques et des menaces réalisées au niveau de l'UE et pour des secteurs spécifiques[8], la Commission préparera des **analyses régulières des menaces pour la sécurité intérieure de l'UE**, afin d'identifier les principaux défis en matière de sécurité, en vue de définir les priorités d'action en connaissance de cause. Ces analyses permettront d'élaborer une politique de sécurité interne souple et réactive, qui répondra efficacement à l'évolution des menaces, protégera mieux les personnes et les entreprises contre les attaques et facilitera des interventions ciblées en temps opportun. Ces analyses des menaces pour la sécurité intérieure de l'UE alimenteront également **l'évaluation complète (intersectorielle et tous risques) des risques et des menaces dans l'UE** élaborée par la Commission et la haute représentante, comme le prévoit la stratégie pour une union de la préparation.

La confiance et le traitement sécurisé sont essentiels pour le partage des informations, ce qui requiert une infrastructure fiable et sécurisée. Les institutions, organes et organismes de l'UE doivent veiller à pouvoir utiliser des **canaux de communication sécurisés** pour échanger, entre eux et avec les États membres, des informations sensibles et classifiées. Les investissements dans des **systèmes sécurisés interopérables** et des technologies fiables accroîtront l'autonomie de l'UE et sa capacité à gérer les crises et à assurer sa résilience opérationnelle. La Commission invite dès lors instamment les colégislateurs à finaliser les négociations sur la **proposition de règlement sur la sécurité de l'information dans les institutions, organes et organismes de l'Union**, en particulier pour disposer d'un cadre commun pour le traitement des informations sensibles non classifiées et des informations classifiées[9].

Pour assurer sa propre sécurité opérationnelle et sa connaissance de la situation, la Commission révisera le cadre de gouvernance de sa sécurité institutionnelle et mettra en place un **centre intégré d'opérations de sécurité (ISOC)** pour protéger les personnes, les biens matériels et les opérations sur tous les sites de la Commission. Elle renforcera également ses capacités opérationnelles et analytiques pour recenser et atténuer les menaces hybrides.

Comme le prévoit la stratégie pour une union de la préparation, les considérations relatives à la préparation et à la sécurité seront intégrées et prises en compte dans l'ensemble des actes législatifs, des politiques et des programmes de l'UE. Lors de l'élaboration ou de la révision d'actes législatifs, de politiques ou de programmes dans une optique de préparation et de sécurité, la Commission déterminera systématiquement les incidences potentielles de l'option privilégiée sur la préparation et la sécurité. À cet effet, des formations régulières seront organisées à l'intention des décideurs politiques au sein de la Commission.

Pour aider les États membres, la Commission examinera avec le Conseil l'évolution des défis en matière de sécurité intérieure et des principales priorités d'action, et l'informera régulièrement sur la mise en œuvre de la stratégie. Par ailleurs, la Commission informera le Parlement européen et les parties prenantes concernées de toutes les actions pertinentes auxquelles ils seront invités à participer.

[8] Les évaluations sectorielles des menaces qui alimenteront ce type d'analyse incluent l'évaluation de la menace que représente la grande criminalité organisée (SOCTA), le rapport sur la situation et les tendances du terrorisme dans l'UE (TE-SAT), le rapport conjoint de l'UE sur la cybersécurité (JCAR), et les futures analyses des menaces, des risques et des méthodes liées au blanchiment de capitaux et au financement du terrorisme qui seront réalisées par la Commission et l'Autorité de lutte contre le blanchiment de capitaux.
[9] COM(2022) 119 final

Actions clés:

La Commission va:

- **établir et présenter des analyses régulières des menaces pour faire face aux défis en matière de sécurité intérieure de l'UE.**

Les États membres sont instamment invités à:

- **intensifier l'échange de renseignement avec le SIAC et améliorer l'échange d'informations avec les organismes et organes de l'UE.**

Le Parlement européen et le Conseil sont invités à:

- **finaliser les négociations relatives à la proposition de règlement sur la sécurité de l'information dans les institutions, organes et organismes de l'Union.**

3. Renforcement des capacités de sécurité de l'UE

Nous mettrons au point de nouveaux outils destinés aux services répressifs, par exemple une agence Europol réorganisée, ainsi que des moyens plus efficaces de coordonner et d'assurer l'échange sécurisé de données et l'accès licite à celles-ci.

Afin de contrer les menaces en constante évolution, l'UE doit renforcer ses capacités de sécurité et favoriser l'innovation. Principaux acteurs de la lutte contre les menaces pesant sur la sécurité intérieure, les services répressifs et les autorités judiciaires doivent disposer des capacités et outils opérationnels appropriés pour agir promptement et efficacement. Il importe que les uns et les autres soient en mesure de communiquer et de se coordonner par-delà les frontières et entre leurs différents services, afin de pouvoir mener des actions efficaces de prévention, de détection, d'enquête et de poursuite.

Organismes et organes de l'UE chargés de la sécurité intérieure

Les organismes et organes de l'UE dans les domaines de la justice, des affaires intérieures et de la cybersécurité jouent un rôle essentiel au sein de l'architecture de sécurité de l'UE, rôle qui ne cesse de croître à mesure que leurs responsabilités s'étendent.

Aujourd'hui, 25 ans après sa création, **Europol** est plus que jamais au cœur du cadre de sécurité de l'UE. L'agence Europol appuie les enquêtes transfrontières complexes, facilite l'échange d'informations, conçoit des outils innovants pour les activités policières et met ses compétences pointues à la disposition des services répressifs. Plusieurs facteurs l'empêchent cependant de déployer tout son potentiel opérationnel de soutien aux activités d'enquête et opérationnelles pour lutter contre la criminalité transfrontière: ils vont d'un niveau insuffisant de ressources au fait que le mandat actuel de l'Agence ne couvre pas les nouvelles menaces pour la sécurité, telles que le sabotage, les menaces hybrides ou la manipulation de l'information. C'est la raison pour laquelle la Commission proposera **une révision ambitieuse du mandat d'Europol**, qui permettra d'en faire une agence de police véritablement opérationnelle, qui apportera un appui plus efficace aux États membres. Cette révision doit conforter l'expertise technologique d'Europol et sa capacité à soutenir les services répressifs nationaux, améliorer la coordination avec les autres organismes et organes et avec les États membres, consolider les partenariats stratégiques avec les pays partenaires et le secteur privé ainsi que renforcer le contrôle sur Europol.

Par ailleurs, la Commission œuvrera à **rendre les organismes et organes de l'UE encore plus efficaces et plus complémentaires dans le domaine de la sécurité intérieure, ainsi qu'à favoriser une coopération harmonieuse** entre eux.

Le mandat d'**Eurojust** sera, lui aussi, évalué et renforcé pour rendre la coopération judiciaire plus efficace, ce qui accroîtra la complémentarité de cette agence et d'Europol ainsi que la coopération entre elles. Il s'agira notamment d'améliorer l'efficience d'Eurojust ainsi que sa capacité à fournir une assistance et une analyse proactives aux autorités judiciaires des États membres. En outre, étant donné la compétence unique du **Parquet européen** en matière d'enquêtes et de poursuites concernant les infractions portant atteinte aux intérêts financiers de l'Union, la Commission étudiera les meilleurs moyens d'améliorer la capacité du Parquet européen à protéger les fonds de l'Union. Il s'agira notamment de renforcer la coopération entre le Parquet européen et Europol.

Un **échange d'informations efficient et sécurisé entre les services** est fondamental pour la coopération. Europol et Frontex doivent pouvoir échanger des informations rapidement, y compris à des fins opérationnelles, et ainsi donner suite à leur déclaration commune de janvier 2024[10]. L'**eu-LISA** joue un rôle central pour assurer le stockage sécurisé et la disponibilité des données en vue d'une meilleure coordination et d'un échange d'informations plus efficient entre les agences. L'**Agence des droits fondamentaux de l'Union européenne** apporte son expertise en matière de protection des droits fondamentaux au stade de l'élaboration et de la mise en œuvre des politiques de sécurité.

L'**Autorité de lutte contre le blanchiment de capitaux (ALBC)** est habilitée à recouper des informations, selon un système de concordance/non-concordance, avec celles mises à disposition par Europol, par le Parquet européen, par Eurojust et par l'Office européen de lutte antifraude, afin de réaliser des analyses communes de cas transfrontières.

L'**Agence de l'Union européenne pour la cybersécurité** (**ENISA**) joue un rôle primordial dans la mise en œuvre de la législation européenne en matière de cybersécurité. Lors de la **révision prochaine du règlement sur la cybersécurité**, la Commission évaluera le mandat de l'ENISA et proposera de le moderniser afin d'en renforcer la valeur ajoutée européenne.

La création proposée de l'**Autorité douanière de l'UE** et de la **plateforme des données douanières de l'UE** , au titre du train de mesures sur la réforme douanière de l'UE, permettra d'accroître la coopération entre les autorités douanières et les autres services répressifs. Les informations provenant de cette future plateforme et les données connexes fournies par Europol, Eurojust, le Parquet européen, l'OLAF, l'ALBC et Frontex, dans le cadre de leurs compétences respectives, permettront d'améliorer les analyses communes et contribueront à une meilleure cohérence des activités opérationnelles, en particulier aux frontières extérieures. La Commission encourage les colégislateurs à conclure rapidement les négociations sur la réforme douanière de l'UE et continuera à leur prêter son concours à cette fin.

La complémentarité accrue du Parquet européen, de l'OLAF, d'Europol, d'Eurojust, de l'ALBC et de l'autorité douanière de l'UE qu'il est proposé de créer sera également favorisée par les résultats du réexamen en cours de l'**architecture antifraude de l'UE**. La sécurité intérieure a tout à gagner de cette approche globale, axée sur une meilleure exploitation des moyens tant pénaux qu'administratifs, sur l'interopérabilité des systèmes informatiques et sur une meilleure coopération.

[10] https://www.europol.europa.eu/cms/sites/default/files/documents/europol-frontex_joint_statement_signed_31.1.2024.pdf.

Communication critique

À l'heure actuelle, les **systèmes de communication critique**[11] fonctionnent, dans la plupart des cas, de manière cloisonnée à l'échelle nationale. Cela signifie que les premiers intervenants ne peuvent souvent pas communiquer avec leurs homologues lorsqu'ils franchissent la frontière pour se rendre dans un autre État membre. Les communications entre différents types de premiers intervenants (par exemple, la police et les ambulances) sont également limitées dans certains États membres. Les normes qui régissent la plupart des systèmes ne satisfont pas aux exigences actuelles en matière de fonctionnalité et de résilience, ce qui restreint considérablement la capacité de réaction des premiers intervenants, en particulier par-delà les frontières.

Afin d'améliorer la capacité de réaction de l'UE aux crises, la Commission présentera une proposition législative visant à créer un **système de communication critique de l'UE (EUCCS)** qui permettra de relier, au sein de l'Union, les systèmes de communication critique de prochaine génération des États membres. L'objectif est de faire reposer l'EUCCS sur trois piliers stratégiques: la mobilité opérationnelle, une grande résilience et l'autonomie stratégique. L'initiative relative à la création de l'EUCCS, qui fixera des exigences harmonisées, permettra de moderniser les systèmes de communication critique des États membres, qui pourront ainsi fonctionner sans discontinuité. Elle prévoira également l'extension de la couverture de ces systèmes grâce au futur système multiorbital IRIS[2] [12]. Les projets financés par l'UE permettront de développer les capacités techniques de l'EUCCS, en s'appuyant principalement sur les fournisseurs européens de technologies, afin de favoriser l'autonomie stratégique de l'UE dans ce secteur sensible.

Accès licite aux données

Les services répressifs et les autorités judiciaires doivent être en mesure d'enquêter sur la criminalité et de prendre des mesures pour la combattre. De nos jours, presque toutes les formes de grande criminalité organisée laissent une empreinte numérique[13]. Quelque 85 % des enquêtes pénales reposent désormais sur la capacité des services répressifs à avoir accès aux informations numériques[14].

Dans son rapport final[15], le **groupe de haut niveau sur l'accès aux données aux fins d'une répression efficace** a mis en évidence qu'au cours de la dernière décennie, les services répressifs et le pouvoir judiciaire avaient perdu du terrain par rapport aux criminels, car ces derniers se procurent des outils et des produits fournis, depuis d'autres pays et territoires, par des prestataires dont les mesures privent ces derniers des moyens de coopérer sur des demandes licites dans des affaires criminelles particulières. Une coopération systématique entre autorités répressives et parties privées, fournisseurs de services compris, sera dès lors essentielle à l'avenir, dans le cadre des efforts qui viseront à déstabiliser les réseaux criminels les plus menaçants ainsi que leurs membres, au sein de l'Union et au-delà.

Alors que la numérisation se généralise toujours plus et offre aux criminels un arsenal croissant d'outils nouveaux, il est essentiel d'ériger un cadre d'accès aux données qui réponde à la

[11] À savoir les réseaux utilisés par les services répressifs, par les garde-frontières, par les autorités douanières, par la protection civile, par les pompiers, par les services médicaux d'urgence et par d'autres acteurs essentiels de la sécurité et de la sûreté publiques.

[12] Infrastructure de l'UE pour la résilience, l'interconnexion et la sécurité par satellite.

[13] https://www.europol.europa.eu/cms/sites/default/files/documents/EU-SOCTA-2025.pdf

[14] https://eur-lex.europa.eu/legal-content/FR/TXT/?uri=CELEX%3A52019PC0070R%2801%29&qid=1744713112287.

[15] Rapport final du groupe de haut niveau sur l'accès aux données aux fins d'une répression efficace - 15.11.2024, 4802e306-c364-4154-835b-e986a9a49281_en.

nécessité de faire respecter nos lois et de protéger nos valeurs. Dans le même temps, il est tout aussi essentiel de maintenir les systèmes numériques à l'abri de tout accès non autorisé, en vue de préserver la cybersécurité et d'offrir une protection contre les menaces émergentes qui pèsent sur la sécurité. Des cadres d'accès de ce type doivent également respecter les droits fondamentaux et assurer notamment une protection adéquate de la vie privée et des données à caractère personnel.

Ces dernières années, l'UE a pris des mesures visant aussi bien à lutter contre **la criminalité en ligne qu'à faciliter l'accès aux preuves numériques pour toutes les infractions**, en adoptant des règles relatives aux preuves électroniques qui seront intégralement applicables à partir du mois d'août 2026[16]. Ces règles seront complétées par des instruments internationaux d'échange d'informations et de preuves. Prochainement, la Commission proposera que la nouvelle **convention des Nations unies contre la cybercriminalité** soit signée et conclue.

Pour donner suite aux recommandations formulées par le groupe de haut niveau[17], la Commission présentera, au premier semestre de 2025, une **feuille de route exposant les mesures juridiques et pratiques** qu'elle propose de prendre **afin d'assurer un accès licite et effectif aux données**. Dans le prolongement de cette feuille de route, la Commission aura pour priorité d'effectuer une analyse d'impact des **règles européennes de conservation des données** et d'élaborer une **feuille de route technologique sur le chiffrement**, afin de recenser et d'évaluer les solutions technologiques qui permettraient aux autorités répressives d'accéder de manière licite aux données chiffrées, tout en préservant la cybersécurité et les droits fondamentaux.

Coopération opérationnelle

La Commission œuvrera avec les États membres, les organismes et organes de l'UE ainsi que les pays partenaires au renforcement de la coopération opérationnelle, indispensable à une approche plus efficace de la lutte contre la criminalité organisée transnationale et contre le terrorisme.

Principal cadre d'action commune de l'UE contre la grande criminalité organisée, la **plateforme pluridisciplinaire européenne contre les menaces criminelles (EMPACT)** a obtenu d'importants résultats opérationnels. Le prochain cycle de l'EMPACT 2026-2029 offre une occasion de renforcer encore ce cadre. Afin de déstabiliser les réseaux criminels les plus menaçants et leurs membres, l'Union doit rationaliser et concentrer ses efforts sur les priorités les plus urgentes, en renforçant les engagements des États membres et en veillant à une utilisation efficace des ressources.

À cette fin, la Commission collaborera avec les présidences du Conseil et les États membres afin d'**optimiser le potentiel de l'EMPACT et d'examiner les grandes priorités de son prochain cycle 2026-2029.** Dans tous ces domaines prioritaires, il est nécessaire de disposer de renseignement sur les réseaux criminels les plus menaçants, de mener des enquêtes conjointes et de se doter de task forces opérationnelles, ainsi que de prendre des mesures robustes sur le plan judiciaire, dont une approche consistant à «suivre l'argent». L'Union doit, en outre, s'attaquer au recrutement et à l'infiltration par les réseaux criminels de même que renforcer la

[16] Règlement (UE) 2023/1543 du Parlement européen et du Conseil du 12 juillet 2023 relatif aux injonctions européennes de production et aux injonctions européennes de conservation concernant les preuves électroniques dans le cadre des procédures pénales et aux fins de l'exécution de peines privatives de liberté prononcées à l'issue d'une procédure pénale (JO L 191 du 28.7.2023).

[17] Conclusions du Conseil sur l'accès aux données en vue d'une répression efficace (12 décembre 2024) https://data.consilium.europa.eu/doc/document/ST-16448-2024-INIT/fr/pdf.

coopération et la formation sur les questions internationales au sein de nombreuses agences et des services répressifs, ainsi qu'entre les unes et les autres.

La Commission soutiendra également d'autres formes de **coopération opérationnelle transfrontière en matière répressive entre les États membres et les pays associés à l'espace Schengen**. Caractérisé par l'absence de contrôles aux frontières intérieures, l'espace Schengen rend nécessaires une coopération étroite et l'échange d'informations entre les autorités répressives des États membres, afin que soit assuré un niveau élevé de sécurité intérieure. À l'heure actuelle, les agents des services répressifs continuent de rencontrer des difficultés lorsqu'ils effectuent des missions de surveillance ou des interventions urgentes par-delà les frontières[18], et la lutte contre les menaces hybrides exige, elle aussi, une coopération transfrontière renforcée. Il conviendrait de créer un **groupe de haut niveau sur l'avenir de la coopération opérationnelle des services répressifs**, chargé d'élaborer une vision stratégique commune.

Un échange de données efficient entre services répressifs est tout aussi essentiel à une coopération transfrontière efficace. Une fois établie, l'**architecture d'interopérabilité** permettra aux autorités répressives et à Europol d'avoir un accès effectif à des informations cruciales. Dans le même temps, l'UE et ses États membres devraient privilégier l'échange bilatéral et multilatéral d'informations, en procédant à la mise en œuvre sur les plans juridique et technique du **règlement Prüm II**[19], en coopération avec l'eu-LISA et Europol. Cela permettra d'échanger de manière automatisée et sécurisée, par les routeurs de l'UE, des empreintes digitales, des profils ADN, des données relatives à l'immatriculation des véhicules, des images faciales et des fichiers de police. À l'échelle nationale, les États membres doivent mettre en œuvre la **directive relative à l'échange d'informations**[20] destinée à renforcer les canaux d'échange d'informations pour créer un flux transfrontière continu d'informations, tout en assurant l'intégration de ceux-ci dans les systèmes existant à l'échelle de l'UE, tels que SIENA[21].

Une coopération transfrontière efficace implique également de développer une **culture commune de l'Union en matière de répression**. Des formations communes, des centres d'excellence et des programmes de mobilité sont essentiels à la réalisation de cet objectif. La Commission étudiera la manière dont l'UE peut soutenir au mieux la formation des autorités des États membres, en faisant appel au **CEPOL**, l'Agence de l'UE pour la formation des services répressifs.

Renforcement de la sécurité des frontières

Il est essentiel de renforcer la résilience et la sécurité des frontières extérieures pour lutter contre les menaces hybrides, telles que l'instrumentalisation de la migration, pour empêcher l'entrée dans l'UE des acteurs et des biens qui représentent une menace, et pour combattre efficacement la criminalité transfrontière et le terrorisme. **Il est prévu d'améliorer le système d'information Schengen (SIS)** en 2026, pour permettre aux États membres d'y introduire des

[18] Comme le mentionne l'évaluation par la Commission de l'effet donné par les États membres à la recommandation (UE) 2022/915 du Conseil du 9 juin 2022 relative à la coopération opérationnelle des services répressifs (document 5909/25).

[19] Règlement (UE) 2024/982 du Parlement européen et du Conseil du 13 mars 2024 relatif à la consultation et l'échange automatisés de données dans le cadre de la coopération policière, et modifiant les décisions 2008/615/JAI et 2008/616/JAI du Conseil et les règlements (UE) 2018/1726, (UE) 2019/817 et (UE) 2019/818 du Parlement européen et du Conseil (règlement Prüm II) (JO L, 2024/982, 5.4.2024).

[20] Directive (UE) 2023/977 du Parlement européen et du Conseil du 10 mai 2023 relative à l'échange d'informations entre les services répressifs des États membres et abrogeant la décision-cadre 2006/960/JAI du Conseil (JO L 134 du 22.5.2023, p. 1).

[21] Secure Information Exchange Network Application (application de réseau d'échange sécurisé d'informations).

signalements concernant les ressortissants de pays tiers impliqués dans des actes de terrorisme, y compris les combattants terroristes étrangers, et dans d'autres formes graves de criminalité, en se fondant sur les données que des pays tiers auront communiquées à Europol.

Une meilleure **interopérabilité** des systèmes d'information à grande échelle de l'UE permettra aux États membres de disposer d'informations essentielles sur les personnes originaires de pays tiers qui franchiront ou auront l'intention de franchir les frontières extérieures de l'UE, ce qui aidera les autorités à évaluer les conditions dans lesquelles l'entrée sur le territoire des États membres sera autorisée[22]. La Commission continuera à collaborer étroitement avec les États membres et l'eu-LISA en vue de la mise en œuvre rapide de ces systèmes, dont le **système d'entrée/de sortie (EES), le système européen d'information et d'autorisation concernant les voyages (ETIAS) et le système d'information sur les visas (VIS) révisé**, afin d'en assurer le bon fonctionnement et d'en concrétiser les avantages en matière de sécurité.

Afin d'améliorer encore la sécurité des frontières et de consolider la coopération de l'UE face à l'évolution des menaces, **la Commission proposera un renforcement de Frontex.** Le corps européen de garde-frontières et de garde-côtes devrait voir ses effectifs tripler, pour compter, au fil du temps, 30 000 agents. L'Agence devrait être dotée de technologies de pointe à des fins de surveillance et de connaissance de la situation, y compris disposer de renseignement utile à la gestion européenne intégrée des frontières et avoir accès aux robustes services gouvernementaux d'observation de la Terre de l'UE pour les besoins du contrôle aux frontières, services qui doivent être déployés d'ici à 2027. Cela lui permettrait non seulement d'accroître encore sa capacité de détection et de prévention de la criminalité transfrontière aux frontières extérieures et de lutte contre ce phénomène, mais aussi d'intensifier son soutien aux États membres dans la mise en œuvre des retours, notamment pour les ressortissants de pays tiers qui présentent un risque pour la sécurité.

La **fraude aux documents et à l'identité** facilite le trafic de migrants, la traite des êtres humains, les mouvements criminels clandestins et le trafic de biens illicites. Une fois opérationnel, le **détecteur d'identités multiples (MID)**[23] améliorera la capacité des autorités nationales à identifier les personnes utilisant plusieurs identités et à lutter contre la fraude à l'identité. La Commission étudiera les moyens de renforcer la sécurité des documents de voyage et de séjour délivrés aux citoyens de l'UE et aux ressortissants de pays tiers. Elle évaluera en outre comment les portefeuilles européens d'identité numérique, qui doivent être introduits au titre du cadre européen relatif à une identité numérique d'ici à la fin de 2026, pourront contribuer à une meilleure sécurité des documents de voyage et améliorer la vérification de l'identité. Cela complétera la proposition relative aux authentifiants de voyage numériques et celle portant création d'une application de voyage numérique de l'UE[24].

Les **informations concernant les voyages** sont indispensables aux autorités pour leur permettre de repérer et d'analyser les déplacements de criminels, de terroristes et d'autres personnes représentant une menace pour la sécurité. Si l'UE dispose d'un cadre pour les

[22] En particulier, le système d'entrée/de sortie (EES) permettra aux États membres d'identifier les ressortissants de pays tiers aux frontières extérieures de l'espace Schengen et d'enregistrer leurs entrées et sorties, rendant ainsi possible l'identification systématique des personnes qui auront dépassé la durée du séjour autorisé. Avant l'arrivée d'un ressortissant de pays tiers aux frontières extérieures, le système européen d'information et d'autorisation concernant les voyages (ETIAS) ainsi que le système d'information sur les visas (VIS) permettront aux États membres d'évaluer à l'avance si la présence de ce ressortissant sur le territoire de l'UE présente un risque pour la sécurité.

[23] Le MID est l'un des éléments d'interopérabilité établis par le règlement (UE) 2019/818 et le règlement (UE) 2019/817.

[24] https://ec.europa.eu/commission/presscorner/detail/fr/ip_24_5047.

informations sur les passagers aériens commerciaux[25], le traitement, à des fins répressives, des données provenant des opérateurs d'autres modes de transport est, quant à lui, fragmenté. Les criminels et les terroristes peuvent, par conséquent, exploiter différents modes de transport pour que leurs activités illégales passent inaperçues. La Commission œuvrera avec les États membres et le secteur des transports au **renforcement du cadre relatif aux informations sur les voyages**, en étudiant un dispositif de l'Union exigeant des opérateurs de vols privés qu'ils recueillent et transfèrent les données relatives aux passagers, en évaluant les règles de traitement des données des dossiers passagers et en étudiant les moyens de rationaliser le traitement des informations sur les passagers maritimes. Pour ce qui est du transport terrestre, la Commission étudiera le recours accru aux systèmes **de reconnaissance automatique des plaques minéralogiques («ANPR»)** et multipliera les possibilités de synergies avec le SIS.

Approche prospective axée sur l'innovation et les capacités

La Commission définira **une approche prospective globale en matière de sécurité intérieure à l'échelle de l'UE**, en s'appuyant sur les bonnes pratiques recensées au niveau national. Cette approche facilitera l'élaboration des politiques et permettra d'orienter les investissements dans des projets de recherche et d'innovation en matière de sécurité financés par l'UE.

La recherche et l'innovation jouent un rôle de premier plan dans la sécurité intérieure par la création de solutions de lutte contre les menaces émergentes, dont celles résultant de l'utilisation abusive des technologies[26]. L'UE doit continuer à investir, au moyen de la recherche et de l'innovation en matière de sécurité financées par son budget[27], dans la mise au point d'outils et de solutions innovants pour contrer les menaces qui pèsent sur la sécurité, dans le respect des règles de l'UE et des droits fondamentaux. La Commission devrait accompagner la transition du stade de la recherche à celui du déploiement, afin d'assurer l'adoption effective de ces moyens modernes, en accordant la priorité aux **technologies modernes** comme l'IA. Cette approche devrait inclure des formations destinées à améliorer l'utilisation, par les services répressifs et les autorités judiciaires, des systèmes d'IA et d'autres moyens techniques. En outre, le potentiel de double usage des technologies devrait, lorsque c'est utile, être exploité dans les deux sens (du civil au militaire et du militaire au civil)[28].

Le **pôle d'innovation de l'UE pour la sécurité intérieure**[29], réseau de laboratoires d'innovation présentant les innovations les plus récentes et des solutions efficaces pour aider les acteurs de la sécurité intérieure dans l'UE et les États membres, contribuera à l'intégration de la recherche dans la pratique et dans les politiques publiques. Europol ne gagnera en efficacité que si son répertoire d'outils est étoffé, pour lui permettre d'identifier et de développer des technologies de pointe, d'en acquérir de manière conjointe et de les appliquer sur le plan opérationnel. Par ailleurs, la Commission créera, au sein de son Centre commun de recherche, un **campus de la recherche et de l'innovation en matière de sécurité**, qui permettra de réunir les chercheurs afin d'écourter le cycle allant des résultats de la recherche à

[25] Cadre relatif aux dossiers passagers (PNR) et aux informations préalables sur les passagers (API) institué par la directive (UE) 2016/681 (la «directive PNR») et par le règlement (UE) 2025/12 et le règlement (UE) 2025/13 (les «règlements API»).

[26] Voir le rapport du Centre commun de recherche de la Commission intitulé «Emerging risks and opportunities for EU internal security stemming from new technologies» https://publications.jrc.ec.europa.eu/repository/handle/JRC139674.

[27] Study on strengthening EU-funded security research and innovation – 20 years of EU-Funded Civil Security Research and Innovation – 2025, https://data.europa.eu/doi/10.2837/0004501.

[28] Comme indiqué dans le rapport Niinistö.

[29] Pôle d'innovation de l'UE pour la sécurité intérieure | Europol.

l'innovation, au développement et à la mise en œuvre réussie, tout en réduisant les coûts de développement, d'essai et de validation.

Du fait de sa nature collaborative, notre **espace européen de la recherche** est perméable aux ingérences étrangères et à la désinformation. À la suite de l'adoption de la recommandation du Conseil sur le renforcement de la sécurité de la recherche[30], la Commission et les États membres prennent actuellement des mesures pour donner aux acteurs concernés les moyens d'agir, parmi lesquelles la création d'un centre d'expertise en matière de sécurité de la recherche.

Actions clés

La Commission:

- **adoptera en 2026 une proposition législative visant à faire d'Europol un service répressif véritablement opérationnel**
- **adoptera en 2026 une proposition législative visant à renforcer Eurojust**
- **adoptera en 2026 une proposition législative visant à accroître le rôle et les tâches de Frontex**
- **adoptera en 2026 une proposition législative portant création d'un système de communication critique de l'UE.**

La Commission entend:

- **présenter en 2025 une feuille de route exposant la voie à suivre en ce qui concerne l'accès licite et effectif aux données à des fins répressives**
- **préparer une analyse d'impact en 2025, en vue d'actualiser, en tant que de besoin, les règles de l'UE relatives à la conservation des données**
- **présenter en 2026 une feuille de route technologique sur le chiffrement, afin de recenser et d'évaluer les solutions technologiques qui permettraient aux autorités répressives d'avoir un accès licite aux données**
- **œuvrer à la création d'un groupe de haut niveau pour renforcer la coopération opérationnelle des services répressifs**
- **créer en 2026, au sein de son Centre commun de recherche, un campus de la recherche et de l'innovation en matière de sécurité.**

En coopération avec les États membres et les agences de l'UE concernées, la Commission va:

- **consolider l'architecture de l'EMPACT**
- **œuvrer en faveur du déploiement rapide de l'architecture d'interopérabilité et de la mise en œuvre du règlement Prüm II**
- **renforcer le cadre relatif aux informations sur les voyages.**

Les États membres sont instamment invités:

- **à transposer et à mettre pleinement en œuvre la directive relative à l'échange d'informations.**

[30] JO C/2024/3510, 30.5.2024.

4. Résilience face aux menaces hybrides et autres actes hostiles

Nous développerons notre résilience face aux menaces hybrides en améliorant la protection de nos infrastructures critiques, en renforçant notre cybersécurité, en sécurisant nos plateformes de transport et nos ports et en luttant contre les menaces en ligne.

Les actes hostiles portant atteinte à la sécurité de l'UE sont devenus plus fréquents et plus sophistiqués, et l'arsenal des acteurs malveillants s'est considérablement élargi. Les campagnes hybrides ciblant l'UE, ses États membres et ses partenaires se sont intensifiées; elles incluent des actes de sabotage d'infrastructures critiques, des incendies criminels, des cyberattaques, des ingérences électorales, des activités de manipulation de l'information et d'ingérence menées depuis l'étranger et pouvant aller jusqu'à la désinformation, ainsi qu'une instrumentalisation de la migration. Du fait de leur rôle politique et opérationnel et de la nature des informations qu'ils traitent, les institutions, organes et organismes de l'Union (ci-après les «entités de l'Union») ne sont pas épargnés.

L'UE doit, dès à présent et à l'avenir, **gagner en résilience**, utiliser efficacement les outils dont elle dispose déjà, et mettre au point de nouveaux moyens d'affronter ces menaces en constante évolution, qui sont le fait d'acteurs tant étatiques que non étatiques.

Infrastructures critiques

Les menaces qui pèsent sur nos **infrastructures critiques**, notamment les menaces hybrides telles que le sabotage et la cybermalveillance, sont un sujet de préoccupation majeur, surtout lorsqu'il s'agit d'infrastructures qui relient plusieurs États membres entre eux, qu'il s'agisse d'interconnexions énergétiques, de câbles de communication transfrontières ou d'infrastructures de transport. Depuis le début de la guerre d'agression menée par la Russie contre l'Ukraine, les actes de sabotage visant des infrastructures critiques ont augmenté, en particulier en 2024, et ont touché de nombreux États membres. La coopération entre les services répressifs, les services de sécurité et de cybersécurité, la protection militaire et civile et les opérateurs privés est essentielle pour anticiper, détecter et prévenir de tels actes et y réagir de manière efficace.

Il est impératif de remédier à nos vulnérabilités et de renforcer la résilience de nos entités critiques si nous voulons assurer la continuité de services essentiels qui sont vitaux pour l'économie et la société. La transposition rapide et la bonne mise en œuvre, par tous les États membres, de la **directive sur la résilience des entités critiques (directive CER)**[31] et de la **directive concernant des mesures destinées à assurer un niveau élevé commun de cybersécurité dans l'ensemble de l'Union (SRI 2)**[32] sont d'une importance cruciale à cet égard.

Pour assurer des progrès rapides, la Commission aidera les États membres à recenser leurs entités critiques[33] et à partager leurs bonnes pratiques en matière de stratégies nationales et d'évaluation des risques pour les services essentiels, en coopération avec le **groupe sur la résilience des entités critiques et le groupe de coopération SRI**. Si des infrastructures critiques subissent des perturbations ayant un impact transfrontière important, les réponses

[31] Directive (UE) 2022/2557 du Parlement européen et du Conseil du 14 décembre 2022 sur la résilience des entités critiques, et abrogeant la directive 2008/114/CE du Conseil..

[32] Directive (UE) 2022/2555 du Parlement européen et du Conseil du 14 décembre 2022 concernant des mesures destinées à assurer un niveau élevé commun de cybersécurité dans l'ensemble de l'Union, modifiant le règlement (UE) nº 910/2014 et la directive (UE) 2018/1972, et abrogeant la directive (UE) 2016/1148 (directive SRI 2).

[33] Les secteurs couverts par la directive sont l'énergie, les transports, la banque, les infrastructures de marchés financiers, la santé, l'eau potable, les eaux usées, les infrastructures numériques, l'administration publique, l'espace et la production, la transformation et la distribution de denrées alimentaires.

apportées au niveau de l'UE seront coordonnées dans le cadre du **schéma directeur de l'UE pour les infrastructures critiques**. La Commission encourage le Conseil à adopter rapidement le **schéma directeur de l'UE en matière de cybersécurité**, qui améliorera encore la coordination dans le contexte de la gestion des crises et favorisera une collaboration plus étroite entre les autorités sur la résilience physique et numérique. À la suite des tests de résistance menés avec succès dans le secteur de l'énergie en 2023, la Commission encouragera la réalisation de **tests de résistance volontaires** dans d'autres secteurs clés pour la sécurité intérieure. En outre, la Commission fournira un **récapitulatif, à l'échelle de l'Union, des risques transfrontières et transsectoriels** qui pèsent sur les services essentiels, afin d'aider les États membres dans leurs propres analyses de risques et de contribuer à une évaluation exhaustive des risques au niveau de l'UE. Conformément à la stratégie pour une Union de la préparation, la Commission coopérera avec les États membres pour identifier d'autres secteurs et services qui ne sont pas couverts par la législation actuelle mais pour lesquels il pourrait être nécessaire d'agir.

La **task-force UE-OTAN sur la résilience des infrastructures critiques** a permis une excellente coopération en matière de partage des bonnes pratiques et de renforcement de la résilience dans les secteurs de l'énergie, des transports, des infrastructures numériques et de l'espace. Ces travaux se poursuivront dans le cadre du **dialogue structuré UE-OTAN sur la résilience**. La **boîte à outils hybride de l'UE** offre aux États membres et aux partenaires une aide précieuse pour se préparer et lutter contre les menaces hybrides. Les **équipes d'intervention rapide en cas de menaces hybrides**[34] peuvent apporter une aide immédiate et sur mesure aux États membres, à diverses missions de l'UE et aux partenaires qui en font la demande. En outre, la Commission développera la coopération au sein de l'UE en matière de lutte contre le sabotage, en organisant des activités pour les experts[35] et notamment en développant un **programme de travail conjoint spécifique** qui permettra aux experts de simplifier leurs échanges d'informations et de définir des contre-mesures.

Les incidents qui endommagent des **câbles sous-marins** en Europe montrent la nécessité de mesures plus fortes et de réponses plus claires. Comme l'annonce le **plan d'action de l'UE pour la sécurité des câbles**[36], la Commission, aux côtés de la haute représentante, collaborera avec les États membres, les agences de l'UE et des partenaires tels que l'OTAN pour prévenir et détecter les menaces qui planent sur les câbles sous-marins, y réagir et les décourager. Afin de dresser un tableau intégré de la situation en termes de menaces, la Commission travaillera avec les États membres à la conception et à la mise en place, sur une base volontaire, d'un mécanisme de surveillance intégré des câbles sous-marins de chaque bassin maritime, en commençant par la zone Mer du Nord/Baltique.

Cybersécurité

La récurrence d'**actes de cybermalveillance**, qui font souvent partie d'un éventail plus large de menaces multidimensionnelles et hybrides, nous impose d'y rester attentifs et de continuer d'agir au niveau européen. Ces dernières années, l'Union a adopté une série de réglementations sur la cybersécurité qui renforcent la cyberrésilience d'entités SRI 2 exerçant dans des secteurs

[34] Boussole stratégique de l'UE en matière de sécurité et de défense (2022), p. 22.

[35] Les conseillers de l'UE en matière de sûreté, le réseau européen d'unités de neutralisation des explosifs et munitions (EEODN), le réseau ATLAS, le réseau de sécurité de l'UE pour la protection des espaces publics à haut risque (EU-HRSN), le groupe consultatif en matière de sécurité CBRN et le groupe sur la résilience des entités critiques (CERG).

[36] JOIN(2025) 9 final.

critiques pour l'UE ainsi que d'entités de l'Union[37], qui rendent les produits numériques plus sûrs (règlement sur la cyberrésilience) et qui instaurent un cadre pour l'aide à la préparation et à la réponse aux incidents (règlement sur la cybersolidarité). En janvier 2025, la Commission a adopté le **plan d'action européen sur la cybersécurité des hôpitaux et des prestataires de soins de santé**[38], afin d'améliorer la détection des menaces, la préparation et la réaction aux crises. Il est impératif de le mettre en œuvre dans son intégralité. Dans le même temps, pour pouvoir affronter des menaces et évolutions inédites, nous devons intensifier nos actions, en particulier en ce qui concerne l'échange d'informations, la sécurité des chaînes d'approvisionnement, les rançongiciels et les cyberattaques, ainsi que la souveraineté technologique.

En outre, pour mettre en œuvre ces mesures, il faut combler le déficit actuel de compétences en matière de cybersécurité, qui se chiffre à 299 000 personnes. La Commission collaborera avec les États membres dans le cadre de l'union des compétences[39] pour accroître le réservoir de talents dans ce domaine, notamment grâce à la nouvelle Académie des compétences en matière de cybersécurité. Le plan stratégique pour l'enseignement des STIM[40] contribue lui aussi à accroître cette réserve de talents et à améliorer la réponse de l'Europe aux besoins du marché du travail dans ce domaine.

En plus de renforcer sa résilience, l'UE continuera d'utiliser pleinement le cadre pour une réponse diplomatique conjointe de l'UE face aux actes de cybermalveillance (la **boîte à outils cyber diplomatique**) afin de prévenir et de décourager les cybermenaces d'acteurs étatiques et non étatiques et d'y répondre.

Sécurité des chaînes d'approvisionnement des TIC

La **boîte à outils pour la cybersécurité de la 5G** est le dispositif approprié pour protéger les réseaux 5G, mais elle n'est pas encore suffisamment utilisée par les États membres. Il subsiste des risques de sécurité inacceptables, en particulier en ce qui concerne le remplacement des fournisseurs à haut risque. Une approche harmonisée de la sécurisation de la chaîne d'approvisionnement des TIC pourrait remédier à la fragmentation actuelle du marché intérieur due aux différences d'approche entre pays, éviter les dépendances critiques et réduire les risques que les fournisseurs à haut risque font peser sur nos chaînes d'approvisionnement, ce qui permettra de sécuriser nos infrastructures critiques.

Dans cet esprit, la Commission procédera, lors de la prochaine **révision du règlement sur la cybersécurité**, à un examen plus large de la sécurité et de la résilience des chaînes d'approvisionnement et infrastructures TIC. Elle proposera également d'améliorer le **cadre européen de certification de cybersécurité**, afin que les futurs systèmes de certification puissent être adoptés rapidement et répondre aux besoins des politiques publiques.

Sur la base d'évaluations sectorielles achevées ou en cours[41], la Commission mettra au point, en collaboration avec les États membres, une **planification stratégique pour réaliser des évaluations coordonnées des risques en matière de cybersécurité**.

---

[37] Règlement (UE/Euratom) 2023/2841 du Parlement européen et du Conseil du 13 décembre 2023 établissant des mesures destinées à assurer un niveau élevé commun de cybersécurité dans les institutions, organes et organismes de l'Union (JO L, 2023/2841, 18.12.2023.

[38] https://digital-strategy.ec.europa.eu/fr/library/european-action-plan-cybersecurity-hospitals-and-healthcare-providers.

[39] COM(2025) 90 final.

[40] COM(2025) 89 final.

[41] Portant, par exemple, sur les réseaux 5G, les télécommunications, l'électricité, les énergies renouvelables ou les véhicules connectés.

Les services d'informatique en nuage et de télécommunications font désormais partie intégrante des chaînes d'approvisionnement des infrastructures critiques, des entreprises et des pouvoirs publics. La Commission prendra des mesures pour encourager les entités critiques à choisir des **services d'informatique en nuage et de télécommunications qui offrent un niveau approprié de cybersécurité**, en tenant compte non seulement des risques techniques, mais aussi des risques et dépendances stratégiques.

Rançongiciels et cyberattaques

L'un des problèmes majeurs auxquels l'UE et le monde demeurent confrontés est l'utilisation de **rançongiciels**, dont le coût annuel mondial, selon les estimations d'un rapport, dépasserait 250 milliards d'EUR d'ici à 2031[42]. La **directive SRI 2** et le **règlement sur la cyberrésilience** amélioreront considérablement la posture de sécurité des entités, ce qui rendra les attaques plus onéreuses pour les réseaux de rançongiciels. En outre, la Commission collaborera étroitement avec les États membres pour que les attaques par rançongiciel, en particulier les menaces persistantes avancées, et les versements de rançons soient davantage signalés aux services répressifs, ce qui facilitera les enquêtes.

En vue de prévenir et de contrer les cyberattaques, l'UE doit renforcer l'échange d'informations entre les services répressifs, les autorités et entités spécialisées dans la cybersécurité et les acteurs privés, sous l'égide d'Europol et de l'Agence de l'Union européenne pour la cybersécurité (ENISA).

Europol et Eurojust devraient continuer de mettre à profit leurs succès en matière de répression des opérations de rançongiciels, en soutenant la coopération entre services répressifs. À cette fin, les services répressifs devraient utiliser au maximum les mécanismes de coopération existants, notamment le **modèle international de réponse aux rançongiciels d'Europol** et l'**initiative internationale de lutte contre les rançongiciels (CRI)**[43], et l'ENISA et Europol devraient coopérer pour élargir le répertoire des outils de déchiffrement des souches de rançongiciels[44].

Souveraineté technologique

La cybersécurité et la souveraineté technologique sont étroitement liées, et les dépendances technologiques doivent être traitées en priorité. L'Union devant **orienter le développement et le déploiement de nouvelles technologies**, la Commission s'emploie à **accroître les capacités dans les technologies stratégiques** comme l'IA, les technologies quantiques, les technologies avancées de connectivité, l'informatique en nuage, l'informatique de périphérie et l'internet des objets[45], grâce à des initiatives à venir telles que le plan d'action pour un continent de l'IA, la stratégie quantique, etc[46]. La Commission continuera de promouvoir le déploiement rapide des derniers **protocoles internet** disponibles, définis au niveau international, qui sont essentiels pour que l'internet demeure évolutif et performant et présente un meilleur niveau de cybersécurité. Les **problèmes liés au spectre radioélectrique**, tels que l'usurpation et le brouillage des signaux du GNSS ou les risques encourus par les chaînes d'approvisionnement du fait de leur dépendance, imposent aussi d'autres mesures, comme l'utilisation de

[42] https://cybersecurityventures.com/global-ransomware-damage-costs-predicted-to-reach-250-billion-usd-by-2031/.
[43] https://counter-ransomware.org/.
[44] Disponibles dans le cadre du projet «No More Ransom», https://www.nomoreransom.org/en/index.html.
[45] https://strategic-technologies.europa.eu/about_en#step-scope.
[46] Par exemple l'entreprise commune EuroHPC (https://eurohpc-ju.europa.eu/index_en), l'initiative phare concernant les technologies quantiques (Quantum Flagship), Homepage of Quantum Flagship | Quantum Flagship, le «réseau 3C» (COM(2024) 81 final) et le plan d'action de l'UE pour la sécurité des câbles (JOIN(2025) 9 final).

technologies de détection quantique et l'étude des possibilités de développement des capacités de surveillance des radiofréquences.

Le déploiement de solutions de **cryptographie post-quantique** (PQC) sera indispensable, à l'ère quantique, pour protéger les communications sensibles, les données au repos et les identités numériques. Se basant sur sa recommandation de 2024 relative à une feuille de route pour la mise en œuvre coordonnée de la transition vers la cryptographie post-quantique[47], la Commission s'emploie, avec les États membres, à favoriser cette transition. Dans cette optique, les États membres devraient identifier les cas à haut risque parmi leurs entités critiques et faire le nécessaire pour qu'ils disposent dès que possible, et au plus tard à la fin de 2030, de solutions de chiffrement à l'épreuve des attaques quantiques. La Commission collabore aussi avec les États membres et l'Agence spatiale européenne (ESA) pour développer et déployer l'**infrastructure européenne de communication quantique (EuroQCI)**[48], basée sur la distribution quantique de clés (QKD), dans le cadre du programme de l'UE pour une connectivité sécurisée (**IRIS²**). À terme, ces deux initiatives permettront aux entités de transmettre des données et de stocker des informations de manière sécurisée.

Les **technologies quantiques** sont aussi appelées à jouer un rôle clé dans les applications de sécurité: une **feuille de route pour la détection quantique dans les applications de sécurité** sera mise au point dans le cadre de la **stratégie quantique**. Dans le même esprit, la Commission travaille actuellement sur ses systèmes internes critiques pour la sécurité, notamment ses systèmes informatiques classifiés, en vue de les rendre résistants aux attaques quantiques.

Un cadre de cybersécurité favorable aux entreprises

La révision à venir du règlement sur la cybersécurité sera l'occasion de **simplifier la législation de l'UE en la matière**, comme le prévoit la boussole pour la compétitivité. La Commission travaillera en étroite collaboration avec les États membres pour assurer une mise en œuvre rapide, uniforme et favorable aux entreprises du cadre horizontal pour la cybersécurité défini par la directive SRI 2, le règlement sur la cyberrésilience et le règlement sur la cybersolidarité, en promouvant la simplicité et la cohérence et en évitant la fragmentation ou la duplication des règles en la matière dans les législations nationales et de l'UE.

Afin de permettre un accès sécurisé aux services en ligne et de renforcer la sécurité numérique dans l'ensemble de l'UE, le **cadre européen relatif à une identité numérique** offrira à tous les citoyens et résidents de l'UE, avant la fin de 2026, un portefeuille d'identité numérique fiable. Le futur **portefeuille européen d'identité numérique pour les entreprises** permettra quant à lui de sécuriser les interactions transfrontières entre entreprises et administrations publiques. Ces deux initiatives sont des préalables indispensables pour que le marché unique fondé sur les données puisse fonctionner de manière sûre et plus efficiente, grâce à des outils tels que le portail numérique unique, la facturation électronique, la passation électronique de marchés publics et le passeport numérique de produit.

Sécurité en ligne

Certaines des menaces hybrides les plus graves, en ce qu'elles compromettent la sécurité et la sûreté des personnes en Europe et ciblent la sphère démocratique de l'UE, se matérialisent en ligne. Il s'agit notamment des activités illégales en ligne, de la diffusion de contenus illicites en ligne, de la manipulation d'informations par leur amplification artificielle, de la diffusion

[47] Recommendation relative à une feuille de route pour la mise en œuvre coordonnée de la transition vers la cryptographie post-quantique | Stratégie numérique de l'UE.
[48] https://digital-strategy.ec.europa.eu/en/policies/european-quantum-communication-infrastructure-euroqci.

d'informations trompeuses et des activités de manipulation de l'information et d'ingérence menées depuis l'étranger.

L'application rigoureuse du **règlement sur les services numériques (DSA)** est primordiale pour garantir un environnement en ligne sûr et accessible, dans lequel les acteurs sont comptables de leurs actes, et qui soit également résilient face aux menaces hybrides. Ce règlement sur les services numériques oblige les fournisseurs de très grandes plateformes en ligne et de très grands moteurs de recherche en ligne à effectuer des évaluations de risques et à prendre des mesures d'atténuation des risques systémiques liés à la conception, au fonctionnement ou à l'utilisation de leurs services. Ces risques peuvent inclure des effets négatifs sur le discours civique et les processus électoraux, ainsi que sur la sécurité publique, tels qu'une ingérence à grande échelle d'acteurs étatiques étrangers malveillants dans le déroulement d'élections, par exemple. Il est important que les autorités compétentes des États membres soient formées à l'utilisation d'outils juridiques permettant de supprimer rapidement les contenus illicites en ligne, en particulier lorsqu'il s'agit de cyberviolence fondée sur le genre. Le règlement sur les services numériques prévoit un mécanisme de réaction aux crises qui peut être activé lorsque des circonstances extraordinaires entraînent une menace grave pour la sécurité publique ou la santé publique dans l'Union ou dans des parties importantes de celle-ci. Pour le compléter, la Commission et les autorités nationales compétentes désignées comme coordinateurs pour les services numériques ont également mis au point un **cadre DSA de réponse aux incidents**, applicable sur base volontaire. Les coordinateurs pour les services numériques ont en outre pris des mesures pour protéger l'intégrité des élections, par exemple en organisant des tables rondes électorales et des tests de résistance[49]. Le règlement sur les services numériques, associé au règlement sur la publicité à caractère politique[50], constitue l'un des axes de préservation de la démocratie et de l'intégrité des processus démocratiques, qui ne sont pas à l'abri des visées d'acteurs hostiles agissant, notamment, à l'aide d'outils numériques et sur les médias sociaux.

La boîte à outils pour lutter contre les activités de manipulation de l'information et d'ingérence menées depuis l'étranger (**FIMI**) offre un autre appui essentiel au niveau de l'UE. Le soutien à la compétence numérique, à l'éducation aux médias et à l'esprit critique est également au cœur de ces efforts[51].

Lutter contre l'instrumentalisation de la migration

La Russie, avec la complicité et le soutien décisif de la Biélorussie, a délibérément instrumentalisé la migration et illégalement facilité des flux migratoires vers les frontières extérieures de l'UE, dans le but de déstabiliser nos sociétés et de saper l'unité de l'Union européenne. Cela met en péril non seulement la sécurité et la souveraineté nationales des États membres, mais aussi la sûreté et l'intégrité de l'espace Schengen et la sécurité de l'Union dans son ensemble. Dans ses conclusions d'octobre 2024, le Conseil européen a insisté sur le fait qu'il ne saurait être toléré que la Russie et la Biélorussie, ou tout autre pays, détournent nos valeurs, y compris le droit d'asile, et sapent notre démocratie.

Comme l'a indiqué la Commission dans sa communication de 2024 sur l'instrumentalisation de la migration, outre un ferme soutien politique, l'Union a pris des mesures financières, opérationnelles et diplomatiques, y compris en coopération avec les pays d'origine et de transit,

[49] Boîte à outils du DSA pour les élections, à l'usage des coordinateurs pour les services numériques - 2025https://digital-strategy.ec.europa.eu/en/library/dsa-elections-toolkit-digital-services-coordinators.
[50] Règlement (UE) 2024/900 du Parlement européen et du Conseil du 13 mars 2024 relatif à la transparence et au ciblage de la publicité à caractère politique, JO L, 2024/900, 20.3.2024.
[51] Plan d'action en matière d'éducation numérique (2021-2027) – Espace européen de l'éducation..

pour réagir efficacement à ces menaces[52]. Elle a notamment recouru au nouveau cadre défini par le Conseil pour sanctionner les individus et organisations impliqués dans des actions et des politiques telles que l'instrumentalisation de la migration par la Russie, en imposant un gel des avoirs et des interdictions de voyager[53]. L'UE continuera d'utiliser ce cadre, lorsque ce sera nécessaire, et d'aider les États membres à contrer cette menace.

Sûreté des transports

Les ports maritimes, les aéroports et les infrastructures terrestres sont des points d'entrée et de sortie essentiels. Ils jouent un rôle vital pour l'économie et la société de l'UE et sont indispensables à la mobilité militaire. Mais ces moyens et plateformes de transport constituent aussi des cibles privilégiées pour les menaces extérieures et les agissements criminels. De récents incidents, notamment des atteintes à la sûreté du fret aérien et des attaques contre des infrastructures ferroviaires, soulignent la gravité de ces risques. Les **opérateurs de transport** peuvent être à la fois ciblés et instrumentalisés par des acteurs malveillants. Les instruments juridiques actuels de l'UE ont renforcé la sûreté aérienne[54], mais compte tenu du niveau élevé des menaces pour l'aviation civile, il faut un moyen de prévoir les incidents et de consulter rapidement les États membres concernés. La Commission collaborera avec les États membres pour apporter à l'actuelle législation d'exécution en matière de sûreté aérienne des modifications concernant le partage d'informations classifiées sur les **événements touchant à la sûreté de l'aviation**. En outre, elle réfléchira à des **mesures réglementaires** pour faire face aux menaces nouvelles, telles que les **incidents de fret aérien**, et pour renforcer les normes de sûreté de l'aviation. Cela passera aussi par un renforcement de la **législation en matière de sûreté aérienne (AVSEC)**, pour qu'il soit possible de réagir immédiatement tout en maintenant dans les aéroports de l'UE la zone de contrôle unique de sûreté.

Lors de l'élaboration de la future **stratégie portuaire de l'UE**, reposant sur l'alliance des ports européens, la Commission étudiera les moyens de renforcer encore la législation en matière de sûreté maritime, afin de lutter efficacement contre les menaces émergentes, de sécuriser les ports et d'accroître la sécurité des chaînes d'approvisionnement de l'UE. À cet effet, elle veillera à ce que cette législation soit rigoureusement mise en œuvre et travaillera à l'harmonisation des pratiques nationales et au renforcement des vérifications d'antécédents des personnels dans les ports. La Commission collaborera avec les États membres et le secteur privé pour étendre les actuels protocoles de sécurité du fret aérien aux chaînes de transport maritimes.

L'Autorité douanière de l'UE qu'il est proposé de créer analysera et évaluera les risques à partir des **informations douanières** relatives à l'entrée, à la sortie ou au transit des marchandises dans l'UE, afin d'aider les États membres à empêcher des acteurs malveillants de mettre à profit les chaînes d'approvisionnement internationales Dans le droit fil de la stratégie de sûreté maritime de l'UE[55], le **pacte européen pour les océans**, qui devrait être adopté prochainement, jouera un rôle clé dans le renforcement de la sûreté maritime, dans les bassins maritimes de l'UE et au-delà, notamment en encourageant l'application à plus grande échelle d'opérations et d'exercices maritimes à finalités multiples.

Résilience des chaînes d'approvisionnement

[52] COM(2024) 570 final.
[53] Règlement (UE) 2024/2642 du Conseil du 8 octobre 2024 concernant des mesures restrictives eu égard aux activités déstabilisatrices menées par la Russie, ST/8744/2024/INIT, JO L, 2024/2642, 9.10.2024.
[54] Règlement (CE) nº 300/2008 du Parlement européen et du Conseil du 11 mars 2008 relatif à l'instauration de règles communes dans le domaine de la sûreté de l'aviation civile (JO L 97 du 9.4.2008, p. 72).
[55] JOIN(2023) 8 final.

L'Europe doit utiliser moins de technologies provenant de pays tiers, en raison des risques qu'elles comportent pour son indépendance et sa sécurité. La Commission s'est fixé pour but de réduire nos dépendances à l'égard de fournisseurs étrangers uniques, de faire en sorte que nos chaînes d'approvisionnement soient moins exposées à des fournisseurs à haut risque et de sécuriser les infrastructures critiques et les capacités industrielles situées sur le sol de l'UE, ainsi qu'il est prévu dans la **boussole pour la compétitivité**[56] et dans le **pacte pour une industrie propre**[57]. Elle promouvra une **politique industrielle favorisant la sécurité intérieure**, en collaborant avec les industries de l'UE dans des secteurs clés (comme les plateformes de transport ou les infrastructures critiques) pour produire des solutions de sécurité, telles que des équipements de détection, des technologies biométriques ou des drones, qui comportent des dispositifs de sécurité dès leur conception. Lors de la **révision des règles de l'UE en matière de marchés publics**, elle évaluera si les préconisations de sécurité de la directive de 2009 sur les marchés publics dans les domaines de la défense et de la sécurité[58] sont suffisantes pour répondre aux besoins en matière de répression et de résilience des entités critiques.

La Commission aidera les États membres à **filtrer les investissements directs étrangers (IDE)** et les acquisitions d'équipements pour plateformes logistiques, de façon à ce que les infrastructures et les technologies critiques restent sûres.

Une fois entré en application, le **règlement sur les situations d'urgence et la résilience du marché intérieur (SURMI)** aidera l'UE à gérer les crises qui perturbent ses chaînes d'approvisionnement critiques et la libre circulation des biens, des services et des personnes. Il permettra de se coordonner rapidement en cas de crise, d'inventorier les biens et services concernés et de disposer d'une panoplie d'instruments pour garantir leur disponibilité. En outre, la Commission, en étroite coopération avec les États membres, proposera la création d'un **mécanisme multi-institutionnel d'alerte de sécurité pour les transports et les chaînes d'approvisionnement**, afin de garantir un partage sûr et rapide des informations pertinentes nécessaires pour anticiper et contrer les menaces.

En outre, avec la mise en œuvre du règlement sur les matières premières critiques et du règlement pour une industrie «zéro net», l'utilisation accrue de critères de durabilité, de résilience et de préférence européenne dans les marchés publics de l'UE favorisera le développement de marchés porteurs. Le renforcement des liens commerciaux dans le cadre, par exemple, de partenariats sur les matières premières ou de partenariats pour des échanges et des investissements propres aidera à diversifier les chaînes d'approvisionnement.

Résilience et préparation aux menaces chimiques, biologiques, radiologiques et nucléaires

La guerre d'agression menée par la Russie contre l'Ukraine a accru le risque de **menaces chimiques, biologiques, radiologiques et nucléaires (CBRN)**. Pour prévenir la potentielle acquisition de substances CBRN pour les transformer en armes, la Commission aidera les États membres et les pays partenaires au moyen de formations et d'exercices spécifiques. Elle s'emploiera aussi à renforcer la préparation et les capacités de réaction à ces risques, ce qui exigera une hiérarchisation des menaces, le financement de l'innovation en matière de contre-mesures, des capacités de rescEU et la constitution de stocks de contre-mesures médicales, dans le cadre d'un nouveau **plan d'action pour la préparation et la réaction aux menaces CBRN**. En outre, la **stratégie de l'UE en matière de contre-mesures médicales** soutiendra la mise au

[56] COM(2025) 30 final.
[57] COM(2025) 85 final.
[58] Directive 2009/81/CE relative à la coordination des procédures de passation de certains marchés de travaux, de fournitures et de services par des pouvoirs adjudicateurs ou entités adjudicatrices dans les domaines de la défense et de la sécurité, et modifiant les directives 2004/216/CE et 2004/2009/CE, JO L 216 du 20.8.2009.

point de parades médicales, du stade de la recherche jusqu'à la fabrication et la distribution, afin de protéger l'UE des pandémies et des menaces CBRN.

L'UE s'est appuyée sur l'expérience acquise lors de la pandémie de COVID-19 pour consolider son cadre de sécurité sanitaire[59]. La Commission a entrepris de désigner des laboratoires de référence de l'UE dans le domaine de la santé publique, en vue de renforcer les capacités de surveillance et de détection rapide de l'UE et des États membres. Un plan de l'Union sur la préparation, la prévention et la réaction en matière de sécurité sanitaire sera publié en 2025.

Actions clés

La Commission va:

- **réexaminer et réviser le règlement sur la cybersécurité en 2025**
- **définir des mesures pour garantir l'utilisation cybersécurisée des services en nuage**
- **proposer une stratégie portuaire de l'UE en 2025**
- **réviser les règles de l'UE en matière de marchés publics pour la défense et la sécurité en 2026**
- **présenter un nouveau plan d'action pour la préparation et la réaction aux menaces CBRN en 2026.**

En coopération avec les États membres, la Commission entend:

- **développer et déployer l'infrastructure européenne de communication quantique (EuroQCI)**
- **veiller à l'application effective du règlement sur les services numériques**
- **lutter contre l'instrumentalisation de la migration**
- **mettre en place un système de communication sur les événements touchant à la sûreté de l'aviation**
- **œuvrer à la mise en place d'un mécanisme multi-institutionnel d'alerte de sécurité pour les transports et les chaînes d'approvisionnement.**

Le Conseil est instamment invité:

- **à adopter la recommandation du Conseil relative au schéma directeur de l'UE en matière de cybersécurité.**

Les États membres sont instamment invités:

- **à transposer et à mettre pleinement en œuvre les directives CER et SRI 2.**

5. Resserrer le filet autour de la grande criminalité organisée

Nous contribuerons à l'éradication de la criminalité organisée en proposant des règles plus strictes pour lutter contre les réseaux de criminalité organisée, portant notamment sur les enquêtes, sur la prévention du recrutement de jeunes de l'UE par ces réseaux et sur le renforcement des mesures visant à couper l'accès des criminels à leurs outils et actifs.

La criminalité organisée, profitant d'un environnement en pleine évolution, prolifère de manière exponentielle. Elle bénéficie de technologies de pointe, opère dans une multitude de pays et a de solides connexions au-delà des frontières de l'UE. Compte tenu de la complexité et du caractère transnational de ces menaces, la coordination et le soutien au niveau de l'UE sont absolument indispensables.

[59] Notamment dans le cadre du règlement (UE) 2022/2371 relatif aux menaces transfrontières graves pour la santé.

Prévention de la criminalité

Le recrutement de jeunes par la criminalité organisée est un problème croissant dans l'UE. Lutter contre cette criminalité nécessite de s'attaquer à ses **causes profondes**, en offrant un accès à l'éducation et d'autres perspectives qu'une vie de délinquant, par une approche englobant l'ensemble de la société. La Commission encouragera l'intégration de questions de sécurité dans les politiques de l'UE en matière d'éducation et d'emploi et dans ses politiques sociales et régionales. L'UE **promouvra des politiques de prévention de la criminalité fondées sur des données probantes**[60] et adaptées aux contextes locaux.

Afin de protéger les utilisateurs de services en ligne, en particulier les mineurs, notamment contre les délinquants pédophiles, les trafiquants d'êtres humains et le recrutement en ligne à des fins criminelles ou d'extrémisme violent, les mesures prévues par le **règlement sur les services numériques** imposent aux fournisseurs de plateformes en ligne accessibles aux mineurs de gérer les risques et d'intervenir contre les contenus illicites, y compris les discours haineux. La Commission prévoit de publier des **lignes directrices sur la protection des mineurs** pour aider ces fournisseurs à garantir un niveau élevé de protection de la vie privée, de sûreté et de sécurité des mineurs en ligne. Ces lignes directrices contiendront une série de recommandations pour tous les services numériques opérant dans l'Union, afin de renforcer la protection des mineurs en ligne. En 2025, la Commission prévoit également de faciliter la mise en place dans l'UE d'un **système de vérification de l'âge respectueux de la vie privée**, qui constituera une solution provisoire en attendant le portefeuille européen d'identité numérique, qui doit voir le jour à la fin de 2026. La Commission adoptera aussi un plan d'action contre le cyberharcèlement.

Par ailleurs, la Commission continuera d'encourager les dialogues multipartites volontaires avec les plateformes en ligne et les autres acteurs concernés, notamment grâce au forum de l'UE sur l'internet et à des codes de conduite ciblés élaborés conformément au règlement sur les services numériques, tels que le code de conduite de 2025 pour lutter contre les discours haineux illégaux en ligne. L'objectif est de sensibiliser, d'apporter une réponse conjointe aux menaces existantes ou émergentes, et de mettre au point et partager des bonnes pratiques relatives aux mesures d'atténuation.

Au niveau local, l'impact de la criminalité organisée confirme la nécessité de solutions régionales pour réduire les sources de vulnérabilité et l'attrait des activités illégales. Le programme de l'UE pour les villes proposera des solutions aux défis que doivent relever ces dernières en matière de sécurité, en s'appuyant sur l'initiative «Villes de l'UE contre la radicalisation». La Commission recourra au Fonds européen de développement régional pour aider les États membres à améliorer la sécurité urbaine et régionale.

La résilience et la cohésion des sociétés passent par le renforcement du socle éducatif et des compétences. Dans le cadre de l'**union des compétences** et du **plan d'action pour l'intégration et l'inclusion**, l'Union agira pour aider les citoyens à mieux résister à la mésinformation et à la désinformation, à la radicalisation et au recrutement dans la criminalité.

La protection des enfants contre toutes les formes de violence, que ce soit la criminalité ou la violence physique ou mentale, en ligne ou hors ligne, est un objectif primordial de l'UE. Pour répondre aux besoins spécifiques de groupes particulièrement vulnérables tels que les enfants, qui sont de plus en plus exposés aux agissements de recruteurs, à la radicalisation, au pédopiégeage, aux abus sexuels, au cyberharcèlement, à la désinformation et à d'autres menaces, l'UE élaborera un **plan d'action pour la protection des enfants contre la criminalité**, englobant les dimensions en ligne et hors ligne. Ce plan définira une approche

[60] https://www.eucpn.org/.

cohérente et coordonnée reposant sur les cadres et outils disponibles, notamment sur le futur centre de l'UE chargé de prévenir et de combattre les abus sexuels à l'encontre d'enfants, ainsi que sur d'autres organes et agences de l'UE, et proposera des pistes pour aller de l'avant là où des lacunes subsistent.

Démanteler les réseaux criminels et lutter contre leurs facilitateurs

La lutte contre les réseaux criminels à haut risque, leurs meneurs et leurs facilitateurs doit s'intensifier. Malgré les succès notables obtenus récemment[61], l'obsolescence de certaines législations et un manque de cohérence dans la définition des réseaux criminels nuisent à l'efficacité de la justice pénale et de la coopération transfrontière. La Commission réexaminera ces dispositions législatives dépassées et proposera un nouveau **cadre juridique sur la criminalité organisée**, afin de renforcer ces réponses.

Il est possible d'obtenir des résultats plus rapides en complétant l'action pénale par l'exécution administrative, comme l'ont montré le Parquet européen et l'Office européen de lutte antifraude (OLAF) dans la lutte contre **la fraude transfrontière et les infractions portant atteinte aux intérêts financiers de l'UE.** La fraude aux subventions se concentre sur des secteurs tels que les énergies renouvelables, les programmes de recherche et l'agriculture[62]. La Commission étudiera les moyens de coordonner le recours aux mesures pénales et administratives, en renforçant la coopération avec Europol, Eurojust et le Parquet européen. Elle continuera également à encourager une application plus large de l'**approche administrative**, afin de donner aux autorités locales et autres autorités administratives les moyens de mettre un terme aux infiltrations criminelles[63].

L'UE s'emploie à consolider son cadre juridique en matière de lutte contre la **corruption**[64]. Le Parlement européen et le Conseil devraient conclure rapidement leurs négociations sur le cadre actualisé de lutte contre la corruption proposé par la Commission. La Commission présentera une stratégie anticorruption de l'UE destinée à favoriser l'intégrité et à renforcer la coordination de toutes les autorités et parties prenantes concernées dans ce domaine.

Les armes à feu jouent un rôle central dans la multiplication des actes de violence perpétrés par des groupes criminels organisés. La Commission proposera des normes pénales communes sur le trafic illicite d'armes à feu. Un nouveau **plan d'action de l'UE contre le trafic d'armes à feu** sera axé sur la préservation des ventes licites et la réduction des activités criminelles, grâce à l'amélioration du renseignement et au renforcement de la coopération internationale, une attention particulière étant accordée à l'Ukraine et aux Balkans occidentaux.

Le commerce illicite d'articles pyrotechniques, utilisés à des fins criminelles, appelle des mesures d'amélioration de la prévention et de la traçabilité. La Commission procède actuellement à l'évaluation de la directive sur les articles pyrotechniques, et elle réfléchira aussi à des **sanctions pénales pour le trafic de ces articles**.

[61] Notamment grâce à l'EMPACT.

[62] https://www.europol.europa.eu/cms/sites/default/files/documents/EU-SOCTA-2025.pdf.

[63] https://administrativeapproach.eu/sites/default/files/page/files/eu-jha-council-9-10-june-conclusions-administrative-approach-org-crime.pdf.

[64] Proposition de directive du Parlement européen et du Conseil relative à la lutte contre la corruption, remplaçant la décision-cadre 2003/568/JAI du Conseil et la convention relative à la lutte contre la corruption impliquant des fonctionnaires des Communautés européennes ou des fonctionnaires des États membres de l'Union européenne, et modifiant la directive (UE) 2017/1371 du Parlement européen et du Conseil, COM(2023) 234 final du 3 mai 2023.

Suivre l'argent

Il est essentiel de «**suivre l'argent**» pour lutter contre la criminalité organisée et le terrorisme, mais cela reste très difficile. Compte tenu du lien entre la criminalité organisée et les flux financiers, des efforts intenses et combinés doivent être déployés pour empêcher les réseaux criminels d'accéder à des sources de financement et pour mieux protéger les citoyens, les entreprises et les budgets publics.

L'UE a renforcé son action avec les nouvelles règles en matière de lutte contre le blanchiment de capitaux, et notamment la création de l'**Autorité de lutte contre le blanchiment de capitaux (ALBC)**[65]. Une collaboration entre l'ALBC, l'OLAF, le Parquet européen, Eurojust et Europol est indispensable pour que les enquêtes financières soient efficaces. La Commission encouragera la mise en place de **partenariats** facilitant la coopération interagences et faisant intervenir le secteur privé.

Pour éradiquer les motivations financières de la criminalité organisée, il est essentiel de saisir les avoirs et de confisquer les profits d'origine criminelle. Les règles plus strictes en matière **de recouvrement et de confiscation d'avoirs**, adoptées récemment[66], devraient être transposées dans les plus brefs délais par les États membres et pleinement exploitées. Pour s'attaquer aux systèmes financiers parallèles qui contournent le cadre de l'UE en matière de lutte contre le blanchiment de capitaux, y compris aux systèmes fondés sur des crypto-actifs, des actions novatrices, un partage des bonnes pratiques entre les États membres et un soutien accru de la part d'Europol et d'Eurojust sont également nécessaires. La Commission étudiera la faisabilité d'un nouveau système à l'échelle de l'UE pour surveiller les profits de la criminalité organisée et le financement du terrorisme, et encouragera aussi la transmission rapide et élargie d'informations aux services répressifs par les **cellules de renseignement financier**. Elle cherchera des moyens de combler les lacunes, aidera les États membres à développer leurs capacités et poursuivra son action en vue d'améliorer la coopération avec les pays tiers dont les criminels se servent pour effectuer des opérations bancaires souterraines.

Lutter contre les formes graves de criminalité

Outre le démantèlement des réseaux criminels, la lutte contre les formes graves de criminalité nécessite des efforts ciblés. Afin de pouvoir mieux lutter contre la **fraude en ligne**, qui cause un préjudice financier considérable[67], la Commission œuvrera en faveur de mesures de prévention, ainsi que de mesures répressives plus efficaces, et collaborera avec les États membres et les parties prenantes pour soutenir et protéger les victimes, notamment en les aidant à récupérer leurs fonds. Ces efforts seront officialisés dans un **plan d'action contre la fraude en ligne**.

S'appuyant sur la stratégie 2020-2025 de l'UE en faveur de la lutte contre les **abus sexuels commis contre des enfants**[68], la Commission aidera les colégislateurs à mettre la dernière touche aux deux propositions législatives[69] visant à prévenir et à combattre les abus sexuels sur enfants en ligne et à rendre plus efficaces les mesures répressives destinées à lutter contre les abus sexuels et l'exploitation sexuelle des enfants. Des dispositions provisoires sont en place jusqu'en avril 2026; il est donc essentiel d'établir un cadre juridique permanent, et la Commission encourage les colégislateurs à entamer des négociations sur le projet de règlement établissant des règles en vue de prévenir et de combattre les abus sexuels sur enfants. Elle les

[65] https://www.amla.europa.eu/index_fr.
[66] Directive (UE) 2024/1260 du Parlement européen et du Conseil du 24 avril 2024 relative au recouvrement et à la confiscation d'avoirs (JO L, 2024/1260, 2.5.2024).
[67] Global Anti-Scam Report 2024.
[68] COM(2020) 607 final.
[69] COM(2022) 209 final et COM(2024) 60 final.

invite également à progresser sur la voie des négociations concernant la directive relative à la lutte contre les abus sexuels et l'exploitation sexuelle des enfants, ainsi que contre les matériels relatifs à des abus sexuels sur enfants, qui établira des règles minimales pour la définition des infractions pénales et des sanctions dans le domaine de l'exploitation sexuelle des enfants.

La moitié des réseaux criminels les plus dangereux de l'UE sont impliqués dans le **trafic de stupéfiants** avec violence. Bien que l'UE ait récemment renforcé sa lutte contre ce type de criminalité[70], notamment en élargissant le mandat de l'**Agence de l'UE sur les drogues**, de nouvelles mesures sont nécessaires. La Commission travaillera en étroite coopération avec les États membres pour proposer une nouvelle **stratégie de l'UE en matière de drogue**. Elle révisera en outre le **cadre juridique relatif aux précurseurs de drogues** et proposera un **plan d'action de l'UE contre le trafic de drogue** afin de désorganiser les filières et de mettre à mal les modèles économiques. Le **partenariat public-privé de l'alliance des ports européens**, visant à renforcer la protection des ports, sera étendu aux ports de petite taille et aux ports intérieurs et permettra de garantir l'application des règles de sûreté maritime. Consciente que le trafic de stupéfiants a de graves conséquences à l'échelon local, la Commission continuera d'œuvrer en faveur d'une politique en matière de drogue qui soit équilibrée, fondée sur des données probantes et pluridisciplinaire et qui permette de faire face à des afflux soudains de drogues, en particulier d'opioïdes de synthèse.

Pour s'attaquer à l'exploitation des personnes, l'UE a adopté de nouvelles règles[71] et présentera une **stratégie renouvelée visant à lutter contre la traite des êtres humains** (2026-2030), qui englobera tous les stades, de la prévention aux poursuites, en mettant l'accent sur l'aide aux victimes, tant au niveau de l'UE qu'à l'échelle internationale.

Afin de combattre le **trafic de migrants**, la Commission dirigera des actions avec des partenaires clés au sein de la nouvelle alliance mondiale pour lutter contre le trafic de migrants, en coopération avec Europol, Eurojust et Frontex, y compris en ligne. Les propositions de la Commission dans ce domaine[72] devraient être adoptées et mises en œuvre dans les plus brefs délais. En outre, à la suite de l'adoption de la **boîte à outils concernant les opérateurs de transport**[73], la Commission a accru ses contacts avec les autorités étrangères et avec les opérateurs, et elle continuera de dialoguer avec le secteur aérien et les organisations de l'aviation civile[74] afin de les sensibiliser au trafic de migrants par voie aérienne[75].

La **criminalité environnementale** menace l'environnement, la santé publique et les économies à long terme. La Commission aidera les États membres à mettre en œuvre la directive relative à la protection de l'environnement par le droit pénal[76] et renforcera les réseaux opérationnels et les actions dans ce domaine[77]. Il est essentiel de veiller au respect rigoureux des règles. En

[70] COM(2023) 641 final.
[71] Directive (UE) 2024/1712 du 13 juin 2024 modifiant la directive 2011/36/UE concernant la prévention de la traite des êtres humains et la lutte contre ce phénomène ainsi que la protection des victimes (JO L, 2024/1712, 24.6.2024).
[72] COM(2023) 755 final et COM(2023) 754 final.
[73] Boîte à outils visant à lutter contre l'utilisation de moyens de transport commerciaux pour faciliter la migration irrégulière vers l'UE.
[74] Dont l'Organisation de l'aviation civile internationale (OACI).
[75] La Commission œuvrera aussi en faveur de la finalisation du règlement concernant des mesures contre les opérateurs de transport qui facilitent la traite des êtres humains ou le trafic de migrants, ou qui se livrent à ces pratiques [COM(2021) 753 final].
[76] Directive (UE) 2024/1203 du Parlement européen et du Conseil du 11 avril 2024 relative à la protection de l'environnement par le droit pénal (JO L, 2024/1203, 30.4.2024).
[77] Réseau de l'UE pour la mise en œuvre de la législation communautaire environnementale et pour le contrôle de son application (IMPEL), Réseau européen des procureurs pour l'environnement (REPE), EnviCrimeNet et Forum des juges de l'UE pour l'environnement (UEFJE).

outre, la convention du Conseil de l'Europe sur la protection de l'environnement par le droit pénal[78], adoptée récemment, incitera les pays à faire des efforts considérables et comparables pour lutter contre la criminalité environnementale, tant en Europe qu'au niveau international.

La réponse de la justice pénale

La criminalité et le terrorisme peuvent toucher tout un chacun; il est donc essentiel de soutenir les **victimes** et de préserver leurs droits, afin de réduire les préjudices causés et d'accroître la sécurité générale et la confiance dans les autorités. S'inspirant de la directive sur les droits des victimes, la Commission présentera une nouvelle **stratégie de l'UE relative aux droits des victimes**.

Les **systèmes de justice pénale de l'UE** doivent être dotés d'outils efficaces pour faire face aux menaces émergentes. À cet effet, la Commission a lancé un **forum de haut niveau sur l'avenir de la justice pénale dans l'UE**. Ce forum réunit les États membres, le Parlement européen, les organismes et organes de l'UE, ainsi que d'autres parties prenantes. Il a pour objectif de réfléchir aux mesures à prendre pour que nos systèmes de justice pénale restent efficaces, équitables et résilients face à des défis changeants, tout en renforçant la coopération judiciaire et la confiance mutuelle, notamment par le passage au numérique[79].

Actions clés

La Commission va:

- **présenter une proposition législative visant à moderniser les règles relatives à la criminalité organisée, en 2026;**
- **présenter une proposition législative visant à réviser le cadre juridique relatif aux précurseurs de drogues, en 2025;**
- **présenter une proposition législative relative à des normes pénales communes en matière de trafic illicite d'armes à feu, en 2025;**
- **évaluer la nécessité de réviser les directives relatives aux articles pyrotechniques et aux explosifs à usage civil;**
- **évaluer la nécessité de renforcer davantage la décision d'enquête européenne et le mandat d'arrêt européen;**
- **présenter une nouvelle stratégie de l'UE en matière de lutte contre la traite des êtres humains, en 2026;**
- **présenter une nouvelle stratégie de l'UE sur les droits des victimes, en 2026;**
- **présenter un plan d'action de l'UE pour la protection des enfants contre la criminalité, d'ici 2027;**
- **présenter un plan d'action de l'UE contre le trafic de drogue, en 2025;**
- **présenter un plan d'action de l'UE contre le trafic d'armes à feu, en 2026;**
- **élargir progressivement l'alliance des ports européens, à partir de 2025;**
- **adopter des lignes directrices sur la protection des mineurs, dans le cadre du règlement sur les services numériques, en 2026;**
- **présenter un plan d'action de l'UE contre le cyberharcèlement, en 2026.**

Les États membres sont instamment invités:

[78] Comité d'experts sur la protection de l'environnement par le droit pénal (PC-ENV) – Comité européen pour les problèmes criminels.

[79] Notamment la mise en place d'e-CODEX (e-Justice Communication via Online Data Exchange) et du système européen d'information sur les casiers judiciaires pour les ressortissants de pays tiers (ECRIS-TCN).

- **à transposer intégralement les nouvelles règles en matière de recouvrement et de confiscation d'avoirs, d'ici la fin de 2026, et à les exploiter pleinement;**
- **à mettre en œuvre l'approche administrative pour lutter contre l'infiltration par des réseaux criminels;**
- **à mettre en place des partenariats public-privé contre le blanchiment de capitaux;**
- **à transposer et à mettre en œuvre intégralement la directive visant à prévenir et à combattre la violence à l'égard des femmes et la violence domestique.**

Le Parlement européen et le Conseil sont instamment invités:

- **à progresser sur la voie des négociations concernant le règlement établissant des règles en vue de prévenir et de combattre les abus sexuels sur enfants et la directive relative à la lutte contre les abus sexuels et l'exploitation sexuelle des enfants, ainsi que contre les matériels relatifs à des abus sexuels sur enfants;**
- **à conclure les négociations sur la directive relative à la lutte contre la corruption.**

6. Lutter contre le terrorisme et l'extrémisme violent

Nous présenterons un programme complet de lutte contre le terrorisme, visant à prévenir la radicalisation, à sécuriser les espaces en ligne et les espaces publics, à tarir les canaux de financement et à réagir aux attaques au moment où elles ont lieu.

Le niveau de menace terroriste demeure élevé dans l'UE. Il est étroitement lié aux retombées des événements géopolitiques, aux nouvelles technologies et aux nouveaux moyens de financement du terrorisme. Nous devons veiller à ce que l'UE soit dotée des moyens nécessaires pour anticiper les menaces, prévenir la radicalisation (tant hors ligne qu'en ligne), protéger les citoyens et les espaces publics contre les attaques et réagir efficacement à ces dernières lorsqu'elles surviennent. Un **nouveau programme de l'UE concernant la prévention du terrorisme et de l'extrémisme violent et la lutte contre ces phénomènes** sera présenté en 2025 afin de définir l'action future de l'UE. Ainsi que le prévoit le nouveau programme, l'UE et les Balkans occidentaux signeront en 2025 le nouveau **plan d'action conjoint** relatif à la prévention du terrorisme et de l'extrémisme violent et à la lutte contre ces phénomènes.

Prévention de la radicalisation et protection des personnes en ligne

Comme pour la criminalité organisée, la lutte contre le terrorisme et l'extrémisme violent commence en **s'attaquant à leurs causes profondes**. Le **pôle de connaissances de l'UE sur la prévention de la radicalisation** accroîtra son soutien aux praticiens et aux décideurs politiques grâce à une nouvelle **boîte à outils complète en matière de prévention**, devant permettre une détection précoce de la radicalisation et la mise en place d'interventions axées sur les personnes vulnérables, en particulier les mineurs. La radicalisation a souvent lieu en prison et, pour aider les États membres à résoudre ce problème, la Commission formulera de nouvelles recommandations.

Les terroristes et les extrémistes violents utilisent les plateformes en ligne pour diffuser des contenus terroristes et préjudiciables, recueillir des fonds et recruter. Des utilisateurs vulnérables, surtout mineurs, se radicalisent en ligne à un rythme alarmant. Le **règlement sur les contenus à caractère terroriste en ligne** joue un rôle déterminant pour contrer la diffusion de contenus à caractère terroriste en ligne, en permettant le retrait rapide des contenus les plus

odieux et dangereux[80]. La Commission évalue actuellement son fonctionnement et examinera la meilleure manière de renforcer ce cadre.

Le **protocole de crise de l'UE**, qui organise une réaction conjointe et rapide des services répressifs et du secteur des technologies en cas d'attaque terroriste, sera modifié pour assurer l'évolutivité et la souplesse nécessaires pour faire face à la dimension en ligne croissante des attaques terroristes. Le forum de l'UE sur l'internet restera la principale enceinte de coopération volontaire avec le secteur des technologies pour lutter contre les contenus terroristes et préjudiciables en ligne. Par ailleurs, la Commission participe à des initiatives internationales telles que la Fondation de l'appel de Christchurch et le Forum mondial de l'internet contre le terrorisme (GIFCT).

Lutte contre le financement du terrorisme

Les terroristes financent leurs activités par des campagnes de financement participatif, des crypto-actifs, des néobanques ou des plateformes de paiement en ligne. Les services répressifs doivent détecter ces flux financiers et mener des enquêtes, ce qui nécessite des moyens, des outils et une expertise. Le **réseau d'enquêteurs financiers dans le domaine de la lutte antiterroriste** joue un rôle essentiel à cet égard. La Commission réfléchira à la création d'un **nouveau système de surveillance du financement du terrorisme à l'échelle de l'UE** couvrant les opérations intra-UE et SEPA, les transferts de crypto-actifs, les paiements en ligne et les virements électroniques, lequel complétera l'accord UE - États-Unis sur le programme de surveillance du financement du terrorisme (TFTP).

Le budget de l'UE doit être **protégé contre toute utilisation abusive visant à renforcer des opinions radicales/extrémistes** dans les États membres. Le **règlement financier** révisé inclut désormais, parmi les motifs d'exclusion des financements de l'UE, la condamnation pour «incitation à la discrimination, à la haine ou à la violence». La Commission continuera d'étudier comment exploiter au mieux la boîte à outils, notamment lors de la sélection des bénéficiaires potentiels. La protection du budget de l'UE repose aussi sur une coopération étroite et le partage d'informations avec les autorités nationales et les organismes et organes de l'UE.

Protection contre les attaques

Outre les investissements dans la prévention de la radicalisation, un volet important de la protection des citoyens consiste à restreindre les moyens dont disposent les terroristes et les criminels pour perpétrer des attentats. Il convient à la fois d'agir sur les outils utilisés par les terroristes et de prendre des mesures pour protéger les cibles potentielles d'attaques.

En plus de ses actions concernant les armes à feu, la Commission **révisera** également **les règles relatives aux précurseurs d'explosifs** afin qu'elles couvrent les produits chimiques à haut risque. Les **espaces publics** demeurent les cibles les plus courantes d'attentats terroristes, en particulier pour les acteurs isolés. Afin d'éviter toute atteinte aux citoyens, le **programme de conseil en matière de sûreté de l'UE** sera renforcé pour que des évaluations de la vulnérabilité des espaces publics, des infrastructures critiques et des événements à haut risque soient réalisées à la demande des États membres et financées par le budget de l'UE, au titre du Fonds pour la sécurité intérieure. L'UE s'efforcera d'augmenter le financement disponible pour la protection des espaces publics. La Commission apporte son soutien aux autorités des États membres et aux opérateurs privés sous la forme de conseils et d'outils spécifiques, tels que le pôle de

[80] Au 31 décembre 2024, 1 426 injonctions de retrait avaient été émises afin de faire supprimer des contenus à caractère terroriste ou de bloquer l'accès à de tels contenus, la grande majorité de ces injonctions ciblant des contenus djihadistes, mais aussi de droite.

connaissances sur la protection des espaces publics[81], et 70 millions d'EUR ont déjà été mis à disposition pour améliorer la protection de ces espaces depuis 2020.

La Commission se penchera aussi sur l'introduction d'obligations imposant aux organisations d'envisager ou d'appliquer des mesures de sécurité dans les lieux accessibles au public, en concertation avec les autorités locales et les partenaires privés.

Compte tenu des vulnérabilités manifestes, la **stratégie européenne de lutte contre l'antisémitisme et de soutien à la vie juive (2021-2030)** continuera d'orienter les actions de la Commission destinées à protéger la communauté juive. De même, la Commission veillera à ce que des outils appropriés soient mis en place pour aider les États membres à lutter contre la **haine antimusulmane**.

L'utilisation des **drones** à des fins d'espionnage et pour mener des attaques pose de plus en plus problème sur le plan de la sécurité. La Commission élaborera une **méthode d'essai harmonisée pour les systèmes antidrones**, créera un **centre d'excellence de la lutte antidrone** et évaluera la nécessité d'harmoniser les législations et procédures des États membres[82].

Combattants terroristes étrangers

Pour identifier, aux frontières extérieures de l'UE, les combattants terroristes étrangers qui reviennent ou qui entrent sur le territoire européen, il est nécessaire de disposer de données sur les personnes qui représentent une menace terroriste. À cette fin, la Commission, conjointement avec Europol, renforcera sa **coopération avec des pays tiers clés afin d'obtenir des données biographiques et biométriques sur les personnes susceptibles de constituer une menace terroriste**, dont les combattants terroristes étrangers, qui pourront ensuite être introduites dans le système d'information Schengen, dans le plein respect des cadres juridiques applicables au niveau de l'UE et à l'échelon national. Il est donc essentiel que les États membres utilisent au mieux tous les outils existants. Il s'agit notamment d'introduire toutes les informations pertinentes dans le **SIS**, de renforcer les contrôles biométriques et de soumettre toutes les personnes à des vérifications systématiques obligatoires aux frontières extérieures de l'UE[83]. En outre, les **indicateurs de risque communs** élaborés par Frontex continueront d'aider les autorités des États membres chargées des contrôles aux frontières à détecter et à évaluer le risque de déplacements suspects de combattants terroristes étrangers potentiels.

Par ailleurs, afin que les États membres conservent l'accès aux **éléments de preuve recueillis sur les champs de bataille** par l'équipe d'enquêteurs des Nations unies chargée de concourir à amener Daech/l'État islamique d'Iraq et du Levant (EIIL) à répondre de ses crimes (UNITAD), en vue de poursuites contre les combattants terroristes étrangers, la Commission, conjointement avec Eurojust, évaluera la possibilité de stocker ces éléments dans la base de données d'Eurojust sur les preuves de grands crimes internationaux. De plus, le nouveau **registre judiciaire européen antiterroriste** continuera d'aider les autorités judiciaires des États membres à repérer rapidement les liens transfrontières dans les affaires de terrorisme.

Actions clés
La Commission va:

[81] Pôle de connaissances sur la protection des espaces publics.
[82] Dans le prolongement de la série d'actions clés décrites dans la communication de 2023 sur les mesures antidrones [COM(2023) 659 final].
[83] Dans le plein respect du code frontières Schengen et du règlement sur le filtrage.

- **adopter un nouveau programme de l'UE concernant la prévention du terrorisme et de l'extrémisme violent et la lutte contre ces phénomènes, en 2025;**
- **signer avec les Balkans occidentaux un nouveau plan d'action conjoint relatif à la prévention du terrorisme et de l'extrémisme violent et à la lutte contre ces phénomènes, en 2025;**
- **élaborer une nouvelle boîte à outils complète en matière de prévention, avec le pôle de connaissances de l'UE;**
- **évaluer l'application du règlement sur les contenus à caractère terroriste en ligne, en 2026;**
- **modifier le protocole de crise de l'UE, en 2025;**
- **présenter une proposition législative visant à réviser le règlement relatif à la commercialisation et à l'utilisation de précurseurs d'explosifs, en 2026;**
- **étudier la faisabilité d'un nouveau système de surveillance du financement du terrorisme à l'échelle de l'UE.**

Les États membres sont instamment invités:

- **à renforcer les contrôles biométriques et à effectuer des vérifications systématiques obligatoires aux frontières extérieures de l'UE;**
- **à exploiter pleinement le registre judiciaire européen antiterroriste.**

7. L'UE, acteur mondial de premier plan dans le domaine de la sécurité

Afin d'améliorer la sécurité de l'UE, nous renforcerons la coopération opérationnelle par des partenariats avec des régions clés, telles que celles de nos partenaires de l'élargissement et du voisinage, l'Amérique latine et la région méditerranéenne. Il sera tenu compte des intérêts de l'UE en matière de sécurité dans le cadre de la coopération internationale, notamment par la mise en œuvre des outils et des instruments de l'UE.

Ces dernières années ont mis au jour les liens intrinsèques qui existent entre la sécurité extérieure et la sécurité intérieure de l'UE. La guerre d'agression menée par la Russie contre l'Ukraine, le conflit à Gaza, la situation en Syrie et les conflits émergents dans le monde ont eu de graves répercussions sur la sécurité intérieure de l'UE. Pour contrer les effets de l'instabilité mondiale sur sa sécurité intérieure, **l'UE doit défendre activement ses intérêts en matière de sécurité**, en s'attaquant aux menaces extérieures, en désorganisant les filières des trafiquants et en préservant les corridors d'intérêt stratégique, tels que les routes commerciales. Dans le même temps, l'UE restera un solide allié des pays partenaires, avec lesquels elle œuvrera pour améliorer la sécurité mondiale et accroître la résilience mutuelle face aux menaces.

Ces dernières années, l'UE a pris des mesures importantes pour renforcer sa coopération en matière de sécurité. Elle a conclu des accords de coopération opérationnelle des services répressifs et judiciaires ainsi que d'autres types d'accords avec des pays partenaires. Elle s'emploie activement à conclure d'autres accords internationaux, conformément aux directives de négociation du Conseil, et à mener des initiatives de renforcement des capacités, facilitées par les organismes et organes de l'UE. L'IVCDCI – Europe dans le monde est également essentiel pour améliorer la sécurité avec les pays partenaires.

L'**ordre multilatéral fondé sur des règles** est indispensable au renforcement de la sécurité mondiale. Les dialogues sur la sécurité, y compris les dialogues thématiques, sont essentiels pour intensifier les efforts en ce sens. La mise en œuvre de la **boussole stratégique en matière de sécurité et de défense**, les cadres de coopération bilatéraux et multilatéraux tels que les accords de stabilisation et d'association et les accords d'association, ainsi que les collaborations

avec des organisations telles que l'ONU et l'OTAN, sont fondamentaux pour élaborer des solutions efficaces en matière de sécurité. L'UE continuera de jouer son rôle dans les enceintes multilatérales[84] et intensifiera sa coopération avec les organisations et cadres internationaux et régionaux concernés, notamment l'OTAN, l'ONU, le Conseil de l'Europe, Interpol, le G7, l'OSCE et la société civile.

Coopération régionale

En priorité, la poursuite du soutien sans faille de l'UE à l'**Ukraine** et le renforcement de la sécurité et de la résilience des **pays visés par l'élargissement de l'UE** constituent un impératif politique et géostratégique. Favoriser la sécurité de l'UE devrait aller de pair avec une **intégration accélérée des pays candidats** dans l'**architecture de sécurité de l'UE**, parallèlement à la consolidation de leur coopération régionale. La Commission se servira de la politique d'élargissement de l'Union pour renforcer la capacité des pays candidats à l'adhésion à l'UE et des candidats potentiels à réagir aux menaces, pour accroître la coopération opérationnelle et l'échange d'informations et pour garantir l'alignement sur les principes, la législation et les outils de l'UE. L'instrument d'aide de préadhésion (IAP III), ainsi que les facilités pour l'Ukraine, la Moldavie et les Balkans occidentaux sont essentiels pour améliorer la sécurité, tant dans les pays candidats que sur le territoire des candidats potentiels.

L'UE poursuivra également l'intégration des **partenaires du voisinage** dans son architecture de sécurité. Dans le cadre du **nouveau pacte pour la Méditerranée** et de la future **approche stratégique à l'égard de la mer Noire**, l'Union entend continuer à mettre en place une coopération régionale et des partenariats stratégiques globaux au niveau bilatéral comportant une dimension liée à la sécurité, lorsque cela se justifiera, avec des dialogues réguliers à haut niveau sur la sécurité. La coopération opérationnelle avec l'Afrique du Nord, **le Moyen-Orient et la région du Golfe** sera renforcée, en particulier en ce qui concerne la lutte contre le terrorisme, le blanchiment de capitaux, le trafic d'armes à feu ainsi que la production et le trafic de stupéfiants, notamment le captagon.

Pour faire face à la montée des activités terroristes et criminelles et à leurs répercussions potentielles **en Afrique subsaharienne, notamment au Sahel, dans la Corne de l'Afrique et en Afrique de l'Ouest**, l'UE augmentera son soutien à l'Union africaine, aux communautés économiques régionales (CER) et aux pays de la région. Conformément à la stratégie de sûreté maritime de l'UE[85], cette dernière intensifiera sa coopération **dans le golfe de Guinée, la mer Rouge et l'océan Indien** afin de lutter contre le trafic et la piraterie, en soutenant la coopération intra-africaine et régionale et avec l'aide des présences maritimes coordonnées (PMC) de l'UE et du Centre d'opération et d'analyse maritime de lutte contre le trafic de drogue (MAOC-N).

Avec **l'Amérique latine et les Caraïbes**, l'UE renforcera la coopération opérationnelle visant à démanteler et poursuivre les réseaux criminels à haut risque et à désorganiser les activités illicites et les filières des trafiquants, en améliorant les cadres de coopération, tels que le cadre UE-CLASI (comité latino-américain de sécurité intérieure) et le mécanisme UE-CELAC de coordination et de coopération en matière de drogues. La résilience et les partenariats des plateformes logistiques ainsi que les approches consistant à «suivre l'argent» figureront parmi les priorités. L'UE continuera de soutenir le développement de la Communauté des polices des Amériques (Ameripol), afin que celle-ci devienne l'équivalent régional d'Europol, et de renforcer la coopération judiciaire entre les États membres et la région. Elle collaborera également avec **l'Asie du Sud et l'Asie centrale** sur des défis communs en matière de sécurité

[84] Le Forum mondial de lutte contre le terrorisme, la coalition internationale de lutte contre Daech, le Forum mondial de l'internet contre le terrorisme (GIFCT), la Fondation de l'appel de Christchurch, la coalition mondiale de lutte contre les menaces liées aux drogues de synthèse.
[85] JOIN(2023) 8 final.

liés au terrorisme, au trafic de marchandises illicites, dont la drogue, à la traite des êtres humains et au trafic de migrants.

En outre, l'UE apportera son soutien à des cadres de coopération régionale dans des pays tiers, afin de continuer à les aider à mettre un terme au trafic illicite à la source, conformément au principe de responsabilité partagée pour l'ensemble de la chaîne d'approvisionnement criminelle. De plus, l'UE contribuera à renforcer la sécurité des plateformes logistiques à l'étranger, en coordonnant des **inspections conjointes dans les ports de pays tiers**.

Coopération opérationnelle

La stratégie «**Global Gateway**» soutiendra des projets d'infrastructures durables et de qualité dans les secteurs du numérique, du climat et de l'énergie, des transports, de la santé, de l'éducation et de la recherche. La Commission inclura désormais, lorsque cela se justifiera, des considérations de sécurité dans les futurs investissements «Global Gateway». Seront notamment concernées des initiatives essentielles pour l'autonomie stratégique de l'UE et de ses pays partenaires, telles que des projets d'infrastructures intégrant des évaluations de sécurité et des mesures d'atténuation des risques.

La Commission s'efforcera de conclure de nouveaux **accords, entre l'UE et des pays tiers, en matière de coopération avec Europol et Eurojust**, notamment avec les pays d'Amérique latine.

En outre, la participation proactive de pays tiers à l'**EMPACT** est l'un des moyens les plus efficaces de renforcer la coopération opérationnelle. L'UE continuera d'encourager des pays tiers, notamment des Balkans occidentaux, du voisinage oriental, d'Afrique subsaharienne, d'Afrique du Nord, du Moyen-Orient, d'Amérique latine et des Caraïbes, à s'associer à ce cadre. Les task forces opérationnelles entre les États membres, coordonnées par Europol et auxquelles les pays tiers peuvent participer, constituent un autre instrument permettant d'intensifier la coopération avec les pays tiers en matière de lutte contre la criminalité. La Commission entend également mener à bonne fin les négociations relatives à l'accord international **UE-Interpol**[86], en vue d'unifier davantage l'approche appliquée à l'égard des menaces pour la sécurité à l'échelle mondiale et de la lutte contre la criminalité transnationale.

L'**Union doit être présente sur le terrain, dans le cadre d'une approche «Équipe Europe»**. Le personnel spécialisé de l'Union et des États membres joue un rôle essentiel pour que l'action extérieure de l'Union repose sur des informations fiables et soit coordonnée et adaptée à la situation. Afin de porter cette approche au niveau supérieur, la Commission, avec l'aide de la haute représentante de l'Union pour les affaires étrangères et la politique de sécurité, renforcera les **réseaux de liaison** et facilitera le déploiement d'**officiers de liaison** régionaux **d'Europol et d'Eurojust**, en fonction des besoins opérationnels des États membres.

L'UE s'efforcera d'approfondir la coopération opérationnelle des services répressifs et judiciaires et encouragera le partage d'informations en temps réel et les opérations conjointes par des **équipes communes d'enquête** dans les pays tiers, avec le soutien d'Europol et d'Eurojust. La Commission aidera également les États membres à mettre en place des **centres communs de fusion** réunissant des experts et les services répressifs locaux dans des pays tiers stratégiques.

Outils de la politique étrangère et de sécurité commune (PESC)

Il sera également tiré le meilleur parti des **missions de la politique de sécurité et de défense commune (PSDC)** pour mieux détecter et contrer les menaces extérieures pesant sur la sécurité

[86] Décision (UE) 2021/1312 du Conseil du 19 juillet 2021 et décision (UE) 2021/1313 du Conseil du 19 juillet 2021.

intérieure de l'UE, conformément aux mandats fixés par le Conseil. Afin de développer les capacités des pays tiers, la haute représentante de l'Union pour les affaires étrangères et la politique de sécurité et la Commission soutiendront les actions de la PSDC au moyen d'instruments de financement spécifiques et étudieront toutes les voies de financement appropriées.

Les **mesures restrictives de l'UE** constituent un outil de la PESC bien établi, également utilisé pour lutter contre le terrorisme. Sur la base de propositions de la haute représentante de l'Union pour les affaires étrangères et la politique de sécurité, des États membres ou de la Commission, le Conseil pourrait évaluer comment rendre les mesures restrictives autonomes de l'UE existantes (la liste de l'UE en matière de terrorisme) plus efficaces, plus opérationnelles et plus souples. En outre, il pourrait envisager d'autres mesures restrictives ciblant les réseaux criminels, conformément aux objectifs de la PESC.

Politique des visas et échange d'informations

La politique de l'UE en matière de visas constitue un outil essentiel pour coopérer avec les pays tiers et sécuriser nos frontières, en contrôlant les entrées dans l'UE et en fixant les conditions applicables à ces dernières. Dans le cadre d'une future stratégie de l'UE relative à la politique des visas, la Commission veillera à l'intégration complète de **considérations de sécurité dans la politique de l'UE en matière de visas**. Elle œuvrera, avec les colégislateurs, à l'adoption de la proposition visant à réviser et à rationaliser le mécanisme de suspension de l'exemption de visa, pour traiter en particulier certains cas d'utilisation abusive du régime d'exemption de visa[87]. Les pays tiers seront encouragés à communiquer des informations sur les personnes susceptibles de représenter une menace pour la sécurité, qui seront introduites dans les systèmes d'information et les bases de données de l'UE.

Pour coordonner les politiques et concentrer les efforts en amont, et parvenir ainsi à une coopération plus efficiente, plus rapide et plus fluide, la Commission s'emploiera à définir des **modalités de transmission des données** et étudiera les moyens d'**améliorer l'échange d'informations** à des fins répressives et de gestion des frontières avec des pays tiers de confiance, dans le respect des droits fondamentaux et des règles en matière de protection des données.

Actions clés

La Commission va:

- **conclure des accords internationaux entre l'UE et des pays tiers prioritaires concernant la coopération avec Europol et Eurojust;**
- **encourager la participation des pays partenaires à l'EMPACT, pour lutter contre la criminalité organisée et le terrorisme;**
- **aider les organismes et organes de l'UE à établir des modalités de travail avec les pays partenaires et à les renforcer;**
- **intégrer davantage des considérations de sécurité dans la politique de l'UE en matière de visas, dans le cadre de la future stratégie relative aux visas;**
- **intensifier l'échange d'informations avec des pays tiers de confiance, à des fins répressives et de gestion des frontières.**

La Commission, en coopération avec la haute représentante de l'Union pour les affaires étrangères, va:

[87] COM(2023) 642.

- **tirer pleinement parti des missions civiles relevant de la politique de sécurité et de défense commune (PSDC);**
- **coordonner des inspections conjointes dans les ports de pays tiers, d'ici à 2027.**

La Commission, en coopération avec la haute représentante de l'Union pour les affaires étrangères et les États membres, va:

- **consolider les réseaux de liaison et la coopération dans le cadre d'une approche «Équipe Europe»;**
- **mettre en place des équipes opérationnelles communes et des centres communs de fusion dans des pays tiers, à partir de 2025.**

Le Parlement européen et le Conseil sont instamment invités:

- **à conclure les négociations relatives à la révision du mécanisme de suspension de l'exemption de visa.**

8. Conclusion

Dans un monde plein d'incertitudes, la capacité de l'Union à anticiper les menaces pour la sécurité, à les prévenir et à y réagir doit être accrue.

Se borner à réagir aux crises lorsqu'elles surviennent ne suffit plus. Nous devons avoir une appréciation plus précise de la situation et disposer d'une image complète des menaces, au fur et à mesure de leur évolution. Il nous faut également veiller à ce que nos outils et nos capacités soient à la hauteur.

L'ensemble exhaustif de mesures détaillées dans la présente stratégie contribuera à créer une Union plus forte sur la scène internationale: une Union capable d'anticiper ses propres besoins en matière de sécurité, de les planifier et d'y répondre, à même de réagir efficacement aux menaces qui pèsent sur sa sécurité intérieure et de faire rendre compte à leurs auteurs, et qui protège ses sociétés et démocraties ouvertes, libres et prospères.

Pour atteindre cet objectif, nous devons envisager la sécurité intérieure autrement. Nous œuvrerons à la création d'une nouvelle culture de la sécurité au sein de l'UE, caractérisée par la prise en considération des aspects liés à la sécurité dans l'ensemble de nos actes législatifs, de nos politiques et de nos programmes, depuis leur conception jusqu'à leur mise en œuvre, et par une collaboration transversale qui nous ouvrira des horizons nouveaux.

Il ne s'agit pas là d'une tâche incombant à une seule institution, à un seul gouvernement ou à un seul acteur, mais d'une entreprise commune à toute l'Europe.