Conseil de
l'Union européenne

Bruxelles, le 18 octobre 2023
(OR. en)

14372/23

JAI 1332	**COPEN 363**
COSI 179	**FREMP 292**
ENFOPOL 431	**JAIEX 66**
ENFOCUSTOM 110	**CFSP/PESC 1410**
IXIM 194	**COPS 489**
CT 155	**HYBRID 73**
CRIMORG 137	**DISINFO 85**
FRONT 327	**TELECOM 306**
ASIM 92	**DIGIT 223**
VISA 208	**COMPET 1008**
CYBER 247	**RECH 456**
DATAPROTECT 278	**CULT 122**
CATS 58	**COTER 185**
DROIPEN 151	**CORDROGUE 94**

NOTE DE TRANSMISSION

Origine:	Pour la secrétaire générale de la Commission européenne, Madame Martine DEPREZ, directrice
Date de réception:	18 octobre 2023
Destinataire:	Madame Thérèse BLANCHET, secrétaire générale du Conseil de l'Union européenne
N° doc. Cion:	COM(2023) 665 final
Objet:	COMMUNICATION DE LA COMMISSION AU PARLEMENT EUROPÉEN ET AU CONSEIL sur le sixième rapport d'avancement de la mise en œuvre de la stratégie de l'UE pour l'union de la sécurité

Les délégations trouveront ci-joint le document COM(2023) 665 final.

p.j.: COM(2023) 665 final

COMMISSION
EUROPÉENNE

Bruxelles, le 18.10.2023
COM(2023) 665 final

COMMUNICATION DE LA COMMISSION AU PARLEMENT EUROPÉEN ET AU CONSEIL

sur le sixième rapport d'avancement de la mise en œuvre de la stratégie de l'UE pour l'union de la sécurité

I. Introduction

Il y a trois ans, la Commission a adopté la stratégie pour l'union de la sécurité 2020-2025[1] définissant les principales priorités de l'Union dans le domaine de la sécurité. Depuis lors, nous avons accompli des progrès considérables dans le cadre des quatre piliers de la stratégie; une législation historique a été mise en place dans tous les secteurs, de la protection des entités critiques au renforcement de la cyberrésilience. Dans l'intervalle, les menaces qui pèsent sur la sécurité en Europe et dans notre voisinage continuent toutefois d'évoluer. Les attentats terroristes perpétrés ces derniers jours dans une école en France et dans les rues de Bruxelles nous rappellent avec force qu'il est urgent de continuer à adapter et à renforcer notre architecture de sécurité. Le danger que représentent les cyberattaques continue de croître, alimenté également par le fait que des acteurs malveillants prennent parti dans les conflits en cours. Les menaces hybrides, dont la désinformation, continuent de se multiplier. Europol a considéré la guerre d'agression menée par la Russie contre l'Ukraine comme la cause d'une hausse significative des cyberattaques contre des cibles de l'UE, avec des attaques majeures à motivation politique coordonnées par des groupes de pirates informatiques pro-russes[2]. Cela s'est traduit par le blocage de l'accès à l'internet et par l'interruption de services essentiels tels que les réseaux énergétiques[3].

La stratégie pour l'union de la sécurité a été conçue pour permettre à l'UE de mieux faire face à l'évolution du panorama des menaces. Alors que nous avons été confrontés aux crises causées par la pandémie et la guerre, les événements ont montré l'importance de l'approche adoptée dans le cadre de la stratégie – notre détermination à resserrer les maillons de l'écosystème de sécurité de l'UE et à abattre les cloisonnements entre la dimension cyber et la dimension physique de la sécurité, y compris en ce qui concerne la lutte contre la criminalité organisée et le terrorisme ainsi que la lutte contre la radicalisation.

La vigilance exige cependant que nous recherchions en permanence ce qui fait défaut dans nos efforts pour préserver la sécurité de nos citoyens. La stratégie a défini des domaines prioritaires dans lesquels l'Union peut apporter une valeur ajoutée pour aider les États membres à renforcer la sécurité de toutes les personnes vivant en Europe. Depuis son adoption, toutes les actions recensées ont été prises en compte et de nouvelles actions ont été intégrées pour répondre aux défis actuels en matière de sécurité.

Dans l'ensemble, la Commission a présenté 36 initiatives législatives dans le cadre de la stratégie pour l'union de la sécurité. Pour plus de la moitié de ces propositions, les négociations interinstitutionnelles ont déjà abouti à une nouvelle législation solide, comme décrit dans le tableau en annexe. Toutefois, plusieurs initiatives clés proposées par la Commission sont toujours en cours de négociation par le Parlement européen et le Conseil. La législature actuelle arrivant à son terme avec les élections européennes de juin 2024, il convient d'œuvrer rapidement à la résolution de ces dossiers en suspens, afin que les citoyens puissent bénéficier

---

1 COM(2020) 605.

2 Attaques par déni de service distribué (DDoS): voir le rapport d'Europol «Europol Spotlight - Cyber-attacks: the apex of crime-as-a-service», 13 septembre 2023.

3 Des logiciels malveillants (wipers) ont été fortement utilisés pendant le conflit en Ukraine pour détruire des données et des systèmes, compromettant par exemple l'accès à l'internet de milliers d'abonnés dans l'UE, ainsi que l'accès d'une grande entreprise allemande du secteur de l'énergie à la surveillance à distance de plus de 5 800 éoliennes. The role of cyber in the Russian war against Ukraine: Its impact and the consequences for the future of armed conflict (Le rôle de la cybernétique dans la guerre menée par la Russie contre l'Ukraine: son incidence et les conséquences sur l'avenir des conflits armés), étude du Parlement européen, septembre 2023 - PE 702.594.

pleinement de l'union de la sécurité. Le 6e rapport sur l'état d'avancement de la stratégie pour l'union de la sécurité se concentre donc sur la présentation des dossiers législatifs et non législatifs essentiels relatifs à l'union de la sécurité adoptés par la Commission, pour lesquels des efforts supplémentaires doivent être réalisés en vue de leur finalisation et de leur mise en œuvre effective.

Pour les actes législatifs de l'UE déjà adoptés, leurs avantages ne se feront sentir que lorsqu'ils seront mis en pratique. Les travaux doivent se concentrer sur leur transposition, leur mise en œuvre et leur application correctes et complètes par les États membres. En 2023, la Commission a continué de veiller à ce que la stratégie de l'UE pour l'union de la sécurité produise ses effets en faisant usage de ses pouvoirs institutionnels pour engager des procédures d'infraction lorsque les États membres n'avaient pas transposé la législation de l'UE ou ne l'avaient pas fait correctement.

Le présent rapport résume également les domaines dans lesquels l'action des États membres et/ou des agences de l'UE est essentielle à la mise en œuvre. Les agences de l'UE jouent un rôle crucial dans le soutien à la mise en œuvre des initiatives liées à l'union de la sécurité, et leurs responsabilités se sont développées ces dernières années. Le rapport décrit certaines des principales nouvelles tâches qui leur ont été assignées pour apporter un soutien accru aux États membres dans la mise en œuvre d'initiatives clés dans le cadre de l'union de la sécurité.

En outre, la situation géopolitique a mis en évidence l'importance de la sécurité extérieure pour notre sécurité intérieure. Le renforcement du cadre interne de l'UE dans le domaine de la sécurité est intrinsèquement lié au renforcement des partenariats et de la coopération avec les pays tiers. L'UE doit continuer à œuvrer activement à la manière dont l'engagement au niveau mondial peut contribuer à garantir la sécurité des citoyens sur son territoire.

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

Cybersécurité et résilience des infrastructures critiques

Dans le cadre de l'union de la sécurité, l'Union est déterminée à veiller à ce que tous les citoyens et entreprises européens soient bien protégés, tant en ligne que hors ligne, et à promouvoir un cyberespace ouvert, sûr et stable. L'ampleur, la fréquence et l'impact croissants des incidents de cybersécurité constituent une menace majeure pour le fonctionnement des systèmes de réseaux et d'information ainsi que pour le marché intérieur. La guerre d'agression menée par la Russie contre l'Ukraine a encore exacerbé cette menace et les tensions géopolitiques actuelles sont aggravées par les interventions d'une multiplicité d'acteurs de niveau étatique, criminels et hacktivistes. Le sabotage, à l'automne dernier, des gazoducs Nord Stream a souligné à quel point des secteurs essentiels tels que l'énergie, les infrastructures numériques, les transports et l'espace sont tributaires d'infrastructures critiques résilientes. L'incident récent concernant un gazoduc et un câble de données sous-marins en Estonie et en Finlande illustre la nécessité d'un niveau élevé de préparation pour faire face à des situations de ce genre. Bien que la cause des dommages reste floue et que des enquêtes soient en cours, le partage d'informations à différents niveaux entre les États membres et la Commission a été encourageant. Les perturbations n'ont eu aucun effet immédiat sur la connectivité internet ni sur la sécurité de l'approvisionnement en gaz au niveau européen ou local. Il s'agit là d'un signe des progrès accomplis et du renforcement des efforts de préparation de ces derniers mois.

Un cadre juridique clair et solide est donc essentiel pour garantir la protection et la résilience de ces infrastructures critiques. Dans ce contexte, une avancée décisive a été réalisée avec l'adoption en parallèle de la directive révisée concernant des mesures destinées à assurer un niveau élevé commun de cybersécurité dans l'ensemble de l'Union (directive SRI 2[4]) et de la directive sur la résilience des entités critiques (directive CER)[5], toutes deux entrées en vigueur le 16 janvier 2023. Les États membres sont à présent instamment invités à transposer rapidement et intégralement ces actes législatifs fondamentaux, au plus tard le 17 octobre 2024, afin de mettre en place un cadre solide de l'Union pour protéger les infrastructures critiques de l'Union contre les menaces physiques et les cybermenaces.

En juillet 2023, la Commission a défini dans un règlement délégué de la Commission des services essentiels dans les onze secteurs régis par la directive CER[6]. La prochaine étape consiste à ce que les États membres procèdent à des évaluations des risques liés à ces services. À la suite de la recommandation du Conseil[7] du 8 décembre 2022, les travaux se sont intensifiés en ce qui concerne les tests de résistance sur les infrastructures critiques, en commençant par le secteur de l'énergie, ainsi que le renforcement de la coopération avec l'OTAN et les principaux pays partenaires. Ces travaux ont abouti, en juin 2023, à un rapport de la task force UE-OTAN sur la résilience des infrastructures critiques, qui recense les défis actuels en matière de sécurité pour les infrastructures critiques dans quatre secteurs clés (énergie, transports, infrastructures numériques et espace) et formule des recommandations visant à renforcer la résilience. Ces recommandations, qui portent notamment sur le renforcement de la coordination, du partage d'informations et des exercices, sont mises en œuvre par les services de l'UE et de l'OTAN dans le cadre du dialogue structuré sur la résilience.

Parallèlement, le 6 septembre 2023, la Commission a adopté une proposition[8] de recommandation du Conseil relative à un schéma directeur visant à renforcer la coordination au niveau de l'Union en réponse aux tentatives de perturbation des infrastructures critiques ayant une dimension transfrontière notable. Le 4 octobre 2023, un exercice a été organisé sous la forme d'une discussion fondée sur des scénarios sur le schéma directeur afin de tester la manière dont il s'appliquerait dans la pratique et d'éclairer les négociations en cours sur la proposition au sein du Conseil.

À la suite des appels lancés par le Conseil[9], la Commission, le haut représentant et le groupe de coopération SRI ont procédé à des évaluations des risques et à l'élaboration de scénarios de risque du point de vue de la cybersécurité. Ces travaux se concentrent dans un premier temps sur les secteurs des télécommunications et de l'électricité. La participation de toutes les agences et de tous les réseaux concernés, civils et militaires, permet d'effectuer, pour la première fois, une évaluation globale et inclusive à l'échelle de l'Union. Cette évaluation complétera les évaluations coordonnées des risques pour la sécurité des chaînes d'approvisionnement critiques réalisées dans le cadre de la directive SRI 2, ainsi que les évaluations des risques et les tests de

---

4 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).

5 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.

6 C(2023) 4878.

7 Recommandation du Conseil du 8 décembre 2022 relative à une approche coordonnée à l'échelle de l'Union pour renforcer la résilience des infrastructures critiques.

8 COM(2023) 526.

9 Conclusions du Conseil du 23 mai 2022 sur la mise en place d'une posture cyber de l'Union européenne et appel de Nevers du 9 mars 2022 à renforcer les capacités de l'UE en matière de cybersécurité.

résistance sur les infrastructures critiques dans les secteurs de l'énergie, des infrastructures numériques, des communications, des transports et de l'espace. Dans un souci de coordination et de cohérence, ces activités devraient s'appuyer les unes sur les autres pour contribuer à établir une approche standard, et orienter le développement des exercices futurs. Le succès de ces actions dépendra à présent de la participation active des États membres.

Le fonctionnement des économies et des sociétés est de plus en plus tributaire des services et des données liés à l'espace, en particulier dans le domaine de la sécurité et de la défense. L'espace est un domaine stratégique de plus en plus disputé et son importance pour la sécurité s'est accrue en particulier à la suite de l'invasion de l'Ukraine par la Russie. La stratégie spatiale de l'UE pour la sécurité et la défense a été adoptée en mars 2023 pour renforcer notre position et notre autonomie stratégiques dans l'espace. La Commission européenne proposera en 2024, en tant qu'action clé découlant de cette stratégie, une législation spatiale de l'UE régissant la sûreté, la durabilité et la résilience/sécurité des activités spatiales dans l'UE.

En ce qui concerne la dimension extérieure, la sûreté des infrastructures sous-tend la résilience de l'économie et des chaînes d'approvisionnement mondiales[10] et, pour cette raison, la stratégie «Global Gateway» de l'UE intègre une forte dimension sécuritaire. De même, compte tenu des interconnexions entre les infrastructures de l'UE et celles des pays partenaires, il est essentiel d'accroître la coopération internationale pour renforcer la cyber-résilience mondiale et soutenir un cyberespace libre, ouvert, sûr et sécurisé.

Acte législatif sur la cyber-résilience

Il est primordial pour la cybersécurité européenne de veiller à ce que les consommateurs et les entreprises puissent compter sur des produits numériques sécurisés. La Commission s'est efforcée de répondre à ce besoin dans sa proposition de législation sur la cyber-résilience[11], adoptée le 15 septembre 2022. Cette législation introduirait des exigences horizontales obligatoires en matière de cybersécurité pour les produits comportant des éléments numériques pendant cinq ans ou tout au long de leur cycle de vie (selon ce qui est plus court). Elle créerait les conditions nécessaires à la conception et au développement de produits sécurisés comportant des éléments numériques, en faisant en sorte que les produits matériels et logiciels mis sur le marché présentent le moins de vulnérabilités possible. Cela constituerait une étape importante dans le relèvement des normes européennes en matière de cybersécurité dans tous les domaines et cette législation devrait devenir un point de référence international, offrant des avantages évidents au secteur de la cybersécurité de l'Union sur les marchés mondiaux. Le Parlement européen et le Conseil ont adopté leurs positions respectives en juillet 2023 et les négociations devraient progresser rapidement.

La certification de cybersécurité joue aussi un rôle crucial pour accroître la confiance dans les produits et services TIC, en permettant aux consommateurs, aux entreprises et aux autorités de faire des choix éclairés avec un niveau approprié de cybersécurité. Les travaux sur la certification de cybersécurité progressent, le schéma européen de certification de cybersécurité fondé sur des critères communs étant évalué dans le cadre de la comitologie. Le schéma candidat de certification de sécurité de l'UE des services en nuage est actuellement en cours d'élaboration par l'Agence de l'Union européenne pour la cybersécurité (ENISA) et fait l'objet de discussions au sein du groupe européen de certification de cybersécurité. Les travaux intensifs effectués avec un ensemble d'experts, de consommateurs et de fournisseurs devraient conduire à une approche juridique et technique solide offrant les garanties de sécurité nécessaires, conformes au droit de l'Union, aux engagements internationaux et aux obligations

[10] JOIN(2021) 30.
[11] COM(2022) 454.

prévues dans le cadre de l'OMC. Par ailleurs, l'ENISA prépare actuellement le schéma candidat EU5G et le portefeuille d'identité numérique de l'UE. Des efforts concertés de tous les États membres sont essentiels pour améliorer la sécurité globale des produits, services et processus TIC.

Règlements relatifs à la sécurité de l'information et à la cybersécurité pour les institutions, organes et organismes de l'UE

Proposés conjointement en mars 2022, les règlements proposés visant à régir la cybersécurité et la sécurité de l'information pour les institutions de l'Union ont évolué à des rythmes différents. Un accord politique a été conclu en juin dernier sur le règlement sur la cybersécurité, ce qui a permis de renforcer la position de l'ensemble des institutions, organes et organismes de l'UE en matière de cybersécurité et de refléter l'importance que l'UE attache à la mise en œuvre rapide de cette proposition. Dans ce contexte, la lenteur inattendue du processus relatif à la proposition parallèle sur la sécurité de l'information, essentielle pour achever un cadre législatif solide pour les institutions, organes et organismes de l'Union, est particulièrement préoccupante. Les deux propositions devraient être adoptées avant les élections au Parlement européen afin de rendre l'administration européenne crédible et résiliente dans le contexte géopolitique actuel. Un ensemble minimal de règles et de normes en matière de sécurité de l'information pour l'ensemble des institutions, organes et organismes de l'Union instaurerait un climat de sécurité pour toutes les parties concernées et garantirait une protection cohérente contre l'évolution des menaces pesant sur leurs informations, tant classifiées que non classifiées. Prises conjointement, ces nouvelles règles fourniraient une base stable pour un échange sécurisé d'informations entre les institutions, organes et organismes de l'Union et avec les États membres, avec des pratiques et des mesures normalisées visant à protéger les flux d'informations. À ce titre, elles répondent aux multiples appels du Conseil visant à renforcer la résilience des institutions, organes et organismes de l'Union et à mieux protéger le processus décisionnel de l'Union contre les ingérences malveillantes.

Règlement sur la cybersolidarité

Reposant sur le cadre stratégique, politique et législatif solide déjà en place, la proposition de règlement sur la cybersolidarité[12] adoptée le 18 avril 2023 par la Commission améliorerait encore la détection des cybermenaces, la résilience et la préparation à tous les niveaux de l'écosystème de cybersécurité de l'UE. Ces objectifs seraient mis en œuvre au moyen de trois actions principales:

(1) le déploiement d'un ***cyberbouclier européen*** afin de mettre en place et de développer des capacités communes de détection et d'appréciation de la situation. Ce cyberbouclier serait constitué de centres d'opérations de sécurité nationaux («SOC nationaux») et de centres d'opérations de sécurité transfrontières («SOC transfrontières»);
(2) la création d'un ***mécanisme d'urgence dans le domaine de la cybersécurité*** afin d'aider les États membres à se préparer aux incidents de cybersécurité importants et majeurs, à y réagir et à s'en rétablir immédiatement. Le soutien à la réaction aux incidents inclurait la réserve de cybersécurité de l'UE, qui serait aussi à la disposition des institutions, organes et organismes de l'Union ainsi que des pays tiers associés au programme pour une Europe numérique, à condition que leur accord d'association adopté au titre du programme pour une Europe numérique le prévoie;
(3) la mise en place d'un ***mécanisme européen d'analyse des incidents de cybersécurité*** afin d'analyser et d'évaluer les incidents de cybersécurité importants ou majeurs

[12] COM(2023) 209.

particuliers. Le rapport d'examen post-incident serait coordonné et élaboré par l'ENISA.

Les discussions ont débuté au Conseil et au Parlement européen. La conclusion des négociations avant la fin du mandat actuel du Parlement européen donnerait une impulsion majeure aux efforts visant à protéger les citoyens et les entreprises dans l'ensemble de l'Union.

Académie des compétences en matière de cybersécurité

Alors que les cybermenaces augmentent, l'UE a besoin de toute urgence de professionnels possédant les aptitudes et les compétences nécessaires pour prévenir, détecter et décourager les cyberattaques, ainsi que pour défendre l'UE contre celles-ci. Ses besoins en personnel dans le domaine de la cybersécurité sont actuellement estimés à 883 000 professionnels, tandis que les postes vacants étaient compris entre 260 000 et 500 000 en 2022. Toutes les composantes de la société devraient être encouragées à contribuer à combler cette lacune; en 2022, les femmes ne représentaient cependant que 20 % des diplômés en cybersécurité et 19 % des spécialistes des technologies de l'information et de la communication. Dans le cadre de l'Année européenne des compétences 2023, la Commission a adopté, le 18 avril 2023[13], une initiative saluée par les États membres[14] visant à mettre en place une Académie des compétences en matière de cybersécurité pour remédier au déficit de talents dans ce domaine. L'Académie des compétences en matière de cybersécurité réunirait les initiatives existantes relatives aux compétences en matière de cybersécurité et améliorerait la coordination. La Commission encourage les États membres, les autorités régionales et locales, ainsi que les entités publiques européennes, à adopter des stratégies ou initiatives spécifiques sur les compétences en matière de cybersécurité, ou à intégrer lesdites compétences dans les stratégies ou initiatives pertinentes ayant un champ d'application plus large (par exemple, cybersécurité, compétences numériques, emploi, etc.). La participation de parties prenantes privées sera également essentielle pour réduire la pénurie de compétences en matière de cybersécurité et la pénurie de main-d'œuvre y afférente en Europe.

Drones

L'utilisation malveillante de drones représente une autre menace croissante pour les espaces publics et les infrastructures critiques. Les incidents impliquant des drones sont devenus plus fréquents à l'intérieur et à l'extérieur de l'Union, et les solutions antidrones constituent un outil essentiel pour les services répressifs et les autres autorités publiques de l'Union, ainsi que pour les opérateurs privés d'infrastructures critiques. Dans le même temps, l'utilisation légitime des drones apporte une contribution importante à la double transition écologique et numérique[15]. Comme annoncé dans la stratégie Drone 2.0 adoptée en novembre 2022, la Commission adopte aujourd'hui une communication relative à la lutte contre les menaces potentielles posées par les drones, étayée par deux manuels contenant des orientations pratiques sur les principaux aspects techniques[16]. Cette initiative vise à offrir un cadre d'action global et harmonisé, en forgeant une compréhension commune des règles en place pour lutter contre les menaces que pourraient représenter les drones et s'adapter, le cas échéant, à l'évolution rapide de la technologie. Les États membres et les opérateurs privés concernés sont invités à collaborer étroitement avec la Commission afin de garantir sa mise en œuvre intégrale.

[13] COM(2023) 207.
[14] Conclusions du Conseil du 22 mai 2023 sur la politique de cyberdéfense de l'UE.
[15] COM(2022) 652.
[16] COM (2023) 659.

Sûreté maritime et aérienne

Les activités illicites, telles que la piraterie, les vols à main armée en mer, le trafic de migrants et la traite des êtres humains, le trafic d'armes et de stupéfiants, ainsi que le terrorisme, demeurent des défis pour la sécurité maritime et la situation est aggravée par l'évolution des menaces, y compris les attaques hybrides et les cyberattaques. Le 10 mars 2023, la Commission et le haut représentant ont adopté une communication conjointe sur la mise à jour de la stratégie de sûreté maritime de l'UE[17], qui devrait maintenant être mise en œuvre conformément au plan d'action actualisé.

Dans le domaine de la sûreté aérienne, la Commission a adopté, le 2 février 2023, un document de travail des services de la Commission intitulé «Working towards an enhanced and more resilient aviation security policy»[18] (Pour une politique de sûreté aérienne renforcée et plus résiliente), qui comporte un programme ambitieux destiné 1) à moderniser l'architecture réglementaire de la sûreté aérienne; 2) à favoriser le développement et l'adoption de solutions plus innovantes; et 3) à mettre à jour les exigences de base en matière de sûreté aérienne afin que les aéroports de l'Union puissent tirer pleinement parti des technologies nouvelles et de pointe pour faire face aux menaces les plus prioritaires. Quatorze actions phares doivent être mises en œuvre dans un délai de deux ans.

La Commission invite le Parlement européen et le Conseil à conclure les négociations de toute urgence, en tout état de cause avant la fin du mandat de l'actuel Parlement européen, sur les dossiers suivants:

- la proposition d'acte législatif sur la cyber-résilience;
- la proposition de règlement sur la cybersolidarité;
- la proposition de règlement sur la sécurité de l'information pour les institutions, organes et organismes de l'Union.

La Commission invite les États membres à:

- assurer en priorité la transposition de la directive sur la résilience des entités critiques, et effectuer les tests de résistance sur les infrastructures critiques dans le secteur de l'énergie;
- adopter la recommandation du Conseil relative à un schéma directeur visant à coordonner la réponse en cas de perturbations des infrastructures critiques ayant une dimension transfrontière notable;
- transposer intégralement et de toute urgence la directive SRI 2 afin de renforcer la cybersécurité des entités essentielles et importantes;
- participer activement à la réalisation d'évaluations des risques en matière de cybersécurité et à l'élaboration de scénarios de risque pour les infrastructures critiques et les chaînes d'approvisionnement;
- assurer le suivi de l'Académie des compétences en matière de cybersécurité grâce à une participation active au niveau européen et à des stratégies ou initiatives nationales spécifiques sur les compétences en matière de cybersécurité, en associant les principales parties prenantes, y compris les autorités régionales et locales;
- collaborer avec les opérateurs privés concernés et la Commission pour garantir la mise en œuvre de toutes les actions énumérées dans la communication relative à la lutte contre les menaces potentielles posées par les drones;

[17] JOIN(2023) 8.
[18] SWD(2023) 37.

- mettre en œuvre le plan d'action de la stratégie de sûreté maritime de l'UE et faire régulièrement rapport sur les résultats obtenus;
- mettre en œuvre les 14 actions phares recensées pour renforcer la sûreté aérienne.

III. Faire face à l'évolution des menaces

Les nouvelles tensions géopolitiques montrent clairement que le défi sécuritaire auquel est confrontée l'UE est toujours plus grand, mais aussi de plus en plus imprévisible et accentué par la nature hybride de nombreuses menaces. La sécurité doit également suivre l'évolution de la société et des technologies. La pandémie de COVID-19 a offert de nouvelles possibilités aux cybercriminels et a notamment permis une prolifération des contenus pédopornographiques en ligne. Les criminels et les acteurs mal intentionnés sont toujours prêts à exploiter les évolutions technologiques. Face à de telles menaces, souvent complexes et multidimensionnelles, l'UE doit agir avec force et cohérence.

Le règlement relatif à la lutte contre les abus sexuels commis contre des enfants en ligne

L'évaluation, réalisée par Europol, de la menace que représente la criminalité organisée sur l'internet a révélé qu'en 2022, l'exploitation sexuelle des enfants et les abus sexuels commis contre eux avaient encore augmenté, tant en fréquence qu'en gravité, les contrevenants continuant à tirer parti des possibilités techniques de masquer leurs actions et leur identité[19]. Le système actuel fondé sur la détection et le signalement volontaires par les entreprises s'est révélé insuffisant pour protéger les enfants. Un règlement provisoire permet la détection et la déclaration volontaires par les entreprises, pour autant qu'elles soient conformes au règlement général sur la protection des données (RGPD). Or ce règlement provisoire expirera en août 2024. En mai 2022, la Commission a donc proposé un règlement[20] visant à lutter contre l'utilisation abusive de services en ligne à des fins d'abus sexuels sur enfants. Le cadre proposé met fortement l'accent sur la prévention. Les entreprises seraient tenues d'évaluer le risque que des abus sexuels soient commis contre des enfants par l'intermédiaire de leurs systèmes et de prendre des mesures préventives. En dernier ressort, en cas de risque important uniquement, des juridictions nationales ou des autorités administratives indépendantes pourraient adresser des injonctions de détection ciblées aux fournisseurs de services. Un nouveau centre de l'UE indépendant viendrait faciliter les efforts des fournisseurs de services, en agissant en tant que pôle d'expertise, en fournissant des informations fiables sur les contenus détectés, en recevant et en analysant les signalements en ligne d'abus sexuels commis contre des enfants transmis par les fournisseurs, afin d'identifier les signalements erronés, et en apportant un soutien aux victimes. Il est essentiel que les nouvelles règles soient adoptées et mises en œuvre dès que possible afin de protéger les enfants contre de nouveaux abus, d'empêcher la réapparition en ligne des contenus effacés et de traduire les auteurs d'infractions en justice. Des négociations sont en cours au Conseil et au Parlement dans le but de parvenir à un accord sur ce dossier avant la fin de la législature du Parlement.

[19] Europol (2023), Évaluation de la menace que représente la criminalité organisée sur l'internet (IOCTA) 2023.
[20] COM(2022) 209.

La directive sur la lutte contre les violences à l'égard des femmes et les violences domestiques

La cyberviolence à l'égard des femmes, y compris dans le contexte des violences domestiques, est apparue comme une nouvelle forme de violence, qui s'étend au-delà des frontières nationales des États membres par l'intermédiaire de l'internet et des outils informatiques. En mars 2022, la Commission a proposé une directive visant à lutter contre les violences à l'égard des femmes et les violences domestiques, qui comportait des règles spécifiques sur la cyberviolence et des mesures visant à combler les lacunes en matière de protection, d'accès à la justice et de prévention. Une adoption et une mise en œuvre rapides fourniraient aux États membres des outils supplémentaires pour lutter contre ces formes de criminalité. Les colégislateurs ont entamé leurs négociations interinstitutionnelles en juillet 2023 et ont pour objectif de finaliser ces négociations avant la fin de la législature actuelle du Parlement européen.

La cybersécurité des réseaux 5G

La sécurité des réseaux 5G est une priorité majeure pour la Commission et un élément essentiel de sa stratégie pour l'union de la sécurité. Les réseaux 5G constituent une infrastructure centrale qui jette les bases d'un large éventail de services essentiels au fonctionnement du marché intérieur et à des fonctions sociétales et économiques vitales. Le 15 juin 2023, les autorités des États membres de l'UE représentées au sein du groupe de coopération SRI, avec le soutien de la Commission et de l'ENISA, ont publié un deuxième rapport sur l'état d'avancement de la mise en œuvre de la boîte à outils de l'UE sur la cybersécurité des réseaux 5G. Selon ce rapport, 24 États membres ont déjà adopté ou élaborent actuellement des mesures législatives conférant à leurs autorités nationales le pouvoir d'évaluer les fournisseurs et d'émettre des restrictions, et 10 États membres ont effectivement imposé de telles restrictions. Toutefois, des mesures supplémentaires sont nécessaires pour éviter les vulnérabilités pour l'Union dans son ensemble, qui pourraient avoir des incidences négatives graves sur la sécurité des utilisateurs individuels et des entreprises dans toute l'Union et des infrastructures critiques de l'Union. Tous les États membres doivent mettre en œuvre la boîte à outils sans délai. Le même jour, la Commission a adopté une communication sur la mise en œuvre de la boîte à outils par les États membres ainsi que sur ses propres communications institutionnelles et sur les activités de financement de l'Union. Il s'agissait de mettre en évidence les préoccupations sérieuses qui se posent au sujet des risques que les fournisseurs d'équipements de communication de réseaux mobiles Huawei et ZTE font peser sur la sécurité de l'UE. Dans ce contexte, la Commission prend des mesures pour éviter que ses propres communications institutionnelles soient exposées aux réseaux mobiles utilisant Huawei et ZTE en tant que fournisseurs. Les marchés publics empêcheront de souscrire à de nouveaux services de connectivité reposant sur des équipements provenant de ces fournisseurs, et la Commission coopérera avec les États membres et les opérateurs de télécommunications pour assurer le retrait progressif de ces fournisseurs des services de connectivité existants utilisés sur les sites de la Commission. La Commission étudie également comment intégrer cette décision dans les programmes et instruments de financement pertinents de l'Union, dans le plein respect du droit de l'Union.

L'accès aux données en vue d'une répression efficace

À notre époque numérique, presque toutes les formes de criminalité comportent une composante numérique. Les technologies et les outils sont également utilisés à des fins criminelles, y compris ceux qui sont nécessaires pour garantir les besoins de notre société en matière de cybersécurité, de protection des données et de respect de la vie privée. Il est donc de plus en plus difficile de maintenir des services répressifs efficaces dans l'ensemble de l'UE afin de préserver la sécurité publique et de prévenir et détecter les infractions pénales, d'enquêter

sur celles-ci et de poursuivre leurs auteurs; même si des efforts considérables ont été déployés au niveau de l'Union et au niveau national, y compris au moyen d'actes législatifs et d'initiatives de renforcement des capacités et d'innovation, des défis juridiques et techniques persistent. La Commission, en y associant la présidence du Conseil, a mis en place un groupe de haut niveau sur l'accès aux données en vue d'une répression efficace afin de fournir une plateforme collaborative à un large éventail de parties prenantes et d'experts pour leur permettre d'étudier les défis auxquels sont confrontés les praticiens des services répressifs (le cryptage, la conservation des données, la 5G et la normalisation, par exemple). La Commission attend du groupe de haut niveau qu'il formule des recommandations équilibrées, solides et réalisables d'ici juin 2024, prenant en compte la complexité de ces questions, y compris du point de vue de la cybersécurité et de la protection des données. Les États membres et les experts participants sont donc encouragés à participer activement à ce processus et à œuvrer à l'élaboration de solutions efficaces, légales et communément acceptées.

Les menaces hybrides

Dans un contexte géopolitique où les menaces hybrides sont de plus en plus complexes et sophistiquées, la boussole stratégique de l'UE en matière de sécurité et de défense[21] (ci-après, la «boussole stratégique») a fourni une évaluation commune des menaces et des défis auxquels l'Union est confrontée, ainsi qu'un plan d'action stratégique. L'augmentation des comportements malveillants dans le cyberespace de la part des États et des acteurs non étatiques, y compris dans le contexte de la guerre contre l'Ukraine, a encore plus mis en évidence l'importance du cyberespace en tant que domaine de politique étrangère et de sécurité. Les risques potentiels d'actions malveillantes et de désinformation requièrent une vigilance particulière en période électorale, notamment dans la perspective des élections européennes de 2024.

Compte tenu des risques élevés de retombées négatives, l'UE a continué de développer des activités de renforcement des capacités en matière de cybersécurité et d'encourager les partenariats avec les pays tiers, y compris au moyen de dialogues spécifiques sur le cyberespace, afin de contribuer activement à sa résilience globale. Un certain nombre d'outils ont été mis au point, révisés et améliorés pour renforcer la capacité de l'Union à faire face efficacement aux menaces hybrides, comme décrit dans le 7e rapport d'avancement sur les menaces hybrides, publié le 14 septembre 2023[22]. Parmi ces outils figurent:

- la boîte à outils hybride de l'UE visant à garantir un cadre pour une réponse coordonnée et éclairée aux menaces et aux campagnes hybrides;
- les travaux en cours visant à mettre en place des équipes d'intervention rapide de l'UE en cas de menaces hybrides pour un soutien adapté à court terme aux États membres, aux pays partenaires et aux missions et opérations relevant de la politique de sécurité et de défense commune (PSDC);
- le protocole révisé de l'Union européenne en matière de lutte contre les menaces hybrides («EU Playbook»)[23], qui décrit les processus et les structures de l'Union permettant de faire face aux menaces et aux campagnes hybrides;
- les lignes directrices révisées pour la mise en œuvre du cadre pour une réponse diplomatique conjointe de l'UE face aux actes de cybermalveillance[24] («boîte à outils cyberdiplomatique»), qui permettent d'élaborer des stratégies durables, adaptées, cohérentes et coordonnées contre les acteurs persistants de cybermenaces;

[21] Document 7371/22 du Conseil.
[22] SWD(2023) 315.
[23] SWD(2023) 116.
[24] 10289/23 du 8 juin 2023.

- la boîte à outils pour lutter contre les activités de manipulation de l'information et d'ingérence menées depuis l'étranger (FIMI), afin de renforcer les outils existants de l'Union pour prévenir et dissuader ces activités ou pour y réagir;
- la politique de cyberdéfense de l'UE[25], qui vise à renforcer les capacités de cyberdéfense de l'UE, à améliorer la connaissance de la situation et à coordonner l'ensemble des options défensives disponibles, afin de stimuler la résilience, de réagir aux cyberattaques et de garantir la solidarité et l'assistance mutuelle.

Les États membres sont donc encouragés à poursuivre et à renforcer leur coopération dans ce domaine, en veillant à la mise en œuvre effective des boîtes à outils susmentionnées, y compris au moyen d'exercices réguliers, et en parvenant à un accord sur le concept d'équipes d'intervention rapide en cas de menaces hybrides, qui fournira des orientations pour la mise en place des équipes.

L'intelligence artificielle dans le contexte répressif

L'intelligence artificielle (IA) s'est rapidement inscrite dans nos vies quotidiennes. Les effets de l'utilisation de l'IA sur la cybercriminalité et la cybersécurité ne sont pas encore pleinement connus, mais poseront clairement de nouveaux défis. Si l'IA peut être bénéfique lorsqu'elle est utilisée de manière sûre et contrôlée, elle peut présenter un potentiel dangereux entre les mains d'acteurs malveillants, notamment en aidant les criminels à dissimuler leur identité dans des crimes tels que le terrorisme et les abus sexuels commis contre des enfants. Il est donc essentiel que les autorités suivent les dernières évolutions technologiques afin de prévenir les abus et d'y réagir[26]. Les négociations sur la proposition de législation sur l'intelligence artificielle visent à traiter ces questions et sont entrées dans une phase cruciale, les colégislateurs discutant à présent de questions techniques et politiques qui détermineront les interactions avec cette technologie dans les années à venir. Il sera primordial de trouver des solutions équilibrées, notamment en ce qui concerne les applications à haut risque, y compris dans le domaine répressif.

La Commission invite le Parlement européen et le Conseil à conclure les négociations interinstitutionnelles de toute urgence, en tout état de cause avant la fin de la législature de l'actuel Parlement européen, sur les dossiers suivants:

- la proposition de règlement relatif à la lutte contre les abus sexuels commis contre des enfants en ligne;
- la proposition de directive sur la lutte contre les violences à l'égard des femmes et les violences domestiques;
- la proposition de règlement établissant des règles harmonisées en matière d'intelligence artificielle (législation sur l'IA).

La Commission invite les États membres à:

- mettre en œuvre, intégralement et sans délai, la boîte à outils de l'UE sur la cybersécurité des réseaux 5G;
- soutenir les travaux du groupe de haut niveau sur l'accès aux données pour des services répressifs efficaces, en vue de formuler des recommandations claires, solides

[25] JOIN(2022) 49.

[26] Voir, par exemple, le rapport d'Europol publié le 17 avril 2023: ChatGPT – The impact of Large Language Models on Law Enforcement (ChatGPT – L'impact des grands modèles linguistiques sur le système répressif).

et réalisables afin de répondre de manière proportionnée aux défis actuels et prévisibles;

- prendre des mesures, en coopération avec le haut représentant, pour assurer la mise en œuvre effective de la boîte à outils hybride de l'UE, de la boîte à outils cyberdiplomatique révisée et de la boîte à outils FIMI, y compris au moyen d'exercices réguliers et en tenant compte des dynamiques mondiales;
- parvenir à un accord sur le concept d'équipes d'intervention rapide en cas de menaces hybrides.

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

Le risque que des événements mondiaux ou locaux provoquent de nouvelles flambées de terrorisme est toujours présent. Parallèlement, la criminalité organisée et le trafic de drogues figurent parmi les menaces les plus graves pour la sécurité de l'UE. Afin d'intensifier les efforts collectifs de l'Union dans la lutte contre ces menaces, des travaux collectifs sont actuellement menés pour mettre en œuvre la stratégie de l'UE visant à lutter contre la criminalité organisée[27], la stratégie de l'UE visant à lutter contre la traite des êtres humains[28], le programme et le plan d'action antidrogue de l'UE[29] et le programme de lutte antiterroriste pour l'UE[30]. Toutefois, pour réagir à la détérioration inquiétante de la situation en matière de criminalité organisée et de trafic de drogues, il est nécessaire que les États membres et l'UE intensifient encore leurs efforts pour renforcer notre action collective face aux réseaux criminels et pour mieux protéger les victimes de la criminalité. Une feuille de route de l'UE en matière de lutte contre le trafic de drogues et la criminalité organisée est publiée en même temps que le présent rapport[31].

Dans le domaine de la lutte antiterroriste, l'UE enrichit également la palette d'instruments dont elle dispose pour son action extérieure[32], en tirant pleinement parti des dialogues de haut niveau sur la lutte contre le terrorisme et du réseau d'experts en matière de sécurité/lutte contre le terrorisme dans les délégations de l'UE, ainsi que par son engagement dans les enceintes multilatérales, y compris en tant que coprésident du Forum mondial de lutte contre le terrorisme (GCTF).

Le trafic de drogues

Grâce au nouveau mandat de l'Agence de l'UE pour les drogues, qui s'appliquera à partir de juillet 2024, l'UE sera mieux équipée pour faire face à un problème complexe de sécurité et de santé qui touche des millions de personnes dans l'UE et dans le monde. La Commission procède

[27] COM(2021) 170.
[28] COM(2021) 171.
[29] COM(2020) 606.
[30] COM (2020) 795.
[31] COM (2023) 641.
[32] Comme le préconisent la boussole stratégique et les conclusions du Conseil intitulées «Faire face à une menace terroriste et extrémiste violente en constante évolution dans sa dimension extérieure», adoptées en juin 2022.

également à la révision[33] des règlements sur les précurseurs de drogues[34], afin de relever les principaux défis recensés dans le cadre de l'évaluation de 2020[35], qui avait mis en avant la nécessité de remédier aux problèmes causés par les précurseurs de drogues[36], en vue de réduire l'offre de drogues illicites.

Toutefois, face à l'augmentation sans précédent de la quantité de drogues illicites disponibles en Europe, la lutte contre le trafic de drogues doit s'intensifier, en coopération avec les partenaires internationaux. Des mesures supplémentaires doivent être prises par les États membres et par l'UE pour démanteler les réseaux criminels et mieux protéger les victimes de la criminalité. La Commission présente aujourd'hui une feuille de route de l'UE en matière de lutte contre le trafic de drogues et la criminalité, qui définit 17 mesures ciblées dans quatre domaines prioritaires: renforcement de la résilience des plateformes logistiques grâce à une alliance des ports européens; démantèlement des réseaux criminels; intensification des efforts de prévention; et renforcement de la coopération avec les partenaires internationaux. Ces mesures doivent être mises en œuvre en 2024 et 2025.

Les armes à feu

Le trafic d'armes à feu alimente la criminalité organisée au sein de l'UE et dans son voisinage. Selon les estimations, pas moins de 35 millions d'armes à feu illicites sont entre les mains de civils dans l'UE, et environ 630 000 armes à feu sont répertoriées comme étant volées ou perdues dans le système d'information Schengen. Avec l'essor de la livraison rapide de colis et de nouvelles technologies comme l'impression 3D, le trafic d'armes à feu prend de nouvelles formes afin d'échapper aux contrôles. La guerre d'agression menée par la Russie contre l'Ukraine a également accru le risque de prolifération des armes à feu. En octobre 2022, la Commission a adopté une proposition visant à mettre à jour la législation applicable à l'importation, à l'exportation et au transit d'armes à feu à usage civil, afin de combler les lacunes des règles existantes et d'empêcher ainsi l'augmentation du nombre d'armes à feu volées et détournées vers l'UE[37]. À moyen terme, ces nouvelles règles contribueront à réduire le risque de contournement des embargos dans le cas des exportations d'armes à feu à usage civil et à renforcer le contrôle des importations de ce type d'armes depuis les pays tiers. Les deux colégislateurs doivent encore adopter leurs positions sur ce dossier, l'objectif étant de parvenir à un accord sur ce dernier avant la fin de la législature du Parlement.

La traite des êtres humains

La traite des êtres humains est une forme particulièrement grave de criminalité organisée et constitue une violation grave des droits fondamentaux. Dans l'UE, les victimes de la traite le sont essentiellement à des fins d'exploitation sexuelle ou d'exploitation par le travail, mais aussi de mendicité forcée, de criminalité forcée et d'autres formes d'exploitation. En décembre 2022, la Commission a proposé de modifier la directive relative à la lutte contre la traite des êtres humains[38], en actualisant les règles afin de remédier aux lacunes du cadre juridique actuel. En particulier, une fois adoptée, la directive révisée ajouterait le mariage forcé et l'adoption illégale au champ d'application de la directive et introduirait également une référence explicite à la dimension en ligne de la traite des êtres humains. Elle comprendrait en outre un régime

[33] Précurseurs de drogues – législation de l'UE (révision des règles) (europa.eu)

[34] Règlement (CE) n° 273/2004 relatif aux précurseurs de drogues et règlement (CE) n° 111/2005 du Conseil fixant des règles pour la surveillance du commerce des précurseurs des drogues entre la Communauté et les pays tiers.

[35] COM(2020) 768.

[36] Action 23 du plan d'action antidrogue, COM(2020) 606.

[37] COM (2022) 480.

[38] COM(2022) 732.

obligatoire de sanctions pour les auteurs d'infractions et formaliserait la mise en place de mécanismes d'orientation nationaux afin d'améliorer l'identification précoce et la prise en charge transfrontière en vue de l'assistance et du soutien aux victimes. Avoir sciemment recours aux services fournis par les victimes de la traite des êtres humains deviendrait une infraction et la collecte annuelle de données sur la traite des êtres humains, qui seraient publiées par Eurostat, deviendrait obligatoire. Le Conseil a adopté son orientation générale en juin 2023 et le Parlement européen doit encore adopter sa position. Une action rapide sera nécessaire pour parvenir à un accord avant la fin de la législature du Parlement.

La criminalité environnementale

La criminalité environnementale est devenue une menace mondiale, qui affiche un taux de croissance estimé entre 5 et 7 % chaque année. Les bénéfices considérables qu'elle peut générer, les lacunes juridiques qui résultent des différences de législation entre les États membres et le faible risque de détection sont autant d'attraits importants pour la criminalité organisée. Selon des indices relevés par Europol, le produit de ces activités sert au financement du terrorisme. En décembre 2021, la Commission a adopté une proposition visant à remplacer la directive de 2008 relative à la protection de l'environnement par une législation pénale. Cette proposition vise essentiellement à affiner et à mettre à jour les définitions des catégories d'infractions environnementales et à définir des types et des niveaux de sanctions efficaces, dissuasifs et proportionnés pour les personnes physiques et les personnes morales. Parmi les nouvelles infractions figurent celles liées à la déforestation illégale, les infractions à la législation de l'UE sur les produits chimiques, celles liées à l'extraction illégale des eaux de surface ou souterraines et celles liées au recyclage illégal de navires. La proposition vise à renforcer considérablement la chaîne répressive et la coopération transfrontière entre les autorités des États membres et les agences et organes de l'UE. Le Parlement européen et le Conseil ont adopté leurs positions respectives sur la proposition et mènent actuellement des négociations qui devraient pouvoir se conclure d'ici la fin de l'année. Un plan d'action révisé[39] contre le trafic des espèces sauvages doit en outre être mis en œuvre afin de renforcer encore la prévention et la répression dans ce domaine.

Le recouvrement et la confiscation d'avoirs

Pour démanteler la criminalité organisée, il est essentiel de priver les criminels de leurs revenus illicites. C'est pourquoi, outre la proposition permettant aux services répressifs d'accéder aux informations relatives aux comptes bancaires dans l'ensemble de l'UE[40] (pour laquelle un accord politique a été conclu en juin 2023), la Commission a présenté, en mai 2022, une proposition sur le recouvrement et la confiscation d'avoirs[41], afin de renforcer les capacités en matière de dépistage, d'identification, de gel, de confiscation et de gestion d'avoirs. Les principales dispositions de la proposition concernent les exigences en matière d'enquêtes financières et les pouvoirs et outils supplémentaires des bureaux de recouvrement d'avoirs, ainsi que des mesures de gel et de confiscation plus efficaces pour un ensemble élargi d'infractions. L'une des nouvelles infractions pénales pour lesquelles ces mesures seraient rendues applicables est la violation des mesures restrictives de l'Union. En décembre 2022, la Commission a adopté une proposition distincte visant à harmoniser les définitions des infractions pénales et des sanctions applicables en cas de violation des mesures restrictives de l'Union. La mise en œuvre et l'application effectives des mesures restrictives de l'Union restent une priorité absolue pour la Commission, soutenue par les travaux de la task-force «gel et

[39] COM(2022) 581.
[40] COM(2021) 429.
[41] COM(2022) 245.

saisie» mise en place par la Commission en réponse à la guerre d'agression menée par la Russie contre l'Ukraine. Pour les deux propositions, le Parlement européen et le Conseil ont adopté leurs positions respectives, l'objectif étant de parvenir à un accord d'ici la fin de l'année.

Le train de mesures relatif à la lutte contre le blanchiment de capitaux

Il est quasiment toujours question de blanchiment de capitaux dès lors que des activités criminelles génèrent des produits dans l'UE[42]; c'est donc un angle d'attaque essentiel pour lutter contre la criminalité dans l'UE. En juillet 2021, la Commission a présenté des propositions ambitieuses visant à renforcer les mesures de l'UE contre le blanchiment de capitaux et le financement du terrorisme[43], avec quatre propositions législatives visant à renforcer la prévention et la détection des tentatives criminelles de blanchir des produits illicites ou de financer des activités terroristes par l'intermédiaire du système financier. L'une des quatre initiatives du train de mesures, qui vise à garantir la traçabilité des transferts de crypto-actifs, a été adoptée par les colégislateurs en mai 2023[44]. Ce règlement entrera en vigueur le 30 décembre 2024, date à laquelle tous les prestataires de services sur crypto-actifs devront collecter et détenir des informations sur l'expéditeur et le bénéficiaire de transferts de crypto-actifs. Les trois autres propositions visent i) à créer une nouvelle autorité européenne de lutte contre le blanchiment de capitaux afin d'assurer une surveillance cohérente et de haute qualité dans l'ensemble du marché intérieur, y compris pour les entités transfrontières les plus risquées, en soutenant et en coordonnant le travail des cellules de renseignement financier, ii) à établir des règles harmonisées pour le secteur privé, y compris l'introduction d'une limite de 10 000 EUR à l'échelle de l'UE pour les paiements en espèces d'un montant élevé en échange de services et de biens, et iii) à renforcer les pouvoirs et les outils de coopération des autorités compétentes. Ce train de mesures devrait renforcer considérablement la capacité de l'UE à lutter contre le blanchiment de capitaux et à protéger ses citoyens du terrorisme et de la criminalité organisée. Des négociations sont en cours entre les colégislateurs au sujet des trois dernières propositions, dans le but de parvenir à un accord sur ce dossier avant la fin de la législature du Parlement.

La Commission invite le Parlement européen et le Conseil à conclure les négociations interinstitutionnelles de toute urgence, en tout état de cause avant la fin de la législature de l'actuel Parlement européen, sur les dossiers suivants:

- la proposition de directive relative au recouvrement et à la confiscation d'avoirs;
- la proposition de directive relative à l'harmonisation des définitions des infractions pénales et des sanctions applicables en cas de violation des mesures restrictives de l'Union;
- la proposition de directive sur la lutte contre la traite des êtres humains;
- la proposition de directive visant à améliorer la protection de l'environnement par le droit pénal;
- la proposition de train de mesures relatives à la lutte contre le blanchiment de capitaux;

[42] Europol, Enterprising criminals – Europe's fight against the global networks of financial and economic crime (Entreprises criminelles – La lutte de l'Europe contre les réseaux mondiaux de criminalité financière et économique), 2020.

[43] COM(2021) 420.

[44] Règlement (UE) 2023/1113 du 31 mai 2023 sur les informations accompagnant les transferts de fonds et de certains crypto-actifs, et modifiant la directive (UE) 2015/849.

- la proposition visant à actualiser la législation existante sur l'importation, l'exportation et le transit d'armes à feu à usage civil.

La Commission invite les États membres et les agences et organes de l'UE à:
- coopérer en vue de la mise en œuvre des 17 mesures de la feuille de route de l'UE en matière de lutte contre le trafic de drogues et la criminalité organisée en 2023 et 2024.

V. Un solide écosystème européen de la sécurité

Les menaces pour la sécurité ayant acquis un caractère de plus en plus transfrontière ces dernières années, davantage de synergies et une coopération plus étroite à tous les niveaux sont nécessaires pour y faire face. Depuis l'adoption de la stratégie de l'UE pour l'union de la sécurité, d'importantes initiatives ont été prises pour tirer le meilleur parti possible de la coopération transfrontière, rationalisant et modernisant les instruments et procédures disponibles, tant aux frontières extérieures qu'au sein de l'espace Schengen, et améliorant l'échange d'informations entre les services répressifs et les autorités judiciaires afin de mieux lutter contre la criminalité organisée. Dans ce contexte, la mise en œuvre effective du cadre d'interopérabilité pour l'échange de données constitue un pilier important en vue de renforcer la sécurité; elle constitue une réponse européenne efficace aux menaces transfrontières, tout en garantissant la libre circulation à l'intérieur de l'Union demeurant.

Renforcement de l'échange d'informations au sein de l'espace Schengen: informations préalables sur les passagers (API), dossiers passagers (PNR) et Prüm II

Les deux propositions relatives aux données API adoptées par la Commission en décembre 2022[45] renforceraient la sécurité intérieure de l'Union en dotant les services répressifs des États membres d'outils supplémentaires pour lutter contre les formes graves de criminalité et le terrorisme. En particulier, l'utilisation conjointe des informations préalables sur les passagers des vols effectués au sein de l'Union et des données des dossiers passagers (données PNR) des voyageurs aériens permettraient aux services répressifs des États membres d'être beaucoup plus efficaces dans leurs enquêtes et de mener des opérations plus ciblées. Il est important que les règles proposées soient adoptées dans les meilleurs délais: non seulement elles soutiendraient la lutte contre la criminalité organisée et le terrorisme, mais elles réduiraient aussi drastiquement la nécessité de contrôles systématiques de l'ensemble des voyageurs en cas de réintroduction temporaire de contrôles aux frontières intérieures et, partant, faciliteraient les voyages aériens et la mise en œuvre de la liberté de circulation. Le 6 septembre 2023, la Commission européenne a recommandé au Conseil d'autoriser des négociations avec la Suisse, l'Islande et la Norvège en vue de la conclusion d'accords sur le transfert des données PNR. L'adoption de ces trois recommandations favoriserait la cohérence et l'efficacité de la politique extérieure de l'Union en ce qui concerne les PNR.

La police procède quotidiennement à des «échanges Prüm» dans leur lutte contre la criminalité organisée, la criminalité liée aux stupéfiants, le terrorisme, l'exploitation sexuelle et la traite des êtres humains. L'objectif de la proposition de règlement relatif à l'échange automatisé de

[45] COM(2022) 729, COM(2022) 73.

données dans le cadre de la coopération policière («Prüm II»)[46] est de réviser le cadre Prüm actuellement en vigueur en vue de combler les lacunes en matière d'information et de renforcer la prévention et la détection des infractions pénales dans l'UE ainsi que les enquêtes en la matière. Les règles révisées relatives à l'échange automatisé de données dans le cadre de la coopération policière complètent les propositions relatives à la coopération policière dans le cadre du présent mandat, de même que la recommandation du Conseil déjà adoptée visant à renforcer la coopération transfrontière opérationnelle et la directive relative à l'échange d'informations entre les services répressifs. L'adoption et la mise en œuvre rapides de ces instruments connexes amélioreraient, faciliteraient et accéléreraient l'échange de données entre les services répressifs et contribueraient à l'identification des criminels.

Un système de gestion des frontières pleinement interopérable pour un espace Schengen sûr, solide, numérique et uni

Le bon fonctionnement d'un espace Schengen sans frontières intérieures repose sur la confiance mutuelle entre les États membres, laquelle dépend de l'efficacité des contrôles, qu'il s'agisse des contrôles effectués aux frontières extérieures de l'Union ou d'autres mesures de contrôle mises en œuvre sur le territoire des États membres. La modification du code frontières Schengen[47] proposée par la Commission définit la manière dont les États membres peuvent davantage tirer parti de solutions autres que les contrôles aux frontières intérieures, susceptibles d'offrir un niveau élevé de sécurité. Il est important que la modification du code frontières Schengen soit adoptée et mise intégralement en œuvre afin de garantir un niveau de sécurité élevé et proportionné au sein de l'espace Schengen. Par ailleurs, le déploiement de la nouvelle architecture des systèmes d'information de l'UE se poursuit. Celle-ci vise à mieux soutenir les efforts déployés par les autorités nationales pour garantir la sécurité et veiller à la bonne gestion des frontières. Cette architecture comprend le système d'information Schengen renouvelé, le système européen d'information et d'autorisation concernant les voyages, le système d'entrée/de sortie, l'actualisation du système d'information sur les visas et le cadre d'interopérabilité visant à relier les systèmes entre eux en toute sécurité. Une fois parachevée, cette nouvelle architecture fournirait aux autorités nationales des informations plus complètes et plus fiables en matière de sécurité. Tous les éléments du cadre d'interopérabilité sont essentiels, ce qui signifie qu'un retard concernant un de ses aspects, ou un retard pris dans un État membre, entraînerait un retard de déploiement général. Il convient donc de réduire autant que possible les retards dans le développement technique du système d'entrée/de sortie, pour que ce dernier puisse commencer à fonctionner dans les plus brefs délais et que tous les éléments clés du cadre d'interopérabilité puissent être mis en place.

La proposition relative au filtrage[48] permettrait de renforcer la sécurité au sein de l'espace Schengen grâce à l'élaboration de règles uniformes concernant l'identification des ressortissants de pays tiers qui ne remplissent pas les conditions d'entrée visées dans le code frontières Schengen, et de les soumettre aux contrôles sanitaires et de sécurité aux frontières extérieures. S'il apparaît, à la suite d'un filtrage, qu'une personne pourrait constituer une menace pour la sécurité intérieure, le système Eurodac proposé le signalerait, réalisant ainsi ces objectifs. Il faciliterait ainsi la mise en œuvre de la proposition de règlement relatif à la gestion de l'asile et de la migration. La Commission encourage les colégislateurs à conclure rapidement les négociations relatives à ces dossiers, avant la fin de la législature actuelle.

[46] COM(2021) 784.
[47] COM(2021) 891.
[48] COM(2020) 612.

Lutte contre la corruption

La corruption nuit gravement à nos démocraties, à l'économie et à notre sécurité, en ce qu'elle contribue à la criminalité organisée et favorise les ingérences étrangères hostiles. Il est essentiel de prévenir et de combattre efficacement la corruption, tant pour sauvegarder les valeurs de l'Union et l'efficacité de ses politiques que pour préserver l'état de droit et la confiance placée dans ceux qui gouvernent et dans les institutions publiques. Comme l'a annoncé la présidente von der Leyen dans son discours sur l'état de l'Union de 2022, la Commission a adopté, le 3 mai 2023, un train de mesures de lutte contre la corruption[49]. La proposition de directive de la Commission relative à la lutte contre la corruption prévoit des règles renforcées qui érigent en infractions pénales les délits de corruption et harmonisent les sanctions dans l'ensemble de l'Union. Elle permet également la conduite d'enquêtes et l'exercice de poursuites efficaces et met fortement l'accent sur la prévention et la création d'une culture de l'intégrité dans laquelle la corruption n'est pas tolérée. Les discussions sur cette proposition ont débuté au Parlement européen et au Conseil. De plus, les États membres sont invités à mettre en œuvre les recommandations découlant du volet anticorruption du rapport sur l'état de droit de 2023 adopté le 5 juillet 2023. Une proposition du haut représentant, soutenue par la Commission, vise à établir un régime de sanctions spécifiques dans le cadre de la politique étrangère et de sécurité commune (PESC), ciblant les actes graves de corruption dans le monde entier.

Renforcement des droits des victimes

Le 12 juillet 2023, la Commission a proposé de modifier la directive relative aux droits des victimes, afin de renforcer l'accès de ces dernières à l'information, au soutien et à la protection, ainsi que leur participation aux procédures pénales et l'accès aux indemnisations. L'un des objectifs généraux de la révision est de contribuer à garantir un niveau de sécurité élevé en créant un environnement plus sûr pour les victimes, de manière à encourager le signalement des délits et de réduire les craintes de représailles.

La Commission invite le Parlement européen et le Conseil à conclure les négociations interinstitutionnelles de toute urgence, en tout état de cause avant la fin du mandat de l'actuel Parlement européen, sur les dossiers suivants:

- la proposition de règlement Prüm II;
- les propositions relatives aux informations préalables sur les passagers (API);
- les propositions sur la lutte contre la corruption et, en particulier, sur la mise en place d'un régime de sanctions spécifiques dans le cadre de la politique étrangère et de sécurité commune (PESC);
- la proposition de modification du règlement relatif au code frontières Schengen;
- la proposition de directive sur les droits des victimes;
- la proposition relative au filtrage.

La Commission invite les États membres à:

- veiller à l'entrée en vigueur du système d'entrée/de sortie dès que possible afin de parachever la mise en œuvre de l'architecture de l'UE en matière d'échange d'informations.

[49] COM(2023) 234.

VI. Mise en œuvre

Assurer la sécurité de l'Europe dans son ensemble est une responsabilité partagée, vis-à-vis de laquelle chaque acteur doit jouer son rôle: la Commission et les colégislateurs en adoptant de nouvelles règles, solides, détaillées et pratiques, les États membres en transposant, en exécutant et en appliquant ces règles en temps utile, et un large éventail d'autorités, d'organisations et de parties prenantes en effectuant le travail opérationnel sur le terrain. Les agences de l'UE actives dans les domaines de la justice, des affaires intérieures et de la cybersécurité jouent également un rôle essentiel et accru depuis que davantage de responsabilités leur ont été attribuées.

Examen renforcé des bénéficiaires de financements de l'UE

Dans le cadre de la mise en œuvre du budget de l'Union, la Commission a la responsabilité de veiller à ce que les bénéficiaires de financements de l'Union respectent les valeurs de celle-ci. Les mécanismes et systèmes de contrôle permettant de déterminer qui peut bénéficier d'un financement de l'UE sont déjà solides, et les négociations en cours sur la refonte du règlement financier visent par ailleurs à doter la Commission de moyens juridiques renforcés pour agir si cela s'avère nécessaire. De plus, la Commission réfléchit actuellement aux moyens d'améliorer encore l'examen des bénéficiaires actuels et des futurs bénéficiaires potentiels des financements de l'UE, en améliorant les lignes directrices relatives aux obligations en matière de respect des valeurs de l'Union et aux conséquences que devrait entraîner une violation de ces valeurs. Cela permettra de clarifier les responsabilités qui incombent tant aux bénéficiaires de financements qu'aux personnes responsables des contrôles au niveau de l'UE, et pourrait constituer une source d'inspiration au niveau national. En cas de non-respect des conditions de financement, la Commission n'hésite pas, et n'hésitera pas à l'avenir, à interrompre la coopération avec les bénéficiaires du projet concerné et, si nécessaire, à recouvrer les fonds. Il importe que les États membres partagent leurs informations avec la Commission de manière proactive lorsqu'ils ont connaissance de possibles risques liés à des organisations soumettant une demande de financement de l'UE.

Infractions

Dans le domaine de la sécurité, la Commission a mené de nombreuses procédures d'infraction. Ainsi, en 2023, un grand nombre de procédures d'infraction ont été engagées sur la base de manquements aux obligations découlant du règlement de 2021 relatif à la lutte contre la diffusion des contenus à caractère terroriste en ligne[50] (seize États membres étaient concernés) et, au cours des années 2022 et 2023, vingt États membres ont reçu des lettres de mise en demeure supplémentaires en raison de leur mise en œuvre incorrecte de la directive de 2011 relative à la lutte contre les abus sexuels et l'exploitation sexuelle des enfants[51]. Un nombre significatif de procédures d'infraction sont toujours ouvertes, pour non-conformité de la législation nationale avec la directive de 2017 relative à la lutte contre le terrorisme[52] et pour défaut de transposition des règles facilitant l'utilisation d'informations financières et d'une autre nature aux fins de la prévention ou de la détection de certaines infractions pénales, ou des enquêtes ou des poursuites en la matière[53]. Des procédures d'infraction sont également en cours

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

[51] Directive 2011/93/UE relative à la lutte contre les abus sexuels et l'exploitation sexuelle des enfants.

[52] Directive (UE) 2017/541 du Parlement européen et du Conseil du 15 mars 2017 relative à la lutte contre le terrorisme et remplaçant la décision-cadre 2002/475/JAI du Conseil et modifiant la décision 2005/671/JAI du Conseil.

[53] Directive (UE) 2019/1153 du Parlement européen et du Conseil du 20 juin 2019 fixant les règles facilitant l'utilisation d'informations financières et d'une autre nature aux fins de la prévention ou de la détection de

dans d'autres domaines, notamment la législation sur les armes à feu, les règles concernant les substances psychoactives contenues dans les stupéfiants, la lutte contre la fraude et la contrefaçon des moyens de paiement autres que les espèces, la lutte contre le blanchiment de capitaux, l'échange d'informations sur les casiers judiciaires entre les États membres de l'UE, et la directive sur les droits des victimes. Un soutien (technique et financier) est à la disposition des États membres qui mettent en œuvre les initiatives et actions convenues, et la Commission reste disposée à collaborer avec ces derniers en vue d'en garantir au mieux la mise en œuvre.

Suivi sur la base du nouveau système de gouvernance et des évaluations Schengen

Le mécanisme d'évaluation et de contrôle de Schengen a continué de contribuer à la mise en œuvre effective des règles Schengen visant à renforcer la sécurité au sein de cet espace sans contrôles internes. En 2023, les premières évaluations dans le cadre du mécanisme renforcé d'évaluation et de contrôle Schengen ont été réalisées, ce qui a permis de recenser et de corriger en temps voulu les vulnérabilités stratégiques, qui ont une incidence transfrontière sur la sécurité et la sûreté au sein de l'UE. En outre, en 2023, la Commission a lancé une évaluation Schengen thématique afin d'évaluer les pratiques des États membres confrontés à des défis similaires dans la lutte contre le trafic de drogue à destination de l'UE, ciblant en particulier le trafic de grande ampleur. Ces évaluations ont permis de mettre l'accent sur les éléments du cadre Schengen portant sur la sécurité et d'apporter un éclairage plus complet à cet égard. Sur la base des résultats des évaluations Schengen périodiques, thématiques et inopinées, le Conseil a établi en juin 2023 les priorités du cycle Schengen 2023-2024, fixant les domaines prioritaires sur lesquels il convient de mettre davantage l'accent, au bénéfice d'un espace Schengen plus sûr et plus fort. Une mise en œuvre efficace et rapide de ces priorités conjuguée à une coordination accrue des politiques au sein du Conseil Schengen renforceront encore la lutte contre la criminalité organisée et permettront de tirer le meilleur parti possible de la coopération opérationnelle transfrontière.

Le rôle des organes et organismes de l'UE

Pour obtenir des résultats concrets, les différentes autorités et instances nationales et européennes doivent travailler de concert. Le partenariat est donc essentiel à la mise en œuvre des initiatives liées à l'union de la sécurité. Ainsi, l'EMPACT (la plateforme pluridisciplinaire européenne contre les menaces criminelles) permet une coopération pluridisciplinaire structurée des États membres, soutenue par l'ensemble des institutions, organes et organismes de l'UE (tels qu'Europol, Frontex, Eurojust, CEPOL, l'OLAF et EU-LISA). Les opérations menées dans le cadre de l'EMPACT, notamment par des cellules opérationnelles d'intervention spécialisées, coordonnent les efforts déployés par les États membres et les partenaires opérationnels dans leur lutte contre les réseaux criminels et les formes graves de criminalité. Au cours de la seule année 2022, 9 922 arrestations au total ont été effectuées dans le cadre de l'EMPACT, des biens et de l'argent ont été saisis pour un montant de plus de 180 millions d'euros, 9 263 enquêtes ont été ouvertes, 4 019 victimes ont été identifiées, plus de 62 tonnes de drogue ont été saisies, 51 cibles de grande importance ont été identifiées et 12 d'entre elles arrêtées, et des opérations ont été menées dans le contexte de la guerre d'agression que subit l'Ukraine, notamment pour lutter contre la traite des êtres humains et les menaces liées aux armes à feu.

Frontex, l'Agence européenne pour la sécurité maritime (AESM) et l'Agence européenne de contrôle des pêches (AECP) continuent de renforcer leur coopération en ce qui concerne les

certaines infractions pénales, ou des enquêtes ou des poursuites en la matière, et abrogeant la décision 2000/642/JAI du Conseil.

fonctions de surveillance côtière afin d'aider les autorités nationales à accroître la sûreté et la sécurité en mer. Ces agences apporteront une contribution majeure à la mise en œuvre de la stratégie de sûreté maritime de l'UE.

Dans le cadre de plusieurs initiatives relatives à l'union de la sécurité, de nouvelles responsabilités et tâches ont été confiées aux agences concernées, avec parfois des implications pour les ressources humaines.

Agence de l'Union européenne pour la cybersécurité (ENISA)

En ce qui concerne la préparation et la réaction aux incidents en vue de renforcer la cybersécurité, la Commission a mis en œuvre une action à court terme pour soutenir les États membres, en transférant des fonds du programme pour une Europe numérique à l'**Agence de l'Union européenne pour la cybersécurité (ENISA)** afin de renforcer la préparation et les capacités de réaction aux cyberincidents majeurs. La proposition de règlement sur la cybersolidarité, adoptée en avril 2023, s'appuie sur cette action et, une fois qu'elle aura été adoptée par les colégislateurs, des tâches supplémentaires pourront être confiées à l'ENISA, comme la gestion et l'administration de la future réserve de cybersécurité de l'Union ou l'élaboration de rapports d'analyse d'incidents établis à la suite d'incidents de cybersécurité à grande échelle. Conformément à la proposition de règlement sur la cyberrésilience, l'ENISA serait chargée de collecter les notifications des fabricants relatives aux vulnérabilités de produits comportant des éléments numériques et aux incidents ayant des répercussions sur la sécurité de ces produits, et de les transmettre aux CSIRT ou aux points de contact uniques concernés des États membres. L'ENISA devrait également élaborer un rapport technique bisannuel sur les tendances émergentes relatives aux risques en matière de cybersécurité que présentent les produits comportant des éléments numériques, et le soumettre au groupe de coopération SRI.

Centre de compétences européen en matière de cybersécurité

Le **Centre de compétences européen en matière de cybersécurité (ci-après le «CCEC»)**, conjointement avec le Réseau de centres nationaux de coordination (ci-après les «CNC»), est le nouvel organe de l'Union chargé de soutenir l'innovation et la politique industrielle dans le domaine de la cybersécurité. Cet écosystème renforcera les capacités de la communauté des technologies de cybersécurité, permettra de maintenir l'excellence de la recherche et renforcera la compétitivité de l'industrie de l'Union dans ce domaine. Le CCEC et les CNC prendront des décisions d'investissement stratégiques et mettront en commun les ressources de l'Union, de ses États membres et, indirectement, de l'industrie afin d'améliorer et de renforcer les capacités technologiques et industrielles en matière de cybersécurité. Le CCEC a donc un rôle essentiel à jouer dans la réalisation des ambitieux objectifs en matière de cybersécurité du programme pour une Europe numérique et du programme Horizon Europe.

Le CCEC a recruté plus de la moitié de son personnel et recrutera bientôt son directeur exécutif. Les travaux déjà en cours comprennent le volet «cybersécurité» du programme DIGITAL et un nouveau programme stratégique[54] pour le développement et le déploiement des technologies, qui expose les actions prioritaires visant à soutenir les PME dans le développement et l'utilisation de technologies, de services et de processus stratégiques en matière de cybersécurité; à soutenir la main-d'œuvre professionnelle et à la développer; et à renforcer l'expertise en matière de recherche, de développement et d'innovation dans l'écosystème européen de cybersécurité au sens large.

[54] https://cybersecurity-centre.europa.eu/strategic-agenda_fr

Europol

Grâce à un tout nouveau mandat, **Europol** sera mieux à même de soutenir les États membres dans la lutte contre la criminalité organisée. Le trafic de stupéfiants prend de plus en plus d'ampleur et a des répercussions négatives toujours plus importantes sur la sécurité des citoyens de l'UE. La lutte contre ce trafic est donc une priorité absolue. À la suite de l'autorisation donnée par le Conseil de l'Union européenne le 15 mai 2023, la Commission a œuvré avec détermination à la conclusion d'accords internationaux avec la Bolivie, le Brésil, l'Équateur, le Mexique et le Pérou portant sur l'échange de données à caractère personnel avec Europol dans le but de prévenir et de combattre les formes graves de criminalité et le terrorisme.

Eurojust

Avec plus de vingt ans d'expérience à son actif dans la fourniture d'un soutien judiciaire aux autorités nationales pour les aider à lutter contre un large éventail de formes graves et complexes de criminalité transfrontière, **Eurojust** a conforté sa position au sein de l'espace de liberté, de sécurité et de justice de l'UE. Afin de renforcer la coopération à tous les niveaux, la Commission négocie des accords internationaux visant à faciliter la coopération entre Eurojust et treize pays tiers en matière d'échange de données à caractère personnel pour lutter contre la criminalité organisée et le terrorisme[55]. Les négociations avec l'Arménie et le Liban ont déjà abouti, elles sont en cours avec l'Algérie et la Colombie, et ont commencé avec la Bosnie-Herzégovine. La Commission encourage le Parlement européen et le Conseil à faire aboutir les accords avec ces pays avant la fin de la législature, afin de renforcer la coopération judiciaire transnationale et d'élargir la portée de la lutte contre la criminalité transfrontière.

Parquet européen

Depuis le début de ses activités opérationnelles en juin 2021, le **Parquet européen** a démontré qu'il était un outil puissant de la boîte à outils de l'Union en matière d'enquêtes et de poursuites relatives aux infractions portant atteinte au budget de l'Union lorsque ce type d'infractions est ciblé, notamment en ce qui concerne celles qui sont liées à la participation à une organisation criminelle. La Commission encourage les États membres qui ne participent pas encore à la coopération renforcée du Parquet européen à le faire dès que possible, ce qui permettra de libérer le plein potentiel du Parquet européen en ce qui concerne la protection de l'argent du contribuable de l'UE.

Agence européenne des drogues

Avec l'adoption d'un nouveau mandat par les colégislateurs en juin 2023, l'Observatoire européen des drogues et des toxicomanies (OEDT) deviendra une agence à part entière, l'**Agence de l'Union européenne pour les drogues (EUDA)**, qui exercera un rôle renforcé. L'agence sera en mesure d'évaluer de manière plus approfondie les nouveaux défis en matière de santé et de sécurité posés par les drogues illicites et de contribuer plus efficacement au travail effectué au niveau des États membres et au niveau international. Si la collecte, l'analyse et la diffusion de données resteront la mission principale de l'agence, le mandat renforcé lui permettra par ailleurs de développer des capacités générales d'évaluation des menaces qui pèsent sur la santé et la sécurité afin de repérer les menaces émergentes, y compris la polyconsommation de substances, de renforcer sa coopération par l'intermédiaire des points focaux nationaux, et de mettre en place un réseau de laboratoires fournissant à l'agence des informations médicolégales et toxicologiques. Cela aidera l'agence à émettre des alertes lorsque

[55] Algérie, Argentine, Arménie, Bosnie-Herzégovine, Brésil, Colombie, Égypte, Israël, Jordanie, Liban, Maroc, Tunisie et Turquie.

des substances particulièrement dangereuses apparaissent sur le marché et à sensibiliser le public en conséquence.

La Commission invite le Parlement européen et le Conseil à conclure les négociations interinstitutionnelles de toute urgence, en tout état de cause avant la fin du mandat de l'actuel Parlement européen, sur le dossier suivant:

- la proposition de refonte du règlement financier.

La Commission invite les États membres à:

- partager leurs informations avec la Commission de manière proactive lorsqu'ils ont connaissance de possibles risques liés à des organisations présentant une demande de financement de l'UE;
- mettre rapidement en œuvre les priorités du cycle Schengen 2023-2024 pour un espace Schengen plus sûr et plus fort;
- traiter les procédures d'infraction engagées à leur égard afin de garantir la transposition correcte de la législation concernée.

VII. Conclusions

Ces trois dernières années, des efforts constants et résolus ont été déployés pour concrétiser l'objectif ambitieux qu'est la création d'une union de la sécurité pour l'UE. Des progrès considérables ont été accomplis en ce qui concerne la politique de sécurité dans son ensemble. Aujourd'hui, les menaces évoluent constamment et face à cette réalité, des efforts constants doivent être consentis, avec une motivation renouvelée. Les travaux relatifs au cadre législatif doivent être achevés en temps opportun, avant la fin de la législature, au printemps 2024. Il est de la responsabilité constante des États membres de transposer, de mettre en œuvre et d'appliquer les nouvelles lois. À cette fin, des efforts concertés, notamment avec le soutien des agences de l'UE, sont nécessaires de même que, très souvent, une coopération plus étroite que jamais avec nos partenaires internationaux.

Ce n'est qu'au prix d'efforts collectifs et résolus de toutes les parties concernées que nous atteindrons dans l'Union les niveaux de sûreté et de sécurité que les citoyens attendent et, dans les circonstances actuelles, il devrait être prioritaire pour chaque acteur concerné d'apporter sa contribution au renforcement de la sécurité de l'UE.