**1.** **INTRODUCTION**

En juillet 2020, la Commission a adopté la stratégie globale pour l’union de la sécurité[[1]](#footnote-2). Depuis lors, le paysage des menaces qui pèsent sur la sécurité a radicalement changé. La crise de la COVID-19 a accentué certaines vulnérabilités, en particulier en lien avec le développement de l’activité en ligne. Les cyberattaques ont continué à prendre de l’ampleur et à se propager sous de nouvelles formes[[2]](#footnote-3). La guerre d’agression menée par la Russie contre l’Ukraine a eu un impact qui s’est fait ressentir sur la sécurité intérieure de l’UE, avec un risque accru de traite des êtres humains, de menace d’incidents chimiques et nucléaires et de circulation illicite d’armes à feu. Elle a également stimulé le recours à la manipulation de l’information et à l’ingérence étrangères. Le récent sabotage 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. Cet incident a montré une fois de plus que la sécurité physique et la sécurité numérique sont étroitement liées et doivent être protégées en parallèle.

Le présent rapport sur l’état d’avancement de la stratégie de l’UE pour l’union de la sécurité vise à donner un aperçu «à mi-parcours» de la mise en œuvre de la stratégie, en soulignant ce qui a été accompli et ce qui doit encore être réalisé d’ici la fin du mandat de la Commission actuelle. Depuis juillet 2020, l’UE a accompli de grands progrès pour mener à bien les actions dans les domaines clés couverts par les quatre piliers de la stratégie[[3]](#footnote-4). Le présent rapport montre que la grande majorité des actions énumérées dans la stratégie ont été traitées[[4]](#footnote-5). Toutefois, il reste encore beaucoup à faire pour que la stratégie pour l’union de la sécurité produise pleinement ses effets pour les citoyens — en particulier l’adoption de propositions législatives en suspens par le Parlement européen et le Conseil et la mise en œuvre par les États membres de la législation adoptée. La meilleure manière d’atteindre les objectifs de l’union de la sécurité consiste également à assurer une collaboration étroite avec des initiatives connexes de l’UE dans des domaines tels que la sécurité énergétique, l’union européenne de la santé et le plan d’action pour la démocratie européenne. La contribution continue de la Commission comprend trois propositions adoptées parallèlement au présent rapport, qui concernent le trafic de biens culturels et les renseignements essentiels offerts par les informations préalables sur les passagers[[5]](#footnote-6), ainsi qu’une proposition visant à lutter contre la traite des êtres humains[[6]](#footnote-7).

**2.** **PROTÉGER LES INFRASTRUCTURES PHYSIQUES ET NUMÉRIQUES CONTRE LES ATTAQUES PHYSIQUES, INFORMATIQUES ET HYBRIDES**

*Protéger les infrastructures critiques au sein de l’UE contre les attaques physiques et numériques*

Avant même les récentes attaques contre des infrastructures critiques, l’UE renforçait sa résilience au moyen de deux initiatives liées: la directive révisée[[7]](#footnote-8) concernant des mesures destinées à assurer un niveau élevé commun de cybersécurité dans l’ensemble de l’Union **(sécurité des réseaux et des systèmes d’information — «directive SRI 2»)[[8]](#footnote-9)** et une nouvelle directive sur la résilience des entités critiques **(«directive CER»)**[[9]](#footnote-10). Ce cadre vise à faire face aux risques actuels et futurs en ligne et hors ligne, qu’il s’agisse de cyberattaques, de catastrophes naturelles ou autres. Ces deux directives ont été approuvées par les colégislateurs et entreront en vigueur dans les semaines à venir. La **directive SRI 2** élargira la couverture des entités de taille moyenne et de grande taille dans une série de secteurs clés[[10]](#footnote-11). Elle renforce les exigences en matière de sécurité, notamment en ce qui concerne la réaction aux incidents et la gestion des crises, la sécurité de la chaîne d’approvisionnement, la gestion et la divulgation des vulnérabilités, les tests de cybersécurité et l’utilisation efficace du chiffrement. Elle rationalise également les obligations de déclaration des incidents, introduit des mesures de surveillance plus strictes et vise à harmoniser les régimes de sanctions entre les États membres[[11]](#footnote-12). La **directive CER** couvre la résilience physique des entités critiques face aux risques d’origine tant humaine que naturelle. Cette directive, qui couvre 11 secteurs, constitue une étape importante en vue de renforcer la capacité des entités critiques fournissant des services essentiels à prévenir tout incident, à s’en protéger, à y réagir, à y résister, à l’atténuer, à l’absorber, à s’y adapter et à s’en remettre.

Dans le secteur **financier**, le règlement sur la résilience opérationnelle numérique (règlement DORA) a également été adopté[[12]](#footnote-13), dans le cadre du train de mesures sur la finance numérique. Une fois mis en œuvre, ce règlement renforcera la résilience opérationnelle numérique des entités du secteur financier de l’UE en rationalisant et en modernisant les règles existantes et en introduisant de nouvelles obligations si nécessaire.

Afin d’accroître encore la protection des **infrastructures critiques contre les cyberattaques à grande échelle**, la Commission, le haut représentant et le groupe de coopération SRI[[13]](#footnote-14) élaborent actuellement des **scénarios de risque** axés sur la cybersécurité dans les secteurs de l’énergie, des télécommunications, des transports et de l’espace. Des travaux portant sur des mesures visant à améliorer le niveau collectif de protection et de cyberrésilience des systèmes et services spatiaux sont également en cours[[14]](#footnote-15). Des évaluations ciblées des risques en matière de cybersécurité sont également en cours pour les infrastructures et réseaux de communication au sein de l’UE (y compris les infrastructures fixes et mobiles, les satellites, les câbles sous-marins et le routage internet)[[15]](#footnote-16). La Commission a également lancé une initiative relative à l’élaboration de scénarios couvrant les **catastrophes naturelles résultant de menaces liées à la sécurité** telles que les cyberattaques ou le terrorisme, afin d’améliorer la prévention des catastrophes ainsi que la préparation et la réaction à celles-ci.

Le sabotage des gazoducs Nord Stream et d’autres incidents récents ont mis en évidence la menace pesant sur les **infrastructures critiques de l’UE** et l’urgence d’agir. Le cadre constitué par les directives CER et SRI 2 est donc préfiguré, afin d’accélérer les actions visant à renforcer la résilience des infrastructures critiques et à améliorer la préparation et la réaction dans des secteurs clés. Ces objectifs font l’objet d’une **recommandation du Conseil**[[16]](#footnote-17) qui permettra d’accélérer la mise en œuvre effective des directives. Cette recommandation propose une approche commune pour soumettre les entités exploitant des infrastructures critiques, en commençant par le secteur de l’énergie, à des **tests de résistance** basés sur des principes communs arrêtés d’un commun accord. Les travaux relatifs aux tests de résistance commenceront immédiatement afin qu’ils puissent être achevés avant la fin de 2023 et les progrès seront examinés en avril 2023. Un schéma directeur, qui sera élaboré par la Commission en coopération avec le Conseil, s’appuyant sur le soutien et les contributions des organismes de l’Union concernés, contribuera à garantir une réponse coordonnée au niveau de l’UE en cas de perturbations importantes des infrastructures critiques.

Dans le **secteur de l’énergie**, la Commission travaille actuellement à l’élaboration d’un code de réseau pour les aspects liés à la cybersécurité des flux transfrontaliers d’électricité[[17]](#footnote-18), comprenant des règles sur l’évaluation des risques, sur les exigences minimales communes, la planification, la surveillance, les rapports et la gestion de crise, qui sera pleinement cohérent avec le cadre SRI 2. Dans le cadre d’une action distincte en réponse à l’agression de la Russie contre l’Ukraine, les réseaux électriques de l’Ukraine et de la République de Moldavie ont été synchronisés avec le réseau d’Europe continentale en mars 2022, ce qui a complété les mesures d’atténuation des risques, notamment en matière de cybersécurité.

Dans le **secteur des transports**, la Commission collabore avec les États membres, l’Agence de l’Union européenne pour la sécurité aérienne (AESA) et le Centre de situation et du renseignement de l’UE (INTCEN) pour évaluer régulièrement le niveau de menace et de risque que représentent les zones de conflit pour l’aviation civile de l’UE. Le système d’alerte de l’UE relatif aux zones de conflit est considéré comme une bonne pratique au niveau international[[18]](#footnote-19). Les actions comprennent la relance d’un projet sur l’évaluation des risques liés au fret aérien, une première évaluation des risques au niveau de l’UE pour évaluer les menaces pesant sur les navires à passagers et un exercice complet de cartographie des risques liés à la sûreté de l’aviation afin de mettre à jour l’évaluation des menaces pesant sur l’aviation civile.

Les **infrastructures maritimes critiques** font également l’objet d’une attention particulière[[19]](#footnote-20). L’environnement commun de partage de l’information pour le domaine maritime est en cours de développement et sera pleinement opérationnel d’ici la fin de 2023, interconnectant les autorités de surveillance maritime sur une base volontaire afin d’échanger des informations en temps quasi réel. Le Forum européen des fonctions de garde-côtes a également renforcé sa capacité à se prémunir contre les cyberattaques.

Plusieurs projets de recherche dans le cadre d’**Horizon Europe** visent également à rendre nos infrastructures numériques plus sûres et à renforcer les capacités de prévention et d’atténuation des cyberattaques[[20]](#footnote-21).

*Renforcer la cybersécurité de l’UE*

Le 16 décembre 2020, la Commission et le haut représentant ont présenté une nouvelle **stratégie de cybersécurité de l’UE pour la décennie numérique[[21]](#footnote-22)**, afin de renforcer la résilience collective de l’Europe face aux cybermenaces et de faire en sorte que les citoyens et les entreprises bénéficient de services et d’outils numériques fiables et dignes de confiance. La stratégie a été presque entièrement mise en œuvre.

La directive SRI 2 prévoit la mise en place du **réseau européen d’organisations de liaison en cas de crises de cybersécurité (UE-CyCLONe)**[[22]](#footnote-23) en vue de contribuer à la gestion coordonnée, au niveau opérationnel, des incidents et crises de grande ampleur en matière de cybersécurité. Un échange régulier d’informations pertinentes entre les États membres et les institutions, organes et organismes de l’UE sera ainsi garanti. La Commission développe actuellement un **centre d’analyse et de situation en matière de cybersécurité** afin de renforcer ses capacités internes. Elle collabore avec les États membres, notamment dans le cadre du suivi de sa recommandation sur la création d’une **unité conjointe de cybersécurité**[[23]](#footnote-24) afin de garantir une réaction coordonnée de l’UE aux cyberincidents de grande ampleur. La Commission et le haut représentant sont par ailleurs activement associés aux exercices de cybersécurité organisés en 2022 avec les États membres[[24]](#footnote-25).

Les réseaux et les systèmes informatiques doivent faire l’objet d’une surveillance et d’une analyse constantes pour détecter les intrusions et les anomalies en temps réel. La Commission a proposé de mettre en place un réseau de **centres d’opérations de sécurité** à l’échelle de l’UE, afin de surveiller les réseaux de communication et de détecter les événements suspects. Les capacités de détection collective seront renforcées grâce à l’expansion des centres existants, à la création de nouveaux centres et à la mise en relation des centres de plusieurs États membres. Ces centres pourraient également s’appuyer sur les outils les plus récents de l’intelligence artificielle (IA) et sur l’analyse des données, pour protéger les réseaux de communication civils et accélérer la détection des cyberattaques[[25]](#footnote-26).

Pour renforcer la préparation aux cyberincidents de grande ampleur et la réaction à ceux-ci, la Commission a également mis en place un programme à court terme pour soutenir les États membres, aux fins duquel des fonds supplémentaires ont été alloués à l’ENISA et qui prévoit, entre autres, des tests de pénétration des entités critiques afin d’en recenser les vulnérabilités. Ce programme peut également fournir une aide aux États membres pour les réponses aux incidents, assurées par l’ENISA avec le soutien de prestataires privés de confiance proposant des services de cybersécurité, après un incident majeur touchant des entités critiques. La prochaine étape consistera à faire en sorte que les États membres exploitent pleinement ces possibilités.

Tant le matériel informatique que les logiciels font de plus en plus l’objet de **cyberattaques**. Celles-ci sont de plus en plus nombreuses et sophistiquées, le vecteur privilégié étant l’exploitation des vulnérabilités logicielles. Deux tiers de tous les incidents signalés dans le cadre de la SRI impliquent l’exploitation de vulnérabilités logicielles. L’impact sur les citoyens, les infrastructures ou les entreprises est également de plus en plus important[[26]](#footnote-27). En septembre 2022, la Commission a fait une proposition de **règlement sur la cyberrésilience**[[27]](#footnote-28), afin de réduire les vulnérabilités des produits comportant des éléments numériques et de veiller à ce que des correctifs et des mesures d’atténuation soient rapidement disponibles. Elle propose que les produits comportant des éléments numériques (matériel et logiciels) n’entrent sur le marché que s’ils satisfont à des exigences essentielles spécifiques en matière de cybersécurité[[28]](#footnote-29). Les fabricants et les développeurs seraient tenus d’assurer la cybersécurité de leurs produits pendant cinq ans et de faire preuve de transparence vis-à-vis des consommateurs en ce qui concerne la cybersécurité. Cela contribuera de manière significative à la sécurité de la chaîne d’approvisionnement[[29]](#footnote-30).

La **certification** joue un rôle crucial dans le renforcement de la sécurité des produits et services importants pour le monde numérique et de la confiance qui leur est accordée. Le règlement sur la cybersécurité[[30]](#footnote-31) établit le cadre européen de certification de cybersécurité en vertu duquel la Commission peut demander à l’ENISA d’élaborer des schémas de certification. Un schéma européen de certification de cybersécurité fondé sur des critères communs a été élaboré et des schémas sont en cours d’élaboration pour les services en nuage et la sécurité des réseaux 5G.

La Commission continue de collaborer avec les États membres pour veiller à ce que les **réseaux 5G** soient sûrs et résilients, et de suivre la mise en œuvre de la boîte à outils de l’UE pour la sécurité des réseaux 5G au niveau national et au niveau de l’UE. Alors qu’une grande majorité d’États membres ont déjà renforcé ou sont en train de renforcer les exigences en matière de sécurité applicables aux réseaux 5G, il est désormais urgent que tous les États membres achèvent la mise en œuvre des mesures de la boîte à outils[[31]](#footnote-32), en particulier qu’ils imposent des restrictions aux fournisseurs à haut risque, car toute perte de temps peut accroître la vulnérabilité des réseaux dans l’Union, et qu’ils renforcent la protection physique et non physique des parties critiques et sensibles des réseaux 5G, y compris au moyen de contrôles d’accès stricts.

Pour aider l’UE et les États membres à adopter une démarche proactive et stratégique en ce qui concerne la politique industrielle de cybersécurité, le **Centre de compétences européen en matière de cybersécurité** (ECCC) collaborera avec les centres nationaux de coordination afin de soutenir l’innovation en matière de cybersécurité et de renforcer les capacités de la communauté des technologies de cybersécurité[[32]](#footnote-33).

En septembre 2022, l’ENISA a officiellement lancé un **cadre européen des compétences en matière de cybersécurité** qui recense les profils professionnels les plus nécessaires dans ce domaine et fournit une base européenne commune pour faciliter la reconnaissance des compétences et développer la formation en matière de cybersécurité. Ce cadre sera une composante essentielle de l’**académie des compétences en matière de cybersécurité** proposée dans le cadre du programme de travail de la Commission pour 2023, qui offrira une approche globale pour répondre aux besoins croissants de professionnels de la cybersécurité en Europe.

Étant donné que les **institutions, organes et organismes de l’UE** traitent des informations sensibles non classifiées et des informations classifiées de l’UE, il importe qu’ils soient bien protégés contre les cyberattaques. La Commission a proposé en mars 2022 un règlement établissant des mesures destinées à assurer un niveau élevé commun de cybersécurité dans les institutions, organes et organismes de l’Union[[33]](#footnote-34), qui applique les principes de base de la directive SRI 2 à l’environnement institutionnel de l’UE. Ce règlement prévoit un nouveau conseil interinstitutionnel de cybersécurité et un centre de cybersécurité renforcé (CERT-UE)[[34]](#footnote-35) afin de garantir une coopération et un échange d’informations appropriés avec les autorités des États membres, par exemple par l’intermédiaire du réseau des centres de réponse aux incidents de sécurité informatiques (CSIRT). Parallèlement, la Commission a adopté une proposition de règlement relatif à la sécurité de l’information dans les institutions, organes et organismes de l’Union[[35]](#footnote-36), afin de renforcer la résilience face aux cybermenaces et aux menaces hybrides en créant un ensemble commun de normes élevées en matière de sécurité de l’information pour l’ensemble des institutions, organes et organismes de l’UE. Il est essentiel que le Conseil accélère ses travaux sur cette proposition, compte tenu des multiples appels lancés par les États membres demandant à la Commission d’œuvrer à des mesures visant à mieux protéger le processus décisionnel de l’UE contre les activités malveillantes de tous types. Le CERT-UE et l’ENISA ont également conçu et testé un nouveau type d’exercice de cybersécurité qui est adapté aux agences de l’UE, comme le recommande la Cour des comptes européenne.

***Exemples clés de mise en œuvre***

**Le mois européen de la cybersécurité (ECSM):** l’initiative ECSM, qui comprend des ateliers, des campagnes sur les médias sociaux et des conférences, est passée de 184 activités en 2014 à 500 activités en octobre 2022. Celles-ci contribuent à améliorer la réaction des utilisateurs en ligne, lorsqu’ils sont confrontés à une menace en matière de cybersécurité (comme l’ont signalé 73 % des répondants dans les États membres sondés en 2021).

**La base de données sur l’enseignement supérieur en matière de cybersécurité (CyberHEAD):** CyberHEAD est la page web de l’ENISA la plus consultée depuis 2 ans, avec environ 70 000 visites par an. Elle permet aux jeunes talents de prendre des décisions éclairées sur les nombreuses possibilités offertes par l’enseignement supérieur dans le domaine de la cybersécurité et aide les universités à attirer des étudiants de grande qualité motivés à préserver la cybersécurité en Europe.

*Lutte contre les menaces hybrides, lutte contre l’ingérence étrangère et renforcement de la cyberdéfense de l’UE*

La **boussole stratégique de l’UE** en matière de sécurité et de défense définit un plan d’action ambitieux visant à accroître la capacité de l’UE à agir, à renforcer la résilience et à mieux investir dans les capacités de défense de l’UE.

Si la lutte contre les **menaces hybrides** relève principalement de la responsabilité des États membres, l’UE complète l’action nationale en soutenant la coordination, en améliorant l’appréciation de la situation, en promouvant la coopération avec les pays partageant les mêmes valeurs et les organisations internationales et en proposant des options de réaction communes. Au cours des dix dernières années, plus de 200 mesures ont été mises en place pour renforcer la résilience et lutter contre les menaces hybrides au niveau de l’UE. La cellule de fusion contre les menaces hybrides du Centre de situation et du renseignement de l’UE (INTCEN) contribue au processus décisionnel de l’UE et est l’organe central chargé de fournir une prospective stratégique et une appréciation globale de la situation, de regrouper des informations provenant de toutes les sources, et de réaliser des évaluations du renseignement sur les menaces hybrides. Les travaux ont commencé pour créer des équipes d’intervention rapide de l’UE en cas de menaces hybrides, annoncées par la boussole stratégique, afin d’aider les États membres et les missions et opérations relevant de la politique de sécurité et de défense commune, ainsi que les pays partenaires, à lutter contre les menaces hybrides en leur permettant de s’appuyer rapidement sur l’expertise nationale et de l’UE pertinente, y compris, le cas échéant, sur l’expertise militaire. Une boîte à outils de l’UE relative à la lutte contre les menaces hybrides est en préparation et fournira un cadre pour une réaction coordonnée aux campagnes hybrides touchant l’UE et les États membres, intégrant la dimension externe et interne dans un flux continu et réunissant les considérations nationales et européennes. Des progrès importants ont également été accomplis en ce qui concerne le renforcement de la résilience et la lutte contre les menaces hybrides grâce au recensement des niveaux de référence sectoriels existants en matière de résilience[[36]](#footnote-37). La Commission a également poursuivi ses recherches analytiques sur le renforcement de la résilience face aux menaces hybrides[[37]](#footnote-38) et a intégré les considérations hybrides dans l’élaboration des politiques.

La pandémie de COVID-19 et la guerre menée par la Russie contre l’Ukraine ont montré l’incidence que peut avoir la manipulation de l’environnement informationnel sur l’UE et ses partenaires dans le monde entier. Visant à éroder la confiance dans l’UE et dans l’ordre international fondé sur des règles, la **manipulation de l’information et l’ingérence étrangères** sont également une composante de plus en plus importante des attaques hybrides. S’appuyant sur le plan d’action pour la démocratie européenne, la Commission a mis en place un ensemble de mesures et de structures concrètes, notamment le code révisé de bonnes pratiques contre la désinformation, la législation sur les services numériques et la proposition relative à la transparence de la publicité à caractère politique, qui fait actuellement l’objet de négociations interinstitutionnelles, afin de lutter contre la manipulation de l’information et la désinformation. Il en résulterait de nouvelles obligations pour les plateformes et, pour la première fois, un cadre de surveillance juridiquement contraignant. En outre, comme annoncé par la boussole stratégique, en étroite coopération avec la Commission et les États membres, le SEAE poursuit le développement de la **boîte à outils de l’UE destinée à lutter contre la manipulation de l’information et l’ingérence étrangères** (boîte à outils FIMI), afin de favoriser une réaction coordonnée aux comportements manipulateurs d’acteurs étrangers[[38]](#footnote-39). Le SEAE a également continué de renforcer la coopération avec des partenaires internationaux tels que le mécanisme de réaction rapide du G7 et l’OTAN.

La Commission condamne toute ingérence étrangère sur le territoire souverain des États membres de l’UE et est préoccupée par les informations faisant état de postes de police chinois à l’étranger dans l’UE, ce qui, si cela devait être avéré, serait totalement inacceptable. Bien qu’il appartienne aux autorités des États membres d’enquêter sur ces allégations, la Commission, avec le soutien d’Europol, est prête à faciliter les échanges entre les États membres. La Commission a soulevé cette question lors du Conseil «Justice et affaires intérieures» de décembre 2022.

En novembre 2022, la Commission et le haut représentant ont présenté une nouvelle politique de l’UE en matière de **cyberdéfense**[[39]](#footnote-40), qui définit les moyens de renforcer la coopération et les investissements dans la cyberdéfense afin d’améliorer la protection contre les cyberattaques. L’objectif est de défendre les intérêts de l’UE dans le cyberespace en renforçant la coopération entre les acteurs de l’UE en matière de cyberdéfense et en développant des mécanismes permettant de mobiliser les capacités au niveau de l’UE, y compris dans le cadre des missions et opérations PSDC. Cette politique favorisera le développement de tout un éventail de capacités de cyberdéfense et renforcera la coopération entre les cybercommunautés militaires et civiles de l’UE, en améliorant l’appréciation de la situation, la coordination de crise et la formation, y compris en collaboration avec le secteur privé. Elle contribuera également à réduire les dépendances stratégiques à l’égard des cybertechnologies critiques, grâce à l’élaboration d’une feuille de route stratégique pour les technologies critiques de cybersécurité et de cyberdéfense, et à renforcer la base industrielle et technologique de défense européenne.

La boussole stratégique définit l’**espace** comme un cinquième domaine opérationnel de guerre (au même titre que la terre, la mer, l’air et le cyberespace) et invite la Commission et le haut représentant à élaborer la première stratégie spatiale pour la sécurité et la défense. Cette stratégie proposera des mesures visant à améliorer le niveau collectif de protection et de résilience des systèmes et services spatiaux, ainsi qu’à décourager les menaces, y compris les cybermenaces, qui pèsent sur les systèmes et services spatiaux sensibles dans l’UE et à y réagir.

**3.** **LUTTE CONTRE LE TERRORISME ET LA RADICALISATION**

Presque toutes les initiatives clés présentées dans la stratégie de sécurité de l’UE visant à soutenir les États membres dans la lutte contre le terrorisme et la radicalisation ont été adoptées. La protection contre les menaces en ligne a fait l’objet d’un thème particulier. La prochaine étape consiste à faire en sorte que ces initiatives produisent pleinement leurs effets.

*Lutte contre le terrorisme*

Depuis son adoption en décembre 2020, le **programme de lutte antiterroriste pour l’UE**[[40]](#footnote-41) a permis à celle-ci de mieux anticiper et prévenir les menaces terroristes et de mieux se protéger et réagir face à ces menaces. Des initiatives géographiques spécifiques ont également contribué à répondre à l’évolution des menaces. À la lumière de l’évolution de la situation en Afghanistan, le coordinateur de l’UE pour la lutte contre le terrorisme, en coordination avec la Commission, le haut représentant, la présidence et les principales agences de l’UE, a élaboré un **plan d’action pour la lutte contre le terrorisme concernant l’Afghanistan[[41]](#footnote-42)**, approuvé par les États membres en octobre 2021. La mise en place d’une procédure volontaire de renforcement des contrôles de sécurité à l’égard des personnes en provenance d’Afghanistan a constitué une avancée manifeste.

La lutte contre la menace que représente le **retour des combattants terroristes étrangers** de Syrie et d’Iraq est une priorité. Si la responsabilité première incombe aux États membres, la coopération au niveau de l’UE aide les États membres à relever des défis communs tels que la poursuite des auteurs d’actes terroristes, la prévention de l’entrée non détectée dans l’espace Schengen et la réintégration et la réhabilitation des combattants terroristes étrangers de retour dans leur pays. La Commission continue de travailler en étroite collaboration avec les États membres et les principaux pays partenaires afin de veiller à ce que les preuves recueillies sur le théâtre des opérations soient introduites dans les bases de données et les systèmes d’information de l’UE. En accord avec les États membres, le coordinateur de l’UE pour la lutte contre le terrorisme étudie, en étroite coopération avec le haut représentant et la Commission, de nouveaux moyens de tirer parti de l’amélioration des conditions de vie dans les prisons et les camps du nord-est de la Syrie pour contribuer à la lutte contre la radicalisation.

La législation de l’UE relative à la lutte contre le terrorisme a été actualisée.La **directive relative à la lutte contre le terrorisme** adoptée en 2017 est désormais mise en œuvre par tous les États membres[[42]](#footnote-43) afin d’ériger en infraction pénale des comportements tels que l’entraînement et les voyages à des fins terroristes, ainsi que le financement du terrorisme. La transposition incorrecte de la directive dans un certain nombre d’États membres doit encore être traitée.

**Priver les terroristes des moyens de commettre un attentat** est essentiel dans la lutte contre le terrorisme. Presque tous les États membres ont désormais adopté la législation actualisée sur les armes à feu[[43]](#footnote-44) dans leur droit national. Une nouvelle législation visant à réduire l’accès aux précurseurs d’explosifs que les terroristes pourraient utiliser pour produire des bombes est entrée en vigueur en février 2021. Se fondant sur l’approche suivie pour réglementer l’accès aux précurseurs d’explosifs, la Commission réfléchit à la manière de restreindre l’accès à certains produits chimiques dangereux susceptibles d’être utilisés pour mener des attaques terroristes.

Les **espaces publics** ont été la cible d’attaques terroristes à maintes reprises. La Commission a publié un manuel visant à promouvoir la sécurité dès la conception des espaces publics[[44]](#footnote-45). Cette publication fait suite à des orientations techniques détaillées,[[45]](#footnote-46) à des outils d’évaluation de la vulnérabilité des espaces publics[[46]](#footnote-47) et à un soutien global aux principales parties prenantes[[47]](#footnote-48), ainsi qu’à une recommandation relative à des exigences de performance d’application volontaire pour les équipements d’imagerie radioscopique utilisés dans les espaces publics (hors aviation)[[48]](#footnote-49). En 2022, le Fonds pour la sécurité intérieure a également financé à hauteur de 14 500 000 EUR des projets visant à améliorer la protection des espaces publics, y compris les lieux de culte. Les **drones** constituent des instruments hautement innovants qui peuvent être utilisés à des fins légitimes mais aussi malveillantes, telles que des attaques contre les espaces publics, les personnes et les infrastructures critiques. En novembre 2022, la Commission a adopté une **stratégie Drone 2.0[[49]](#footnote-50)**, qui sera suivie en 2023 par une approche plus détaillée de l’UE en matière de lutte contre l’utilisation malveillante des drones.

*Lutte contre la radicalisation conduisant à l’extrémisme violent et au terrorisme en ligne et hors ligne*

La prévention de la **radicalisation** et la lutte contre celle-ci sont essentielles à l’efficacité des politiques de lutte contre le terrorisme. La Commission soutient les États membres grâce au réseau de sensibilisation à la radicalisation (RSR), qui réunit 6 000 experts actifs dans le domaine de la prévention. Parmi les principaux domaines de soutien aux États membres figurent la lutte contre les idéologies extrémistes violentes et la polarisation conduisant à la radicalisation, la radicalisation en ligne et l’utilisation abusive des nouvelles technologies, et la gestion et la préparation de la réintégration des délinquants libérés de prison. Les liens entre les groupes extrémistes violents, les idéologies et les manifestations de discours de haine sont abordés dans le code de conduite de l’UE pour la lutte contre les discours haineux illégaux en ligne.[[50]](#footnote-51).

L’UE s’emploie également à prévenir les influences étrangères et les financements soutenant des points de vue radicaux/extrémistes dans les États membres. Pour sa part, la Commission reste vigilante afin d’empêcher que les fonds de l’UE ne soutiennent des projets incompatibles avec les valeurs européennes ou poursuivant des objectifs illégaux. À cet égard, depuis la fin de l’année 2021, les projets gérés par la Commission sont publiés dès la signature de la convention de subvention, sur une plateforme unique, le «portail des possibilités de financement et des appels d’offres». Il est essentiel que les États membres utilisent ce portail pour passer eux-mêmes les bénéficiaires au crible et fournir à la Commission toute information supplémentaire dont ils disposent à leur sujet. Dans ce contexte, la proposition de révision du règlement financier présentée par la Commission prévoit d’ajouter les condamnations pour «incitation à la haine» parmi les motifs d’exclusion du financement de l’UE. La Commission invite le Parlement européen et le Conseil à régler cette question de manière effective dans le texte final. En outre, la Commission prend des mesures internes de sensibilisation et met au point des méthodes de travail internes pour garantir un contrôle accru de la sélection des projets.

La prévention de la radicalisation en ligne est une autre priorité essentielle. Le **règlement relatif à la lutte contre la diffusion des contenus à caractère terroriste en ligne**[[51]](#footnote-52) est entré en vigueur en juin 2022. Depuis lors, les autorités nationales compétentes peuvent exiger que les contenus à caractère terroriste soient retirés dans un délai d’une heure à compter de l’injonction officielle de retrait. Les fournisseurs de services en ligne exposés à des contenus à caractère terroriste doivent prendre des mesures spécifiques pour protéger leurs plateformes contre les abus. Cette initiative complète les travaux du **Forum de l’UE sur l’internet** (EUIF), lancé par la Commission pour réunir les États membres, les entreprises de l’internet et la société civile afin d’empêcher la diffusion de contenus extrémistes et terroristes violents en ligne. Le soutien apporté récemment par l’EUIF aux entreprises technologiques et aux fournisseurs d’infrastructures internet dans leurs efforts de modération des contenus comprend un répertoire des sites web exploités à des fins terroristes et un ensemble de connaissances actualisé chaque année sur les groupes, symboles et manifestes extrémistes de droite violents[[52]](#footnote-53). Depuis 2019, la prévention des abus sexuels sur enfants en ligne est également abordée dans le cadre de ce forum.

***Exemples clés de mise en œuvre***

**Comment la coopération avec Eurojust a conduit à la condamnation pour terrorisme d’un combattant étranger:** la principale cible d’une [enquête liée au terrorisme](https://www.eurojust.europa.eu/annual-report-2021/terrorism/case-examples) a été condamnée en 2021 à quatre ans d’emprisonnement pour participation à une organisation terroriste après que les autorités italiennes ont utilisé le registre de la lutte contre le terrorisme pour identifier les liens entre un combattant étranger soupçonné de terrorisme et d’autres affaires de terrorisme. Les autorités nationales ont été mises en relation par Eurojust, ce qui a donné lieu à l’exécution de décisions d’enquête européennes et de demandes d’entraide judiciaire.

**Coordination d’Europol pour lutter contre les manuels de fabrication de bombes disponibles en ligne:** dans le cadre d’une série d’initiatives conjointes régulières, lors d’une journée d’action en février 2022, soutenue par Europol et à laquelle ont participé 8 États membres et le Royaume-Uni, des centaines d’articles en ligne ont été trouvés, y compris des instructions sur la manière de fabriquer des bombes avec des précurseurs et de les utiliser pour commettre des attentats terroristes. Ces informations ont été transmises aux fournisseurs de services en ligne.

**4.** **LUTTE CONTRE LA CRIMINALITÉ ORGANISÉE**

Dans le paysage de la criminalité organisée en Europe, la coopération entre les criminels est en constante évolution. Les réseaux criminels peuvent être impliqués dans toute une série d’activités criminelles, combinant trafic de drogue, criminalité organisée contre les biens, fraude, trafic de migrants et traite des êtres humains[[53]](#footnote-54). La cybercriminalité et la cyberviolence à caractère sexiste ont encore été attisées par l’utilisation accrue de l’internet et des services en ligne. L’utilisation croissante de canaux de communication cryptés, tout en protégeant la vie privée et les droits fondamentaux, pose des défis supplémentaires aux services répressifs[[54]](#footnote-55). Entre-temps, les perturbations causées par la guerre d’agression menée par la Russie contre l’Ukraine ont créé de nouvelles ouvertures, rapidement exploitées par des groupes criminels organisés.

En avril 2021, la Commission a adopté la **stratégie de l’UE visant à lutter contre la criminalité organisée 2021-2025**[[55]](#footnote-56). Cette stratégie insiste sur l’importance du démantèlement des structures de la criminalité organisée, en ciblant les groupes qui présentent un risque plus élevé pour la sécurité de l’Europe et les personnes aux échelons les plus élevés des organisations criminelles. Sa mise en œuvre est à présent bien engagée, plusieurs actions clés ayant déjà été adoptées ou mises en œuvre. La Commission a également apporté un soutien financier aux États membres pour lutter contre les menaces criminelles auxquelles l’UE est confrontée[[56]](#footnote-57).

*Cybercriminalité*

L’accélération de la numérisation durant la pandémie de COVID-19 a stimulé la propagation de cybermenaces telles que les rançongiciels[[57]](#footnote-58). Les **rançongiciels** suscitent des risques considérables en matière de cybersécurité pour les infrastructures critiques et la sécurité publique. Le Centre de lutte contre la cybercriminalité d’Europol (EC3), en collaboration avec la Force d’action anticybercriminalité européenne (J-CAT), a récemment mis au point l’ «International Ransomware Response Model» (modèle international de réponse aux rançongiciels) afin de mettre en œuvre une réponse répressive globale. L’UE a participé au sommet de 2022 de l’Initiative de lutte contre les rançongiciels visant à renforcer la coopération internationale en matière de rançongiciels. 36 pays et l’UE sont convenus de faire avancer les travaux relatifs à l’«International Counter Ransomware Task Force» (task-force internationale de lutte contre les rançongiciels) afin de coordonner les travaux en matière de résilience et de perturbations et de lutter contre les activités de financement illicite[[58]](#footnote-59). La Commission et Europol ont mis en place conjointement une plateforme de décryptage[[59]](#footnote-60), ce qui permet à la police scientifique d’accéder plus rapidement aux preuves numériques et contribue à lutter contre les réseaux de communication criminelle cryptés, permettant ainsi d’entraver sévèrement les activités de la criminalité organisée.

L’UE a joué un rôle déterminant dans la réussite des négociations sur le deuxième protocole additionnel à la **convention de Budapest sur la cybercriminalité** qui se sont tenues en mai 2022. Il s’agit notamment d’outils indispensables à la coopération transfrontière dans le cadre d’enquêtes et de poursuites en matière de cybercriminalité, ainsi que de conditions et de garanties détaillées en matière de protection des données. Tous les États membres devraient signer rapidement le deuxième protocole additionnel et le Parlement européen est invité à donner son approbation afin de permettre une ratification rapide. La Commission négocie également, au nom de l’UE, une nouvelle convention des Nations unies sur la cybercriminalité.

Avec 85 millions de photos et de vidéos représentant des **abus sexuels commis sur des enfants** signalés à l’échelle mondiale pour la seule année 2021, sachant que bien d’autres ne le sont pas, les abus sexuels sur les enfants sont répandus à un niveau alarmant. Les enfants passent plus de temps en ligne et sont de ce fait plus vulnérables à la manipulation psychologique, ce qui a entraîné une augmentation du matériel d’exploitation autoproduit. Conformément à la stratégie de l’UE en faveur d’une lutte plus efficace contre les abus sexuels commis contre des enfants, adoptée en juillet 2020[[60]](#footnote-61), et à la stratégie globale de l’UE sur les droits de l’enfant de mars 2021[[61]](#footnote-62), la Commission a adopté, en mai 2022, une proposition établissant des règles en vue de prévenir et de combattre les abus sexuels sur enfants en ligne[[62]](#footnote-63), assortie de nouvelles obligations pour les fournisseurs de services en ligne. Lorsque la prévention ne permet pas de réduire un risque important, les fournisseurs de services pourraient être enjoints de détecter, de signaler, de supprimer et de rendre inaccessibles les abus sexuels sur les enfants en ligne. La proposition créerait également un centre de l’UE spécialisé, afin de faciliter la mise en œuvre. La législation temporaire adoptée en août 2021 afin de permettre aux fournisseurs de services en ligne de poursuivre la détection et le signalement volontaires des abus sexuels commis sur des enfants en ligne[[63]](#footnote-64) expirera à l’été 2024. Il est donc essentiel que le Parlement européen et le Conseil trouvent rapidement un accord sur la proposition de règlement. Au début de l’année prochaine, cette initiative sera complétée par une proposition visant à actualiser la directive relative à la lutte contre les abus sexuels et l’exploitation sexuelle des enfants, ainsi que la pédopornographie[[64]](#footnote-65).

La cyberviolence envers les femmes et les filles est une nouvelle dimension émergente de la **cyberviolence à caractère sexiste**. En 2020, il a été estimé qu’une jeune femme sur deux a été victime de cette forme de violence[[65]](#footnote-66). Dans sa proposition de directive sur la lutte contre la violence à l’égard des femmes et la violence domestique[[66]](#footnote-67), adoptée en mars 2022, la Commission a proposé des règles ciblées en matière de violence fondée sur le genre à l’égard des femmes en ligne ou hors ligne[[67]](#footnote-68).

*Criminalité organisée*

La **traite des êtres humains** est une des activités principales de la criminalité organisée dans l’UE[[68]](#footnote-69). Bien qu’elle soit déjà désignée comme prioritaire dans la stratégie de l’UE pour l’union de la sécurité, les criminels ont trouvé de nouvelles possibilités de générer des profits importants et d’intensifier les activités criminelles pendant la pandémie de COVID-19. Une coordination rapide au niveau de l’UE contribue à prévenir l’intensification de la menace de traite des êtres humains à la suite de la guerre d’agression menée par la Russie contre l’Ukraine. Le coordinateur de l’UE pour la lutte contre la traite des êtres humains a élaboré un [**plan commun de lutte contre la traite des êtres humains**[[69]](#footnote-70)](https://home-affairs.ec.europa.eu/system/files/2022-05/Anti-Trafficking%20Plan_en.pdf) visant à regrouper les travaux de la Commission, des États membres, des agences de l’UE et du Service européen pour l’action extérieure afin de parer aux risques de traite des êtres humains et de soutenir les victimes potentielles. Ces efforts ont contribué à faire en sorte que le nombre de cas de traite confirmés reste limité, même si la menace reste élevée.

En avril 2021, la stratégie de l’UE visant à lutter contre la traite des êtres humains (2021-2025) a fourni un cadre d’action global, tant interne qu’externe[[70]](#footnote-71). La Commission va poursuivre sur cette voie au moyen de l’adoption à venir d’une proposition modifiant la **directive relative à la lutte contre la traite des êtres humains**[[71]](#footnote-72) afin de combler les lacunes du cadre juridique actuel et de le mettre à jour afin de tenir compte de la dimension en ligne, et afin de chercher à réduire la demande. En septembre 2022, dans le cadre d’un premier hackathon organisé à l’échelle de l’UE contre la traite des êtres humains avec le soutien d’Europol et d’Eurojust et la participation des autorités répressives de 20 pays, une journée d’action conjointe EMPACT a ciblé les réseaux criminels utilisant des sites web et des plateformes de médias sociaux pour recruter des victimes aux fins de leur exploitation sexuelle. Onze personnes soupçonnées de se livrer à la traite d’êtres humains et 45 victimes potentielles ont été recensées[[72]](#footnote-73).

Contrairement à ce qui se passe dans le cas de la traite des êtres humains, ceux qui paient les passeurs pour entrer irrégulièrement dans l’UE le font volontairement. L’activité des passeurs est toutefois criminelle, met souvent des vies en danger et peut entraîner des risques supplémentaires pour la sécurité de l’UE. La prévention et la lutte contre le **trafic de migrants** constituent un objectif clé de la stratégie de l’UE pour l’union de la sécurité, de la stratégie de l’UE visant à lutter contre la criminalité organisée et du nouveau pacte sur la migration et l’asile[[73]](#footnote-74). Cet objectif nécessite une coopération et une coordination internationales continues à tous les niveaux. La mise en œuvre du plan d’action de l’UE contre le trafic de migrants (2021-2025)[[74]](#footnote-75) progresse, des partenariats opérationnels de lutte contre le trafic de migrants sont en cours d’élaboration avec le Maroc, le Niger et les Balkans occidentaux, et sont soutenus par les institutions, organes et agences de l’UE, ainsi que par un financement de l’UE.

Le marché des **drogues illicites**, sur lequel la valeur des ventes au détail est estimée à un minimum de 30 000 000 000 d’EUR par an, continue de représenter le plus important marché criminel dans l’UE et une source de revenus majeure pour les organisations criminelles. ainsi qu’une menace pour la stabilité sociale et la santé. En 2021, l’action et la coopération de l’UE ont permis de retirer du marché une quantité de drogues estimée à 7 000 000 000 d’EUR[[75]](#footnote-76). Le **programme et le plan d’action antidrogue de l’UE pour la période 2021-2025**[[76]](#footnote-77) de juillet 2020 définissent des actions concrètes visant à renforcer l’action au niveau de l’UE, notamment la transformation de l’Observatoire européen des drogues et des toxicomanies en l’Agence de l’Union européenne pour les questions liées aux drogues. Le mandat révisé de l’Agence proposé en janvier 2022[[77]](#footnote-78) renforcerait ses capacités de surveillance et d’évaluation des menaces et sa capacité à répondre aux nouveaux défis. Le Conseil a adopté une orientation générale en juin 2022 et les travaux au Parlement européen sont en cours. La Commission a également lancé une coopération au sein du forum de l’UE sur l’internet afin de lutter contre le trafic de drogue en ligne et a proposé qu’il soit procédé à une évaluation thématique spécifique de Schengen sur le trafic de cocaïne dans les ports de l’UE. Le soutien au Centre d’opération et d’analyse maritime de lutte contre le trafic de drogue a été renforcé. L’UE poursuit également ses dialogues politiques sur les questions liées à la drogue avec les pays tiers, un deuxième dialogue ayant été organisé avec la Chine en juillet 2022 et un nouveau dialogue ayant été lancé avec la Colombie en juin 2022.

Selon Europol, près de 99 % des profits générés par la criminalité échappent à la confiscation dans l’UE et restent entre les mains des criminels[[78]](#footnote-79). Les propositions de l’UE visant à renforcer la lutte contre le blanchiment de capitaux et le financement du terrorisme, proposées par la Commission en juillet 2021, progressent au sein du Conseil[[79]](#footnote-80). En mai 2022, la Commission a proposé de renforcer et de moderniser les règles de l’UE en matière de recouvrement et de confiscation des avoirs[[80]](#footnote-81). La proposition a été examinée au sein des groupes de travail du Conseil et des progrès ont été réalisés dans plusieurs domaines.

Le **Parquet européen** a à présent achevé sa première année complète de travail en faveur de la protection des intérêts financiers de l’UE. Il a reçu 4 006 signalements d’infraction, ouvert 929 enquêtes et accordé des décisions de gel pour un montant total de 259 000 000 d’EUR. Au cours de ses sept premiers mois d’activité, les affaires faisant l’objet d’une enquête étaient potentiellement responsables d’un préjudice estimé à 5400 000 000 d’EUR pour le budget de l’Union[[81]](#footnote-82).

La Commission travaille également à la préparation de la **boîte à outils européenne de lutte contre la contrefaçon**, comme annoncé dans le plan d’action en faveur de la propriété intellectuelle[[82]](#footnote-83) et relevé dans la stratégie de lutte contre la criminalité organisée.

En plus de nuire à la confiance entre l’État et les citoyens, la **corruption** constitue une menace pour la sécurité. Elle constitue un outil essentiel de la criminalité organisée et rend possible un large éventail d’activités criminelles. Il s’agit d’un thème central du cycle annuel de rapport sur l’état de droit[[83]](#footnote-84). Si certains États membres de l’UE restent parmi les pays les plus performants au niveau mondial en matière de lutte contre la corruption, des problèmes subsistent, en particulier en ce qui concerne les enquêtes pénales, les poursuites et l’application de sanctions pour corruption dans certains États membres. De nombreux États membres ont pris des mesures pour renforcer les cadres relatifs à la prévention de la corruption et à l’intégrité mais les ressources allouées à la lutte contre la corruption sont souvent insuffisantes. La Commission travaille actuellement à l’élaboration d’un paquet anticorruption pour 2023, qui mettra à jour et rationalisera la législation dans ce domaine.

Le plan d’action de l’UE en matière de lutte contre le **trafic d’armes à feu**[[84]](#footnote-85) et la stratégie de l’UE pour l’union de la sécurité ont été adoptés conjointement. Le plan d’action a fait l’objet d’un suivi dans une proposition d’octobre 2022 visant à réviser les règles relatives aux autorisations d’exportation, aux importations et aux mesures de transit pour les armes à feu[[85]](#footnote-86), en mettant davantage l’accent sur la numérisation. Dans l’ensemble, la traçabilité des armes à feu civiles devrait s’en trouver améliorée. Des travaux sont également en cours pour mieux soutenir l’Ukraine et la République de Moldavie en ce qui concerne les **armes légères et de petit calibre** (ALPC) dans le contexte de l’agression russe contre l’Ukraine.

Le trafic illicite de biens culturels est une activité lucrative pour les organisations criminelles et, dans certains cas, pour les parties au conflit et les terroristes[[86]](#footnote-87). Il bénéficie donc à la criminalité organisée et a des effets néfastes sur le patrimoine culturel. Les criminels peuvent même faire un usage abusif de biens culturels acquis légalement, à des fins de blanchiment de capitaux, de contournement de sanctions, d’évasion fiscale ou de financement du terrorisme. Afin de renforcer la **lutte contre le trafic de biens culturels**, la Commission adopte aujourd’hui un plan d’action[[87]](#footnote-88).

Selon Interpol et le Programme des Nations unies pour l’environnement, la **criminalité environnementale** est la quatrième activité criminelle la plus importante au monde après le trafic de drogue, la traite des êtres humains et la contrefaçon. Des propositions ambitieuses de la Commission concernant une nouvelle directive relative à la protection de l’environnement par le droit pénal[[88]](#footnote-89), un nouveau règlement relatif aux transferts de déchets[[89]](#footnote-90) et un nouveau règlement sur la déforestation[[90]](#footnote-91) sont en cours de négociation. Une fois adoptées, elles renforceront la chaîne répressive et prévoiront des sanctions plus sévères et des outils d’enquête appropriés. Elles sont également complétées par un plan d’action révisé contre le trafic d’espèces sauvages[[91]](#footnote-92).

***Exemples clés de mise en œuvre***

**Encrochat**: avec le soutien d’Europol et d’Eurojust, les services répressifs et les autorités judiciaires de Belgique, de France et des Pays-Bas ont coopéré afin de bloquer l’utilisation de communications cryptées par des groupes de la grande criminalité organisée. Au moment de sa fermeture, le service comptait 60 000 abonnés, dont, selon les estimations, 90 % de criminels.

**La coopération judiciaire et policière de l’UE a conduit au démantèlement d’un groupe de grande envergure de la criminalité organisée (l’«affaire Pollino»):** une équipe commune d’enquête établie en 2016 entre l’Italie, l’Allemagne et les Pays-Bas a lancé une journée d’action, coordonnée par Eurojust et soutenue par Europol, qui a conduit à la condamnation de 34 personnes, dont les peines cumulées s’élèvent à plus de 400 ans de prison. Plus tard, 12 autres personnes ont été condamnées à plus de 173 ans de prison et des procédures sont toujours en cours dans plusieurs États membres.

**4.** **ASSURER LA SÉCURITÉ DE NOS FRONTIÈRES ET SOUTENIR LA COOPÉRATION POLICIÈRE ET JUDICIAIRE**

Outre les avantages économiques et sociaux qu’il présente, le bon fonctionnement de l’**espace Schengen** est essentiel à la sécurité de l’UE. Cela nécessite une gestion efficace des frontières extérieures de l’UE et une coopération renforcée en matière répressive. En juin 2021, la Commission a adopté une «Stratégie pour un espace Schengen pleinement opérationnel et résilient»[[92]](#footnote-93), qui expose la façon dont les mesures prises dans le domaine de la sécurité, de la coopération policière et judiciaire peuvent garantir que l’UE reste forte face aux menaces pour la sécurité, même sans contrôles aux frontières intérieures. La stratégie passe désormais par le cycle annuel Schengen, un nouveau modèle de gouvernance pour l’espace Schengen, et dont les progrès ont fait l’objet du premier rapport sur la situation dans l’espace Schengen, adopté en mai 2022[[93]](#footnote-94). Une étape essentielle est la modification du code frontières Schengen[[94]](#footnote-95) au moyen de la proposition de la Commission de décembre 2021, qui a prévu de nouvelles dispositions visant à soutenir une coopération efficace en matière de sécurité et les mesures à prendre pour gérer plus efficacement les frontières extérieures dans les situations de crise. Une orientation générale du Conseil ayant été définie juin 2022, il est important que le Parlement européen et le Conseil concluent rapidement les négociations. La Commission a également souligné les avantages de l’inclusion de la Bulgarie, de la Roumanie et de la Croatie dans tous les aspects de Schengen, qui renforcera la sécurité et la confiance mutuelle dans l’espace Schengen[[95]](#footnote-96). En décembre 2022, le Conseil a adopté une décision relative à l’application de la totalité de l’acquis de Schengen en Croatie[[96]](#footnote-97).

Dans un espace sans contrôles aux frontières intérieures, les policiers d’un État membre devraient avoir accès aux mêmes informations que celles dont disposent leurs homologues dans un autre État membre. Une coopération entière et effective doit être la norme. C’est pourquoi il est essentiel de renforcer les outils dont disposent les services répressifs et les autorités judiciaires dans l’ensemble de l’UE aux fins de l’**échange d’informations et de la coopération transfrontière**. Le train de mesures sur la coopération policière de décembre 2021[[97]](#footnote-98) a permis d’améliorer considérablement les outils disponibles. La **directive relative à l’échange d’informations** a désormais fait l’objet d’un accord politique entre le Parlement européen et le Conseil, et une recommandation du Conseil visant à renforcer les opérations de coopération policière transfrontalière a été adoptée par le Conseil en juin 2022. Les négociations se poursuivent sur un règlement révisant le cadre Prüm[[98]](#footnote-99), avec pour objectif de permettre un échange de données automatisé plus efficace entre les services répressifs dans des domaines spécifiques tels que l’ADN, les données dactyloscopiques et les données relatives à l’immatriculation des véhicules, et d’ajouter les catégories de casiers judiciaires et d’images faciales. Un accord rapide sur le **règlement Prüm II** permettrait à l’ensemble des nouveaux outils d’échange d’informations de devenir une réalité sur le terrain pour les services répressifs dans les États membres.

Afin de lutter plus efficacement contre la criminalité transfrontière, les services répressifs et les autorités judiciaires des États membres doivent collaborer étroitement avec le soutien d’agences de l’UE telles qu’Europol et Eurojust. Le nouveau mandat d’**Europol** est entré en vigueur en juin 2022, ce qui lui permet de renforcer son expertise et ses capacités opérationnelles afin de mieux soutenir les États membres dans la lutte contre la grande criminalité organisée et le terrorisme. Le mandat renforce également le cadre d’Europol en matière de protection des données et la surveillance du Contrôleur européen de la protection des données. Les autorités chargées des enquêtes et les juridictions des différents États membres doivent coopérer et se soutenir mutuellement dans le cadre des enquêtes et des poursuites pénales et échanger des informations et des éléments de preuve de manière sécurisée et rapide. Le **train de mesures sur la justice numérique**[[99]](#footnote-100) adopté en décembre 2021 prévoit des mesures concrètes visant à améliorer l’échange d’informations numériques sur les affaires de terrorisme transfrontières, à mettre en place une plateforme de coopération destinée à soutenir le fonctionnement des équipes communes d’enquête et à renforcer la numérisation de la coopération judiciaire transfrontière et l’accès à la justice en matière civile, commerciale et pénale. L’adoption rapide de ce train de mesures par le Parlement européen et le Conseil faciliterait considérablement l’échange d’informations entre les autorités judiciaires.

Les preuves électroniques font partie de presque toutes les enquêtes. L’accord politique provisoire conclu en novembre 2022 sur les **preuves électroniques**[[100]](#footnote-101) permettra aux autorités judiciaires des États membres d’échanger de manière sécurisée les preuves revêtant une importance cruciale afin de lutter plus efficacement contre la criminalité.

La sécurisation des frontières extérieures de l’UE est une responsabilité commune. Les premières équipes du contingent permanent du corps européen de garde-frontières et de garde-côtes ont été déployées avec succès depuis janvier 2021 et le contingent permanent compte désormais quelque 4 800 agents de Frontex et des autorités nationales.

L’augmentation du nombre d’arrivées irrégulières cette année sur la plupart des routes migratoires a mis en évidence l’importance de contrôles d’identité et de sécurité systématiques pour tous les migrants arrivant aux frontières extérieures de l’UE, ainsi que de contrôles sanitaires répondant à des normes communes. La sécurité est un thème important du nouveau pacte sur la migration et l’asile. L’orientation rapide des migrants vers les procédures appropriées prévues par la **proposition relative au filtrage** contribuerait à garantir l’application des contrôles de sécurité, dans le plein respect de toutes les obligations en matière de droits fondamentaux. Une position du Parlement européen sur cette proposition est toujours attendue.

L’**instrumentalisation des migrants** à des fins politiques par le régime biélorusse au cours du second semestre de 2021 a posé des problèmes juridiques, opérationnels et humains sans précédent, notamment pour la sécurité. La proposition de code frontières Schengen aborde également la question de l’instrumentalisation des migrants par des pays tiers à des fins politiques. Les États membres confrontés à cette situation seraient par exemple en mesure de limiter le nombre de points de passage frontaliers et d’intensifier la surveillance des frontières.

Une nouvelle architecture des **systèmes d’information** de l’UE est en cours d’élaboration afin de mieux soutenir les efforts déployés par les autorités nationales pour assurer la sécurité ainsi que la gestion des frontières et des migrations. Le système d’information Schengen renouvelé, qui devrait démarrer ses activités en mars 2023, est au cœur de ce système. D’autres outils essentiels sont le système d’entrée/de sortie (dont les travaux devraient débuter en mai 2023), le système européen d’information et d’autorisation concernant les voyages (ETIAS) (qui devrait entrer en service d’ici la fin de 2023) et la mise à jour du système d’information sur les visas (VIS). Ils permettront d’accroître les contrôles et de combler les lacunes en matière d’informations liées à la sécurité grâce à un meilleur échange d’informations entre les États membres. L’interopérabilité des systèmes est cruciale pour ces travaux: il est essentiel que l’eu-LISA et les États membres prennent sans délai les mesures nécessaires pour mener à bien ce projet ambitieux en vue de sa mise en œuvre intégrale d’ici à la fin 2024.

Les **contrôles des marchandises entrantes** doivent être efficaces pour réduire les risques pour l’UE et ses citoyens, tout en garantissant la compétitivité des entreprises légitimes de l’UE. Les contrôles de sécurité ont été renforcés pour ces marchandises grâce à la modernisation du système de contrôle des importations de l’UE[[101]](#footnote-102), afin de soutenir des contrôles douaniers efficaces fondés sur les risques et des mesures visant à protéger la renforcer la sûreté du fret aérien contre les menaces terroristes. Le programme de l’instrument relatif aux équipements de contrôle douanier (CCEI)[[102]](#footnote-103) finance également l’achat, la maintenance et la mise à niveau en toute transparence d’équipements de contrôle douanier pertinents, modernes et fiables.

La capacité de l’**information préalable sur les passagers (API)** à contribuer à la sécurité est entravée par des règles obsolètes et appliquées de manière inégale. Les nouvelles propositions de la Commission abrogeraient l’actuelle directive API de manière à clarifier et à améliorer l’utilisation des API, à la fois dans le cadre de la gestion des frontières et du fonctionnement des services répressifs[[103]](#footnote-104). Cela élargirait l’utilisation des API à certains vols intra-UE, étoffant ainsi la boîte à outils à la disposition des services répressifs des États membres au sein de l’espace Schengen. Des réflexions sur la dimension extérieure de la politique de l’UE relative aux **données des dossiers passagers** (PNR) sont en cours afin de prendre en considération le fait qu’un nombre croissant de pays tiers développent actuellement la capacité de traiter ces informations à des fins répressives et de sécurité des frontières. La Commission prépare également une proposition législative relative à un cadre pour un accès réciproque aux informations liées à la sécurité pour les agents de première ligne entre l’UE et les pays tiers afin de détecter efficacement les criminels et les terroristes.

La **fraude liée aux documents de voyage** facilite les mouvements clandestins des criminels et des terroristes et joue un rôle essentiel dans la traite des êtres humains et le trafic de stupéfiants. Il convient d’y remédier tout en répondant à la nécessité de faciliter la circulation des voyageurs en règle, de sorte que, depuis août 2021, les États membres délivrent des cartes d’identité assorties de normes de sécurité harmonisées, dont une puce électronique contenant des éléments d’identification biométriques qui peuvent être vérifiés par toutes les autorités frontalières de l’UE[[104]](#footnote-105). La Commission prépare actuellement une nouvelle initiative relative à la numérisation des documents de voyage et la facilitation des déplacements[[105]](#footnote-106), qui renforcera la sécurité et accélérera les déplacements et les procédures aux frontières grâce à une communication avancée sans support papier des données relatives aux déplacements et des données à caractère personnel et grâce aux contrôles biométriques aux frontières.

*Répression et nouvelles technologies*

Les technologies telles que l’**intelligence artificielle** ou le cryptage peuvent apporter une valeur ajoutée aux services répressifs et aux autorités judiciaires, mais peuvent également entraver leur travail. Dans sa communication sur l’intelligence artificielle (IA) et dans la législation sur l’intelligence artificielle[[106]](#footnote-107), la Commission a souligné que l’IA peut jouer un rôle considérable dans la réalisation des objectifs de la stratégie de l’UE pour l’union de la sécurité, capable de contrer les menaces actuelles et d’anticiper les risques et les possibilités susceptibles de se présenter dans l’avenir[[107]](#footnote-108). Dans le cadre d’Horizon Europe, le programme de recherche et d’innovation de l’UE pour la période 2021-2027, un financement est disponible pour des actions de **recherche et d’innovation en matière de sécurité civile**, notamment en matière d’IA ou de biométrie. Pour les seuls exercices 2021 et 2022, 413,8 000 000 d’EUR ont déjà été programmés en 2022[[108]](#footnote-109).

***Exemple clé de mise en œuvre***

**Utilisation du système d’information Schengen (SIS)**: En 2021, les États membres ont effectué près de 7 milliards de recherches dans le SIS. Les autorités des États membres ont effectué dans le système près de 20 millions de recherches par jour en moyenne, lesquelles ont donné lieu à une moyenne de 600 réponses positives par jour concernant des signalements étrangers et contribué à résoudre un nombre équivalent de cas. Par exemple, après un double meurtre brutal commis en Roumanie en 2021, l’auteur du crime a été retrouvé en Italie quelques jours plus tard grâce à un signalement SIS en vue d’une arrestation qui a alerté les enquêteurs italiens, qui ont pu arrêter l’homme à Rome.

**5.** **LE LIEN ENTRE SÉCURITÉ INTÉRIEURE ET SÉCURITÉ EXTÉRIEURE: SÉCURITÉ DANS LE VOISINAGE DE L’UE ET DANS LES PAYS PARTENAIRES**

Les événements qui surviennent en dehors des frontières de l’UE et la sécurité à l’intérieur de l’Europe sont étroitement liés. Pour renforcer la sécurité intérieure de l’UE, il est indispensable de soutenir et d’aider nos voisins et nos partenaires à renforcer leur sécurité intérieure et à coopérer avec nos alliés et avec les organisations internationales telles que l’OTAN ou les Nations unies.

Le Service européen pour l’action extérieure (SEAE) et les services de la Commission collaborent étroitement avec les principaux pays partenaires et organisations internationales, dans le cadre de dialogues réguliers s**ur la lutte contre le terrorisme**. Plus de 30 dialogues sur la lutte contre le terrorisme sont en cours avec des pays tiers et des organisations internationales[[109]](#footnote-110). Parallèlement, le réseau d’experts en matière de lutte contre le terrorisme et de sécurité au sein des délégations de l’UE dans les principaux pays tiers a été renforcé.

Afin de mieux contrer les menaces pour la sécurité intérieure qui découlent de la guerre d’agression menée par la Russie contre l’Ukraine, les services de la Commission et le SEAE, conjointement avec le coordinateur de l’UE pour la lutte contre le terrorisme, ont convenu avec l’**Ukraine** d’établir une coopération structurée et continue en matière de sécurité. Cette collaboration vise à renforcer la coopération opérationnelle, notamment avec Europol et Frontex, et à renforcer l’échange d’informations relatives aux menaces pesant sur la sécurité intérieure. Les agences de l’UE ont apporté un soutien immédiat pour relever les défis qui se sont présentés à la suite de l’invasion. Frontex emploie actuellement 277 personnes dans la région, Europol 15 et l’Agence de l’Union européenne pour l’asile 60.

Les autorités répressives des États membres et leurs partenaires collaborent dans le cadre de la **plateforme pluridisciplinaire européenne contre les menaces criminelles (EMPACT)** pour organiser des actions opérationnelles et des journées d’action communes de lutte contre les menaces criminelles nouvelles ou en évolution liées à l’agression russe contre l’Ukraine.

Le dialogue sur la cybersécurité entre l’UE et l’Ukraine a été intensifié grâce à un soutien politique, financier et matériel coordonné de l’UE afin d’aider l’Ukraine à renforcer sa cyberrésilience. Une enveloppe globale de 29 000 000 d’EUR destiné à accroître la cyberrésilience et la résilience numérique de l’Ukraine a financé des équipements, des logiciels et la transformation numérique résiliente en matière de cybersécurité.

En raison de sa situation géographique, la République de **Moldavie** a un rôle essentiel à jouer pour faire face aux répercussions de l’invasion de l’Ukraine par la Russie dans les domaines de la criminalité et de la sécurité. En juillet 2022, la Commission, en coopération avec le SEAE, a créé une plateforme de l’UE de soutien à la sécurité intérieure et à la gestion des frontières avec la République de Moldavie. Son rôle principal est de faciliter la coopération et l’action opérationnelle afin de faire face aux menaces communes pour la sécurité dans six domaines prioritaires définis conjointement par l’UE et la République de Moldavie: le trafic d’armes à feu, le trafic de migrants, la traite des êtres humains, la prévention du terrorisme et de l’extrémisme violent et la lutte contre ceux-ci, la cybercriminalité et le trafic de drogues. En mars 2022, la République de Moldavie a signé un accord sur le statut avec Frontex, sur la base de son mandat renforcé.

La coopération en matière répressive entre l’UE et les **pays des Balkans occidentaux**, qui s’appuie également sur les agences de l’UE, a continué de s’intensifier au cours des trois dernières années. Conformément aux conclusions du Conseil de mars 2021, la coopération en matière répressive avec des pays tiers a été intégrée dans tous les plans d’actions opérationnels de la plateforme EMPACT (plateforme pluridisciplinaire européenne contre les menaces criminelles), ce qui a dopé la participation des Balkans occidentaux aux activités d’EMPACT. Un financement important au titre de l’instrument de préadhésion continue d’être fourni pour la réforme et les performances des services répressifs, les agences de l’UE assurant également le renforcement des capacités des acteurs de la sécurité. Le plan d’action conjoint relatif à la lutte contre le terrorisme signé en 2018 a bien progressé et, dans le cas de la Macédoine du Nord et de l’Albanie, étant donné que la plupart des actions ont été menées à bien, une version actualisée révisée des accords bilatéraux respectifs a été signée en décembre 2022, afin de renforcer encore notre coopération dans le domaine de la lutte contre le terrorisme ainsi que de la prévention et de la lutte contre l’extrémisme violent.

Le 18 novembre 2022, le Conseil a autorisé l’ouverture de négociations relatives à des **accords sur le statut** entre l’Union européenne et la République d’Albanie, la Serbie, le Monténégro et la Bosnie-Herzégovine[[110]](#footnote-111). Ces accords permettraient à Frontex de déployer des équipes chargées de la gestion des frontières pour effectuer des tâches de contrôle aux frontières, sous le commandement des autorités nationales compétentes. Cela revêtira une importance particulière dans le cadre de la lutte contre le trafic de migrants. La Macédoine du Nord a signé un accord sur le statut avec Frontex en octobre 2022, sur la base de son mandat renforcé.

L’**UE et les États-Unis** ont également une longue tradition de partenariat et de coopération dans les domaines liés à la sécurité et visent à échanger plus systématiquement et en temps utile des informations sur des questions telles que le terrorisme, la radicalisation et la criminalité organisée. L’UE et les États-Unis tiennent régulièrement des réunions conjointes dans le domaine de la justice et des affaires intérieures afin d’approfondir la coopération dans les domaines d’intérêt commun, de promouvoir la sécurité mondiale et de s’informer mutuellement des progrès législatifs réalisés concernant les dossiers JAI. Les autorités judiciaires et les services répressifs européens coopèrent étroitement avec leurs homologues américains en ce qui concerne les questions opérationnelles et législatives. Les autorités répressives américaines participent activement à plusieurs actions et réseaux d’EMPACT, sur la base d’un accord de coopération opérationnelle entre les États-Unis et Europol. Un exemple particulièrement fort de coopération efficace est la task-force opérationnelle Greenlight/Trojan Shield, l’une des opérations répressives les plus importantes et les plus sophistiquées à ce jour dans la lutte contre les activités criminelles cryptées. Le programme de surveillance du financement du terrorisme entre l’UE et les États-Unis fournit de nombreuses pistes concrètes pour les enquêtes terroristes[[111]](#footnote-112). La coopération repose également sur un suivi clair des garanties et des contrôles.

Les dialogues réguliers UE-États-Unis en matière de cybersécurité renforcent la coopération et la coordination en matière de cyberdiplomatie et de cyber-résilience, notamment la normalisation de la cybersécurité. Le Conseil du commerce et des technologies (CCT) a également permis d’approfondir la coopération, au moyen d’une déclaration conjointe en matière de cybersécurité et des mesures ont été proposées en vue d’une coopération éventuelle en matière de recherche et de développement au-delà de la 5G et de la 6G, de contrôles des exportations et de filtrage des investissements, ainsi que sur les sanctions contre de la Russie et la Biélorussie. Le CCT poursuivra également la coopération entre l’UE et les États-Unis en matière de manipulation de l’information et l’ingérence étrangères.

D’importants défis liés à la sécurité en Afrique ont une incidence directe sur les Africains eux-mêmes ainsi que sur la sécurité de l’UE. De nombreux projets sont mis en œuvre pour aider les pays partenaires à renforcer leurs capacités à relever ces défis, par l’intermédiaire du financement de l’Académie internationale de lutte contre le terrorisme (AILCT) en Afrique de l’Ouest ou de l’initiative régionale visant à renforcer les capacités de lutte contre le blanchiment de capitaux et le financement du terrorisme dans la région de la Grande Corne.

Les pays d’**Amérique latine et des Caraïbes** (ALC) sont des partenaires essentiels de l’UE et une nouvelle initiative régionale Équipe Europe sur la sécurité et la justice a été lancée en mai 2022 afin de mettre en place un partenariat UE-ALC sur le renforcement de l’État de droit et de la lutte contre la criminalité organisée.

Le règlement de l’UE relatif au **filtrage des investissements directs étrangers** est entré en vigueur en octobre 2020[[112]](#footnote-113) et fournit un cadre visant à améliorer la protection contre les investissements directs étrangers qui présentent un risque pour la sécurité ou l’ordre public dans plusieurs États membres. Au cours de sa première année complète de fonctionnement, plus de 400 cas ont été notifiés à la Commission. Le règlement sur les biens à double usage[[113]](#footnote-114) adopté en septembre 2021 a amélioré et renforcé le système de **contrôle des exportations de biens à double usage** de l’UE et a introduit de nouvelles dispositions qui permettent à l’UE, en coordination avec les États membres, d’adopter des contrôles autonomes des exportations de biens et de technologies ne figurant pas sur la liste.

Dans un monde globalisé où les formes graves de criminalité et le terrorisme présentent un caractère de plus en plus transnational, les autorités répressives et judiciaires devraient être parfaitement équipées pour coopérer avec des partenaires extérieurs afin de garantir la sécurité des citoyens. Cela nécessite d’ouvrir la voie à la coopération et à l’échange d’informations entre les autorités judiciaires des pays tiers et **Europol et Eurojust**. Un accord signé en juin 2022 entre Europol et la Nouvelle-Zélande sur l’échange de données à caractère personnel dans le cadre de la lutte contre les formes graves de criminalité et le terrorisme[[114]](#footnote-115) est actuellement suivi de négociations avec un certain nombre d’autres pays, mais, dans la plupart des cas, les progrès restent lents. En ce qui concerne Eurojust, les négociations sont bien avancées avec l’Arménie, avec qui un accord sur le texte a été dégagé, et elles ont débuté avec la Colombie, l’Algérie et le Liban.

En avril 2022, au cours du quatrième dialogue des dirigeants sur la lutte contre le terrorisme, l’**UE et les Nations unies** ont pris des mesures concrètes visant à renforcer leur partenariat existant dans le cadre de la lutte contre les menaces persistantes mais en évolution qui pèsent sur la paix et la sécurité internationales. Le partenariat stratégique a encore été renforcé par le lancement de la nouvelle facilité UE-ONU de lutte contre les menaces terroristes à l’échelle mondiale («EU-UN Global Terrorism Threats Facility»), une initiative financée par l’UE visant à soutenir les États confrontés au terrorisme et à l’extrémisme violent, notamment au moyen d’une assistance, d’une formation et d’un encadrement. Parmi les autres questions d’intérêt commun figurent les menaces émergentes liées aux nouvelles technologies, notamment la manière dont elles affectent les jeunes en tant que groupe cible particulier de la radicalisation à la violence, et le terrorisme fondé sur la xénophobie, le racisme et d’autres formes d’intolérance, ou au nom de la religion ou des convictions.

La coopération entre l’**UE et l’OTAN** a également été renforcée, avec des résultats tangibles dans tous les domaines de coopération[[115]](#footnote-116). L’UE et l’OTAN ont intensifié leurs travaux et leur coopération à la suite de la guerre d’agression menée par la Russie, ils ont adopté une position politique unie et ont coordonné leurs efforts afin d’aider l’Ukraine à se défendre et à protéger sa population. Le partenariat stratégique UE-OTAN est plus solide et plus pertinent que jamais en cette période cruciale pour la sécurité euro-atlantique. En ce qui concerne la résilience, un dialogue structuré spécifique a été lancé en janvier 2022 et est en cours d’approfondissement afin de soutenir la protection des infrastructures critiques et une task-force UE-OTAN sera mise en place dans ce contexte. En ce qui concerne la mobilité militaire, de nouvelles améliorations ont été apportées en ce qui concerne les aspects liés au transport et à la réglementation, notamment le transport de marchandises dangereuses. La lutte contre les menaces hybrides reste également un domaine essentiel de coopération avec l’OTAN. Les échanges portent notamment sur la lutte contre le terrorisme, ainsi que sur la communication stratégique, la manipulation de l’information et l’ingérence étrangères et les questions liées au cyberespace. Parmi les exercices, on peut citer l’EU Integrated Resolve réalisé en novembre 2022 dans le cadre du concept d’exercice parallèle et coordonné (PACE), avec la participation du personnel de l’OTAN afin d’améliorer l’interaction entre les différents mécanismes de réaction aux crises.

Depuis septembre 2022, l’UE assure la coprésidence du **Forum mondial de lutte contre le terrorisme**. Parmi les priorités figurent la lutte contre la menace terroriste en Afrique et l’intégration de l’égalité entre les hommes et les femmes et de l’éducation dans la politique de lutte contre le terrorisme.

La négociation d’un accord de coopération entre l’Union et **Interpol** est en cours en vue de parvenir à une conclusion au niveau technique au cours du premier semestre de 2023. L’objectif principal est de renforcer encore l’échange d’informations entre Interpol et les agences et organes de l’UE, de mieux soutenir les États membres et d’accroître la sécurité des citoyens, non seulement dans l’UE, mais aussi dans le monde entier.

***Exemple clé de mise en œuvre***

**Opération «Desert Light»: démantèlement d’un cartel de la drogue européen dans six pays:** En novembre 2022, des raids coordonnés ont été effectués dans toute l’Europe et dans les Émirats arabes unis (EAU), ciblant à la fois le centre de commandement et de contrôle et l’infrastructure logistique du trafic de drogue en Europe. Des cibles de grande importance avaient formé un «supercartel» qui contrôlait environ un tiers du commerce de cocaïne en Europe. Au total, 49 suspects ont été arrêtés à la suite d’enquêtes menées en Espagne, en France, en Belgique, aux Pays-Bas et dans les Émirats arabes unis avec le soutien d’Europol. 30 tonnes de stupéfiants ont été saisies par les services répressifs au cours des enquêtes.

**6.** **CONCLUSIONS**

Au cours des deux dernières années et demie, la Commission, en étroite coopération avec le Service européen pour l’action extérieure, a mené à bien la quasi-totalité des actions prévues dans la stratégie pour l’union de la sécurité. Le large éventail de propositions doit être adopté et surtout mis en œuvre. Les décisions et les actions du Parlement européen, du Conseil et des différents États membres seront essentielles pour faire en sorte que l’UE mette en place un écosystème de sécurité solide pour ses citoyens.

Dans le même temps, l’environnement de sécurité dans lequel nous vivons continuera d’évoluer. Depuis l’adoption de la stratégie pour l’union de la sécurité, l’UE a été confrontée à la pandémie de COVID-19 et aux répercussions de l’agression de la Russie contre l’Ukraine. On a observé une prolifération exponentielle des menaces en ligne et la nécessité d’une adaptation et d’une prospective rapides. L’UE doit continuer à se doter des moyens nécessaires pour faire face à l’évolution des menaces qui pèsent sur la sécurité de ses citoyens. La vigilance constante, la détermination à agir et les réponses collectives seront essentielles à la réussite collective de l’UE à l’avenir.

1. COM(2020) 605. [↑](#footnote-ref-2)
2. Voir le rapport 2022 de l’ENISA sur le paysage des menaces. [↑](#footnote-ref-3)
3. 1) un environnement de sécurité à l’épreuve du temps, 2) faire face à l’évolution des menaces, 3), protéger les Européens contre le terrorisme et la criminalité organisée, 4) un solide écosystème européen de la sécurité. [↑](#footnote-ref-4)
4. Un tableau en annexe donne un aperçu des actions législatives et non législatives depuis le lancement de la stratégie pour l’union de la sécurité. [↑](#footnote-ref-5)
5. Un plan d’action sur le trafic de biens culturels [COM(2022) 800] et deux propositions sur la révision de la directive concernant les informations préalables sur les passagers [COM(2022) 729 et 731]. [↑](#footnote-ref-6)
6. Une proposition de révision de la directive relative à la lutte contre la traite des êtres humains [COM(2022) 732] et le quatrième rapport sur l’état d’avancement de la lutte contre la traite des êtres humains devraient être adoptés le 19 décembre 2022. [↑](#footnote-ref-7)
7. Proposition de révision de la directive (UE) 2016/1148. [↑](#footnote-ref-8)
8. COM(2020) 823. [↑](#footnote-ref-9)
9. COM(2020) 829. [↑](#footnote-ref-10)
10. Les secteurs suivants sont couverts par la directive SRI 2 et la directive CER: énergie, transports, banques, finances, infrastructures des marchés financiers, infrastructures numériques, santé, eau potable, eaux usées, administration publique, espace, et production, transformation et distribution de denrées alimentaires. [↑](#footnote-ref-11)
11. Des discussions sont en cours entre les experts nationaux au sein du groupe de coopération SRI afin d’aider les États membres à transposer et à mettre en œuvre la directive SRI 2. [↑](#footnote-ref-12)
12. COM(2020) 595. Accord politique conclu en mai 2022. [↑](#footnote-ref-13)
13. Le groupe réunit des représentants des États membres, de la Commission et de l’Agence de l’Union européenne pour la cybersécurité (ENISA) ayant pour mission de soutenir et de faciliter la coopération stratégique entre les États membres en ce qui concerne la sécurité des réseaux et des systèmes d’information. [↑](#footnote-ref-14)
14. Conclusions du Conseil sur la mise en place d’une posture cyber de l’Union européenne, 23 mai 2022. [↑](#footnote-ref-15)
15. Conformément à l’[appel de Nevers](https://presse.economie.gouv.fr/08-03-2022-rmi-telecom-les-etats-membres-appellent-les-entreprises-du-secteur-numerique-a-renforcer-la-lutte-contre-la-desinformation-en-ligne/) à renforcer les capacités de l’UE en matière de cybersécurité adopté lors de la réunion informelle des ministres des télécommunications le 9 mars 2022. [↑](#footnote-ref-16)
16. La proposition de la Commission [[COM(2022) 551](https://eur-lex.europa.eu/legal-content/FR/TXT/?uri=CELEX%3A52022DC0551&qid=1666351317270)](https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52022DC0551&qid=1666351317270) a été suivie par l’adoption d’une recommandation du Conseil le 8 décembre 2022. [↑](#footnote-ref-17)
17. Comme l’exige le règlement sur le marché intérieur de l’électricité (UE) 2019/943. [↑](#footnote-ref-18)
18. Organisation de l’aviation civile internationale (Doc. 10084 intitulé «Manuel d’évaluation des risques pour les vols d’aéronefs civils au-dessus et à proximité de zones de conflit», 2018) [↑](#footnote-ref-19)
19. Y compris par la mise en œuvre de projets capacitaires CSP et de projets Horizon 2020. [↑](#footnote-ref-20)
20. EU-CIP, pour un pôle européen de connaissance et un banc d’essai pour la protection des infrastructures critiques et ATLANTIS — Plateforme atlantique d’essai pour la robotique maritime: nouvelles frontières pour l’inspection et la maintenance d’infrastructures énergétiques en mer. [↑](#footnote-ref-21)
21. JOIN(2020) 18. [↑](#footnote-ref-22)
22. EU-CyCLONe est composé de représentants des autorités des États membres chargées de la gestion des crises cyber avec la participation de la Commission dans les cas où un cyberincident de grande ampleur a ou est susceptible d’avoir des incidences importantes sur les services et activités prévus par la directive. [↑](#footnote-ref-23)
23. C(2021) 4520. [↑](#footnote-ref-24)
24. À titre d’exemples, on peut citer l’exercice de simulation Blue OLEx («Blueprint Operational Level Exercise») organisé par la Lituanie et l’ENISA, et la séquence d’exercice «EU CyCLES» (Cyber Crisis Linking Exercise on Solidarity), organisée par la présidence française. [↑](#footnote-ref-25)
25. Une première phase a été lancée avec un appel à propositions sur le renforcement des capacités des centres d’opérations de sécurité et un appel à manifestation d’intérêt pour la passation conjointe de marchés d’outils et d’infrastructures, avec le centre de compétences européen en matière de cybersécurité (ECCC), dotés d’un financement total de l’UE de 110 000 000 EUR au titre du programme pour une Europe numérique (DIGITAL), publiés en novembre 2022. [↑](#footnote-ref-26)
26. Voir le rapport 2022 de l’ENISA sur le paysage des menaces. [↑](#footnote-ref-27)
27. COM(2022) 454. [↑](#footnote-ref-28)
28. Entre-temps, la Commission a adopté, en octobre 2021, un règlement délégué au titre de la directive relative aux équipements radioélectriques, qui impose aux fabricants de dispositifs sans fil l’obligation d’améliorer leur niveau de cybersécurité, de respect de la vie privée et de protection contre la fraude. [↑](#footnote-ref-29)
29. Conformément aux conclusions du Conseil du 17 octobre 2022 sur la sécurité des chaînes d’approvisionnement des TIC. [↑](#footnote-ref-30)
30. Le règlement (UE) 2019/881, qui introduit un cadre de certification de cybersécurité à l’échelle de l’UE pour les produits, services et processus TIC. [↑](#footnote-ref-31)
31. Les États membres, avec le soutien de la Commission et de l’ENISA, ont publié au début de cette année un rapport sur la cybersécurité du RAN ouvert, qui, lorsqu’il sera plus mature, offrira une méthode alternative de déploiement de la partie accès radio des réseaux 5G fondée sur des interfaces ouvertes. [↑](#footnote-ref-32)
32. Le conseil de direction de l’ECCC est en place et a tenu sa 4e réunion le 20 octobre 2022. [↑](#footnote-ref-33)
33. COM(2022) 122. [↑](#footnote-ref-34)
34. Le CERT-UE a également beaucoup investi dans la poursuite de l’amélioration des services qu’il propose déjà aux institutions, organes et organismes de l’UE et dans l’ajout de nouveaux services, afin de mieux prévenir et détecter les cyberattaques et de mieux y réagir. [↑](#footnote-ref-35)
35. COM(2022) 119. [↑](#footnote-ref-36)
36. SWD(2022) 21. [↑](#footnote-ref-37)
37. Hybrid threats: a comprehensive resilience ecosystem, (Menaces hybrides: résilience globale des écosystèmes), JRC 130097. [↑](#footnote-ref-38)
38. Des travaux sont en cours dans le cadre des tâches relevant de la boussole stratégique afin de mettre en place un espace de données FIMI et fournir aux missions et opérations PSDC des capacités et des ressources pour déployer les instruments pertinents de cette boîte à outils. Le SEAE continue de fournir aux États membres de l’UE une appréciation de la situation en source ouverte par l’intermédiaire du système d’alerte rapide de l’UE, sensibilise le public, en particulier au moyen de la campagne EUvsDisinfo, et a encore renforcé sa coopération avec des parties prenantes telles que l’OTAN et le mécanisme de réaction rapide du G7. [↑](#footnote-ref-39)
39. JOIN(2022) 49. [↑](#footnote-ref-40)
40. COM(2020) 795. [↑](#footnote-ref-41)
41. Afghanistan: plan d’action pour la lutte contre le terrorisme, 29 septembre 2021. [↑](#footnote-ref-42)
42. COM(2021) 701. Les États membres étaient tenus de transposer cette directive dans leur droit interne au plus tard le 8 septembre 2018. [↑](#footnote-ref-43)
43. COM(2015) 750. [↑](#footnote-ref-44)
44. SWD(2022) 398. [↑](#footnote-ref-45)
45. Guideline — Building Perimeter Protection, EUR 30346 EN. [↑](#footnote-ref-46)
46. http://counterterrorism.jrc.ec.europa.eu [↑](#footnote-ref-47)
47. Voir en particulier: École d’automne numérique de l’UE, JRC127168 et base de données sur le terrorisme et l’extrémisme — Guide de l’utilisateur JRC130461. javascript:viewRequest('130461','registered') [↑](#footnote-ref-48)
48. Ce document recommande aux États membres de se conformer aux exigences de performance de l’UE lors de l’acquisition d’équipements d’imagerie radioscopique utilisés dans les espaces publics [C(2022) 4179]. [↑](#footnote-ref-49)
49. COM(2022) 652. [↑](#footnote-ref-50)
50. <https://ec.europa.eu/commission/presscorner/detail/fr/IP_16_1937> [↑](#footnote-ref-51)
51. Règlement (UE) 2021/784 du Parlement européen et du Conseil du 29 avril 2021 relatif à la lutte contre la diffusion des contenus à caractère terroriste en ligne, JO L 172 du 17.5.2021, p. 79. [↑](#footnote-ref-52)
52. Parmi les autres réalisations figurent: une mise à jour du protocole de crise de l’UE, des manuels contenant des lignes directrices sur l’utilisation malveillante de contenus ambigus et de jeux vidéo conduisant à la radicalisation, et une étude concernant les effets de l’amplification algorithmique sur le cheminement des utilisateurs d’internet vers la radicalisation. [↑](#footnote-ref-53)
53. Europol (2021), European Union serious and organised crime threat assessment, a corrupting influence: the infiltration and undermining of Europe’s economy and society by organised crime (Évaluation de la menace que représente la grande criminalité organisée dans l’Union européenne, Économie et société européennes sous influence: l’insidieux travail de sape de la criminalité organisée),, Office des publications de l’Union européenne, Luxembourg. [↑](#footnote-ref-54)
54. Évaluation de la menace que représente la criminalité organisée sur l’internet (iOCTA) 2021. [↑](#footnote-ref-55)
55. COM(2021) 170. [↑](#footnote-ref-56)
56. En juillet 2022, la Commission a alloué, par l’intermédiaire du Fonds pour la sécurité intérieure (FSI), 15 700 000 EUR aux États membres pour soutenir des projets et des activités à long terme dans le cadre de la plateforme pluridisciplinaire européenne contre les menaces criminelles (EMPACT), abordant les [dix priorités de l'UE en matière de criminalité](https://www.consilium.europa.eu/fr/press/press-releases/2021/05/26/fight-against-organised-crime-council-sets-out-10-priorities-for-the-next-4-years/) adoptées par le Conseil pour la période 2022-2025. [↑](#footnote-ref-57)
57. Rapport d’évaluation de la menace que représente la criminalité organisée sur l’internet (iOCTA). [↑](#footnote-ref-58)
58. Initiative internationale de lutte contre les rançongiciels de 2022, Washington DC, 1er novembre 2022. [↑](#footnote-ref-59)
59. La plateforme de décryptage d’Europol est hébergée sur le site d’Ispra du Centre commun de recherche de la CE. [↑](#footnote-ref-60)
60. COM(2020) 607. [↑](#footnote-ref-61)
61. COM(2021) 142. [↑](#footnote-ref-62)
62. COM(2022) 209. [↑](#footnote-ref-63)
63. COM(2020) 568. [↑](#footnote-ref-64)
64. #  Directive 2011/93/UE du Parlement européen et du Conseil du 13 décembre 2011 relative à la lutte contre les abus sexuels et l’exploitation sexuelle des enfants, ainsi que la pédopornographie (JO L335 du 17.12.2011).

 [↑](#footnote-ref-65)
65. Service de recherche du Parlement européen (EPRS), Lutte contre la violence fondée sur le genre: cyberviolence, évaluation de la valeur ajoutée européenne, 2021. [↑](#footnote-ref-66)
66. COM(2022) 105. [↑](#footnote-ref-67)
67. La proposition prévoit la criminalisation au niveau de l’UE du partage non consenti de matériels intimes, de la traque furtive en ligne, du cyberharcèlement et de l’incitation à la violence ou à la haine en ligne. Ces règles seraient complétées par un nouveau cadre de coopération entre les plateformes internet afin de mieux protéger la sécurité des femmes en ligne. [↑](#footnote-ref-68)
68. Évaluation de la menace que représente la grande criminalité organisée (SOCTA, 2021). [↑](#footnote-ref-69)
69. [«An Anti-Trafficking Plan to protect people fleeing the war in Ukraine (europa.eu)» [Un plan de lutte contre la traite des êtres humains pour protéger les personnes fuyant la guerre en Ukraine (europa.eu)]](https://home-affairs.ec.europa.eu/news/anti-trafficking-plan-protect-people-fleeing-war-ukraine-2022-05-11_en#:~:text=Five%20objectives%20of%20the%20Common%20Anti%2DTrafficking%20plan&amp;text=It%20sets%20forward%20five%20goals,to%20trafficking%20in%20human%20beings). [↑](#footnote-ref-70)
70. COM(2021) 171. [↑](#footnote-ref-71)
71. Le 4e rapport d’étape sur la traite des êtres humains, qui doit être adopté parallèlement à la présente proposition, prévoit des informations détaillées sur la mise en œuvre de la stratégie de l’UE de 2019 à 2022, ainsi que des données clés et des statistiques. [↑](#footnote-ref-72)
72. [«*20 countries spin a web to catch human traffickers during a hackathon*» [20 pays tendent un filet pour attraper des trafiquants d’êtres humains lors d’un hackathon] | Europol (europa.eu)](https://www.europol.europa.eu/media-press/newsroom/news/20-countries-spin-web-to-catch-human-traffickers-during-hackathon) [↑](#footnote-ref-73)
73. COM(2020) 609. [↑](#footnote-ref-74)
74. COM(2021) 591. [↑](#footnote-ref-75)
75. Rapport annuel d’Eurojust de 2021. [↑](#footnote-ref-76)
76. COM(2020) 606. [↑](#footnote-ref-77)
77. COM(2022) 18. [↑](#footnote-ref-78)
78. Europol, «Does crime still pay? Criminal Asset Recovery in the EU» [Le crime paie-t-il encore? Le recouvrement des avoirs d’origine criminelle dans l’UE] — Enquête statistique 2010-2014, 2016. [↑](#footnote-ref-79)
79. COM(2021) 421, COM(2021) 420, COM(2021) 423, COM(2021) 422. Un accord politique a été conclu en juin 2022 concernant le règlement sur les transferts de fonds et une orientation générale partielle a également été définie en juin 2022 concernant le règlement instituant l’Autorité de lutte contre le blanchiment de capitaux et le financement du terrorisme (à l’exception des dispositions relatives aux ressources et au siège). [↑](#footnote-ref-80)
80. COM(2022) 245 final. [↑](#footnote-ref-81)
81. Premier rapport annuel du Parquet européen, 2022. [↑](#footnote-ref-82)
82. COM(2020) 760. [↑](#footnote-ref-83)
83. La dernière édition du rapport a été adoptée le 13 juillet 2022 [COM (2022) 500]. [↑](#footnote-ref-84)
84. COM(2020) 608 final. [↑](#footnote-ref-85)
85. COM(2022) 480. [↑](#footnote-ref-86)
86. Voir, par exemple, les résolutions 2199 (2015), 2253 (2015), 2322 (2016), 2347 (2017), 2462 (2019) et 2617 (2021) du Conseil de sécurité de l’Organisation des Nations unies; Déclaration de Rome des ministres de la culture du G20 du 30 juillet 2021. [↑](#footnote-ref-87)
87. COM(2022) 800. [↑](#footnote-ref-88)
88. COM(2021) 851. [↑](#footnote-ref-89)
89. COM(2021) 709. [↑](#footnote-ref-90)
90. COM(2021) 706. [↑](#footnote-ref-91)
91. COM(2022) 581. [↑](#footnote-ref-92)
92. COM(2021) 277. [↑](#footnote-ref-93)
93. COM(2022) 301. [↑](#footnote-ref-94)
94. COM(2021) 891. [↑](#footnote-ref-95)
95. COM(2022) 636. [↑](#footnote-ref-96)
96. À compter du 1er janvier 2023, les contrôles de personnes aux frontières terrestres et maritimes intérieures entre la Croatie et les autres pays de l’espace Schengen seront levés. Les contrôles aux frontières aériennes intérieures seront levés à partir du 26 mars 2023. [↑](#footnote-ref-97)
97. COM(2021) 782, COM (2021) 780. [↑](#footnote-ref-98)
98. C(2021) 784. [↑](#footnote-ref-99)
99. COM (2021) 756, COM (2021 757, COM (2021) 759. [↑](#footnote-ref-100)
100. COM(2018) 225, COM (2018) 226. [↑](#footnote-ref-101)
101. Le système de contrôle des importations 2 (ICS2) sera déployé en trois phases (mars 2021, mars 2022 et mars 2023). Chaque phase concerne différents opérateurs économiques (OE) et modèles de transport. [↑](#footnote-ref-102)
102. Règlement (UE) 2021/1077 du 24 juin 2021 portant création, dans le cadre du Fonds pour la gestion intégrée des frontières, de l’instrument de soutien financier relatif aux équipements de contrôle douanier. [↑](#footnote-ref-103)
103. COM(2022) 729 et 731. [↑](#footnote-ref-104)
104. Fondée sur le règlement (UE) 2019/1157 du Parlement européen et du Conseil du 20 juin 2019 relatif au renforcement de la sécurité des cartes d'identité des citoyens de l'Union et des documents de séjour délivrés aux citoyens de l'Union et aux membres de leur famille exerçant leur droit à la libre circulation (JO L 188 du 12.7.2019, p. 67). [↑](#footnote-ref-105)
105. EUR-lex 52022PC0658. [↑](#footnote-ref-106)
106. COM(2021) 206. [↑](#footnote-ref-107)
107. COM(2021) 205. [↑](#footnote-ref-108)
108. Horizon Europe investit également des fonds considérables dans des technologies innovantes au profit des services répressifs dans le cadre de la lutte contre la radicalisation, ainsi que dans des projets dans le domaine de la détection de stupéfiants et d’explosifs, du trafic illicite des biens culturels, du trafic de migrants, de la sécurité dans les espaces publics et de l’usurpation d'identité. [↑](#footnote-ref-109)
109. En 2022, des dialogues sur la lutte contre le terrorisme ont eu lieu avec les Nations unies, Israël et l’Inde. Des dialogues avec la Turquie, le Qatar et les Émirats arabes unis sont prévus. En 2023, les principaux dialogues attendus concernent le Maroc, la Tunisie, l’Égypte, le Kenya, les États-Unis et l’Arabie saoudite et peut-être également l’Algérie. [↑](#footnote-ref-110)
110. Décision (UE) 2022/2271 du Conseil – Albanie; Décision (UE) 2022/2272 du Conseil – Bosnie-Herzégovine; Décision (UE) 2022/2273 du Conseil – Monténégro; Décision (UE) 2022/2274 du Conseil – Serbie. [↑](#footnote-ref-111)
111. Voir le sixième réexamen conjoint de la mise en œuvre de l’accord TFTP, COM(2022) 585. [↑](#footnote-ref-112)
112. Règlement UE/2019/452. [↑](#footnote-ref-113)
113. Règlement UE/2021/821 refonte. [↑](#footnote-ref-114)
114. L’accord a été décrit favorablement par le Contrôleur européen de la protection des données (CEPD) comme un modèle pour les futurs accords relatifs à l’échange de données à caractère personnel à des fins répressives. [↑](#footnote-ref-115)
115. Voir le septième rapport d’étape sur les suites données aux propositions communes entérinées le 6 décembre 2016 et le 5 décembre 2017 par le Conseil de l’Union européenne et le Conseil de l’Atlantique Nord, 20 juin 2022. [↑](#footnote-ref-116)