COMMISSION
EUROPÉENNE

Bruxelles, le 26.2.2026
COM(2026) 101 final

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

ProtectEU: un programme pour prévenir et combattre le terrorisme

1. Introduction

Le présent programme, annoncé dans la communication «**ProtectEU: une stratégie européenne de sécurité intérieure**[1]», marque le début d'un nouvel effort visant à lutter contre le terrorisme et l'extrémisme violent qui ne connaissent pas de frontières, ni physiques ni numériques. Le terrorisme[2] et l'extrémisme violent[3] continuent de représenter un défi persistant pour l'UE et ses États membres. Les liens grandissants entre le terrorisme et d'autres domaines liés à la criminalité, une plus grande fluidité des réseaux et des acteurs moins motivés idéologiquement, ainsi qu'une frontière plus floue entre les opérations en ligne et les opérations physiques font qu'il est particulièrement difficile de définir et de recenser les infractions terroristes. Dans un tel contexte de menace complexe, **la meilleure approche réside dans une action concertée,** et si les États membres restent les seuls responsables de leur sécurité nationale[4], l'UE doit travailler main dans la main avec eux.

S'il est un fait que l'UE a subi moins d'attentats terroristes coordonnés de grande ampleur, **la menace n'a pas pour autant disparu, elle a évolué**. Entre 2019 et 2023, le nombre d'incidents terroristes a plus que doublé (passant de 57 à 120), avant de retomber à 58 en 2024[5]. Les récentes attaques ont essentiellement été le fait d'acteurs isolés et de cellules de petite taille. Le **niveau global de la menace reste élevé** et est déterminé par la **multiplication des facteurs de menace**[6]. Si le **terrorisme djihadiste** demeure la menace terroriste la plus importante et la plus mortelle[7], les terroristes et les extrémistes violents obéissent à un éventail toujours plus grand de motivations, pas toujours reliées à une idéologie spécifique, dont le rejet des valeurs démocratiques européennes, l'antisémitisme ou la haine à l'égard des musulmans[8].

L'UE a d'ores et déjà pris des mesures pour lutter contre le terrorisme et l'extrémisme violent, faisant du **programme de lutte antiterroriste pour l'UE de 2020**[9] sa feuille de route pour l'avènement d'une UE plus sûre. Dans la décennie qui a suivi la vague d'attentats odieux perpétrés à travers l'Europe, notamment à Paris et à Bruxelles, l'UE a mis en place un **cadre**

---

[1] Communication de la Commission au Parlement européen, au Conseil européen, au Conseil, au Comité économique et social européen et au Comité des régions intitulée «ProtectEU: une stratégie européenne de sécurité intérieure [COM(2025) 148 final]». Le présent programme s'inscrit en complément des réalisations obtenues dans le cadre de la stratégie européenne pour une union de la préparation [JOIN(2025) 130 final], de la communication intitulée «Préserver la paix — Feuille de route pour la préparation de la défense à l'horizon 2030» [JOIN(2025) 27 final], et de la communication intitulée «Bouclier européen de la démocratie: renforcer la position de démocraties fortes et résilientes» JOIN(2025) 791 final».

[2] Les infractions terroristes sont définies à l'article 3 de la directive (UE) 2017/541 relative à la lutte contre le terrorisme comme étant «des actes criminels qui, par leur nature ou leur contexte, peuvent porter gravement atteinte à un pays ou à une organisation internationale lorsqu'ils sont commis intentionnellement et dans un but terroriste».

[3] Il n'existe aucune définition juridique de l'extrémisme violent au niveau de l'UE. Les actes relevant de l'extrémisme violent n'atteignent pas le seuil établi par la définition des infractions terroristes; ils n'en constituent pas moins une menace grave pour la sécurité. Une collaboration fondée sur des projets portant sur l'extrémisme violent de droite a donné lieu à une définition opérationnelle.

[4] Article 4, paragraphe 2, du traité sur l'Union européenne.

[5] Rapport sur la situation et les tendances du terrorisme en Europe (Rapport TE-SAT), Europol, 2025.

[6] Selon un récent rapport Europol TE-SAT et les estimations du Centre de situation et du renseignement de l'UE (INTCEN) (confidentiel).

[7] Rapport Europol TE-SAT 2025.

[8] Parmi les autres motivations, on peut citer la haine contre les LGBTQ+, la misogynie, le racisme, les idéologies anti-système, le nihilisme et l'«accélérationnisme», une panoplie d'idéologies qui postulent que la situation dans laquelle se trouve actuellement la société est irrémédiable et nécessite la destruction du «système», ainsi qu'un «nouveau départ».

[9] Communication de la Commission au Parlement européen, au Conseil européen, au Conseil, au Comité économique et social européen et au Comité des régions intitulée «Programme de lutte antiterroriste pour l'UE: anticiper, prévenir, protéger et réagir» [COM(2020) 795 final]..

juridique complet visant à ériger les infractions terroristes en infractions pénales, à lutter contre les contenus terroristes en ligne et à restreindre l'accès au financement du terrorisme, aux armes à feu et aux explosifs. Elle a renforcé sa capacité à **détecter et arrêter les déplacements de terroristes** à ses frontières extérieures à l'aide de systèmes de sécurité et d'une gestion des frontières modernisés, d'un meilleur partage de l'information et d'une coopération plus étroite, tant en son sein qu'avec des pays tiers.

Les agences de l'UE ont procuré aux États membres un soutien opérationnel et des outils, **renforçant ce faisant l'efficacité des enquêtes et des poursuites relatives au terrorisme**, avec plus de 2 000 arrestations et plus de 1 800 condamnations pour infractions terroristes[10] enregistrées ces cinq dernières années. Les structures de soutien au niveau de l'UE, telles que le **pôle de connaissances de l'UE sur la prévention de la radicalisation** et le **programme de conseil en matière de sûreté de l'UE**, ont permis aux États membres de bénéficier de pratiques et d'expertises communes, **ce qui a eu pour effet d'accroître la résilience** dans toute l'UE. Fort de ces résultats, le présent programme, fruit d'une concertation étroite avec les États membres et d'autres parties prenantes, recense les lacunes qui subsistent et définit des mesures concrètes destinées à les combler.

Les évolutions géopolitiques et les conflits extérieurs génèrent des risques accrus et ont une incidence sur la sécurité de l'UE. Le 7 octobre 2023, les attaques du Hamas et le conflit qui s'est ensuivi à Gaza ont alimenté une montée de la haine et une incitation à la violence de part et d'autre du spectre idéologique. Les membres de la mouvance djihadiste ont instrumentalisé ces événements par de la mésinformation en ligne et des appels explicites à la violence. Des récits similaires ont également été exploités par des acteurs de l'extrême gauche comme de l'extrême droite. Tout cela contribue à un risque accru d'attentats. L'État islamique et les groupuscules qui lui sont inféodés constituent toujours l'une des principales menaces extérieures pour l'UE, du fait de leur capacité à inspirer des attentats. La situation instable en Syrie suscite des inquiétudes sur le plan de la sécurité en raison de la possible résurgence de l'organisation de l'État islamique et de l'avenir incertain des combattants terroristes étrangers se trouvant dans des centres de détention et des camps dans le nord-est de la Syrie. Les organisations terroristes ciblent de plus en plus le personnel et les opérations humanitaires par des actes de violence, d'intimidation et d'obstruction.

En outre, dans le contexte de sa **guerre d'agression** contre l'Ukraine, **la Russie** mène un éventail toujours plus large d'actions de sabotage et d'actions hybrides contre l'UE. Ces actions violent la souveraineté territoriale des États membres, sapent l'intégrité des institutions démocratiques et menacent directement la sécurité et la sûreté de la population civile. Elles sont assorties d'activités d'influence coordonnées menées par des acteurs liés à la Russie, répandant en Europe des récits d'extrémisme violent et d'autres discours clivants. Ce conflit a également mis en lumière de potentiels risques en matière de sécurité liés au retour de volontaires étrangers et d'ex-soldats russes ayant une expérience du combat.

L'UE a également fait face à des **menaces complexes commanditées par des groupes terroristes, ainsi que par des acteurs étrangers étatiques et non étatiques**. Des acteurs hostiles ont recouru à des modes opératoires terroristes, en plaçant notamment des dispositifs incendiaires dans du fret aérien, en procédant à des cyberattaques, en sabotant des infrastructures critiques et en se servant de terroristes et d'extrémistes violents comme supplétifs. Des alliances de circonstance persistent entre le terrorisme, la criminalité organisée et la cybercriminalité, qui utilisent le crime sous forme de service, partagent le même vivier de

[10] Rapports Europol TE-SAT 2021-2025.

recrutement, fréquentent les mêmes plateformes criminelles et font appel aux mêmes réseaux bancaires clandestins[11]. L'augmentation des connexions entre le terrorisme, la cybercriminalité, les activités d'ingérence hostile menées depuis l'étranger et la criminalité organisée rend difficiles l'imputation de la responsabilité pénale et la coordination des réponses au niveau national et au niveau de l'UE.

Le nombre de mineurs impliqués dans des activités terroristes et d'extrémisme violent a fortement augmenté à travers l'Europe. En 2024, près d'un tiers des personnes soupçonnées de terrorisme dans l'UE avaient moins de 20 ans, les plus jeunes n'étant âgés que de 12 ans. La plupart de ces mineurs ont noué des liens avec le terrorisme djihadiste, même si l'extrémisme violent de droite a gagné en popularité, en particulier dans le cadre des réseaux accélérationnistes, des «Active Clubs»[12] et des réseaux extrémistes en ligne[13], qui diffusent des contenus violents et forcent des mineurs vulnérables à commettre des actes d'automutilation et de violence. L'époque actuelle est marquée par l'hétérogénéité des idéologies, la fascination pour la violence constituant la principale motivation de nombreux attentats d'acteurs isolés.

Les terroristes et les extrémistes violents **exploitent de plus en plus l'environnement en ligne et les nouvelles technologies, les médias sociaux et les plateformes de jeux** pour partager des contenus préjudiciables, diffuser la désinformation, radicaliser, lever des fonds et recruter. L'amplification algorithmique de contenus extrémistes favorise la radicalisation. Les acteurs terroristes coordonnent leurs plans sur des plateformes de communication chiffrées de bout en bout et financent leurs réseaux et leurs attaques au moyen de **cryptomonnaies**, d'actifs numériques non fongibles (NFT) et d'«hawala numérique»[14]. L'IA générative est utilisée à mauvais escient pour élaborer des modes d'emploi pour attentats. La technologie de l'impression 3D (par exemple pour la fabrication d'armes à feu) et l'utilisation accrue de systèmes d'aéronefs sans équipage à bord (UAS/drones) exacerbent davantage encore cette menace.

S'appuyant sur de vastes consultations menées auprès des parties prenantes et sur les récentes conclusions du Conseil[15] relatives au terrorisme, le programme combine d'importantes activités en cours avec de nouvelles initiatives afin de suivre l'évolution rapide du paysage des menaces. Il définit des actions spécifiques visant à **anticiper les menaces, à prévenir la radicalisation, à protéger les personnes tant en ligne que hors ligne, à garantir des réponses rapides et coordonnées aux attentats,** et à **renforcer la lutte mondiale contre le terrorisme,** dans le respect du droit international, notamment des droits de l'homme et du droit humanitaire.

---

[11] Europol (2025), Évaluation de la menace que représente la grande criminalité organisée dans l'Union européenne 2025 (EU-SOCTA). Beneath the Surface: Terrorist and Violent Extremist Use of the Dark Web and Cybercrime-As-A-Service for Cyber-Attacks (Sous la surface : utilisation du Dark Web et du cybercrime sous forme de service par les terroristes et extrémistes violents pour des cyberattaques) - Bureau de lutte contre le terrorisme

[12] Les «Active Clubs» sont des réseaux extrémistes peu structurés et axés sur des activités de mise en forme ou sur les arts martiaux, qui servent de plaques tournantes en matière d'idéologie, de cohésion et de recrutement dans des cercles d'extrémisme violent de droite.

[13] Connus sous l'appellation réseaux «764» ou «Com».

[14] L'hawala numérique fournit une méthode de transferts pseudo-anonymes transfrontières faisant appel à diverses méthodes numériques (technologie des chaînes de blocs, argent mobile, etc.) ressemblant au réseau informel physique de l'hawala, tout en introduisant des niveaux de sécurité supplémentaires. Rapport 2025 sur la situation et les tendances du terrorisme en Europe (TE-SAT 2025).

[15] Conclusions du Conseil du 9 juin 2022 intitulées «Protéger les Européens du terrorisme: actions accomplies et prochaines étapes».
Conclusions du Conseil du 12 décembre 2024 sur les priorités futures pour le renforcement des efforts conjoints de l'Union européenne et de ses États membres en matière de lutte contre le terrorisme.

La réponse la plus efficace au terrorisme est celle qui démontre l'attachement à nos valeurs attaquées; toutes les actions sont dès lors ancrées dans **le respect des droits fondamentaux**. Afin de compléter et de finaliser cette réponse, les États membres sont invités à adopter et à mettre régulièrement à jour leurs stratégies nationales, conformément au cadre stratégique énoncé par le présent programme.

2. Piliers de la lutte contre le terrorisme et l'extrémisme violent

2.1 Anticiper les menaces

La sécurité suppose d'abord **une anticipation et une prospective efficaces**. L'UE s'est dotée de solides capacités d'appréciation de la situation en matière de lutte contre le terrorisme. La **capacité unique d'analyse du renseignement (SIAC) dont dispose l'UE**, qui est le point d'entrée unique pour le renseignement dans les États membres, fournit des évaluations rapides de la menace, tandis qu'**Europol** produit des rapports réguliers sur les tendances fondés sur les informations des services répressifs.

La haute représentante pour les affaires étrangères et la politique de sécurité (ci-après la «haute représentante») donnera la priorité au **renforcement de la SIAC** sur le plan des ressources et des capacités. Outre le **déploiement de canaux de communication sécurisés** et la finalisation des négociations sur la **proposition de règlement sur la sécurité de l'information** dans les institutions, organes et organismes de l'Union, la Commission et la haute représentante s'emploieront à **renforcer encore la sensibilisation du personnel de l'UE** afin de promouvoir une **culture du «besoin de partager»** tout en préservant le principe du «besoin d'en connaître» pour les informations classifiées.

Le caractère dynamique et imprévisible des menaces émergentes nécessite un renforcement des capacités répressives d'anticipation. Ainsi qu'énoncé dans la stratégie de sécurité intérieure ProtectEU, la Commission proposera de renforcer **l'aide à l'analyse d'Europol, y compris les capacités de renseignement de source ouverte (RSO)**. Dans la mesure du possible, les rapports d'Europol sur les tendances, les briefings contextuels et les analyses thématiques pourraient être communiqués sous des formes non classifiées, de manière à sensibiliser la population aux tendances émergentes à l'appui des efforts en matière de détection rapide et de prévention. De surcroît, les analyses que la Commission est en train de préparer concernant les menaces, comme annoncé dans la stratégie de sécurité intérieure ProtectEU, contribueront aussi à recenser les menaces émergentes et les réponses stratégiques visant à lutter contre le terrorisme et l'extrémisme violent.

La prospective est tout aussi essentielle pour permettre d'inventorier les risques et les possibilités émanant des nouvelles technologies[16]. Les travaux du **Centre commun de recherche** continueront de guider la recherche en matière de sécurité. Afin d'exploiter le potentiel des nouvelles technologies au profit des services répressifs et de se préparer à combattre leur utilisation frauduleuse par les terroristes et les extrémistes violents, la Commission **renforcera la recherche en matière de sécurité dans le cadre d'Horizon Europe et du financement de la sécurité intérieure** au moyen d'appels spécifiques en 2026 et au-delà. Parmi les priorités de la recherche figureront les capacités de détection précoce et l'innovation dans les technologies, telles que l'IA, la lutte contre l'utilisation des plateformes en ligne par les extrémistes, les nouvelles méthodes de financement du terrorisme (par exemple,

[16] Voir la publication du Centre commun de recherche de la Commission européenne intitulée «Emerging risks and opportunities for EU internal security stemming from new technologies (2025)» EUR 40239 JRC139674.

les crypto-actifs), et la protection des citoyens et des espaces publics face aux menaces posées par le recours aux explosifs, aux drones et aux armes imprimées en 3D, ainsi que par les attaques au véhicule-bélier et à l'arme blanche. Pour garantir l'adoption des résultats de la recherche, la Commission **soutiendra également l'expérimentation et le déploiement de solutions financées par l'UE visant à doter les services répressifs d'outils et de méthodologies de pointe** permettant de prévenir et de détecter efficacement le terrorisme et l'extrémisme violent et d'y faire face.

ACTIONS CLÉS

La Commission:

- soutiendra le déploiement de canaux de communication sécurisés entre les institutions, organes et organismes de l'UE;
- renforcera la recherche en matière de sécurité dans le cadre d'Horizon Europe et le financement de la sécurité intérieure;
- soutiendra l'expérimentation et le déploiement de solutions financées par l'UE visant à doter les services répressifs d'outils de pointe.

La haute représentante:

- renforcera la SIAC de toute urgence, conformément au document conjoint de la haute représentante et des États membres.

Europol:

- renforcera l'aide à l'analyse et les capacités de renseignement de source ouverte (RSO).

Le Parlement européen et le Conseil sont invités à:

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

2.2 Prévenir la radicalisation

La prévention de la radicalisation consiste à s'attaquer à ses vecteurs avant qu'ils ne soient profondément ancrés. Cela passe par une **approche englobant l'ensemble de la société**, associant les acteurs des milieux éducatifs, sociaux et culturels, des services pour la jeunesse, des services répressifs, pénitentiaires et de probation, des communautés locales, des organisations de la société civile et des environnements en ligne. La création, en juin 2024, du **pôle de connaissances de l'UE sur la prévention de la radicalisation** (ci-après le «pôle de connaissances»)[17] et la dotation de 60 millions d'EUR sur quatre ans ont traduit un changement majeur dans la politique de l'UE en matière de prévention.

Le pôle de connaissances permet à plus de 6 000 décideurs politiques, chercheurs et praticiens de toute l'Europe de se connecter entre eux et élabore **des orientations pour décideurs politiques et praticiens, des outils pratiques, des formations et des services d'assistance sur mesure.** Il opère dans le cadre des orientations stratégiques[18] fixées par les États membres, qui seront actualisées en 2027. Le présent programme définit des missions concrètes pour le pôle de connaissances et veille à ce qu'il remplisse intégralement son mandat en traduisant ces missions en une assistance opérationnelle aux États membres, en aidant ces derniers à anticiper les risques émergents et en inventoriant les ripostes nationales à la radicalisation.

2.2.1 Élaborer une boîte à outils en matière de prévention à destination des mineurs

[17] Pôle de connaissances de l'UE sur la prévention de la radicalisation.

[18] Orientations stratégiques en vue d'une approche coordonnée de l'UE en matière de prévention de la radicalisation.

Les conséquences de la participation de mineurs à la radicalisation et au terrorisme sont d'une ampleur considérable et touchent non seulement les mineurs concernés, mais également des communautés et des sociétés dans leur ensemble. Pour remédier au taux inquiétant de mineurs en voie de radicalisation en Europe, la Commission s'appuiera sur les activités du pôle de connaissances et fournira des orientations stratégiques relatives à la **prévention de la radicalisation des mineurs**. Elle mettra l'accent sur la détection précoce, sur le renforcement des facteurs de protection, sur la résilience grâce à l'éducation[19] et à l'intégration sociale, notamment des mineurs vulnérables, sur le soutien aux familles et aux communautés, sur une participation sûre en ligne et sur la coopération intersectorielle, en s'appuyant aussi sur l'action des réseaux existants des centres pour un internet plus sûr dans les États membres et les pays candidats.

La Commission prend acte du fait que les **problèmes liés à la santé mentale** peuvent rendre les mineurs plus vulnérables aux discours extrémistes, ainsi qu'à la violence et au recrutement inhérents. Elle fera dès lors la promotion d'une coopération plus étroite entre les acteurs de la prévention et les services de la santé mentale, dans le cadre d'une approche intégrée de la protection de l'enfance[20]. Dans cette optique, les États membres sont encouragés à intégrer une expertise et un soutien psychosociaux dans leurs cadres de prévention.

2.2.2 Construire des sociétés résilientes

Afin de renforcer la résilience des communautés, la Commission lance actuellement le **programme de participation et d'autonomisation des communautés (CEEP)**, qui prévoit une enveloppe de 5 millions d'EUR pour doter la société civile et les praticiens des compétences numériques nécessaires à des interventions en ligne efficaces et pour faire entendre la voix des jeunes engagés dans la prévention.

Protéger toutes les communautés religieuses contre la haine, la discrimination et la violence demeure un engagement fondamental de l'UE. La Commission accélérera la mise en œuvre de la **stratégie européenne de lutte contre l'antisémitisme et de soutien à la vie juive[21]** et mettra en place un réseau pour lutter contre les discours de haine antisémites en ligne. Conformément à cette stratégie, la SIAC continuera d'inclure, dans ses évaluations régulières des menaces, des analyses des menaces spécifiques qui pèsent sur les juifs, les communautés juives et les lieux de culte juifs. Les États membres sont encouragés à suivre les **recommandations de la collaboration sur l'antisémitisme en matière de prévention et de lutte contre l'extrémisme violent, fondée sur des projets**[22].

Afin de renforcer la réponse pénale européenne à toutes les formes de haine, y compris la montée de la haine antimusulmane, la Commission examine actuellement une initiative législative visant à harmoniser la **définition des infractions à caractère haineux commises**

---

[19] Pour des mesures supplémentaires visant à favoriser la résilience grâce à l'éducation, notamment en ce qui concerne les médias, l'habileté et la citoyenneté numériques, voir la: Communication conjointe au Parlement européen, au Conseil, au Comité économique et social européen et au Comité des régions intitulée «Bouclier européen de la démocratie: renforcer la position de démocraties fortes et résilientes,»[JOIN (2025) 791 final].

[20] Conformément à la recommandation (UE) 2024/1238 de la Commission du 23 avril 2024 relative au développement et au renforcement de systèmes intégrés de protection de l'enfance dans l'intérêt supérieur de l'enfant,.

[21] Stratégie européenne de lutte contre l'antisémitisme et de soutien à la vie juive (2021-2030) [COM(2021) 615 final].

[22] Commission européenne - Série de recommandations de la PBC sur l'antisémitisme en matière de prévention de l'extrémisme violent et de lutte contre ce phénomène (P/CVE), mars 2025. À la suite de ces recommandations, le pôle de connaissances de l'UE a élaboré un manuel sur les principaux symboles, récits et mécanismes de signalement qui sera publié.

en ligne[23]. Elle coopérera avec Europol en vue d'améliorer **la détection assistée par l'IA des contenus à caractère extrémiste** et les indicateurs de menace communs, et d'accélérer la coopération entre les plateformes, les services répressifs et les chercheurs pour détecter la propagande générée par l'IA et les campagnes de radicalisation coordonnées.

2.2.3 Lutter contre la radicalisation dans les prisons, traiter le problème des détenus radicalisés libérés de prison et gérer le retour des combattants terroristes étrangers et des membres de leur famille

Compte tenu de la possibilité que des détenus ayant purgé leur peine, mais susceptibles de s'être **radicalisés** en prison[24], soient libérés, il est nécessaire de renforcer la coordination et de prévoir des mesures de réinsertion adaptées. Les États membres devraient **renforcer le partage d'informations** entre les autorités pénitentiaires, les autorités de probation et les autorités répressives et mettre en œuvre des programmes de désengagement et de réinsertion fondés sur des données probantes.

Le pôle de connaissances soutiendra ces efforts en **mettant au point des outils permettant d'évaluer et de gérer les risques au cours de la phase de préparation à la sortie de détention**, tandis que la Commission fournira des **orientations** pour soutenir les approches nationales à l'égard des détenus radicalisés libérés de prison.

Afin de remédier aux problèmes complexes liés au **retour des combattants terroristes étrangers et des membres de leur famille**, les États membres sont encouragés à continuer d'empêcher les départs vers les zones de conflit et à poursuivre effectivement les combattants terroristes étrangers de retour. Le pôle de connaissances soutiendra les États membres au moyen d'outils permettant d'évaluer les risques et de gérer le retour des combattants étrangers dans de bonnes conditions de sécurité, ainsi que de formations sur la réadaptation et la réinsertion, en mettant l'accent sur la protection des enfants dans leur intérêt supérieur.

2.2.4 Soutenir les victimes du terrorisme

Les victimes du terrorisme gardent des séquelles durables et ont besoin d'un soutien spécialisé. Les colégislateurs sont récemment parvenus à un accord sur la proposition de **révision de la directive sur les droits des victimes**[25], qui renforcera la protection des droits des victimes du terrorisme et sera complétée par une **nouvelle stratégie de l'Union européenne en matière de droits des victimes**. La Commission renforcera également la visibilité de la **Journée européenne de commémoration des victimes du terrorisme et soutiendra les associations de victimes** en promouvant leur rôle actif dans les programmes de prévention.

ACTIONS CLÉS

En coopération avec le pôle de connaissances de l'UE, la Commission:

- mettra au point une boîte à outils de prévention à l'intention des mineurs, y compris un guide destiné aux parents visant à protéger les jeunes contre la radicalisation dans

[23] Au niveau de l'UE, la décision-cadre du Conseil sur la lutte contre certaines formes et manifestations de racisme et de xénophobie (décision-cadre 2008/913/JAI du Conseil) et la directive sur la lutte contre la violence à l'égard des femmes et la violence domestique [directive (UE) 2024/138], qui forment le cadre juridique actuel, ne couvrent respectivement que les infractions à caractère haineux fondées sur le racisme et la xénophobie et l'incitation à la violence ou à la haine fondée sur le genre en ligne.

[24] Selon les évaluations d'Europol (données non publiques).

[25] Proposition de directive du Parlement européen et du Conseil modifiant la directive 2012/29/UE établissant des normes minimales concernant les droits, le soutien et la protection des victimes de la criminalité et remplaçant la décision-cadre 2001/220/JAI du Conseil [COM(2023) 424 final].

l'environnement en ligne et des modèles pratiques pour les lignes directes et les centres d'appels permettant de signaler les signes de radicalisation et d'agir en conséquence;
- élaborera des procédures normalisées et une méthode commune d'évaluation des risques liés aux détenus radicalisés au cours de la phase de préparation à la sortie de détention.

La Commission:
- lancera, en même temps que le présent programme, le programme de participation et d'autonomisation des communautés;
- élaborera des recommandations relatives à la prévention de la radicalisation des mineurs et aux détenus libérés de prison;
- présentera une nouvelle stratégie de l'UE sur les droits des victimes;
- coopérera avec Europol afin d'améliorer la détection assistée par l'IA des contenus à caractère extrémiste et des campagnes de radicalisation.

Les États membres sont encouragés à:
- intégrer la prévention de la radicalisation dans l'éducation et le sport, en s'appuyant sur les recommandations, les outils et les bonnes pratiques établis au niveau de l'UE;
- renforcer les campagnes de communication stratégique et de sensibilisation, en s'appuyant sur le soutien apporté par le pôle de connaissances de l'UE;
- renforcer le partage d'informations et à mettre en œuvre des programmes de désengagement et de réinsertion à l'intention des détenus libérés de prison;
- empêcher les départs vers les zones de conflit et à poursuivre les combattants terroristes étrangers de retour.

2.3 Protéger les personnes en ligne

Ces dernières années, l'UE a mis en place l'un des cadres réglementaires les plus avancés au monde pour lutter contre les activités terroristes en ligne. Ce cadre est complété par la coopération volontaire des États membres, des plateformes en ligne et d'Europol.

Pourtant, la menace continue d'évoluer. Les réseaux extrémistes s'adaptent rapidement, exploitent les technologies émergentes et passent de plateformes ouvertes à l'exploitation de forums de discussion fermés et de services chiffrés, ce qui complique considérablement la détection et la prévention des projets terroristes, la cartographie des réseaux terroristes et de leurs soutiens, ainsi que les enquêtes et les poursuites concernant des activités terroristes. En outre, les contenus à caractère terroriste prolifèrent plus facilement, ce qui nécessite des outils de détection plus intelligents pour faire en sorte que les contenus à caractère terroriste identifiés ne réapparaissent pas sur une autre plateforme. La Commission renforcera le contrôle de l'application du règlement sur les services numériques (ci-après le «règlement DSA») et soutiendra la mise en œuvre effective du règlement sur les contenus à caractère terroriste en ligne (ci-après le «règlement TCO»), comblera les lacunes qui subsistent et garantira des réponses plus rapides et mieux coordonnées afin de préserver la sécurité et la résilience de l'espace en ligne face aux utilisations abusives, tout en veillant au respect des droits fondamentaux. Comme annoncé dans la stratégie de sécurité intérieure ProtectEU, la Commission présentera également un **plan d'action pour la protection des enfants contre la criminalité**, qui prévoira des mesures visant à lutter contre leur radicalisation et leur recrutement à des fins criminelles, tant en ligne que hors ligne.

2.3.1 Tirer pleinement parti des cadres réglementaires pour lutter contre les contenus à caractère terroriste et extrémiste en ligne

Le **règlement TCO** joue un rôle déterminant dans la lutte contre la diffusion de contenus à caractère terroriste, en permettant la suppression rapide de ces contenus. Son importance a été démontrée à la suite des attaques perpétrées par le Hamas en Israël le 7 octobre 2023, lorsque plusieurs centaines d'injonctions de suppression ont été émises à l'égard de contenus à caractère terroriste[26].

En décembre 2025, les autorités des États membres avaient déjà envoyé 2 032 injonctions de suppression et plus de 97 900 signalements en vue d'un retrait volontaire[27]. Afin de soutenir davantage la mise en œuvre, Europol mettra au point une **base de données européenne de partage des hachages** [soit une base de données des empreintes numériques («hachages»)] pour les contenus à caractère terroriste et extrémiste violent. Cela permettra aux États membres et aux fournisseurs de services d'hébergement de signaler, de mettre en correspondance et de supprimer de manière sécurisée des contenus sur l'ensemble des plateformes, y compris les contenus supprimés en application du règlement TCO.

La Commission achèvera l'évaluation du règlement TCO d'ici la fin de 2026. Sur la base de cette évaluation, la Commission étudiera la possibilité de renforcer encore le règlement TCO afin qu'il reste adapté à sa finalité et, dans la mesure du possible, le simplifiera, tout en préservant les garanties permettant de protéger effectivement les droits fondamentaux. Parallèlement, la Commission veillera à l'application rigoureuse des autres actes législatifs pertinents qui protègent l'espace numérique, tels que le **règlement DSA** et la **directive «Services de médias audiovisuels» (SMA)**.

En se renforçant mutuellement, le règlement TCO et le règlement DSA forment une architecture renforcée [28] pour lutter contre les activités terroristes et l'extrémisme violent en ligne. Alors que le règlement DSA établit un cadre horizontal d'obligations de diligence pour les intermédiaires en ligne, afin de lutter contre les contenus illicites en ligne et leur amplification algorithmique, et d'atténuer les risques systémiques associés à leurs services, le règlement TCO fixe des exigences sectorielles à l'égard des contenus à caractère terroriste et en ce qui concerne la rapidité des outils opérationnels de suppression. Les très grandes plateformes en ligne et les très grands moteurs de recherche en ligne ont déjà reconnu le terrorisme et l'extrémisme violent en ligne comme des risques systémiques[29]. La Commission suivra de près les mesures d'atténuation mises en œuvre et veillera, s'il y a lieu, à l'application du règlement DSA.

En outre, le comité européen des services numériques joue un rôle essentiel pour ce qui est de garantir l'application effective et cohérente du règlement DSA dans l'ensemble des États membres, y compris l'obligation qui est faite aux fournisseurs de services de lutter contre la diffusion des contenus illicites menant à la radicalisation et des contenus illicites à caractère extrémiste violent. Le **règlement sur l'IA**[30] harmonise les règles applicables à l'intelligence

[26]Europol, chiffre tiré de la base de données PERCI (Point d'entrée pour le retrait de contenus terroristes sur Internet).
[27] Ibid.
[28] La Commission évalue l'interaction de la législation sur les services numériques avec d'autres actes législatifs de l'UE et son seuil de désignation pour les très grandes plateformes en ligne et les très grands moteurs de recherche en ligne | Bâtir l'avenir numérique de l'Europe
[29] Le rapport sur la législation sur les services numériques présente le paysage des risques systémiques en ligne | Bâtir l'avenir numérique de l'Europe
[30] Règlement (UE) 2024/1689 du Parlement européen et du Conseil du 13 juin 2024 établissant des règles harmonisées concernant l'intelligence artificielle et modifiant les règlements (CE) nº 300/2008, (UE) nº 167/2013, (UE) nº 168/2013, (UE) 2018/858, (UE) 2018/1139 et (UE) 2019/2144 et les directives 2014/90/UE, (UE) 2016/797 et (UE) 2020/1828 (règlement sur l'intelligence artificielle).

artificielle, y compris aux outils d'IA à haut risque. La Commission adoptera des lignes directrices afin d'aider les services répressifs et les autorités judiciaires à améliorer leur capacité à détecter et à prévenir les menaces au moyen de systèmes d'IA certifiés dignes de confiance pour les utilisations à haut risque, tout en respectant les droits fondamentaux. La **stratégie pour l'application de l'IA** continuera de soutenir le développement et l'adoption de solutions d'IA à des fins de sécurité intérieure. À partir d'août 2026, les interdictions prévues par le règlement sur l'IA seront appliquées: les systèmes d'IA et les dialogueurs qui manipulent les utilisateurs, en particulier lorsque cette manipulation conduit à la radicalisation et incite à commettre des infractions terroristes ou est susceptible de causer un préjudice important, seront bannis du marché de l'UE. En outre, si les grands modèles d'IA générative amplifient la manipulation préjudiciable conduisant à la radicalisation des utilisateurs, les fournisseurs devront évaluer et atténuer ces risques, et le Bureau européen de l'IA sera chargé de dialoguer avec eux pour remédier à ces problèmes.

2.3.2 Coopérer avec le secteur du numérique

La coopération volontaire avec les fournisseurs de services en ligne est indispensable pour réagir aux tendances émergentes et à l'évolution du paysage des menaces en ligne. À cette fin, le **forum de l'UE sur l'internet** est la principale voie de la Commission, et celui-ci sera encore renforcé. Ce forum est un excellent exemple de collaboration public-privé réunissant ministères, services répressifs, acteurs de la société civile et fournisseurs de services en ligne des États membres de l'UE, y compris des plateformes de médias sociaux. Ce type de collaboration permet un échange sur les priorités et soutient des réponses coordonnées et globales en matière de lutte contre la radicalisation et de limitation de la diffusion des contenus à caractère terroriste et extrémiste violent.

La Commission travaillera également avec le **comité européen des services numériques**, en coopération avec les entreprises et les acteurs des services répressifs concernés, afin de renforcer les efforts de lutte contre la diffusion des contenus à caractère terroriste et extrémiste violent, ainsi que contre la radicalisation en ligne, dans le cadre du règlement DSA. Il pourra s'agir, le cas échéant, d'actions spécifiques visant à aider les fournisseurs de services en ligne à se conformer audit règlement et à le faire respecter. Ces actions pourront comprendre la définition de mesures d'atténuation efficaces pour faire face aux risques systémiques, l'élaboration et la mise en œuvre de lignes directrices et de codes de conduite volontaires ou de cadres de coopération volontaires. Elles pourront également consister à adresser des recommandations ou des conseils aux coordinateurs pour les services numériques afin de soutenir une action coordonnée au niveau national, en particulier en ce qui concerne les services qui ne sont pas considérés comme de très grandes plateformes en ligne ou de très grands moteurs de recherche en ligne. Elles pourront également être axées sur l'amélioration et la rationalisation de l'échange d'informations pertinentes sur les tendances et les risques émergents associés aux services fournis par les intermédiaires en ligne.

Les théories du complot, les discours extrémistes et les contenus extrêmement violents et ambigus alimentent la radicalisation et la polarisation. Dans le cadre du forum de l'UE sur l'internet, Europol facilitera la coopération avec les fournisseurs de services en ligne afin d'améliorer le traitement de ces contenus, lorsqu'ils sont intégrés dans des discours incitant au terrorisme ou recrutant pour le terrorisme[31], tout en respectant les droits fondamentaux.

[31] Selon le principe de la «déconfliction», qui désigne le processus de recoupement des informations opérationnelles et de coordination des activités d'enquête entre les autorités compétentes afin d'éviter les chevauchements ou les interférences entre des enquêtes parallèles.

Les terroristes et les acteurs extrémistes exploitent de plus en plus les **jeux en ligne** pour diffuser de la propagande, désensibiliser à la violence et recruter des sympathisants, y compris des mineurs. Pour lutter contre ce phénomène, le forum de l'UE sur l'internet encouragera la **coopération entre le secteur des jeux et les services répressifs**, en mettant l'accent sur la protection des mineurs, et étudiera la possibilité d'élaborer des **orientations pour empêcher le recrutement** dans ces espaces. Europol développera une **capacité spécifique** de surveillance et d'analyse de ces utilisations abusives. En outre, la Commission abordera les aspects liés à la sécurité des jeux en ligne dans le cadre de sa stratégie globale en matière de jeux vidéo, qui sera publiée en 2026.

Parallèlement, la Commission veillera à ce que les fournisseurs de services en ligne respectent les engagements qu'ils ont pris dans le cadre du **code de conduite pour la lutte contre les discours haineux illégaux en ligne+**.

2.3.3 Assurer une réaction efficace et coordonnée aux crises en ligne

Le **protocole de crise de l'UE** fournit un cadre volontaire pour la coopération entre les services répressifs et les fournisseurs de services en ligne à la suite d'un attentat terroriste ayant des répercussions majeures en ligne. Il fera l'objet d'une révision visant à en faire un **cadre de l'UE pour la réaction aux crises en ligne** et permettra aux États membres de l'appliquer lorsqu'un incident entraînera une intensification de l'activité en ligne liée à un attentat, et à l'ancrer dans le règlement DSA, ce qui garantira une réponse coordonnée tirant parti des dispositions dudit règlement relatives aux crises. Europol facilitera la réaction opérationnelle aux crises grâce à une plateforme technique permettant une coordination rapide. La Commission élaborera également des **orientations** à l'intention des services répressifs et des fournisseurs de services en ligne sur le **traitement des images d'attentats terroristes filmées par de simples spectateurs**, en préservant la dignité des victimes.

Le comité européen des services numériques travaille actuellement à l'élaboration de conseils pratiques destinés à aider les coordinateurs pour les services numériques à contrôler le respect des obligations pertinentes. Ces obligations imposent aux fournisseurs de services d'hébergement d'alerter rapidement les autorités répressives ou judiciaires. Cela s'applique lorsque des fournisseurs ont connaissance d'informations leur permettant de soupçonner qu'une infraction pénale présentant une **menace pour la vie ou la sécurité d'une personne** est en train d'être commise, a été commise ou est susceptible de l'être. Ces infractions peuvent également consister en des formes de terrorisme et d'extrémisme violent illégal.

ACTIONS CLÉS

La Commission:

- étudiera la révision du règlement TCO, sur la base de son évaluation;
- continuera à contrôler et à renforcer l'application des obligations des très grandes plateformes en ligne et des très grands moteurs de recherche en ligne au titre du règlement DSA afin d'atténuer les risques systémiques liés à la diffusion de contenus à caractère terroriste et extrémiste violent;
- facilitera une coopération plus étroite entre le comité européen des services numériques, d'une part, et les autorités répressives et les entreprises, d'autre part, en matière de lutte contre le terrorisme et l'extrémisme violent en ligne;
- définira un nouvel axe de travail dans le cadre du forum de l'UE sur l'internet afin de renforcer les mécanismes de soutien aux utilisateurs de services en ligne et les

interventions positives des fournisseurs de services en ligne visant à prévenir la radicalisation en ligne;
- intégrera le cadre de l'UE pour la réaction aux crises en ligne dans le règlement DSA;
- élaborera des orientations sur le traitement des images d'attentats terroristes filmées par de simples spectateurs.

Europol:
- développera une base de données européenne de partage des hachages pour les contenus à caractère terroriste et extrémiste;
- facilitera la coopération au niveau de l'UE avec les fournisseurs de services en ligne afin d'améliorer le traitement des formes de contenus illicites liés au terrorisme et d'autres contenus préjudiciables;
- surveillera le détournement à des fins extrémistes des plateformes de jeux et fournira des évaluations régulières;
- mettra en place une plateforme de réaction aux crises.

Les États membres sont encouragés à:
- veiller à la mise en œuvre et à l'application effectives des règlements TCO et DSA.

Les fournisseurs de services en ligne sont instamment invités à:
- réexaminer et mettre à jour régulièrement leurs conditions générales afin de tenir compte de l'évolution des menaces;
- renforcer leurs mécanismes de surveillance afin de détecter et de supprimer rapidement les contenus à caractère terroriste;
- intensifier la coopération avec les autorités nationales et Europol afin de garantir des échanges d'informations en temps utile et des réponses coordonnées.

2.4 Protéger les personnes dans l'environnement physique

Ces dernières années, des progrès significatifs ont été accomplis dans l'ensemble de l'UE pour protéger les personnes, les espaces publics et les infrastructures critiques contre les attentats terroristes. L'UE apporte un soutien pratique par l'intermédiaire de ses **conseillers en matière de sûreté**, qui peuvent fournir des conseils en ce qui concerne les vulnérabilités et formuler des recommandations spécifiques en vue d'améliorations. Parallèlement, le **programme de lutte antidrone de l'UE**[32] a renforcé les capacités répressives afin de faire face à la menace que représentent les drones non coopératifs. L'adoption en 2022 de la **directive sur la résilience des entités critiques**[33] a constitué une étape essentielle, faisant passer l'UE d'une approche axée sur la «protection» à une approche axée sur la «résilience».

Cependant, les terroristes ont continué d'élargir leurs moyens de commettre des attentats: des nouvelles technologies, telles que les drones et les armes imprimées en 3D, aux moyens de fortune, tels que les armes blanches et les voitures-béliers. Il convient de restreindre davantage l'accès aux moyens de perpétrer des attentats et de développer les outils de protection des espaces publics et des infrastructures critiques. Parallèlement, pour lutter contre les voyages à des fins de terrorisme et le retour potentiel de combattants terroristes étrangers, nous devons

[32]Lancée par la communication de la Commission au Conseil et au Parlement européen relative à la lutte contre les menaces potentielles posées par les drones [COM(2023) 659 final].
[33] Directive (UE) 2022/2557 du Parlement européen et du Conseil du 14 décembre 2022 sur la résilience des entités critiques, et abrogeant la directive 2008/114/CE du Conseil (*JO L 333 du 27.12.2022*).

améliorer les mesures existantes de l'UE visant à sécuriser les frontières extérieures et à empêcher ce type de voyages.

2.4.1 Empêcher les voyages à des fins de terrorisme

Assurer une protection solide des frontières extérieures constitue la première ligne de défense de l'UE contre les voyages à des fins de terrorisme. Une fois pleinement opérationnels, les **nouveaux systèmes d'information à grande échelle de l'UE**, notamment le système d'entrée/de sortie (EES), le système européen d'information et d'autorisation concernant les voyages (ETIAS), le système d'information sur les visas (VIS) révisé et le cadre d'interopérabilité, fourniront aux États membres des informations essentielles sur les personnes provenant de pays tiers qui entrent dans l'UE. Ces systèmes aideront également les autorités nationales à neutraliser les personnes présentant un risque pour la sécurité, y compris les individus soupçonnés d'activités terroristes.

L'identification des combattants terroristes étrangers et des terroristes présumés aux frontières nécessite également un accès rapide aux données. À cette fin, la Commission, conjointement avec Europol, **renforcera sa coopération avec des pays tiers de confiance afin d'obtenir des données biographiques et biométriques sur les personnes susceptibles de représenter une menace terroriste**, qui pourront ensuite être introduites dans le système d'information Schengen (SIS), dans le plein respect des cadres juridiques applicables au niveau de l'UE et à l'échelon national. Afin de renforcer ce flux d'informations, le **«signalement pour information» du SIS[34] devrait entrer en service en 2026**. Sur proposition d'Europol et sur la base d'informations provenant de pays tiers, les États membres pourront introduire des signalements pertinents dans le SIS, de sorte que les informations sur les terroristes et les personnes soupçonnées d'activités terroristes soient accessibles aux autorités frontalières et répressives[35].

À la suite des récentes conclusions du Conseil sur les priorités futures pour le renforcement des efforts conjoints en matière de lutte contre le terrorisme[36], dans le cadre de l'évaluation globale du système d'information Schengen, la Commission **proposera une voie à suivre pour la mise en place d'une «procédure post-concordance»** afin que les réponses positives concernant les signalements liés au terrorisme puissent être partagées également avec les États membres volontaires. Elle évaluera également l'**application des signalements aux fins de non-admission**[37] et mettra à jour le manuel SIS si nécessaire. En outre, la Commission travaillera en étroite collaboration avec les États membres afin de faire progresser la coopération et le partage d'informations sur les personnes susceptibles de représenter une menace terroriste ou extrémiste violente («**Gefährder**»)[38].

Comme annoncé dans la stratégie de sécurité intérieure ProtectEU, la Commission évaluera les mesures visant à **renforcer l'échange d'informations à des fins répressives et de gestion des**

[34] Règlement (UE) 2022/1190 du Parlement européen et du Conseil du 6 juillet 2022 modifiant le règlement (UE) 2018/1862 en ce qui concerne l'introduction dans le système d'information Schengen (SIS) de signalements pour information concernant des ressortissants de pays tiers dans l'intérêt de l'Union (*JO L 185 du 12.7.2022*).

[35] Ibid.

[36] Conclusions du Conseil du 12 décembre 2024 sur les priorités futures pour le renforcement des efforts conjoints de l'Union européenne et de ses États membres en matière de lutte contre le terrorisme.

[37] Article 24 du règlement (UE) 2018/1862 du Parlement européen et du Conseil du 28 novembre 2018 sur l'établissement, le fonctionnement et l'utilisation du système d'information Schengen (SIS) dans le domaine de la coopération policière et de la coopération judiciaire en matière pénale *(JO L 312 du 7.12.2018)*.

[38] Note du Conseil intitulée «A shared understanding of when a person should be regarded as a potential terrorist or violent extremist threat ("Gefährder")» (Une compréhension commune des cas dans lesquels une personne devrait être considérée comme une menace terroriste ou extrémiste violente potentielle) (ST 8807 2024 REV 1 — NOTE).

frontières avec des pays tiers de confiance. À des fins de sécurité et de gestion des frontières, cela pourrait être mis en œuvre au moyen d'une solution technique permettant l'échange contrôlé et limité d'un sous-ensemble sélectionné de données provenant des bases de données de l'UE, sur la base d'un accord international et du principe de réciprocité. À des fins répressives, cela pourrait être mis en œuvre en étendant le cadre de l'UE pour l'échange automatisé d'informations policières (Prüm) et le système d'information Schengen (SIS) à des pays tiers de confiance, en renforçant les enquêtes transfrontières tout en respectant pleinement les droits fondamentaux ainsi que les normes de l'UE en matière de protection des données et de sécurité.

Le nouveau **processus de filtrage**[39], qui entrera en application en juin 2026, facilitera l'identification des ressortissants de pays tiers qui ont franchi illégalement les frontières extérieures ou qui sont en séjour irrégulier sur le territoire des États membres sans avoir été soumis à des vérifications à l'entrée. Des vérifications systématiques devront être effectuées pour évaluer si ces personnes présentent un risque pour la sécurité. En ce qui concerne les personnes représentant une menace terroriste, les procédures de droit pénal et d'extradition pourront être engagées. La Commission encouragera le **retour efficace des personnes présentant un risque pour la sécurité**, en facilitant l'adoption rapide de règles plus strictes dans la **proposition de règlement sur le retour**[40] et grâce aux travaux du coordinateur chargé des retours et du réseau de haut niveau pour les retours. Elle encouragera également les États membres à continuer de renforcer la **coopération et la coordination entre les autorités chargées de la lutte contre le terrorisme et les autorités compétentes en matière de migration et d'asile**.

En outre, les **informations préalables sur les voyageurs** [telles que les informations préalables sur les passagers (API) et les données des dossiers passagers (PNR)] sont indispensables aux autorités répressives pour planifier effectivement et déployer efficacement leurs efforts de lutte contre le terrorisme tant aux frontières extérieures que sur le territoire de l'UE. Le cadre actuel de l'UE se limite au transport aérien commercial, ce qui crée des failles juridiques et opérationnelles que les terroristes peuvent exploiter pour se déplacer dans l'ensemble de l'UE. La Commission, en étroite coordination avec les États membres et le secteur des transports, étudie les **possibilités d'étendre le cadre actuel** à d'autres modes de transport tels que les transports maritime et terrestre, ainsi qu'aux vols privés, et de renforcer la directive PNR, sous réserve de son évaluation[41].

2.4.2. Restreindre l'accès aux moyens utilisés pour perpétrer des attentats

Il est essentiel de restreindre davantage l'accès aux moyens utilisés pour perpétrer des attentats. Il ressort de saisies récentes, notamment d'armes à feu imprimées en 3D, que les terroristes et les extrémistes violents d'ultradroite, en particulier, continuent de disposer d'armes[42]. La Commission présentera, au début de 2026, une **proposition législative visant à harmoniser l'incrimination du trafic d'armes à feu et d'autres infractions liées à celles-ci**, parmi

[39] Règlement (UE) 2024/1356 du Parlement européen et du Conseil du 14 mai 2024 établissant le filtrage des ressortissants de pays tiers aux frontières extérieures (*JO L, 2024/1356, 22.5.2024*).
[40] Proposition de règlement du Parlement européen et du Conseil établissant un système commun en matière de retour des ressortissants de pays tiers en séjour irrégulier dans l'Union, et abrogeant la directive 2008/115/CE du Parlement européen et du Conseil, la directive 2001/40/CE du Conseil et la décision 2004/191/CE du Conseil [COM(2025) 101 final].
[41] Directive (UE) 2016/681 du Parlement européen et du Conseil du 27 avril 2016 relative à l'utilisation des données des dossiers passagers (PNR) pour la prévention et la détection des infractions terroristes et des formes graves de criminalité, ainsi que pour les enquêtes et les poursuites en la matière (*JO L 119 du 4.5.2016*).
[42] Europol, TE-SAT 2025.

lesquelles la création, la détention et la diffusion illicites de modèles pour l'impression d'armes à feu en 3D.

Les terroristes et les extrémistes violents continuent également de montrer un intérêt pour les explosifs artisanaux, comme en témoignent les manuels et les modes d'emploi qui circulent en ligne. Pour contrer ces menaces, la Commission procède actuellement à un **réexamen du règlement de l'UE sur les précurseurs d'explosifs**[43]. L'évaluation, récemment achevée, de la **directive sur les articles pyrotechniques**[44] a mis en évidence des lacunes en matière de sécurité publique, notamment l'accès étendu des utilisateurs non autorisés aux feux d'artifice professionnels à haut risque. La Commission étudie actuellement différentes options, parmi lesquelles une éventuelle **révision** de la directive.

Les incidents chimiques, biologiques, radiologiques et nucléaires (CBRN) dans le contexte du terrorisme sont des événements peu probables, mais à fort impact, auxquels il est indispensable de se préparer à l'échelle de l'UE. La Commission présentera, en 2026, un **nouveau plan d'action pour la préparation et la réaction aux menaces CBRN**. Elle proposera, entre autres, un programme de formation et d'exercice plus solide à l'échelle de l'UE et explorera les pistes possibles pour lutter contre l'utilisation abusive de nouvelles technologies telles que la synthèse d'acides nucléiques et les biotechnologies fondées sur l'IA. Parallèlement, la **stratégie de constitution de stocks à l'échelle de l'UE** et la **stratégie de l'UE en matière de contre-mesures médicales** participeront à la préparation sanitaire visant à atténuer les conséquences des incidents CBRN.

2.4.3. Faire face à la menace posée par les drones

Il faut également que l'UE soit préparée à contrer les menaces qui résultent du recours à des technologies nouvelles et émergentes, telles que l'utilisation malveillante de drones par des acteurs terroristes. Les drones, qu'ils soient aériens, maritimes, sous-marins ou terrestres, posent des problèmes importants en matière de protection des infrastructures critiques et des espaces publics. Dans le prolongement de la communication de 2023 relative à la lutte contre les menaces potentielles posées par les drones[45] ainsi que de la stratégie Drone 2.0[46], la Commission a récemment présenté un **plan d'action** intersectoriel global **de l'UE relatif à la sûreté des drones et des systèmes antidrones**. Ce nouveau plan d'action renforcera encore les capacités des services répressifs, des gardes-frontières et des gardes-côtes à lutter contre les menaces posées par les drones grâce à une formation spécialisée à la lutte antidrones, à la mise en place éventuelle d'une plateforme des incidents liés aux drones, ainsi qu'à la mise en commun et au partage des ressources.

2.4.4. Protéger les espaces publics

Les espaces publics restent les principales cibles des attentats terroristes. Il est donc essentiel d'adopter le principe de sécurité dès la conception lors de la planification des zones urbaines,

[43] Règlement (UE) 2019/1148 du Parlement européen et du Conseil du 20 juin 2019 relatif à la commercialisation et à l'utilisation de précurseurs d'explosifs, modifiant le règlement (CE) nº 1907/2006 et abrogeant le règlement (UE) nº 98/2013, *JO L 186 du 11.7.2019.*

[44] Document de travail des services de la Commission - Résumé de l'évaluation de la directive 2013/29/UE du Parlement européen et du Conseil du 12 juin 2013 relative à l'harmonisation des législations des États membres concernant la mise à disposition sur le marché d'articles pyrotechniques (refonte), SWD (2025) 269 final.

[45] Communication de la Commission au Conseil et au Parlement européen relative à la lutte contre les menaces potentielles posées par les drones, COM(2023) 659 final.

[46] Communication de la Commission au Conseil et au Parlement européen intitulée «Une stratégie Drone 2.0 pour favoriser un écosystème intelligent et durable d'aéronefs sans équipage à bord en Europe», COM(2022) 652 final.

des espaces publics et des lieux de culte en Europe[47]. La sécurité dès la conception devrait être une responsabilité partagée fondée sur une coopération solide entre secteurs public et privé. Par conséquent, la Commission examinera et évaluera les possibilités d'introduire un **«engagement à protéger» pour les exploitants d'espaces publics** (installations sportives, salles de spectacle ou lieux de culte, par exemple) en vue de la mise en œuvre de mesures de sécurité fondées sur les risques face aux menaces terroristes potentielles dans les lieux publics.

Parallèlement, la Commission investit **30 millions d'EUR dans des projets qui visent à améliorer la sécurité générale des espaces publics** et ciblent notamment les lieux de culte de toutes confessions, les menaces CBRN, le trafic d'armes à feu, les chiens détecteurs d'explosifs et les drones non coopératifs. Sur ce montant, 5 millions d'EUR sont affectés à la protection des lieux de culte juifs, les résultats des projets concernés étant attendus d'ici à 2027[48]. La Commission continuera de soutenir la protection des lieux de culte dans le cadre des politiques relatives aux affaires intérieures, dont elle a proposé de tripler l'enveloppe budgétaire dans le prochain CFP[49].

Afin de renforcer encore la coopération entre les secteurs public et privé, la Commission transformera le **forum de l'UE sur la protection des espaces publics**[50] en un organe consultatif chargé de soutenir l'élaboration des politiques. Parallèlement, elle actualisera les **lignes directrices de l'UE concernant les partenariats public-privé pour la protection des espaces publics** et les **bonnes pratiques nationales en matière de mesures de protection de l'espace public**, avec une attention particulière pour la protection des lieux de culte, en s'appuyant sur les résultats des projets financés par l'UE dans ce domaine.

Le **programme de conseil en matière de sûreté** a joué un rôle déterminant dans le renforcement des capacités nécessaires pour pouvoir procéder à des évaluations de la vulnérabilité des espaces publics et des infrastructures critiques, **plus de 50 missions de conseil** ayant été menées à bien depuis 2022. Face à la demande croissante des États membres, la Commission évaluera le programme en 2026 et entend le doter de moyens financiers et opérationnels supplémentaires dans le nouveau CFP.

Conformément à ses recommandations concernant les rayons X et la détection des métaux[51], la Commission, en collaboration avec les États membres, continuera à élaborer de nouvelles **exigences de performance d'application volontaire pour les équipements de détection hors aviation** et mettra en place des **systèmes, eux aussi d'application volontaire, de vérification et de certification** pour la détection des produits chimiques, des explosifs et des armes à feu, ainsi que pour les chiens détecteurs.

---

[47] Commission européenne, Security by Design: Protection of public spaces from terrorist attacks (2023) JRC131172.

[48] Voir les projets financés dans le cadre de l'appel à propositions SFI concernant la protection des espaces publics: ISF-2024-TF2-AG-PROTECT.

[49] Proposition de règlement du Parlement européen et du Conseil établissant le soutien de l'Union en faveur de la sécurité intérieure pour la période 2028-2034.

[50] Le forum de l'UE sur la protection des espaces publics rassemble des collectivités locales et régionales, des exploitants privés d'espaces publics, des organisations du secteur privé et des organisations confessionnelles en vue d'échanger des bonnes pratiques en matière de mesures de protection.

[51] Recommandation (UE) 2022/1341 de la Commission du 23 juin 2022 relative à des exigences de performance d'application volontaire pour les équipements d'imagerie radioscopique utilisés dans les espaces publics (hors aviation), C/2022/4179.
Recommandation (UE) 2023/1468 de la Commission du 10 mai 2023 relative à des exigences de performance définies par l'UE, d'application volontaire, pour les détecteurs de métaux utilisés dans les espaces publics (hors aviation) , C/2023/3039.

2.4.5. Résilience des entités critiques, et sécurité des chaînes de transport et d'approvisionnement

Bien que les États membres n'aient signalé que quatre attaques classées comme «terroristes» contre des infrastructures critiques en 2024[52], les incidents liés à des campagnes hybrides et à des actes de sabotage potentiels de la part d'acteurs étatiques hostiles et de leurs mandataires suscitent de plus en plus d'inquiétude. Pour accroître la résilience, il convient que tous les États membres transposent et mettent en œuvre d'urgence la directive sur la résilience des entités critiques (directive CER) et la directive SRI 2[53]. Des **exercices seront organisés au niveau de l'UE** en coopération avec les États membres afin de tester la résilience physique et cyber des infrastructures critiques en cas d'incidents transfrontières importants. Pour favoriser la mise en œuvre effective de la directive CER et améliorer la résilience transfrontière et transsectorielle des infrastructures critiques face aux menaces d'origine humaine, la Commission mettra **15 millions d'EUR à disposition pour financer des projets** et adoptera des **lignes directrices** afin d'aider les entités critiques recensées par les États membres à prendre des mesures pour renforcer leur résilience. La Commission a par ailleurs proposé de renforcer encore la protection et la résilience des entités critiques dans le cadre du mécanisme pour l'interconnexion en Europe et du Fonds européen pour la compétitivité dans le prochain CFP.

Les transports restent une cible de premier plan et tout porte à croire que la menace continuera d'évoluer avec l'apparition de nouveaux modes opératoires d'attaque. La Commission s'appuiera sur la cartographie complète des risques en matière de sûreté aérienne pour élaborer de **nouvelles exigences de base en matière de sûreté aérienne adaptées aux évolutions futures**, notamment en renforçant la législation en matière de sûreté aérienne (AVSEC)[54] pour qu'il soit possible de réagir immédiatement tout en maintenant dans l'UE la zone de contrôle unique de sûreté. La Commission a également proposé de mettre en place un **système de comptes rendus des événements de sûreté aérienne au niveau de l'UE**, fondé sur les mécanismes existants, pour faciliter le partage d'informations sur les événements et incidents de sûreté, ainsi qu'un mécanisme multi-agences de l'UE permettant de donner l'alerte en cas de menace et de réagir à d'éventuelles crises émergentes dans les chaînes de transport et d'approvisionnement.

À la suite d'incidents de fret aérien, les règles de l'UE en matière de sûreté de l'aviation civile ont été modifiées[55] pour **améliorer la résilience** et la **protection de la chaîne d'approvisionnement du fret et du courrier aériens**. Afin d'atténuer les effets des attaques et des actes de sabotage ciblant les chemins de fer, la Commission et l'Agence de l'UE pour les chemins de fer (AFE) renforceront la robustesse du système de gestion du trafic ferroviaire en vue de garantir la poursuite des opérations en cas de défaillances à l'échelle du système.

Dans le cadre de la **stratégie portuaire européenne**, la Commission renforcera encore la législation en matière de sûreté maritime afin de lutter efficacement contre les menaces émergentes, d'accroître la sécurité des chaînes d'approvisionnement de l'UE et d'évaluer l'introduction des vérifications des antécédents des travailleurs portuaires. La Commission

[52] Europol, TE-SAT 2025.

[53] Directive (UE) 2022/2555 du Parlement européen et du Conseil du 14 décembre 2022 concernant des mesures destinées à assurer un niveau élevé commun de cybersécurité dans l'ensemble de l'Union, modifiant le règlement (UE) nº 910/2014 et la directive (UE) 2018/1972, et abrogeant la directive (UE) 2016/1148 (directive SRI 2), *JO L 333 du 27.12.2022*.

[54] Document de travail des services de la Commission intitulé «Working towards an enhanced and more resilient aviation security policy: a stocktaking», SWD (2023) 37 final.

[55] Règlement d'exécution (UE) 2025/920 de la Commission du 19 mai 2025, décision d'exécution de la Commission (SENSITIVE) du 19 mai 2025 – COM(2025) 3014 final.

collaborera également avec les autorités répressives et douanières, les organisations internationales, les pays tiers et le secteur privé afin d'atténuer les menaces CBRN pesant sur les chaînes d'approvisionnement maritimes.

ACTIONS CLÉS

La Commission:

- proposera une voie à suivre pour la mise en place d'une «procédure post-concordance» dans le cadre de l'évaluation du SIS;
- soutiendra la mise en service des signalements pour information dans le SIS;
- étudiera les possibilités de renforcer et d'étendre le cadre de l'UE en matière d'informations concernant les voyages (API/PNR);
- présentera une proposition législative visant à harmoniser l'incrimination des infractions liées aux armes à feu;
- procédera à la révision du règlement sur les précurseurs d'explosifs;
- présentera un nouveau plan d'action pour la préparation et la réaction aux menaces CBRN;
- mettra en œuvre le nouveau plan d'action relatif à la sûreté des drones et des systèmes antidrones;
- examinera et évaluera les possibilités d'introduire un «engagement à protéger» pour les exploitants d'espaces publics;
- renforcera le programme de conseil en matière de sûreté dans le cadre du nouveau CFP.

La Commission, en coopération avec Europol:

- renforcera sa coopération avec les pays tiers de confiance afin d'obtenir des données de qualité suffisante (biographiques, biométriques et contextuelles) sur les personnes susceptibles de constituer une menace terroriste.

Il convient que les États membres:

- fassent pleinement usage des procédures à la frontière et des systèmes en matière de gestion de la sécurité et des frontières déjà en place;
- renforcent les contrôles biométriques et effectuent des vérifications systématiques obligatoires aux frontières extérieures de l'UE;
- déploient pleinement l'EES et accélèrent les préparatifs en vue de la mise en service de l'ETIAS;
- mettent en œuvre les recommandations du mécanisme d'évaluation et de contrôle Schengen;
- transposent et mettent en œuvre rapidement les directives CER et SRI 2.

2.5 Réagir aux menaces et aux attentats

Europol et Eurojust apportent une expertise et un appui opérationnel précieux aux États membres dans le cadre des enquêtes et des poursuites en matière de terrorisme. Néanmoins, pour garantir une réaction rapide et coordonnée en cas de menaces ou d'attentats terroristes, il est nécessaire de renforcer encore la réponse des services répressifs et judiciaires dans l'ensemble de l'Europe. En outre, des efforts supplémentaires s'imposent pour combler les lacunes qui subsistent afin de pouvoir prévenir et combattre le financement du terrorisme. L'UE reste déterminée à empêcher l'utilisation de fonds publics pour la promotion de l'extrémisme et du terrorisme.

2.5.1. Lutter contre le financement du terrorisme et de l'extrémisme violent

La menace que représente le financement du terrorisme évolue rapidement, profitant de l'expansion de certains modes de financement tels que les financements par crypto-actifs, l'hawala numérique et les services de paiement en ligne. Dans le même temps, vu la nature mondiale des services financiers, il est nécessaire que **l'UE apporte une solution dynamique au problème du financement du terrorisme**. L'UE a mis en place un cadre global, dont la dernière mise à jour remonte à 2024, pour prévenir le blanchiment de capitaux et le financement du terrorisme. Les États membres sont instamment invités à transposer la **6e directive antiblanchiment** d'ici le 10 juillet 2027, à temps pour l'entrée en vigueur du **règlement de l'UE relatif au blanchiment de capitaux**. L'**interconnexion des registres des comptes bancaires** d'ici à 2029 renforcera encore ce cadre. En outre, depuis 2010, l'**accord entre l'Union européenne et les États-Unis sur le programme de surveillance du financement du terrorisme (TFTP)** autorise les États membres, Europol et Eurojust à demander au Trésor des États-Unis d'effectuer des recherches dans les données de messagerie financière, qui offrent des pistes précieuses pour l'identification des terroristes et de ceux qui les financent.

Afin de combler les lacunes existantes en matière de surveillance du financement du terrorisme, la Commission lancera, au début de 2026, une étude visant à **passer en revue et** à **répertorier les mesures nécessaires à la mise en place, à l'échelle de l'UE, d'un nouveau système de recherche de données financières aux fins de la surveillance du financement du terrorisme** et des produits de la criminalité organisée. Ce système, qui devrait être instauré d'ici à 2030, s'appliquera aux opérations effectuées au sein de l'UE et de l'espace unique de paiement en euros (SEPA), aux transferts de crypto-actifs, aux paiements en ligne et aux virements électroniques.

Le **réseau d'enquêteurs financiers dans le domaine de la lutte antiterroriste** fournit un cadre d'échange d'informations sur les enquêtes et de bonnes pratiques concernant un large éventail de méthodes de financement du terrorisme et de tendances émergentes, telles que l'utilisation des crypto-actifs, l'utilisation abusive des organisations à but non lucratif et des plateformes de médias sociaux, l'hawala et d'autres systèmes bancaires informels. Le réseau permet d'établir des partenariats avec des parties prenantes publiques et privées et des pays partenaires en dehors de l'UE et vise à inclure systématiquement les contributions du **partenariat public-privé d'Europol en matière de renseignement financier**.

La Commission favorisera également une **coopération plus étroite et le partage d'informations** entre les cellules de renseignement financier (CRF), les services répressifs, les institutions financières, les entreprises de technologie financière et les fournisseurs de services en ligne. Plus précisément, la lutte contre les **financements étrangers inopportuns**[56] exige des CRF et des services de renseignement qu'ils coopèrent plus étroitement en s'appuyant sur les protocoles pour l'échange d'informations existants. Il convient que les États membres **veillent à ce que les CRF aient le mandat et la capacité nécessaires pour détecter les financements étrangers inopportuns et échanger à ce sujet**. Les évaluations nationales des risques de blanchiment de capitaux et de financement du terrorisme devraient également porter sur les financements étrangers inopportuns, de sorte que les CRF puissent les détecter et les traiter de manière systématique.

Le **budget de l'UE ne doit jamais être utilisé de manière abusive** pour financer des projets qui promeuvent des opinions radicales ou extrémistes. Depuis la révision du règlement

[56] Flux financiers d'acteurs étatiques ou non étatiques étrangers vers des personnes physiques ou morales opérant dans l'UE qui exercent ou ont l'intention d'exercer une influence malveillante sur les sociétés européennes en facilitant des activités qui remettent en cause les valeurs de l'UE (définition juridiquement non contraignante utilisée par le pôle de connaissances de l'UE sur la prévention de la radicalisation).

financier[57], toute conduite fautive entraînant une «incitation à la discrimination, à la haine ou à la violence» constitue un motif clair d'exclusion du financement de l'UE. La Commission veillera à la bonne mise en œuvre de cette disposition, notamment en menant des actions de sensibilisation, en mettant en place un réseau interne d'échange d'informations et en renforçant les processus qui permettent de tenir compte des informations provenant des États membres et d'autres sources lorsque ces informations peuvent être utilisées pour évaluer le respect des valeurs de l'UE par les bénéficiaires et les projets.

L'efficacité de la protection du budget de l'UE dépend également de la communication active, par les États membres, d'informations destinées à soutenir les efforts déployés par la Commission. Les résultats du réexamen de l'**architecture antifraude**, qui sera réalisé en 2026, permettront de renforcer la surveillance et l'obligation de rendre des comptes de manière à garantir une protection plus efficace des intérêts financiers de l'Union.

2.5.2. Renforcer la réponse des services répressifs

Comme annoncé dans la stratégie de sécurité intérieure ProtectEU, la Commission proposera une révision ambitieuse du mandat d'Europol, qui **renforcerait son rôle de pôle central d'information, de technologie et d'innovation pour les services répressifs**, afin d'apporter un soutien accru aux États membres à la fois sur le plan opérationnel et sur le plan médico-légal.

Sous réserve du réexamen du mandat d'Europol, le Centre européen de la lutte contre le terrorisme d'Europol devrait consolider et continuer à développer les informations opérationnelles en matière de lutte contre le terrorisme à l'intention des services répressifs dans son **pôle central d'information sur la lutte contre le terrorisme**. Ce pôle pourrait également rendre possible l'échange d'informations en temps réel entre les services répressifs et favoriser la coopération entre ces derniers et le secteur privé. Sur le plan médico-légal, le Centre européen de la lutte contre le terrorisme, en collaboration avec le laboratoire d'innovation d'Europol, le Centre européen de lutte contre la cybercriminalité (EC3) et d'autres centres concernés, **apportera un soutien opérationnel, analytique et technique accru aux États membres**. Cette collaboration permettra le renforcement des capacités de traitement d'ensembles de données vastes et complexes et la mise au point d'outils pour détecter et contrer les contenus terroristes et extrémistes en ligne, ainsi que le financement du terrorisme.

La Commission continuera de **soutenir les réseaux européens de services répressifs**[58]. Elle collaborera aussi étroitement avec les États membres pour actualiser la recommandation du Conseil relative à la coopération opérationnelle des services répressifs[59], afin de faciliter l'assistance opérationnelle dans les scénarios transfrontières, y compris le déplacement d'équipes opérationnelles et d'équipements dans le cadre d'exercices et pas uniquement en cas de crise.

2.5.3. Renforcer la coopération judiciaire

Pour contrer la menace terroriste et extrémiste violente à l'ère numérique, il est indispensable que les services répressifs et les autorités judiciaires disposent d'un accès licite aux données. La mise en œuvre de la **feuille de route de 2025 sur un accès licite et effectif aux données à**

[57] Article 138, paragraphe 1, point c) vi), et considérant 113 du règlement (UE, Euratom) 2024/2509 du Parlement européen et du Conseil du 23 septembre 2024 relatif aux règles financières applicables au budget général de l'Union (refonte), *JO L, 2024/2509, 26.9.2024*.

[58] AIRPOL, AQUAPOL, ENLETS, ESG, EIFS, HRSN, RAIPOL et ATLAS.

[59] Recommandation (UE) 2022/915 du Conseil du 9 juin 2022 relative à la coopération opérationnelle des services répressifs, *JO L 158 du 13.6.2022*.

des fins répressives[60] contribuera à lever les principaux obstacles qui entravent les enquêtes et les poursuites. Les **règles de l'UE relatives à l'accès transfrontière aux preuves électroniques**[61] deviendront applicables en août 2026, ce qui permettra aux autorités judiciaires de conserver des preuves et d'en obtenir directement auprès des fournisseurs de services qui proposent leurs services au sein de l'UE. Dans la foulée du **projet SIRIUS financé par l'UE**[62] et de la future entrée en vigueur de la **convention des Nations unies contre la cybercriminalité** et du **deuxième protocole additionnel à la convention sur la cybercriminalité du Conseil de l'Europe**, la coopération internationale en vue de l'obtention de preuves électroniques sera renforcée au moyen d'une formation spécifique et d'un échange d'informations.

La coopération judiciaire et le partage d'informations sur les affaires de terrorisme sont essentiels pour faire face à la menace terroriste au cours des phases de prévention et de réaction. Pour faciliter l'identification des liens transfrontières entre les affaires de terrorisme, Eurojust modernisera le **registre judiciaire européen antiterroriste** en le dotant, d'ici au 1er décembre 2027, d'un nouveau système de gestion des dossiers à la pointe de la technologie. Les États membres sont instamment invités à communiquer en temps utile des informations sur les affaires de terrorisme à Eurojust. En outre, la **révision du mandat d'Eurojust** contribuera à renforcer la capacité d'analyse de l'Agence et lui permettra de coopérer plus étroitement avec Europol, pour un meilleur soutien aux enquêtes et aux poursuites transfrontières en matière de terrorisme. En outre, la directive de 2016 relative à la mise en place de garanties procédurales en faveur des enfants[63] continuera d'offrir un soutien et des mesures de protection adaptés aux enfants qui entrent dans le système de justice pénale. Les **éléments de preuve obtenus sur le champ de bataille** sont essentiels pour poursuivre les combattants terroristes étrangers à leur retour. Une fois introduites dans le SIS, les données tirées de ces éléments de preuve aident également à repérer les combattants terroristes étrangers aux frontières de l'UE. La dissolution de l'Équipe d'enquêteurs des Nations unies chargée de concourir à amener Daech/EIIL à répondre de ses crimes (UNITAD) limite la disponibilité de tels éléments de preuve. La Commission, avec le soutien d'Eurojust, cherchera à déterminer si les informations recueillies par **les autorités iraquiennes et l'UNITAD** pourraient être mises à la disposition des États membres dans le cadre d'une coopération renforcée entre **Eurojust** et le **Centre national de coopération judiciaire internationale de l'Iraq** et, dans l'affirmative, selon quelles modalités elles le seraient, et si les informations liées aux cas individuels pourraient être stockées dans la **base de données sur les preuves de grands crimes internationaux d'Eurojust**.

[60] Communication de la Commission au Parlement européen, au Conseil, au Comité économique et social européen et au Comité des régions - Feuille de route pour un accès licite et effectif aux données à des fins répressives, COM(2025) 349 final.

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

[62] Le projet SIRIUS, financé par l'UE, sert de point de départ pour obtenir des données électroniques auprès de fournisseurs de services établis dans d'autres juridictions, et ce pour plus de 8 000 membres dans 47 juridictions.

[63] Directive (UE) 2016/800 du Parlement européen et du Conseil du 11 mai 2016 relative à la mise en place de garanties procédurales en faveur des enfants qui sont des suspects ou des personnes poursuivies dans le cadre des procédures pénales, *JO L 132 du 21.5.2016*.

ACTIONS CLÉS

La Commission:

- passera en revue et répertoriera les mesures nécessaires à la mise en place d'un système européen de recherche de données financières aux fins de la surveillance du financement du terrorisme et des produits de la criminalité organisée;
- renforcera le système de protection du budget de l'UE contre les abus, notamment en révisant l'architecture antifraude de l'UE;
- proposera des révisions des mandats d'Europol et d'Eurojust, afin de renforcer leur rôle dans la réponse répressive et judiciaire au terrorisme.

En collaboration avec les États membres et Europol, la Commission:

- renforcera la coopération et le partage d'informations entre les cellules de renseignement financier (CRF), les services répressifs, les institutions financières, les entreprises de technologie financière, les fournisseurs de services en ligne et les plateformes de médias sociaux;
- mettra en œuvre les actions prévues dans la feuille de route pour un accès licite et effectif aux données à des fins répressives.

Europol:

- consolidera et continuera à développer son pôle central d'information sur la lutte contre le terrorisme;
- renforcera son soutien opérationnel, analytique et technique aux efforts déployés par les services répressifs des États membres pour lutter contre le terrorisme.

En collaboration avec la Commission, Eurojust:

- étudiera les moyens de mettre les informations recueillies par l'UNITAD et les autorités iraquiennes à la disposition des États membres.

2.6 Coopération avec les partenaires internationaux

Les dimensions extérieure et intérieure du terrorisme et de l'extrémisme violent sont intrinsèquement liées[64]. La Commission, en collaboration avec la haute représentante et le coordinateur de l'UE pour la lutte contre le terrorisme, renforcera la coopération internationale au titre de l'ensemble des piliers du présent programme, en suivant une approche fondée sur les droits de l'homme.

2.6.1. Mesures restrictives en matière de terrorisme

L'inscription sur la liste des personnes, groupes et entités faisant l'objet des mesures restrictives de l'UE qui visent à lutter contre le terrorisme[65] (ci-après la «liste de l'UE en matière de terrorisme») reste un outil indispensable pour démanteler les réseaux terroristes. Il convient que cette liste soit mise à jour en continu afin de tenir compte de l'évolution des menaces et d'y faire face en interrompant les flux financiers et en empêchant le soutien des activités terroristes. La haute représentante et les États membres de l'UE **étudient actuellement les moyens de rendre la liste de l'UE en matière de terrorisme plus efficace, plus opérationnelle et plus souple**. L'élargissement du champ d'application du régime et une coopération plus étroite avec des pays tiers qui partagent les mêmes valeurs participeront à son bon fonctionnement.

[64] Conclusions du Conseil du 16 décembre 2024 sur le renforcement des liens entre les aspects extérieurs et intérieurs de la lutte contre le terrorisme et l'extrémisme violent.

[65] Position commune 2001/931/PESC du Conseil du 27 décembre 2001 relative à l'application de mesures spécifiques en vue de lutter contre le terrorisme, *JO L 344 du 28.12.2001*.

2.6.2. Accélérer la conclusion d'accords internationaux

La Commission proposera de signer et de conclure, au nom de l'UE, le **nouveau protocole modifiant la définition des infractions terroristes** dans la convention du Conseil de l'Europe pour la prévention du terrorisme. Une fois en vigueur, ce cadre fournira à plus de 40 pays une **définition paneuropéenne commune des infractions terroristes**.

La Commission entend **encore renforcer la coopération extérieure d'Europol et d'Eurojust** en matière de lutte contre le terrorisme au moyen d'accords internationaux sur l'échange de données à caractère personnel avec des pays tiers et des organisations internationales, en mettant l'accent sur les régions clés.

2.6.3. Approfondir la coopération bilatérale et régionale

La coopération avec les **partenaires concernés par l'élargissement** sera renforcée afin de faciliter leur intégration accélérée dans l'architecture de sécurité de l'UE et de promouvoir l'alignement de leurs cadres juridiques et stratégiques sur l'acquis et les normes de l'UE. Dans la mesure du possible, ces partenaires seront **progressivement associés aux actions de l'UE** telles que le pôle de connaissances sur la prévention de la radicalisation et les activités d'Europol, d'Eurojust et du CEPOL et bénéficieront des outils, des orientations et du renforcement des capacités offerts aux États membres.

Le nouveau **plan d'action conjoint 2025-2030 relatif à la prévention du terrorisme et de l'extrémisme violent dans les Balkans occidentaux et à la lutte contre ces phénomènes** soutient également l'alignement des Balkans occidentaux sur l'acquis de l'UE, fait progresser la coopération opérationnelle et renforce les capacités de nos partenaires dans la région. Les pays candidats et les candidats potentiels à l'adhésion à l'UE bénéficieront en outre d'une assistance technique spécifique, d'un renforcement des capacités et du financement de projets par l'UE, par exemple en matière de protection des espaces publics et des infrastructures critiques ou de gestion des frontières.

Le **Moyen-Orient et l'Afrique du Nord** occupent une place stratégique dans la lutte mondiale contre le terrorisme. Dans le cadre du **pacte pour la Méditerranée**, l'aide de l'UE sera centrée sur le renforcement de la gestion des frontières, l'intensification de la coopération des services répressifs et judiciaires et la prévention de l'extrémisme violent et du terrorisme, avec le soutien du pôle de connaissances sur la prévention de la radicalisation. Un dialogue régional sur la sécurité intérieure contribuera à la lutte contre la grande criminalité organisée et le terrorisme.

L'UE continuera de soutenir le redressement de la **Syrie** en favorisant une transition et une réconciliation pacifiques et inclusives dans le pays et en soutenant la réintégration de celui-ci dans sa région. En outre, l'UE mettra à disposition une enveloppe d'aide financière d'environ 620 millions d'EUR pour 2026 et 2027, qui permettra notamment de financer une aide humanitaire, une aide au redressement rapide et un soutien bilatéral, tout en continuant à faire face aux conséquences de la crise dans le nord-est de la Syrie et dans les camps. La Commission encourage aussi les institutions et les États membres de l'UE à mettre en œuvre les conclusions du Conseil du 23 juin 2025 sur la Syrie, ainsi que les recommandations qui figurent dans le **plan d'action visant à lutter contre la menace terroriste émanant de la Syrie**, publié par le coordinateur de l'UE pour la lutte contre le terrorisme

En **Afrique**, notamment en Afrique subsaharienne, divers groupes terroristes gagnent en puissance. En **Asie centrale** et en **Asie du Sud**, la situation, marquée par la montée des tensions régionales et l'influence croissante de l'ISKP, exige, elle aussi, une surveillance étroite. L'UE renforcera sa réponse intégrée en **tenant compte des considérations de sécurité dans l'approche à 360 degrés de la stratégie «Global Gateway»** et en **augmentant son soutien direct au renforcement des capacités**. Les programmes amélioreront la sécurité aux

frontières, favoriseront la coopération opérationnelle, renforceront la capacité à détecter et à enrayer les flux financiers illicites, s'attaqueront à la propagande extrémiste et violente, lutteront contre le détournement des nouvelles technologies et contre le lien toujours plus étroit entre terrorisme et criminalité organisée dans plusieurs régions, augmenteront la résilience des communautés face à la radicalisation et au recrutement dans des groupes terroristes, et faciliteront la réhabilitation et la réintégration des anciens combattants et de leurs familles.

La **coordination de l'action extérieure de l'UE et des États membres dans les pays tiers** est particulièrement importante pour éviter les doubles emplois. La Commission, en collaboration avec les États membres, recensera régulièrement les projets financés par l'UE et par les États membres, cultivera de nouvelles initiatives Équipe Europe et favorisera les synergies entre l'action de l'UE et les missions et opérations relevant de la politique de sécurité et de défense commune dans les pays particulièrement touchés par le terrorisme.

Les **dialogues sur la lutte contre le terrorisme** facilitent les échanges stratégiques avec les pays tiers et devraient conduire à des conclusions claires susceptibles de déboucher sur des actions qui seront effectivement mises en œuvre. Le **réseau d'experts de l'UE en matière de lutte contre le terrorisme** est essentiel au partage d'informations sur la situation en matière de sécurité dans les pays tiers. La haute représentante s'emploiera à renforcer le réseau, en veillant à en étendre la couverture régionale et à intensifier la coopération, pour s'attaquer au lien entre le terrorisme et la criminalité organisée, au financement du terrorisme et à la propagande terroriste.

2.6.4. Renforcer le rôle de l'UE sur la scène multilatérale

La haute représentante, la Commission et le coordinateur de l'UE pour la lutte contre le terrorisme **assureront une coordination étroite au niveau de l'UE et renforceront le rôle moteur joué par l'UE dans les enceintes multilatérales**. L'UE continuera de tirer parti de sa coprésidence du Forum mondial de lutte contre le terrorisme (GCTF) pour faire progresser les actions menées par des civils contre le terrorisme et promouvoir des efforts multilatéraux durables et coordonnés.

L'UE mettra également à profit le rôle qu'elle joue au sein de la coalition internationale de lutte contre Daech pour renforcer la coordination dans la région. L'UE, aux côtés des États membres, jouera un rôle important dans le **réexamen de la stratégie antiterroriste mondiale des Nations unies** en 2026 afin de promouvoir ses valeurs et ses priorités, et continuera de contribuer au **processus de réforme des Nations unies actuellement en cours**, à savoir l'initiative ONU80, qui porte entre autres sur **l'architecture antiterroriste** de l'organisation.

La coopération avec le **Conseil de l'Europe, le Groupe d'action financière (GAFI), Interpol et l'OTAN** sera maintenue sur une base thématique. En collaborant avec des enceintes telles que le Groupe d'action financière et le Forum mondial de lutte contre le terrorisme, l'UE s'attaquera également aux problèmes étroitement entremêlés que posent le financement du terrorisme, le recrutement et la propagande, en particulier sur les réseaux sociaux. Le **Forum mondial de l'internet contre le terrorisme (GIFCT)** continuera lui aussi de compter parmi les partenaires essentiels de la Commission. Enfin, la Commission continuera de coopérer avec la **Fondation de l'appel de Christchurch**[66].

ACTIONS CLÉS

[66] La Fondation de l'appel de Christchurch est une organisation non gouvernementale créée par la Nouvelle-Zélande et la France en réponse à l'horrible attentat terroriste perpétré à Christchurch en 2019, dans le but d'éliminer les contenus terroristes et extrémistes violents en ligne.

La Commission:

- proposera de signer et de conclure le protocole modifiant la définition des infractions terroristes dans la convention du Conseil de l'Europe pour la prévention du terrorisme;
- recommandera au Conseil de l'autoriser à négocier, avec des pays tiers supplémentaires, des accords internationaux sur la coopération avec Eurojust et Europol;
- soutiendra la mise en œuvre du plan d'action conjoint 2025-2030 relatif à la prévention du terrorisme et de l'extrémisme violent dans les Balkans occidentaux et à la lutte contre ces phénomènes;
- étendra les activités du pôle de connaissances aux pays candidats à l'adhésion à l'UE et à la région méditerranéenne;
- tiendra compte des considérations de sécurité dans les programmes relevant de la stratégie «Global Gateway» et augmentera son soutien direct au renforcement des capacités.

La Commission, en coopération avec les États membres:

- recensera régulièrement les projets en matière de lutte contre le terrorisme et de prévention et de lutte contre l'extrémisme violente financés par l'UE et les États membres.

La haute représentante:

- poursuivra la mise en œuvre des dialogues sur la lutte contre le terrorisme en collaboration avec la Commission, le coordinateur de l'UE pour la lutte contre le terrorisme et les États membres;
- renforcera le réseau d'experts de l'UE en matière de lutte contre le terrorisme;
- assurera une coordination étroite au niveau de l'UE et veillera à ce que l'UE joue un rôle moteur dans les enceintes multilatérales, en collaboration avec la Commission et le coordinateur de l'UE pour la lutte contre le terrorisme.

La haute représentante et le Conseil devraient:

- réexaminer régulièrement la position commune 2001/931/PESC (la «liste de l'UE en matière de terrorisme»).

3. Conclusion

Le terrorisme et l'extrémisme violent continuent de menacer la sécurité de l'Europe. Le présent programme définit la réponse de l'UE: un engagement collectif à faire face à ces menaces avec prévoyance, unité et détermination. Il oriente tous nos efforts: **prévention avant que la violence ne s'enracine, protection là où les personnes sont les plus vulnérables et justice contre ceux qui cherchent à nuire.**

Le présent programme permettra à l'Union européenne d'affûter sa capacité collective à anticiper les menaces, à prévenir la radicalisation, à protéger ses citoyens tant en ligne que hors ligne et à réagir fermement en cas d'attentats, en modernisant son approche à l'intérieur et à l'extérieur de ses frontières. Le programme permettra de mener des actions ambitieuses dans tous les piliers, en donnant la priorité à **plusieurs initiatives** qui répondent aux défis émergents, telles que:

- **une boîte à outils en matière de prévention pour lutter contre la radicalisation des mineurs;**
- **un renforcement potentiel du règlement sur les contenus à caractère terroriste en ligne;**

- **une procédure «post-concordance» pour partager les informations relatives aux réponses positives concernant les signalements liés au terrorisme dans le système d'information Schengen et**
- **un nouveau système de recherche de données financières.**

La Commission pilotera et suivra la mise en œuvre dans l'ensemble des piliers et veillera à ce que les instruments, la législation et les financements de l'Union soient utilisés à la hauteur de leur potentiel. Elle informera le Parlement européen, le Conseil, le coordinateur de l'UE pour la lutte contre le terrorisme, les États membres, le secteur privé ainsi que la société civile et les associera à la mise en œuvre du présent programme.