



COMMISSION EUROPÉENNE

Bruxelles, le 25.11.2011
COM(2011) 790 final

**COMMUNICATION DE LA COMMISSION AU PARLEMENT EUROPÉEN ET AU
CONSEIL**

**Premier rapport annuel sur la mise en œuvre de la stratégie de sécurité intérieure de
l'Union européenne**

COMMUNICATION DE LA COMMISSION AU PARLEMENT EUROPÉEN ET AU CONSEIL

Premier rapport annuel sur la mise en œuvre de la stratégie de sécurité intérieure de l'Union européenne

I. Introduction

En juillet de cette année, un extrémiste de droite a commis une effroyable attaque terroriste en Norvège. En août, une saisie record de 1,2 tonne de cocaïne a été effectuée au Royaume-Uni. Dans l'ensemble de l'Union européenne, des cyberattaques causent de plus en plus de dégâts aux systèmes informatiques d'entités publiques et privées. Ces événements sont autant de durs rappels de l'importance d'apporter une riposte aux menaces pesant sur la sécurité intérieure.

La «stratégie de sécurité intérieure de l'UE en action»¹ adoptée en novembre 2010 a présenté les priorités auxquelles l'Union devra s'attacher durant les quatre prochaines années, à savoir: 1) perturber les réseaux criminels internationaux, 2) prévenir le terrorisme et s'attaquer à la radicalisation et au recrutement de terroristes, 3) accroître le niveau de sécurité des citoyens et des entreprises dans le cyberspace, 4) renforcer la sécurité par la gestion des frontières et 5) renforcer la résilience de l'Europe aux crises et aux catastrophes.

L'Union doit être prête à réagir à mesure que les menaces surviennent et évoluent. Des évaluations régulières des menaces et des risques s'imposent de la part d'organismes de l'UE tels qu'Europol, Eurojust, Frontex et le centre de situation conjoint (SitCen).

Le dernier rapport d'Europol² énumère trois menaces émergentes particulièrement préoccupantes.

Premièrement, les problèmes liés à l'évolution rapide de la **technologie de l'internet**. L'internet fait désormais partie du quotidien des citoyens de l'Union et leur est indispensable, mais il devient aussi un canal essentiel pour un large éventail d'activités criminelles et un vecteur de la propagande terroriste. De plus en plus dépendante de la technologie de l'internet, notre société s'en trouve plus vulnérable aux piratages retentissants, qui peuvent viser des administrations, des systèmes de contrôle industriel ou des banques.

Deuxièmement, les répercussions potentielles de la **crise économique actuelle**. Des contraintes financières accrues pourraient réduire les ressources mises à la disposition des pouvoirs publics pour contrer les menaces pesant sur la sécurité intérieure. Il n'existe certes aucune solution évidente et immédiate pour remédier à cette situation, mais nous devons prendre conscience des contraintes et des répercussions qu'elle entraîne.

Troisièmement, l'incidence sur l'Union de la **dimension extérieure de la sécurité**. La sécurité intérieure de l'UE est étroitement liée à celle des pays voisins, comme l'ont démontré les événements récents survenus dans le monde arabe. Ces événements encourageants, porteurs de démocratie et de prospérité pour la région, ont également généré d'importants mouvements

¹ Communication de la Commission intitulée «La stratégie de sécurité intérieure de l'UE en action: cinq étapes vers une Europe plus sûre» — COM(2010) 673/3 (ci-après, la «SSI en action»).

² Voir le rapport d'évaluation de la menace que représente la criminalité organisée (EMCO) publié en 2011 par Europol.

migratoires, accroissant ainsi la pression exercée sur les capacités de gestion des frontières, y compris de la frontière extérieure de l'Union, dans les pays voisins. De même, le déplacement continu de populations et les insuffisances de la gouvernance pourraient créer les conditions propices à l'essor d'activités criminelles et terroristes dans la région du Sahel. Au sud-est de l'Union, les pays des Balkans occidentaux restent une source de préoccupations en raison de la persistance de la criminalité organisée transnationale, telles que le trafic de drogues, la traite des êtres humains et la contrebande de produits de contrefaçon.

La nécessité d'une coopération au niveau de l'UE pour relever ces défis n'a jamais été aussi criante. Il faudra, dans les prochaines années, mettre en œuvre les actions définies. Cela ne suffira pourtant pas. Ces objectifs stratégiques doivent être traduits en plans et actions concrets. À cet égard, la Commission salue la méthode retenue pour le cycle politique «Harmony» de l'UE qui transformera les priorités politiques et les évaluations des menaces en plans d'action opérationnels, essentiellement dans les domaines de la grande criminalité internationale organisée, de la cybercriminalité et de la gestion des frontières, grâce à la mise en œuvre des huit priorités approuvées par le Conseil³.

Tout en faisant progresser la mise en œuvre de la stratégie de sécurité intérieure en action, la Commission continuera à garantir le plein respect de l'État de droit et de la Charte des droits fondamentaux de l'Union européenne, et notamment le droit au respect de la vie privée dont bénéficient les citoyens.

Le rapport ci-après évalue la mise en œuvre en 2011 de la SSI en action. Il décrit l'état de la sécurité intérieure de l'UE au regard de chacun des cinq objectifs de la SSI⁴ et envisage les actions possibles en 2012. Son annexe évalue dans le détail les mesures clés mises en œuvre en 2011.

³ Voir les conclusions du Conseil sur la définition des priorités de l'UE pour la lutte contre la criminalité organisée entre 2011 et 2013; doc. 11050 11/JAI, 396 COSI 46, ENFOPOL 184 CRIMORG 81, ENFOCUSTOM 52 PESC 718 RELEX 603. Voir également l'annexe.

⁴ L'état de la sécurité intérieure a été évalué par Europol avec les contributions d'Eurojust, de Frontex, de la Commission/DG ECHO, notamment sur la base de documents stratégiques – rapport d'évaluation de la menace que représente la criminalité organisée (EMCO) et rapport sur la situation et les tendances du terrorisme en Europe (rapport TE-SAT) publiés par Europol en 2011; analyse annuelle des risques (AAR) et analyse annuelle des risques pour les Balkans occidentaux (AAR BO) effectuées en 2011 par l'agence FRONTEX – et des affaires traitées par Eurojust, telles décrites dans son rapport annuel de 2010.

II. L'état de la sécurité intérieure de l'UE

1. Les réseaux de criminalité organisée et les réseaux criminels internationaux

Un nouveau paysage criminel voit le jour, qui se caractérise de plus en plus par des groupes très mobiles et souples, actifs dans plusieurs pays et secteurs de la criminalité et s'appuyant notamment sur une utilisation illicite à une grande échelle de l'internet. Les groupes les plus nantis ont diversifié leurs activités criminelles lucratives, ce qui améliore leur résilience dans un contexte d'austérité économique et renforce leur aptitude à découvrir et exploiter de nouveaux marchés illicites. La fraude relative aux crédits d'émission de carbone et aux cartes de paiement, ainsi que la contrefaçon de diverses marchandises sont des activités auxquelles les groupes criminels bien établis portent un intérêt croissant, car les risques encourus sont perçus comme faibles.

Bien que les groupes s'adonnant au terrorisme et à la criminalité organisée poursuivent des objectifs différents, les liens entre leurs activités respectives semblent se multiplier. La criminalité est largement utilisée pour financer des activités terroristes⁵. Les groupes terroristes peuvent être directement impliqués dans la criminalité organisée ou liés à des criminels et groupes criminels, dans des domaines tels que le trafic d'armes et de drogues, la traite des êtres humains, ou la fraude financière, le blanchiment d'argent et l'extorsion.

La coopération transfrontière entre les autorités est essentielle pour surmonter les défis qui se posent sous l'angle de la sécurité intérieure de l'Union. Cependant, les instruments disponibles pour l'échange d'informations, et, en particulier, l'initiative suédoise⁶ et les décisions Prüm⁷, ne sont pas encore entièrement mis en œuvre dans les États membres. Il faut encore consolider l'échange transfrontière d'informations entre les services répressifs et en renforcer la cohérence.

Les citoyens européens doivent avoir l'assurance que le démantèlement effectif des réseaux criminels va de pair avec la coordination de poursuites pénales efficaces et équitables. Toutefois, plusieurs instruments relevant du domaine de la coopération judiciaire et policière doivent encore être ratifiés et appliqués par tous les États membres⁸. En outre, les exigences divergentes des États membres en matière de perquisition et de saisie transfrontières peuvent gêner la coordination d'actions urgentes à mener sur plusieurs territoires. La création d'une décision d'instruction européenne étayerait le principe de la reconnaissance mutuelle et résoudrait les difficultés rencontrées actuellement pour obtenir des informations et des preuves dans les affaires comportant un élément d'extranéité.

La valeur globale des avoirs gelés et confisqués dans l'UE reste faible par rapport à la richesse estimée des organisations criminelles. Il faut faire davantage pour localiser et saisir plus efficacement les avoirs d'origine criminelle. Étant donné que la criminalité organisée cherche aujourd'hui à réinvestir ses avoirs dans des activités licites, il y a lieu de durcir la

⁵ Voir le rapport 2011 d'Europol sur la situation et les tendances du terrorisme en Europe (rapport TE-SAT).

⁶ Décision-cadre 2006/960/JAI du Conseil du 18 décembre 2006.

⁷ Décisions 2008/615/JAI et 2008/616/JAI du Conseil (décisions Prüm).

⁸ Comme la convention européenne sur la transmission des procédures répressives de 1972 et la convention relative à l'entraide judiciaire en matière pénale entre les États membres de l'Union européenne de 2000.

réglementation pour lutter contre le blanchiment de capitaux, et d'axer davantage l'action sur les moyens par lesquels les criminels infiltrent l'économie légale.

En 2011, pour consolider les outils dont l'Union dispose pour combattre la criminalité organisée, la Commission a notamment adopté un train de mesures anticorruption et a présenté une proposition législative relative à la collecte des données des passagers (PNR) empruntant des vols à destination et au départ du territoire de l'UE.

Pistes à suivre en 2012

La Commission entend:

- adopter un train de mesures concernant la confiscation et le recouvrement des avoirs d'origine criminelle;
- présenter une proposition de réforme d'Europol et du CEPOL, ainsi qu'un programme de formation européen;
- présenter une proposition de réforme d'Eurojust;
- conclure deux nouveaux accords PNR avec les États-Unis et le Canada;
- poursuivre ses travaux en vue de l'adoption de sa proposition de directive relative à la collecte des données des passagers aériens;
- présenter une communication sur un modèle européen d'échange d'informations;
- élaborer une stratégie en matière d'enquêtes financières;
- présenter une proposition de révision de la directive sur la lutte contre le blanchiment d'argent et le financement du terrorisme; et
- publier une stratégie quinquennale de lutte contre la traite des êtres humains.

Les États membres sont encouragés:

- à mettre en œuvre les actions prévues dans le cycle politique de l'UE;
- à redoubler d'efforts pour élaborer une approche administrative associant tous les organes du secteur public, et pas uniquement les services répressifs, afin de protéger l'économie contre la criminalité et la corruption;
- à poursuivre leurs travaux en vue de mettre en place des bureaux de recouvrement des avoirs pleinement efficaces et de faciliter les échanges d'informations et des meilleures pratiques;
- à ratifier et à mettre en œuvre les instruments actuels de coopération judiciaire et policière et d'échange d'informations, en particulier l'initiative suédoise, la directive sur la conservation des données, les décisions Prüm, ainsi que la convention sur la transmission des procédures répressives et la convention relative à l'entraide judiciaire en matière pénale; et
- à transposer sans tarder la directive relative à la lutte contre la traite des êtres humains.

2. Le terrorisme et la radicalisation

Une décennie après les événements du 11 Septembre, les statistiques relatives aux auteurs présumés d'actes terroristes indiquent que le terrorisme islamiste reste la menace prédominante pour l'UE. Cependant, les événements tragiques survenus en Norvège en juillet nous rappellent que la menace terroriste ne se cantonne pas à un ensemble d'idéologies ou de motivations politiques ou religieuses. Le réseau de première intervention, constitué à la suite des attentats perpétrés à Londres en 2005, a été mobilisé pour la première fois lors de l'attaque commise en Norvège et s'est avéré utile.

Le terrorisme endogène et la radicalisation de citoyens de l'Union sont une source de préoccupation croissante. L'Union doit anticiper l'évolution tant du point de vue du processus de radicalisation que des technologies utilisées. Le réseau de sensibilisation à la radicalisation de l'UE, qui a été lancé en septembre 2011, a pour mission de faciliter le partage des connaissances, de contribuer à la sensibilisation et de dégager des solutions nouvelles et créatives pour combattre l'extrémisme violent. La Commission veillera à l'adoption d'une approche cohérente, avec le SEAE et le coordinateur de la lutte contre le terrorisme, pour réprimer l'extrémisme violent à la fois dans l'Union et à l'extérieur de celle-ci.

Le risque de radicalisation d'individus ne saurait être entièrement écarté. Par conséquent, les initiatives visant à empêcher les terroristes d'avoir accès aux sources de financement et à certaines substances, ainsi qu'à améliorer la sûreté des transports sont déterminantes pour la lutte contre le terrorisme. En 2010, la Commission a proposé un plan d'action de l'Union pour renforcer la sûreté du fret aérien, établissant de nouvelles règles et définissant des critères permettant de détecter le fret à haut risque, et elle a maintenant atteint le stade final de l'élaboration d'une évaluation des risques pour la sûreté de l'aviation à l'échelle de l'UE. Par ailleurs, la prévention des actes terroristes et les poursuites contre leurs auteurs seraient facilitées par une amélioration des échanges d'informations avec Europol et Eurojust.

Pistes à suivre en 2012

La Commission entend:

- **organiser une conférence à haut niveau sur la lutte contre l'extrémisme violent, avec le soutien du réseau de sensibilisation à la radicalisation de l'UE;**
- **préparer une série de propositions sur l'utilisation de l'internet par les terroristes, explorant les moyens de riposte à la radicalisation en ligne;**
- **proposer un instrument législatif autorisant le gel d'avoirs pour réprimer le terrorisme et les activités qui y sont associées;**
- **réexaminer la directive concernant la désignation des infrastructures critiques européennes;**
- **présenter un rapport à mi-parcours sur la mise en œuvre du plan d'action de l'UE dans le domaine CBRN et réexaminer le plan d'action de l'UE relatif aux explosifs; et**
- **présenter les options envisageables pour la création d'un système européen de surveillance du financement du terrorisme, sur la base de discussions avec le Conseil et le Parlement européen; et**
- **proposer des options pour le renforcement de la sûreté des transports, axées notamment sur les questions relatives au transport terrestre.**

Les États membres sont encouragés:

- **à mettre en œuvre le plan d'action en matière de sûreté du fret aérien; et**
- **à redoubler d'efforts pour combattre l'extrémisme violent.**

3. La cybercriminalité et la cybersécurité

L'Union est une cible toute désignée pour la cybercriminalité en raison notamment de son infrastructure internet avancée, de son grand nombre d'internautes et de l'intervention croissante de l'internet dans les transactions commerciales et les systèmes de paiement. Le rythme et la sophistication de l'évolution des technologies expliquent que la cybercriminalité soit en mutation constante. Les nouvelles tendances technologiques, comme l'essor de l'informatique en nuage et l'utilisation accrue de dispositifs mobiles, créent d'autres menaces pour les utilisateurs et amplifient les défis que les services répressifs ont à relever⁹. L'usage très répandu de la technologie de l'internet dans l'UE s'est également traduit par une expansion sans précédent du marché des contenus pédopornographiques et des vols de propriété intellectuelle.

L'internet ignore les frontières mais les compétences en matière de répression de la cybercriminalité sont, elles, limitées au territoire national. Les États membres doivent donc unir leurs efforts à l'échelon de l'UE pour définir une stratégie commune. À cet effet, il conviendrait d'exploiter plus largement les capacités existantes des agences de l'Union. Grâce à une coopération avec ses partenaires internationaux, l'Union sera également plus forte pour faire face à la cybercriminalité.

En 2011, des progrès ont été enregistrés en ce qui concerne les préparatifs de la création du centre européen de lutte contre la cybercriminalité, ainsi que l'assistance offerte aux États membres pour la mise en place d'équipes nationales/publiques d'intervention en cas d'urgence informatique. Le groupe de travail UE/USA sur la cybercriminalité est parvenu à des résultats, tant en matière de coopération pour la lutte contre la pédopornographie que d'exercices conjoints de prévention des cyberattaques.

Pistes à suivre en 2012

La Commission entend:

- **élaborer une stratégie européenne globale pour la sécurité de l'internet;**
- **prendre toutes les dispositions utiles à la configuration du centre européen de lutte contre la cybercriminalité devant être mis en place d'ici 2013; et**
- **s'appuyer sur les travaux du groupe de travail UE/USA sur la cybersécurité et la cybercriminalité, et établir une coopération avec d'autres partenaires internationaux.**

⁹ Voir le rapport d'évaluation de la menace que représente la criminalité organisée facilitée par l'internet, publié en 2011 par Europol.

Les États membres sont encouragés:

- **à mettre en œuvre les actions prévues dans le cycle politique de l'UE;**
- **à poursuivre les efforts qu'ils déploient pour favoriser une sensibilisation à la cybercriminalité au niveau national, développer leurs capacités de formation et créer des centres d'excellence;**
- **à ratifier la convention du Conseil de l'Europe sur la cybercriminalité¹⁰;**
- **à constituer des équipes nationales/gouvernementales d'intervention en cas d'urgence informatique (CERT) et à créer un réseau fonctionnant bien;**
- **et à améliorer les dispositifs de signalement en matière de cybercriminalité.**

4. La gestion des frontières

Tout au long de 2011, les États membres et Frontex ont redoublé d'efforts pour faire face aux pressions accrues exercées sur les frontières extérieures de l'UE. Depuis le lancement de l'«opération Hera» en 2006, Frontex a réussi à bloquer la filière d'immigration illégale qui partait d'Afrique du Nord à destination des îles Canaries. La frontière orientale de l'UE demeure le théâtre d'une contrebande massive. Cette année, la Commission a toutefois présenté une série de mesures à prendre pour s'attaquer à ce problème¹¹. La frontière maritime en Méditerranée et la frontière terrestre avec la Turquie sont et devraient rester des lieux clés d'entrée clandestine dans l'Union.

À la suite des événements survenus récemment en Afrique du Nord, plus de 50 000 migrants sont entrés dans l'UE en franchissant la frontière maritime en Méditerranée, souvent avec l'aide de réseaux criminels. Le déploiement en février 2011 de l'opération conjointe «Hermes» coordonnée par Frontex a joué un rôle déterminant dans l'organisation des patrouilles le long de cette route migratoire. De même, l'équipe d'intervention rapide aux frontières (RABIT) mise en place par Frontex, qui a pour la première fois apporté son soutien pour la gestion de la frontière terrestre gréco-turque, a contribué à une réduction de 75 % du nombre de franchissements illégaux de la frontière pendant son déploiement.

En janvier 2011, la Commission a présenté le cadre du système européen de surveillance des frontières (EUROSUR). En collaboration avec six États membres, Frontex a lancé un projet pilote à la frontière extérieure terrestre et maritime. La Commission s'en est inspirée pour élaborer sa proposition législative relative à l'EUROSUR qu'elle devrait présenter en décembre 2011, dans le but que ce système soit opérationnel en 2013.

La gestion des frontières extérieures doit à la fois renforcer la sécurité et faciliter les déplacements. C'est sous l'angle de ces objectifs que la Commission a présenté en 2011 des propositions visant à améliorer le système d'évaluation et de suivi de Schengen, ainsi qu'une analyse de la mise en place éventuelle d'un système d'entrée/sortie et d'un programme d'enregistrement des voyageurs, répondant ainsi à une demande du Conseil.

¹⁰ L'Autriche, la Belgique, la République tchèque, la Grèce, l'Irlande, le Luxembourg, Malte, la Pologne et la Suède n'ont pas encore ratifié la convention.

¹¹ http://ec.europa.eu/anti_fraud/documents/Working-paper.pdf

Pistes à suivre en 2012

La Commission entend:

- **présenter des propositions basées sur les résultats des discussions relatives à la communication sur les frontières intelligentes (système d'entrée/sortie et programme d'enregistrement des voyageurs); et**
- **suggérer des mesures pour améliorer la coordination des vérifications aux frontières effectuées par les différents services nationaux (police, gardes-frontières et douaniers).**

Les États membres sont encouragés:

- **à mettre en œuvre les actions prévues dans le cycle politique de l'UE;**
- **à poursuivre leurs efforts en vue de la mise en place de l'EUROSUR; et**
- **à participer activement aux dialogues sur la migration, la mobilité et la sécurité avec les nouveaux gouvernements formés en Afrique du Nord et au Moyen-Orient.**

5. La gestion des crises et des catastrophes

Ces dernières années, les citoyens européens ont connu plusieurs catastrophes, d'origine naturelle et humaine. Ils restent sous la menace de la perpétration d'actes malveillants, tels que des attentats ou des cyberattaques, et de la dissémination hostile ou accidentelle d'agents infectieux et pathogènes. Le tremblement de terre qui a frappé Aquila en Italie, la crise liée au nuage de cendres formé à la suite d'une éruption volcanique en Islande et l'attaque terroriste commise en juillet en Norvège soulignent davantage encore la nécessité pour l'Union de renforcer sa capacité de gestion des crises et des catastrophes. Par ailleurs, l'accident de Fukushima a révélé non seulement l'éventualité d'un enchaînement d'événements – un tremblement de terre à l'origine d'un tsunami lui-même suivi d'une crise nucléaire – mais aussi l'impact planétaire potentiel de ces événements, par exemple sur le transport international, les douanes et la sûreté alimentaire, ce qui appelle des solutions élaborées de gestion des risques.

La complexité et l'ampleur de ces défis nécessitent l'adoption d'une approche globale en matière d'évaluation des risques et d'élaboration des prévisions, ainsi qu'en ce qui concerne la prévention des catastrophes, la préparation à celles-ci et l'atténuation de leurs effets. L'Union et ses États membres doivent à cette fin combiner les politiques, instruments et services divers auxquels ils peuvent recourir.

Europol, Frontex, le centre de situation conjoint de l'UE (SitCen) et le centre de suivi et d'information géré par la Commission permettent à l'Union de mobiliser certaines capacités et expertises en matière de collecte de données, d'analyse, d'évaluation des menaces et de réaction d'urgence, dans divers domaines liés à la sécurité intérieure. Cependant, l'un des principaux défis qu'elle aura à relever dans les prochaines années consistera à passer progressivement à une politique cohérente de gestion des risques, associant l'évaluation des menaces et des risques à la formulation et à la mise en œuvre des politiques. Au cours de 2011, de premières démarches ont été effectuées en ce sens.

Pistes à suivre en 2012

La Commission entend:

- contribuer à la poursuite de l'élaboration d'une politique européenne d'évaluation des menaces et des risques, et présenter une vue d'ensemble des principaux risques d'origine naturelle et humaine auxquels l'Union pourrait être exposée à l'avenir;
- amplifier ses capacités d'évaluation stratégique, notamment en rassemblant l'expertise des différents acteurs (Europol, Frontex et SitCen) dans le domaine de la sécurité intérieure; et
- présenter une proposition conjointe sur la mise en œuvre de la clause de solidarité avec la haute représentante de l'Union pour les affaires étrangères et la politique de sécurité.

Les États membres sont encouragés:

- à procéder régulièrement à des évaluations des menaces et des risques; et
- à s'allier aux efforts d'accroissement de la capacité de réaction européenne aux catastrophes.

III. Conclusion

Le présent rapport sur la sécurité intérieure de l'UE met en lumière certaines des questions qui doivent être approfondies par le Parlement européen, les États membres, la Commission et la société en général.

Les menaces mises en évidence en novembre 2010 dans la SSI en action ne sont pas d'une moindre ampleur en 2011 et devraient rester la principale cible de l'action de l'UE en matière de sécurité intérieure.

Des progrès considérables ont été réalisés dans le domaine de la **lutte contre la criminalité organisée**, en particulier grâce à la proposition législative de l'UE sur la collecte des données des passagers empruntant des vols à destination ou au départ du territoire de l'UE, et grâce au train de mesures anticorruption. Des progrès supplémentaires doivent être accomplis dans la coopération entre les autorités judiciaires et répressives, et dans l'élaboration d'une approche administrative de la répression des formes graves de criminalité.

En matière de **terrorisme** et de **radicalisation**, une des réalisations à noter en particulier est la mise en place du réseau européen de sensibilisation à la radicalisation. L'adoption d'une communication relative à un système européen de surveillance du financement du terrorisme constitue aussi une étape importante. Cependant, il y a lieu de consentir des efforts supplémentaires en vue de définir un cadre pour les mesures administratives liées au gel des avoirs des terroristes et pour améliorer la sécurité des transports terrestres.

Les actions de lutte contre la **cybercriminalité** se développent bien. Des progrès ont été accomplis en vue de la mise en place du centre européen de lutte contre la cybercriminalité et de la constitution d'équipes d'intervention en cas d'urgence informatique. Plusieurs États membres doivent prendre d'urgence des dispositions pour ratifier la convention de Budapest.

Dans le domaine de la **gestion des frontières**, la mise sur pied de l'EUROSUR est en bonne voie, mais il convient de poursuivre les discussions sur les propositions relatives aux

frontières intelligentes et de continuer les travaux visant à améliorer la coopération interservices au niveau national.

Les actions liées à la **gestion des crises et des catastrophes** ont également progressé. Des travaux ont été entrepris en 2011, par exemple, dans le domaine de l'évaluation des risques. Toutefois, dans le domaine de la gestion des crises, des efforts supplémentaires sont nécessaires pour atteindre l'objectif fixé. Il est essentiel que les États membres, la Commission et le SEAE s'engagent et coopèrent pleinement.

Des travaux poussés ont été accomplis pour jeter des ponts entre la sécurité intérieure et la sécurité extérieure. Plusieurs initiatives ont été lancées pour favoriser la coopération et la coordination: il s'agit notamment de la coopération opérationnelle en matière de terrorisme, de criminalité transnationale et de migration irrégulière dans les Balkans occidentaux, la Corne de l'Afrique et le Sahel. En outre, le SEAE et la Commission ont élaboré un document conjoint sur le renforcement des liens entre les acteurs associés à la politique de sécurité et de défense commune (PSDC) et ceux qui œuvrent dans le domaine de la liberté, de la sécurité et de la justice (JAI), et notamment sur les possibilités de coopération entre les missions de police menées dans le cadre de la PSDC et Europol.

Enfin, la réussite de toute stratégie dépend de sa capacité à produire des résultats concrets. Pour la SSI en action, l'année 2011 a constitué un début prometteur. Il y aura toutefois encore beaucoup à faire au cours des trois années restantes pour garantir la sécurité du citoyen européen. D'ici au prochain rapport annuel, des progrès doivent être réalisés dans tous les domaines prioritaires, et notamment en matière de lutte contre la grande criminalité organisée et contre la menace croissante qui pèse sur les systèmes informatiques.

Annexe

La mise en œuvre des cinq objectifs de la SSI en 2011

La présente annexe fait le point sur la mise en œuvre des cinq priorités de la stratégie de sécurité intérieure en action, en fournissant des informations sur les principaux résultats attendus en 2011 et en présentant un tableau illustrant l'état d'avancement des mesures prévues dans le cadre de chaque objectif.

Depuis l'adoption de la SSI en action en 2010, le Conseil a également adopté, pour la période 2011-2013, le cycle politique «Harmony» de l'UE pour lutter contre la criminalité organisée. Ce dernier comprend huit priorités axées sur la lutte contre la grande criminalité organisée et la cybercriminalité, ainsi que sur le renforcement de la gestion des frontières¹². Cette méthodologie est une étape importante pour traduire les priorités politiques et la SSI en des mesures donnant des résultats collectifs concrets pour la sécurité intérieure.

Objectif 1 — Perturber les réseaux criminels internationaux

Les données relatives aux passagers aériens (PNR) dans l'UE

En février 2011, la Commission a présenté une proposition législative sur la collecte des données relatives aux passagers (PNR) empruntant des vols à destination ou au départ du territoire de l'Union. L'objectif en est de permettre aux autorités compétentes des États membres d'analyser ces données en vue de prévenir et de mettre au jour les infractions terroristes et les actes graves de criminalité, ainsi que de poursuivre leurs auteurs. Cette proposition est actuellement soumise à l'examen du Parlement européen et du Conseil. Elle fait partie d'une politique plus large en matière de données PNR qui comprend la conclusion d'accords avec des pays tiers dans ce domaine. Ces accords permettent aux services répressifs de ces pays d'utiliser les données PNR en provenance de l'UE aux mêmes fins. Les accords en

¹² Le cycle politique «Harmony» de l'UE englobe les huit priorités suivantes:

1. affaiblir la capacité des groupes criminels organisés présents ou basés en Afrique occidentale d'acheminer clandestinement la cocaïne et l'héroïne dans l'UE;
2. limiter le rôle des Balkans occidentaux en tant que zone clé pour le transit et le stockage des produits illicites destinés à l'UE et centre logistique pour les groupes criminels organisés, notamment ceux de langue albanaise;
3. affaiblir la capacité des groupes criminels organisés de faciliter l'immigration illégale à destination de l'UE, en particulier à travers l'Europe méridionale, sud-orientale et orientale et notamment à la frontière gréco-turque et dans des zones de crise de la Méditerranée proches de l'Afrique du Nord;
4. réduire la production et la distribution dans l'UE de drogues de synthèse, notamment de nouvelles substances psychoactives;
5. démanteler les filières d'envoi conteneurs à destination de l'UE, notamment par voie maritime et aérienne, de produits illicites tels que la cocaïne, l'héroïne, le cannabis, les contrefaçons et les cigarettes;
6. lutter contre toutes les formes de traite des êtres humains et de trafic de migrants en ciblant les groupes criminels organisés qui mènent ces activités criminelles sur les plateformes de la criminalité situés au sud, au sud-ouest et au sud-est de l'UE;
7. réduire d'une manière générale le potentiel des groupes criminels organisés mobiles (itinérants) à entreprendre des activités criminelles;
8. intensifier la lutte contre la cybercriminalité et l'utilisation de l'internet à des fins délictueuses par des groupes criminels organisés.

vigueur avec le Canada et les États-Unis sont actuellement en cours de renégociation, tandis qu'un nouvel accord avec l'Australie a été signé en septembre 2011.

Dans le programme de travail annuel 2012¹³ adopté au titre du programme «Prévenir et combattre la criminalité (ISEC)», la Commission a prévu un montant de 25 millions d'euros pour le financement de la création d'unités PNR dans les États membres.

Les équipes communes d'enquête

Pour soutenir la constitution d'équipes communes d'enquête - en particulier à brève échéance - et apporter une contribution positive et pratique à la lutte contre la criminalité transfrontière, la Commission a prévu un deuxième cycle de financement, d'un montant de 2,1 millions d'euros, pour le projet d'Eurojust appelé «Favoriser un recours plus important aux équipes communes d'enquête». Ce projet soutient la création de nouvelles équipes communes d'enquête ainsi que le fonctionnement des équipes existantes en améliorant leur accès à l'aide financière qui sera disponible dans les années à venir. Au cours de la première année, le projet actuel d'Eurojust a soutenu 33 équipes communes d'enquête chargées d'enquêter sur des infractions telles que le trafic de drogues, la traite des êtres humains, l'immigration clandestine, la criminalité liée au trafic de véhicules volés, la cybercriminalité et la criminalité financière. Europol a également contribué à la constitution et aux travaux d'équipes communes d'enquête grâce à son réseau sûr et rapide de communication et d'échange d'informations et à ses capacités d'appui logistique et de police scientifique, ainsi qu'à ses capacités en matière d'analyse.

Exemple 1:

Eurojust a notamment apporté son concours à la création d'une équipe commune d'enquête associant l'Allemagne et la Roumanie, chargée d'enquêter sur les activités d'un groupe criminel organisé impliqué dans la traite des êtres humains. Par suite de cette enquête, 50 personnes ont été inculpées de traite d'êtres humains et de délits connexes, six auteurs ont été condamnés jusqu'à présent, 148 témoins ont été interrogés et une somme de 860 000 euros a été saisie (argent liquide et autres biens). Dans le cadre du projet concernant le financement des équipes communes d'enquête, Eurojust a couvert les frais de voyage et d'hébergement des membres de cette équipe, ce qui leur a permis d'établir une communication directe et de mener les actions communes susmentionnées. Eurojust a également fourni une aide financière pour la traduction de documents relatifs à l'enquête.

Exemple 2:

Une équipe commune d'enquête multilatérale, coordonnée par Eurojust, a contribué de façon déterminante à la réussite d'une enquête et à l'ouverture de poursuites concernant un trafic de cocaïne à grande échelle entre l'Amérique du Sud et l'Europe. La convention instituant cette équipe a été conclue pour une période initiale de six mois, prolongée à plusieurs reprises pour permettre aux enquêteurs de poursuivre leurs travaux qui ont duré plus de deux ans. Les services d'enquête et les autorités

¹³ C(2011) 6306 final; adopté le 19 septembre 2011.

judiciaires participant à l'équipe commune d'enquête se sont réunis régulièrement pour arrêter des stratégies communes et ont échangé des informations et des éléments de preuve sans devoir subir les retards enregistrés dans le cadre des demandes d'entraide judiciaire traditionnelles. Les procureurs et les services répressifs du pays X étaient présents pendant les auditions des suspects dans le pays Y. La désignation de responsables habilités à diriger l'équipe dans son ensemble lorsqu'elle mène des activités dans leur propre pays a facilité l'exécution rapide de mesures de coopération entre les autorités judiciaires et les services répressifs sur différents territoires. Eurojust a coordonné les travaux de l'équipe commune d'enquête lors de réunions organisées à La Haye, en pouvant compter sur la participation active d'Europol et son concours en matière d'analyse. Les ressources financières accordées à cette équipe par Eurojust ont servi à couvrir notamment les frais d'interprétation, de traduction de documents, de voyage et d'hébergement. Eurojust a également fourni des dispositifs permettant une communication sécurisée entre les membres de l'équipe. L'équipe a concouru à l'arrestation de quelque 30 principaux suspects dans le monde, ainsi qu'à la saisie de plus de 1 000 kg de cocaïne et d'actifs estimés à plusieurs millions d'euros.

Depuis février 2011, le secrétariat du réseau d'équipes communes d'enquête a pris ses fonctions au sein d'Eurojust¹⁴, qui consistent à contribuer à la sensibilisation, à résoudre les problèmes et à organiser l'échange des meilleures pratiques entre les concernés. Certaines dispositions de la décision révisée relative à Eurojust, qui subordonnent l'octroi d'un financement communautaire aux équipes communes d'enquête à une invitation d'Eurojust à y participer (article 9 septies) et qui font obligation aux États membres d'informer Eurojust de la constitution d'une équipe commune d'enquête (article 13, paragraphe 5) permettront de se faire une idée plus précise de toutes les équipes créées dans l'Union.

La lutte contre la corruption

La corruption a longtemps été considérée comme un problème principalement national. Au fil du temps, il est devenu évident qu'elle avait également des effets transfrontières et ne pouvait être réprimée avec succès par des actions isolées. La criminalité organisée transfrontière a souvent recours à la corruption pour infiltrer plus facilement le système judiciaire. Les législations et institutions nécessaires pour s'attaquer à la corruption sont largement en place, mais la mise en œuvre des politiques de lutte contre ce phénomène reste inégale dans l'UE. Le programme de Stockholm demande à la Commission d'élaborer des indicateurs pour mesurer les efforts consentis par les États membres pour combattre la corruption.

En juin 2011, la Commission a adopté un ensemble de mesures anticorruption qui créent un mécanisme d'établissement de rapports à l'échelle de l'Union (ci-après, le «rapport anticorruption de l'UE») destiné à évaluer périodiquement les efforts déployés par les États membres contre la corruption. Le rapport anticorruption de l'UE procédera à une évaluation

¹⁴ Décision 2002/187/JAI du Conseil du 28 février 2002 instituant Eurojust afin de renforcer la lutte contre les formes graves de criminalité, modifiée par la décision 2003/659/JAI du Conseil et par la décision 2009/426/JAI du Conseil du 16 décembre 2008 sur le renforcement d'Eurojust.

des réalisations, échecs et points vulnérables des États membres, en vue de renforcer la volonté politique de mettre en œuvre de véritables approches de tolérance zéro face à la corruption, d'encourager l'apprentissage par les pairs et de faciliter l'échange de meilleures pratiques. La Commission publiera ce rapport tous les deux ans, à partir de 2013. Il sera axé sur des questions transversales, décrira les tendances observées dans l'Union et fournira des analyses et des recommandations pour chaque pays.

Dans le cadre du train de mesures anticorruption, un rapport de la Commission sur la participation de l'Union européenne au groupe d'États contre la corruption (GRECO) créé par le Conseil de l'Europe analyse différents moyens pour renforcer la coopération entre l'UE et le GRECO, en concluant que l'adhésion de l'Union au GRECO est la meilleure voie à suivre pour atteindre les objectifs du programme de Stockholm. Sur la base de ces constats, la Commission demandera au Conseil l'autorisation d'entamer des négociations en vue de la participation de l'Union au GRECO. Des synergies seraient ainsi créées entre le système d'évaluation du GRECO et le rapport anticorruption de l'UE, et une approche cohérente de la lutte contre la corruption serait adoptée au niveau européen.

Avec le soutien financier du programme «Prévenir et combattre la criminalité (ISEC)», l'ONG Transparency International a effectué une recherche comparative entre États membres de l'Union européenne pour évaluer la pertinence des délais de prescription dans le domaine de la lutte contre la corruption (projet achevé en mars 2011). En vue de recenser à la fois les faiblesses et les meilleures pratiques en matière de prescription, cette recherche examine la situation dans les 27 États membres (analyses approfondies pour 11 d'entre eux et état des lieux général pour les 16 autres). Eu égard aux résultats de cette recherche, Transparency International demandera l'adoption, au besoin, des meilleures pratiques recensées¹⁵.

La confiscation et le recouvrement des avoirs d'origine criminelle

Afin de récupérer les avoirs d'origine criminelle, la Commission proposera une législation¹⁶ destinée à renforcer le cadre juridique de l'UE¹⁷ concernant la confiscation et le recouvrement de ces avoirs dans l'Union européenne, ainsi que le renforcement de la reconnaissance mutuelle des décisions de gel et de confiscation dans le domaine de la grande criminalité.

¹⁵ Countdown to Impunity: Corruption-related Statutes of Limitation in the European Union (EU) (Compte à rebours vers l'impunité: délais de prescription liés à la corruption dans l'Union européenne (UE) — JLS/2008/ ISEC 100.

¹⁶ Adoption prévue en 2012.

¹⁷ Décisions-cadres 2001/500/JAI concernant le blanchiment d'argent et la confiscation, 2005/212/JAI relative à la confiscation élargie, 2003/577/JAI et 2006/783/JAI sur la reconnaissance mutuelle des décisions de gel et de confiscation, respectivement.

Grâce au programme ISEC, l'Union a aidé les États membres à créer et à renforcer leur bureau de recouvrement des avoirs (BRA). Par exemple, un projet financé par ce programme a permis, en 2010, la mise en place du bureau hongrois de recouvrement des avoirs, et notamment l'élaboration de nouvelles méthodes de travail sur la base des meilleures pratiques recensées dans d'autres États membres¹⁸. Ce projet et d'autres qui sont en cours, visant à encourager l'échange des meilleures pratiques entre les bureaux de recouvrement des avoirs (par exemple, CEART, FENIX), sont régulièrement présentés aux professionnels concernés lors des réunions de la plateforme des BRA de l'UE.

¹⁸ Élaboration de méthodes et de techniques d'enquête dans le domaine du recouvrement des avoirs — JLS/2008/ ISEC/FPA/C1/018.

État d'avancement – tableau récapitulatif de l'ensemble des objectifs et actions de la SSI

OBJECTIF 1: Perturber les réseaux criminels internationaux			
	Action 1: Découvrir et démanteler les réseaux criminels	Action 2: Protéger l'économie contre l'infiltration par les réseaux criminels	Action 3: Confisquer les avoirs d'origine criminelle
2011	<p>Proposition concernant l'utilisation des données relatives aux passagers aériens de l'UE (PNR)</p>	<p>Proposition relative au suivi et au soutien des mesures prises par les États membres pour lutter contre la corruption</p> <p>Mise en place d'un réseau de points de contact nationaux pour les instances gouvernementales et réglementaires en matière d'approche administrative</p>	<p>Proposition[s] de la Commission en vue d'une directive sur la confiscation et la récupération des avoirs criminels et [d'un règlement] sur l'application du principe de reconnaissance mutuelle des décisions de gel et de confiscation</p>
2012	<p>Lignes directrices sur l'utilisation de registres centraux des comptes bancaires pour suivre les mouvements des fonds d'origine criminelle</p> <p>Stratégie de l'UE en matière d'enquêtes financières: une approche intégrée pour prévenir et détecter la manifestation des menaces criminelles modernes dans l'économie légale, ainsi que pour les éradiquer</p>		
2013	<p>Révision éventuelle de la législation antiblanchiment de l'UE afin de permettre l'identification des propriétaires d'entreprises et de comptes fiduciaires</p>		<p>Indicateurs communs pour évaluer les résultats des bureaux de recouvrement des avoirs et lignes directrices pour empêcher les groupes criminels de récupérer les avoirs confisqués</p>
2014	<p>Code des couleurs: <u>Vert</u>: action (devant être) terminée en 2011 <u>Jaune</u>: action en cours <u>Rouge</u>: action non entamée</p>		<p>Mise en place de bureaux efficaces de recouvrement des avoirs et élaboration de dispositions nécessaires à la gestion des avoirs</p>

Intensification du recours aux équipes communes d'enquête à court terme

Actions visant à faire respecter les droits de propriété intellectuelle et à lutter contre la vente de marchandises de contrefaçon sur l'internet

Objectif 2 – Prévenir le terrorisme et s’attaquer à la radicalisation et au recrutement de terroristes

Le réseau européen de sensibilisation à la radicalisation

La Commission a mis en place le réseau européen de sensibilisation à la radicalisation (RSR), en partenariat avec le Comité des régions. Le RSR a été inauguré le 9 septembre 2011 par Madame Cecilia Malmström, commissaire chargée des affaires intérieures. Il s’agit d’un groupement à l’échelon de l’UE de réseaux des professionnels engagés dans la lutte contre les formes violentes d’extrémisme, qui réunit des décideurs politiques, des agents des services répressifs et de sécurité, des autorités locales, des universitaires, des experts de terrain et des organisations de la société civile, y compris des groupes de victimes. Les principaux objectifs de ce réseau sont de mettre en commun les expériences, les connaissances et les bonnes pratiques, et en particulier:

- de permettre la communication et le travail en réseau entre les membres du RSR afin d’accroître la sensibilisation à la radicalisation et d’améliorer les techniques de communication et, partant, de s’opposer à la diffusion des idées terroristes;
- de recenser, de tester, d’évaluer et de comparer les approches et les enseignements tirés de la lutte contre les formes violentes d’extrémisme; et
- d’informer les responsables de l’élaboration des politiques, tant au niveau de l’UE qu’au niveau des États membres, et de constituer un canal de communication entre la Commission et les professionnels de première ligne.

Par le biais de l’ISEC, la Commission a soutenu le travail des organisations de la société civile et des organisations publiques qui mettent au jour, traduisent et contestent la propagande terroriste, et notamment ses manifestations sur l’internet.

Afin de renforcer la coopération opérationnelle dans la lutte contre les activités terroristes sur l’internet, la Commission a financé un certain nombre de projets tels que le projet multilatéral, dirigé par l’Allemagne, consacré à l’étude des sites web extrémistes islamistes en Europe («Exploring the Islamist Extremist Web of Europe»), qui vise plus particulièrement les contenus terroristes ciblant les jeunes Européens.

En outre, les fonds de l’ISEC ont été également utilisés pour financer un dialogue public/privé visant à mettre au point un code de conduite européen volontaire décrivant les bonnes pratiques pour la coopération entre les services répressifs et le secteur privé, notamment les fournisseurs de services internet, ainsi que les opérateurs de réseau et les permanences téléphoniques pour les plaintes.

La Commission a également utilisé les fonds de l’ISEC pour aider les responsables de l’élaboration des politiques et renforcer les capacités des services répressifs de l’UE grâce à un certain nombre d’études, dont une consacrée aux méthodologies et aux outils technologiques permettant de détecter efficacement les contenus violents sur l’internet et de retrouver leurs auteurs, qui devrait livrer ses résultats pour la fin de 2011 et permettre de rechercher et de poursuivre plus facilement les responsables de contenus illégaux.

L'extraction et l'analyse des données de messagerie financière (le SFFT de l'UE)

L'Union a signé avec les États-Unis l'accord sur le programme de surveillance du financement du terrorisme (*US Terrorist Financing Tracking Programme*, US TFTP), qui fournit le cadre légal nécessaire au transfert de données de messagerie financière à partir de l'Union européenne vers les États-Unis aux fins de la lutte antiterroriste. Une analyse réalisée en mars 2011 a démontré l'efficacité de cet accord dans la lutte contre le terrorisme. Une communication relative à un système européen de surveillance du financement du terrorisme (SFFT) a également été adoptée en juillet 2011, qui expose les principales options envisageables pour la mise en place d'un tel système et souligne les grandes questions qui doivent encore être résolues avant qu'un système puisse être proposé officiellement. Cette communication vise à susciter un débat avec le Parlement européen et le Conseil, et la Commission attendra l'issue de ces discussions avant de présenter une proposition législative.

La sécurité des transports

Les secteurs du transport maritime et du transport aérien ont déjà démontré la valeur ajoutée que peuvent apporter de bons mécanismes de communication et de coordination, ainsi que des règles de sécurité communes au niveau de l'UE, compte tenu de la nature transfrontière du domaine des transports. La communication prochaine de la Commission sur la sécurité des transports visera principalement la mise en place d'une approche équivalente dans l'UE de la sécurité des transports terrestres. Elle insistera également sur la nécessité de doter les transports de systèmes appropriés (mesures préventives, planification de plans d'urgence pour gérer les incidents liés à la sécurité, plans de reprise, formations, etc.) et mettra l'accent sur la fixation d'objectifs à atteindre en matière de sécurité, plutôt que sur la définition de normes à respecter pour le secteur des transports.

Afin de faciliter l'élaboration d'une politique dans ce domaine, un groupe consultatif sur la sécurité des transports terrestres sera créé en 2012. Parmi les questions prioritaires qui lui seront soumises figurera la nécessité de fixer des normes de sécurité à l'échelle de l'UE pour le réseau ferroviaire à grande vitesse.

État d'avancement – tableau récapitulatif de l'ensemble des objectifs et actions de la SSI

OBJECTIF 2: Prévenir le terrorisme et s'attaquer à la radicalisation et au recrutement de terroristes			
	<i>Action 1: Donner aux communautés les moyens de prévenir la radicalisation et le recrutement de terroristes</i>	<i>Action 2: Couper l'accès des terroristes aux sources de financement et aux substances CBRN, et suivre leurs transactions</i>	<i>Action 3: Protéger les transports</i>
2011	<div style="border: 1px solid black; background-color: #d9ead3; padding: 5px; width: fit-content; margin: auto;">Créer un réseau européen de sensibilisation à la radicalisation avec un forum en ligne et des conférences au niveau de l'Union. Soutenir les travaux des organisations de la société civile qui mettent au jour, traduisent et contestent la propagande extrémiste et violente</div>	<div style="display: flex; justify-content: space-around; align-items: center;"> <div style="border: 1px solid black; background-color: #fff2cc; padding: 5px; width: 150px;">Cadre relatif à un mécanisme de gel des avoirs issus du terrorisme</div> <div style="border: 1px solid black; background-color: #fff2cc; padding: 5px; width: 150px;">Politique relative à l'extraction et à l'analyse des données de messagerie financière</div> </div>	<div style="border: 1px solid black; background-color: #f4cccc; padding: 5px; width: fit-content; margin: auto;">Communication relative à la politique de sécurité des transports</div>
2012	<div style="border: 1px solid black; background-color: #fff2cc; padding: 5px; width: fit-content; margin: auto;">Conférence ministérielle sur la prévention de la radicalisation et du recrutement</div>		
2013			
2014	<div style="border: 1px solid black; background-color: #d9ead3; padding: 5px; width: fit-content; margin: auto;"> Code des couleurs: <u>Vert</u>: action (devant être) terminée en 2011 <u>Jaune</u>: action en cours <u>Rouge</u>: action non entamée </div>	<div style="border: 1px solid black; background-color: #fff2cc; padding: 5px; width: fit-content; margin: auto;">Manuel sur la prévention de la radicalisation, la lutte contre le recrutement, et le désengagement et la réhabilitation des terroristes</div>	

Mettre en œuvre des plans d'action destinés à prévenir l'accès aux explosifs et aux substances chimiques, biologiques, radiologiques et nucléaires

Objectif 3 – Relever le niveau de sécurité pour les citoyens et les entreprises dans le cyberspace

Le centre européen de lutte contre la cybercriminalité

La Commission a commandé une étude de faisabilité sur le lieu et les modalités d'installation du centre européen de lutte contre la cybercriminalité (CEC), qui doit être le futur centre de liaison pour la répression de la cybercriminalité au niveau européen. Cette étude, lancée en mai 2011, produira ses premiers résultats d'ici à la fin de cette année. Les résultats définitifs, qui seront accompagnés de recommandations, seront disponibles début 2012. En attendant les recommandations de l'étude, Europol a décidé, en juin 2011, de regrouper ses compétences dans le domaine de la cybercriminalité et a réaffecté ses ressources pour prendre en compte cette forme de criminalité qui connaît une expansion rapide.

L'ISEC finance différents projets de formation destinés aux services répressifs chargés d'enquêter sur des faits de cybercriminalité. Par exemple, un projet ISEC qui s'est terminé au début de l'année 2011 a permis de concevoir et de dispenser des cours de formation sur les enquêtes de police scientifique et l'internet. La formation était destinée au personnel de différents services répressifs et d'organismes européens et internationaux. Un accent particulier était mis sur l'établissement d'une coopération plus étroite avec le secteur privé. Des partenaires de tous les États membres de l'Union et Europol participaient au projet¹⁹.

Au niveau national, la Commission a soutenu financièrement les efforts nationaux de sensibilisation à la cybercriminalité et le renforcement des capacités de formation, y compris des centres d'excellence. En 2011, quatre centres de ce type ont démarré leurs activités: 2CENTRE (en France et en Irlande), B-CENTRE (en Belgique) et 2CENTRE EST (en Estonie).

Les équipes d'intervention en cas d'urgence informatique (CERT)

En mars 2011, la Commission a adopté une communication relative à la protection des infrastructures d'information critiques (PIIC)²⁰, qui a fait le bilan de la mise en œuvre du plan d'action PIIC 2009²¹ et décrit les prochaines actions à entreprendre à la fois au niveau européen et au niveau international. En mai 2011, le Conseil Télécommunications a adopté des conclusions connexes. Un certain nombre de domaines ont été recensés, dans lesquels des efforts supplémentaires sont nécessaires pour renforcer les capacités nationales en matière de cybersécurité, notamment en ce qui concerne la mise en place de CERT nationales/publiques et leur regroupement au sein d'un réseau efficace en Europe d'ici à 2012; l'élaboration de

¹⁹ Titre et référence: *Cybercrime Investigation – Developing and disseminating an accredited international training programme for the future* (Enquêtes en matière de cybercriminalité – conception et diffusion d'un programme international de formation agréé pour l'avenir) - JLS/2008/ISEC/FP/C4-077.

²⁰ COM(2011) 163, communication de la Commission relative à la protection des infrastructures d'information critiques «Réalizations et prochaines étapes: vers une cybersécurité mondiale».

²¹ COM(2009) 149, communication de la Commission relative la protection des infrastructures d'information critiques «Protéger l'Europe des cyberattaques et des perturbations de grande envergure: améliorer l'état de préparation, la sécurité et la résilience».

plans d'urgence nationaux et d'un plan d'urgence européen en cas d'incident informatique; et l'organisation, à intervalles réguliers, d'exercices nationaux et paneuropéens pour répondre aux incidents informatiques. Les institutions de l'Union européenne ont progressé sur la voie de la mise en place de leur propre CERT en créant une équipe de préconfiguration CERT le 1^{er} juin 2011. Cette équipe fera l'objet d'une évaluation dans un délai de 12 mois, qui permettra de décider des conditions de mise en place d'une CERT pour les institutions de l'UE.

Le groupe de travail UE-États-Unis sur la cybersécurité et la cybercriminalité

Outre les mesures susmentionnées, la Commission a poursuivi son étroite collaboration dans le cadre du partenariat stratégique concrétisé par le groupe de travail UE-États-Unis sur la cybersécurité et la cybercriminalité, en travaillant sur la protection des ressources essentielles de l'internet contre les abus et sur la prévention de la pédopornographie en ligne, ainsi que la poursuite des utilisateurs de contenus pédopornographiques.

Le comportement sur l'internet

En collaboration avec le service européen pour l'action extérieure, la Commission travaille à la définition d'une position européenne vis-à-vis des initiatives récentes visant à recommander un certain comportement sur l'internet, et à permettre à des pays tiers d'adopter une législation sur la cybercriminalité, de mettre en place des capacités d'enquête et d'améliorer la résilience des réseaux sur la base des dispositions de la convention de Budapest sur la cybercriminalité.

État d'avancement – tableau récapitulatif de l'ensemble des objectifs et actions de la SSI

OBJECTIF 3: Augmenter le niveau de sécurité des citoyens et des entreprises dans le cyberspace			
	<i>Action 1: Développer les capacités répressives et judiciaires</i>	<i>Action 2: Collaborer avec les entreprises afin de donner des moyens d'action aux citoyens et de les protéger</i>	<i>Action 3: Améliorer la capacité de réaction aux cyberattaques</i>
2011	<div style="border: 1px solid black; background-color: #d9ead3; padding: 5px; width: fit-content; margin: auto;"> Étude de faisabilité sur la création d'un centre européen de lutte contre la cybercriminalité </div>	<div style="border: 1px solid black; background-color: #fff2cc; padding: 5px; width: fit-content; margin: auto;"> Orientations sur la coopération en matière de lutte contre les contenus illégaux sur l'internet </div>	
2012			<div style="border: 1px solid black; background-color: #fff2cc; padding: 5px; width: fit-content; margin: auto;"> Créer un réseau d'équipes d'intervention en cas d'urgence informatique dans chaque EM et une équipe pour les institutions de l'UE, ainsi que des plans nationaux d'urgence et de réaction et des exercices de récupération </div>
2013	<div style="border: 1px solid black; background-color: #fff2cc; padding: 5px; width: fit-content; margin: auto;"> Création d'un centre européen de lutte contre la cybercriminalité </div> <div style="border: 1px solid black; background-color: #fff2cc; padding: 5px; width: fit-content; margin: auto; margin-top: 10px;"> Développer les capacités d'enquête et de poursuite dans le domaine de la cybercriminalité </div>		<div style="border: 1px solid black; background-color: #fff2cc; padding: 5px; width: fit-content; margin: auto;"> Mise en place d'un système européen de partage d'informations et d'alerte (SEPIA) </div>
2014	<div style="border: 1px solid black; background-color: #d9d9d9; padding: 5px; width: fit-content; margin: auto;"> Code des couleurs: Vert: action (devant être) terminée en 2011 Jaune: action en cours Rouge: action non entamée </div>		

Adopter des dispositions de signalement des actes de cybercriminalité et fournir des orientations aux citoyens en ce qui concerne la cybersécurité et la cybercriminalité

Objectif 4 – Renforcer la sécurité par la gestion des frontières

La création de l'EUROSUR

En 2011, la conception et la mise en œuvre de l'EUROSUR ont progressé notablement. En janvier 2011, la Commission a présenté le cadre technique et opérationnel de l'EUROSUR et a énuméré les actions à entreprendre afin de le rendre opérationnel pour 2013²². Dans ces conditions, 16 États membres sur les 18 situés à la frontière maritime méridionale et à la frontière terrestre orientale de l'UE ont créé leur centre de coordination national au cours de l'année 2011. Dans le même temps, l'agence FRONTEX met actuellement en place le réseau EUROSUR, qui lui permettra d'échanger des informations d'une manière sécurisée avec les centres nationaux de coordination. Après avoir mené des essais fructueux avec le centre de coordination national polonais au cours de l'été, FRONTEX a étendu le réseau EUROSUR à cinq autres États membres (situation au mois de novembre 2011). La Commission finalise actuellement ses travaux sur la proposition législative relative à l'EUROSUR, qui sera présentée au Conseil à la mi-décembre 2011.

Dans le contexte de l'EUROSUR et en coopération étroite avec le COSI, plusieurs États membres du sud ont commencé à préparer la création du réseau régional «SEAHORSE Mediterraneo», avec certains pays africains voisins. Parallèlement, FRONTEX, l'Agence européenne pour la sécurité maritime (AESM) et le Centre satellitaire de l'Union européenne (CSUE) ont élaboré conjointement un concept d'opérations pour une utilisation commune des satellites, des systèmes de comptes rendus des navires et d'autres outils de surveillance. Plusieurs applications de ce projet de coopération entre agences ont été testées dans le courant de 2011, entre FRONTEX, l'AESM, EUROPOL et le CeCLAD-M²³ en Méditerranée occidentale dans le cadre de l'opération conjointe de FRONTEX Indalo. Enfin, des progrès ont été accomplis dans l'extension de l'environnement commun de partage des informations (ECPI) relatives à la surveillance du domaine maritime de l'UE.

La création du système d'information sur les visas (VIS)

En 2011, des progrès considérables ont été accomplis dans la mise au point définitive du VIS. Les deux dernières phases d'essais du VIS central ont été menées avec la participation des États membres. Les essais opérationnels du système et les essais de réception provisoire du système ont été menés à terme avec succès au deuxième trimestre de 2011 et au troisième respectivement. À l'issue de ces tests exhaustifs et après réception des notifications d'achèvement des préparatifs de la part de tous les États membres participant au VIS, le VIS a été mis en service le 11 octobre 2011 dans la première région d'utilisation (l'Afrique du Nord). Le système sera progressivement étendu aux régions suivantes au cours des prochains

²² Document de travail des services de la Commission déterminant le cadre technique et opérationnel de l'EUROSUR et les actions à mener pour sa mise en place, SEC(2011) 145 final du 28.1.2011. Voir également COM(2008) 68 final du 13.2.2008 et SEC(2009) 1265 final du 24.9.2009.

²³ Centre européen de coordination pour la lutte antidrogue en Méditerranée.

mois et des prochaines années. La gestion opérationnelle du VIS sera confiée à C-SIS, l'autorité chargée de la gestion opérationnelle du SIS 1.

La gestion commune des risques liés au franchissement des frontières par les marchandises

La mise en œuvre à l'échelle de l'UE des modifications en matière de sécurité apportées au code des douanes communautaire et du cadre commun de gestion des risques douaniers (CGRD) s'est achevée le 1^{er} janvier 2011, et notamment l'instauration du dépôt systématique des déclarations préalables à l'arrivée et à la sortie par voie électronique, de l'analyse de risque électronique par les douanes de l'UE, de l'échange de messages via le système de gestion des risques en matière douanière (SGRD) et du programme relatif aux opérateurs économiques agréés (OEA). Cette mise en œuvre complète pose les fondations pour des initiatives destinées à renforcer les capacités de ciblage et d'analyse des risques.

État d'avancement – tableau récapitulatif de l'ensemble des objectifs et actions de la SSI

OBJECTIF 4: Renforcer la sécurité par la gestion des frontières				
	<i>Action 1: Exploiter pleinement le potentiel de l'EUROSUR</i>	<i>Action 2: Accroître la contribution de Frontex aux frontières extérieures</i>	<i>Action 3: Gérer en commun les risques liés au franchissement des frontières extérieures par les marchandises</i>	<i>Action 4: Améliorer la coopération interservices au niveau national</i>
2011	<div style="border: 1px solid black; padding: 2px; width: fit-content;">Proposition en vue de la création de l'EUROSUR</div> <div style="border: 1px solid black; padding: 2px; width: fit-content; margin-left: 20px;">Projet pilote opérationnel à la frontière sud ou sud-ouest de l'UE</div>	<div style="border: 1px solid black; padding: 2px; width: fit-content;">Rapports conjoints sur la traite d'êtres humains, le trafic de clandestins et la contrebande de marchandises illicites, comme base d'opérations conjointes</div>	<div style="border: 1px solid black; padding: 2px; width: fit-content;">Initiatives pour améliorer les capacités d'analyse et de ciblage des risques</div>	<div style="border: 1px solid black; padding: 2px; width: fit-content;">Développer les analyses communes des risques au niveau national, associant la police, les gardes-frontières et les autorités douanières, afin de détecter les points sensibles aux frontières extérieures</div>
2012				<div style="border: 1px solid black; padding: 2px; width: fit-content;">Propositions visant à améliorer la coordination des vérifications aux frontières effectuées par les différents services nationaux</div>
2013				
2014	<div style="border: 1px solid black; padding: 2px; width: fit-content;"> Code des couleurs: Vert: action (devant être) terminée en 2011 Jaune: action en cours Rouge: action non entamée </div>			<div style="border: 1px solid black; padding: 2px; width: fit-content;">Établir des normes minimales et les meilleures pratiques aux fins de la coopération interservices</div>

Objectif 5 – Renforcer la résilience de l'Europe aux crises et aux catastrophes

La mise en œuvre de la clause de solidarité

Par la mise en œuvre de la clause de solidarité, l'UE vise à concrétiser le principe de solidarité inscrit dans le traité de Lisbonne (article 222). Le travail requis a commencé.

Les orientations pour l'évaluation et la cartographie des risques en vue de la gestion des catastrophes, et les approches nationales de la gestion des risques

Dans la perspective de la mise en place d'une politique de gestion des risques cohérente, établissant un lien entre, d'une part, l'évaluation des menaces et des risques et, de l'autre, la prise de décision, la Commission, en collaboration avec les États membres, a élaboré des orientations pour l'évaluation et la cartographie des risques en vue de la gestion des catastrophes dans l'Union européenne²⁴, fondées sur une approche multi-aléas et multirisques, couvrant en principe toutes les catastrophes d'origine naturelle et humaine, y compris les conséquences des actes terroristes. D'ici à la fin de 2011, les États membres devraient avoir mis au point une approche nationale de la gestion des risques, comportant une analyses de risques.

Les menaces pour la santé

La Commission européenne élabore actuellement une initiative sur la sécurité sanitaire dans l'Union européenne pour mieux protéger la santé des citoyens contre les menaces transfrontières graves. Une réponse législative avait déjà été apportée en 1998 à la question de la prévention et du contrôle des menaces posées par les maladies transmissibles au niveau de l'UE, qui apportait la base nécessaire à la surveillance épidémiologique et à la coordination de la réaction. Ce système s'est révélé efficace pendant plus d'une décennie. Toutefois, aucune législation comparable n'existe en ce qui concerne les menaces pour la santé que posent les agents chimiques et biologiques sans lien avec des maladies transmissibles ou des incidents environnementaux. L'objectif de cette initiative est donc d'examiner la possibilité et la nécessité de s'assurer que tous les types de menaces pour la santé publique reçoivent la même attention que les maladies transmissibles. Dans le cadre de la procédure d'évaluation des incidences, la Commission a lancé une consultation des parties prenantes ciblée sur les acteurs du domaine de la santé publique dans les États membres. Les résultats de cette consultation serviront à l'élaboration d'une initiative législative dont la présentation devrait intervenir d'ici à la fin de 2011²⁵.

La protection des informations classifiées

L'Union européenne doit concevoir une approche intégrée fondée sur des appréciations communes et partagées des situations de crise. Certaines agences de l'UE ont un rôle clé à jouer dans ce processus et la possibilité d'échanger des informations classifiées au niveau approprié constitue une condition préalable à un meilleur partage des informations et, le cas

²⁴ Document de travail des services de la Commission sur des orientations pour l'évaluation et la cartographie des risques en vue de la gestion des catastrophes, SEC(2010) 1626 final du 21.12.2010.

²⁵ L'adoption est prévue le 7 décembre 2011.

échéant, à l'élaboration de rapports conjoints d'évaluation des menaces et des risques dans l'UE. Une coordination efficace entre les institutions, les organes et les agences de l'UE requiert un cadre général cohérent de protection des informations classifiées. La Commission travaille à l'élaboration d'un cadre général cohérent pour l'échange d'informations classifiées avec les agences de l'UE, qui garantisse que les informations classifiées y bénéficient du même niveau de protection que dans les autres institutions de l'UE et dans les États membres.

La capacité européenne de réaction d'urgence

La Commission a présenté une proposition visant à créer une capacité européenne de réaction d'urgence²⁶ fondée sur des ressources mises à disposition à l'avance par les États membres pour des actions de l'UE et sur des plans d'urgence préapprouvés. L'UE doit passer de la coordination ad hoc actuelle à un système planifié, convenu au préalable et prévisible, ce qui donnera un surcroît d'efficacité, d'efficacité, de cohérence et de visibilité aux mesures qu'elle prend pour réagir aux catastrophes. Cet objectif sera atteint grâce à un certain nombre de mesures, y compris des évaluations des risques régulières, l'élaboration de scénarios de référence, la cartographie des actifs et la planification des mesures d'urgence, et la mise en place d'une capacité européenne de réaction d'urgence sous la forme d'une mise en commun volontaire des actifs des États membres participants affectés aux opérations de l'UE, ce qui contribuera davantage à la planification et à la disponibilité des actifs en vue d'une réaction européenne d'urgence. Une analyse d'impact (qui inclut une consultation des parties prenantes) a été lancée en vue d'étayer la proposition de la Commission visant à renouveler la législation de l'UE relative à la protection civile d'ici à la fin de 2011.

²⁶ Communication de la Commission «Vers une capacité de réaction renforcée de l'UE en cas de catastrophe: le rôle de la protection civile et l'aide humanitaire», 26.10.2010, COM(2010) 600 final.

État d'avancement – tableau récapitulatif de l'ensemble des objectifs et actions de la SSI

OBJECTIF 5: Renforcer la résilience de l'Europe aux crises et aux catastrophes				
	<i>Action 1: Tirer pleinement parti de la clause de solidarité</i>	<i>Action 2: Une approche tous risques de l'évaluation des menaces et des risques</i>	<i>Action 3: Interconnecter les différents centres de reconnaissance des situations</i>	<i>Action 4: Mettre en place une capacité européenne de réaction d'urgence aux catastrophes</i>
2011	Proposition relative à la mise en œuvre de la clause de solidarité	<p>Orientations pour l'évaluation et la cartographie des risques en vue de la gestion des catastrophes</p> <p>Proposition relative aux menaces sanitaires</p>	Proposition de cadre général cohérent pour la protection des informations classifiées	Propositions en vue de la mise en place d'une capacité européenne de réaction d'urgence
2012		<p>Approches nationales de la gestion des risques</p> <p>Aperçu horizontal des risques d'origine naturelle ou humaine potentiels</p>	Renforcer les liens entre les systèmes sectoriels d'alerte précoce et les mécanismes de coopération en cas de crise	
2013		Bilans réguliers des menaces en cours		
2014	<p>Code des couleurs: <u>Vert</u>: action (devant être) terminée en 2011 <u>Jaune</u>: action en cours <u>Rouge</u>: action non entamée</p>	Mettre en place une politique cohérente de gestion des risques		

Les questions transversales

La cohérence entre les dimensions intérieure et extérieure de la sécurité

Une série d'initiatives sont actuellement en cours d'élaboration qui visent à renforcer la coopération entre les volets intérieur et extérieur de la sécurité. Pour aboutir à une coopération et une coordination plus étroites dans le domaine de la sécurité de l'UE, des réunions interinstitutionnelles seront régulièrement organisées en vue d'améliorer la planification et la circulation des informations. La première réunion de ce genre entre le COSI et le Comité politique et de sécurité a eu lieu le 1^{er} juin 2011 et a permis de procéder à un échange de vues sur la manière d'améliorer les synergies entre les dimensions intérieure et extérieure de la sécurité de l'UE. En outre, le SEAE et la Commission ont élaboré un document conjoint destiné à renforcer les liens entre la politique de sécurité et de défense commune (PSDC) et les acteurs du domaine de la liberté, de la sécurité et de la justice (JAI), qui défend l'idée qu'une coopération plus étroite entre les missions civiles de la PSDC et les acteurs JAI pourrait déboucher sur des améliorations tangibles en matière de sécurité européenne. Les recommandations spécifiques du document conjoint soulignent l'importance du partage des informations, qui doit encore être amélioré pour dégager des pistes d'anticipation des événements plutôt que de réaction aux événements. Dans un deuxième temps, la coordination de la planification de l'action extérieure de l'UE doit être renforcée, car la coopération en amont est essentielle pour la programmation des missions.

Un autre domaine dans lequel des résultats tangibles peuvent être obtenus est celui de la coopération entre les missions de police de la PSDC et Europol. Le Conseil a souvent reconnu que la PSDC²⁷ et de nombreuses actions extérieures JAI avaient des objectifs communs ou complémentaires. Les missions relevant de la PSDC ont également contribué grandement à la sécurité intérieure de l'UE en ce sens qu'elles visent à renforcer la lutte contre la grande criminalité transnationale dans les États où elles se déroulent et à instaurer le respect de l'État de droit. Le Conseil européen a encouragé une plus grande coopération entre la JAI et la PSDC en vue de développer ces objectifs partagés. De même, il est affirmé dans le programme de Stockholm, adopté par le Conseil européen, qu'Europol devrait coopérer plus étroitement avec les missions de police menées dans le cadre de la PSDC et contribuer à promouvoir des normes et des bonnes pratiques pour la coopération européenne en matière répressive en dehors de l'UE.

Il est particulièrement intéressant pour la politique concernant la JAI de s'assurer qu'elle est étroitement associée en tout début de processus, en particulier pour établir et évaluer la nécessité d'une action de l'UE en situation de crise. Il sera ainsi possible d'évaluer correctement et en temps utile l'expertise requise en tenant compte de l'état de la criminalité organisée dans la région ou le pays tiers concerné. Cela contribuera également à l'amélioration des décisions politiques et opérationnelles et de la définition des tâches qui seront mises en œuvre par la suite par la mission civile de police. Les capacités d'analyse d'Europol et son application de réseau d'échange sécurisé d'informations (*Secure Information Exchange Network Application* - SIENA), qui relie les autorités répressives des 27 États membres de l'UE, peuvent aider à ajuster les méthodes des missions menées dans le cadre de

²⁷ À la suite de l'entrée en vigueur du traité de Lisbonne, il ne faut désormais plus faire référence à la PESD (politique européenne de sécurité et de défense) mais à la PSDC (politique de sécurité et de défense commune).

PSDC et à affiner leurs objectifs en fonction d'une vue paneuropéenne de la criminalité organisée, fournie par Europol grâce à ses évaluations et analyses des menaces.

D'autre part, l'échange d'informations entre les missions de police relevant de la PSDC et Europol représente un aspect important de la coopération. Le mécanisme de coopération qui prévoit l'échange de données à caractère non personnel est, dans une large mesure, bien établi, grâce à un accord administratif conclu entre Europol et le secrétariat général du Conseil. La question essentielle qui se pose est dès lors de savoir comment rendre possible l'échange direct avec Europol des données à caractère personnel collectées par les missions de police relevant de la PSDC ou qui sont collectées en relation avec celles-ci. Dans le cas d'EULEX KOSOVO²⁸, dont le mandat inclut également des tâches d'exécution, des dispositions particulières ont été mises en place pour permettre l'échange de données à caractère personnel avec Europol. Ce mécanisme pourrait servir d'exemple de meilleure pratique et être appliqué lors d'autres missions menées dans le cadre de la PSDC, au cas par cas. Il convient d'évaluer la nécessité d'établir un cadre de protection des données qui soit également applicable à la PSDC.

La politique d'élargissement de l'UE reste l'un des éléments essentiels qui contribuent à la sécurité intérieure de l'UE. Le processus d'élargissement incite grandement les pays concernés à mettre en place les réformes qui renforcent leurs capacités répressives et judiciaires. En outre, le dialogue consacré à la libéralisation du régime des visas et le mécanisme de suivi de cette libéralisation ont fortement contribué à la mise en œuvre de réformes dans les pays des Balkans occidentaux.

L'UE a également pour objectif d'augmenter la capacité des pays partenaires à jouer le rôle qui est le leur dans la réponse à apporter aux principales menaces qui pèsent actuellement sur la sécurité, la paix et la stabilité de par le monde. À cet effet, les priorités à long terme définies dans l'instrument de stabilité (IS) prévoient un renforcement innovant des capacités associant aide financière et assistance technique à l'échelle nationale, régionale et interrégionale. La première priorité de cet instrument porte sur le soutien aux efforts internationaux visant à atténuer les risques chimiques, biologiques, radiologiques et nucléaires (CBRN). Les mesures financées par l'IS ont pour but d'atténuer les risques CBRN, y compris la prolifération des armes de destruction massive (ADM), notamment par le contrôle effectif des matières et agents CBRN, le contrôle des exportations de biens à double usage et la réorientation vers des activités de recherche pacifiques des scientifiques autrefois spécialisés dans l'armement. Pour la période 2007-2013, 300 millions d'EUR ont été affectés à cet effet et une initiative intitulée «Centres d'excellence CBRN» a été lancée avec une dotation budgétaire de quasiment 100 millions d'EUR. Cette initiative vise à mettre en place, aux niveaux national et régional, les capacités institutionnelles nécessaires pour lutter contre les risques CBRN, qu'ils soient d'origine criminelle (prolifération, vol, sabotage et trafic), accidentelle (catastrophes industrielles, comme celles de Bhopal ou Fukushima, ou transport) ou naturelle (principalement des pandémies).

²⁸ À la suite de l'adoption d'un projet de conclusions du Conseil de l'Union européenne sur l'instauration de mécanismes de coopération entre les missions civiles relevant de la PESD et Europol en ce qui concerne l'échange d'informations, le 17 novembre 2008, l'échange de données à caractère personnel a été mis en œuvre entre Europol et EULEX KOSOVO: les données à caractère personnel sont transférées entre EULEX (par l'EUOCI, *European Union Office for Criminal Intelligence*) et Europol par l'intermédiaire des unités nationales d'Europol (UNE) situées dans les capitales de trois États membres (FI, SE, UK).

En ce qui concerne la criminalité organisée, le trafic de drogues ou d'armes, la traite des êtres humains et les menaces pour les infrastructures critiques, la deuxième priorité de l'IS vise particulièrement le renforcement des capacités, en consultation étroite avec les pays bénéficiaires. Généralement, les capacités de sécurité sont renforcées aux niveaux national, régional et, enfin, interrégional. Pour la période 2007-2013, 118 millions d'EUR ont été affectés à ces mesures.

Le soutien financier

La Commission tient à s'assurer que les activités en rapport avec la sécurité, y compris la recherche en matière de sécurité, la politique industrielle et les projets menés dans le cadre de programmes de financement relatifs à la sécurité intérieure de l'UE, correspondent aux objectifs stratégiques de la SSI. Le financement de l'UE qui pourrait se révéler nécessaire pour la période 2012-2013 sera mis à disposition dans le cadre des programmes financiers actuels «Prévention et lutte contre la criminalité – ISEC» et «Prévention, préparation et gestion des conséquences en matière de terrorisme et autres risques liés à la sécurité» – CIPS). À cet égard, le programme de travail annuel 2011 adopté au titre de l'ISEC reflète les domaines prioritaires de la SSI en action. Par ailleurs, la Commission a procédé à une évaluation²⁹ des résultats obtenus et des aspects qualitatifs et quantitatifs du programme-cadre «Sécurité et protection des libertés (2007-2013)», qui se compose des deux programmes ISEC et CIPS.

Pour la période postérieure à 2013, le financement de la sécurité intérieure sera examiné dans le cadre d'un large débat au sein de la Commission portant sur l'ensemble des propositions qui seront formulées dans cette perspective. Dans le cadre de ce débat, la Commission a proposé de créer un fonds pour la sécurité intérieure (FSI) dans le prochain cadre financier pluriannuel, qui reflète les priorités et les objectifs stratégiques de la stratégie pour la sécurité intérieure, qui facilite la meilleure mise en œuvre possible des actions prioritaires par les autorités nationales et agences compétentes, et qui reste suffisamment souple pour s'adapter aux nouvelles menaces et aux nouveaux défis en matière de sécurité. La Commission estime qu'il convient de combler l'écart qui existe actuellement entre le financement de la recherche et le financement opérationnel en soutenant des activités spécifiques de test et de validation (de systèmes prototypes, par exemple) dans le cadre du FSI proposé. Cette démarche facilitera l'exploitation plus systématique des résultats des recherches de grande qualité menées en matière de sécurité, et permettra de les faire appliquer à grande échelle par les autorités répressives.

La recherche en matière de sécurité et la coopération avec le secteur privé

La recherche en matière de sécurité est financée au titre d'un volet spécifique du septième programme-cadre de recherche (2007-2013). La Commission s'assure que l'ensemble de la programmation respecte pleinement les politiques de sécurité de l'UE, comme en témoignent plus de 200 projets de recherche financés jusqu'à présent au titre de ce programme. Les objectifs de la SSI sont bien reflétés dans les programmes de travail 2011 et 2012 pour la recherche en matière de sécurité. Pour ce qui est du programme de travail 2013, qui apportera environ 290 millions d'EUR à lui seul, une analyse est actuellement en cours afin de recenser

²⁹ Communication de la Commission sur l'évaluation à mi-parcours du programme-cadre «Sécurité et protection des libertés (2007-2013)», COM(2011) 318 final.

les lacunes et les besoins les plus criants dans la recherche, sans oublier de prendre en compte les priorités définies dans la SSI en action.

Après 2013, la recherche en matière de sécurité continuera à être financée par le futur instrument pluriannuel de recherche et d'innovation («Horizon 2020»). La proposition de la Commission relative au budget total destiné à la recherche et à l'innovation dans le prochain cadre financier pluriannuel prévoit une augmentation de 46 %, qui devrait se répercuter sur le montant consacré à la recherche en matière de sécurité.

Afin d'aboutir à une meilleure adéquation entre les financements et les politiques en matière de sécurité, la Commission a également intensifié son dialogue avec le secteur privé, et notamment avec l'industrie. À cette fin, elle a proposé d'organiser à intervalles réguliers (chaque année), une table ronde régulière à haut niveau entre le secteur public et le secteur privé, autour de laquelle les institutions et organes de l'UE, les États membres et le secteur privé pourraient échanger leurs idées sur les meilleurs moyens de progresser dans la mise en œuvre des priorités de la SSI. La première table ronde consacrée à la sécurité et réunissant des représentants du secteur public de l'UE et des États membres, d'une part, et des représentants du secteur privé, de l'autre, s'est tenue en février 2011. En outre, afin de tirer parti du potentiel encore inexploité que représente le marché de la sécurité, totalement opérationnel, la Commission est en train d'élaborer une communication sur une politique pour le secteur de la sécurité dans l'UE.