Conseil de
l'Union européenne

Bruxelles, le 22 novembre 2019
(OR. en)

14297/19

LIMITE

COSI 239
ENFOPOL 508
ENFOCUSTOM 196
FRONT 333
DAPIX 346
CYBER 322
JAI 1217

NOTE

Origine:	la présidence
Destinataire:	Comité des représentants permanents/Conseil
Objet:	L'orientation future de la sécurité intérieure de l'UE - Résultats des travaux - Rapport de la présidence

L'environnement de sécurité évolue rapidement: une approche intégrée s'impose donc, face aux menaces et aux défis nouveaux. Appréhender de façon globale la question de la sécurité intérieure apparaît comme un moyen approprié de faire face à des menaces qui sont plus complexes et variées qu'auparavant, pour que les réponses fournies puissent englober l'ensemble de la société.

Dans le cadre de la mise en œuvre du programme stratégique pour la période 2019 - 2024 dans le domaine de la justice et des affaires intérieures, la présidence a mené une série de discussions thématiques en vue d'approfondir la réflexion sur la voie à suivre en ce qui concerne l'orientation future de la sécurité intérieure de l'UE. La présidence a mis en évidence trois principes fondamentaux qui doivent guider ces réflexions:
offrir aux citoyens un espace de liberté, de sécurité et de justice; lutter contre l'exclusion sociale et la discrimination; et promouvoir les valeurs de l'Union.

Les discussions ont été lancées en juillet 2019, lors de la réunion informelle du comité permanent de coopération opérationnelle en matière de sécurité intérieure (COSI), en vue de la session informelle du Conseil "Justice et affaires intérieures" (Conseil JAI), sur la base d'un certain nombre de thèmes horizontaux essentiels[1]. Des débats thématiques ont également eu lieu au sein des groupes compétents, tels que le groupe "Application de la loi", le groupe "Terrorisme" et le groupe "Échange d'informations", et le COSI a poursuivi les travaux préparatoires en vue du débat ministériel. Un certain nombre de sujets ont été examinés de façon approfondie, comme le renforcement du cadre de coopération opérationnelle pour les services répressifs, l'impact des nouvelles technologies et des menaces hybrides sur la sécurité intérieure, le rôle des agences JAI de l'UE, la gestion de l'information et l'automatisation, ainsi que la formation des services répressifs. Les différents volets de ces discussions sont présentés dans les documents qui ont été publiés pour les différentes réunions et sont énumérés à l'annexe du présent rapport.

Le présent rapport présente, pour certains aspects choisis, le point de vue de la présidence sur les questions clés qui sont ressorties de ces débats et dont l'examen se poursuivra pendant le cycle législatif 2019-2024.

1. Une approche proactive des nouvelles technologies

L'évolution technologique a une incidence majeure sur la vie des citoyens de l'UE et, ensuite, sur le travail des services répressifs. Des évolutions telles que l'intelligence artificielle, les drones, les nouveaux réseaux de communication et l'environnement en temps réel, pour n'en citer que quelques-unes, peuvent appuyer les travaux des autorités mais peuvent aussi être exploitées à des fins illicites. Ainsi, tant les services répressifs que les premiers intervenants peuvent utiliser des drones dans le cadre de la lutte contre le terrorisme et au lendemain d'un attentat. Le rythme de l'innovation s'accélère, et les services répressifs ont des difficultés à s'adapter à l'évolution rapide de la technologie. Dans le contexte de la numérisation, il serait nécessaire d'évaluer dans quelle mesure les cadres juridiques dans lesquels opèrent les services répressifs et les agences de l'UE concernées correspondent aux besoins actuels[2]. Toute évolution dans ce sens se doit de préserver et de promouvoir les droits fondamentaux, tout en respectant les exigences strictes en matière d'activités répressives, qui découlent du cadre de la protection des données, où l'Union occupe une position de premier plan en matière de fixation de normes.

---

1 Document de la présidence sur l'orientation future de la sécurité intérieure dans l'UE (WK 13264/19)

2 Documents 12496/19 et 12224/19, nouvelles technologies et sécurité intérieure

Le but est de donner aux services répressifs de l'UE un rôle proactif afin de pouvoir tirer parti des nouvelles technologies, tout en anticipant et en maîtrisant les risques qui y sont associés. Il est nécessaire d'adopter une approche intégrée et globale au niveau de l'UE dans ce domaine.
La création d'un laboratoire d'innovation commun au sein d'Europol visant à exploiter les évolutions et tendances technologiques, l'innovation et la recherche, et à en évaluer l'intérêt potentiel pour les services répressifs et le dialogue avec l'industrie et le monde universitaire appuie cet objectif.
Pour pouvoir pleinement exploiter les nouvelles technologies, il est nécessaire de mener constamment des recherches et des activités de formation. Il serait intéressant, d'un point de vue de la rationalisation et de la rentabilité, de centraliser certaines activités et de mettre en commun, au sein du laboratoire d'innovation, les résultats des travaux menés par les réseaux existants, surtout dans des domaines où les États membres ne disposent pas des ressources suffisantes pour agir seuls ou des domaines où le fait d'agir ensemble et d'échanger les meilleures pratiques comporte une valeur ajoutée.

Étant donné que les activités de recherche et développement technologiques ont souvent lieu dans des universités et dans le secteur privé, les services répressifs n'y sont associés qu'à un stade relativement tardif. Afin de tenir compte des préoccupations des services répressifs par rapport à l'avenir, la présidence estime qu'il faudrait s'efforcer d'associer de manière proactive les autorités répressives aux processus de développement technologique dès le départ, notamment en renforçant encore la participation et la coordination des professionnels des services répressifs dans les programmes de recherche et développement financés par l'UE dans le domaine de la sécurité.

La présidence encourage l'idée d'associer de manière proactive les services répressifs à la mise au point de nouvelles technologies. Le laboratoire d'innovation devrait servir de plateforme à cet effet. Il est important que les besoins des services répressifs soient connus et pris en compte à un stade précoce de la mise au point de nouvelles technologies qui influencent leur travail ou qui sont nécessaires pour améliorer l'efficacité de l'action des services répressifs. En outre, dans la législation relative aux nouvelles technologies, il conviendrait de mieux tenir compte des intérêts en termes de sécurité intérieure et de services répressifs afin de moduler les limites du cadre juridique, notamment par une prise en compte systématique dans les évaluations de la menace.

2. Une gestion efficace de l'information

La coopération entre les services répressifs au niveau de l'UE sera de plus en plus fondée sur de meilleures solutions technologiques et des systèmes d'information plus efficaces et sur leur interopérabilité[3]. À l'ère des grands volumes de données numériques, les données et les informations auxquelles les services répressifs ont accès sont plus considérables que jamais. Cela doit se refléter dans les solutions techniques et les capacités proposées. Mais parallèlement, on ne dispose pas de statistiques essentielles sur diverses formes de criminalité. Aussi est-il particulièrement important de veiller à que les systèmes d'information soient alimentés en données complètes et de qualité, et à ce qu'ils soient utilisés efficacement. Nous devons faire en sorte que les autorités nationales concernées aient accès à ces systèmes et qu'elles aient la formation nécessaire pour pouvoir les utiliser au mieux.

L'analyse criminelle continue d'occuper une place centrale dans les services répressifs. En effet, elle apporte une valeur ajoutée aux données brutes qu'elle transforme en informations exploitables susceptibles d'être utilisées au niveau national, ainsi que dans les opérations transfrontières dans toute l'UE. Il manque toutefois une vision claire en ce qui concerne des normes applicables aux travaux d'analyse de la criminalité au niveau de l'UE. En tout état de cause, l'analyse fait partie intégrante de tous les processus d'information dans le cadre de l'application de la loi. Il est nécessaire de disposer des ressources humaines et financières suffisantes pour traiter et analyser les informations. Pour parvenir à améliorer et normaliser l'analyse, il est donc indispensable de mieux cerner les besoins des services répressifs dans leur ensemble et ceux des différents processus d'information impliqués en particulier, y compris les besoins de l'enquête pénale et ceux de la collecte de renseignements en matière pénale.

Les règlements sur l'interopérabilité[4] sont entrés en vigueur le 11 juin 2019. Il est primordial d'en assurer la mise en œuvre efficace. Cette révolution technologique des systèmes informatiques de l'UE exigera une grande quantité de ressources et le respect du calendrier, tant au niveau de l'UE que dans les États membres. Pendant que se construit l'architecture d'interopérabilité, il importe que les solutions techniques tiennent toujours compte des besoins des utilisateurs finaux. En outre, il est essentiel de prévoir une formation appropriée et continue pour les utilisateurs finaux afin qu'ils puissent utiliser ces nouveaux systèmes d'information, et d'achever leur interopérabilité. Il est clair que l'interopérabilité va bien au-delà du simple développement de systèmes informatiques; elle implique également un changement de mentalité. Par conséquent, la réussite de la mise en œuvre nécessite en plus un changement dans nos cultures opérationnelles et administratives.

---

3 Document 13510/19, Gestion de l'information dans l'UE - automatisation, échange et analyse des informations et accès à celles-ci.

4 Règlement (UE) 2019/817 et règlement (UE) 2019/818.

À plus grande échelle, l'amélioration de l'échange d'informations n'est pas uniquement une évolution technique. Pour obtenir les avantages escomptés, il convient de veiller à ce que les compétences, les ressources et les interfaces des utilisateurs finaux au niveau national soient adaptées à l'usage prévu. L'information n'est pas une valeur absolue: elle doit être utilisable et conduire à une action. Sans une mise en œuvre appropriée, ces évolutions et leurs avantages risquent d'être compromis.

Les services répressifs doivent non seulement mener efficacement leurs enquêtes mais aussi s'attacher à prévenir et désorganiser la criminalité. Pouvoir disposer d'informations efficaces et de qualité, au bon endroit et au bon moment, contribue à la réalisation de cet objectif. En ce qui concerne la répression fondée sur le renseignement, Europol et Frontex sont idéalement placés pour soutenir ces travaux avec leurs capacités d'analyse, y compris grâce à l'accès plus large au système d'information Schengen (SIS), pour autant que les États membres leur fournissent systématiquement des données brutes de qualité.

La présidence demande la mise en place d'un cadre global de gestion de l'information dans l'UE, afin de veiller à ce que toutes les informations existantes nécessaires soient accessibles, traitées et échangées de manière rapide et efficace, de sorte qu'il en découle une action fondée sur le renseignement.

3. Coopération transfrontière pluridisciplinaire

Il est essentiel pour une action efficace de renforcer la coopération opérationnelle transsectorielle en réduisant les doubles emplois et en amélioration l'efficacité de la coordination. En raison de l'évolution constante et de la nature transversale des différentes menaces pesant sur la sécurité, telles que les armes CBRN et les activités hybrides, les mesures prises pour faire face à ces activités et les empêcher requièrent une approche horizontale, tenant compte de la compétence des États membres en matière de sécurité nationale. Une approche intégrée et cohérente est nécessaire pour assurer une coopération opérationnelle pluridisciplinaire allant au-delà de la coopération transfrontière en matière répressive, associant donc d'autres autorités, comme les acteurs de la protection civile.

Les différences entre les processus décisionnels, la législation et les modèles opératoires nationaux constituent des défis majeurs pour une coopération transfrontière opérationnelle. En outre, les disparités dans les pratiques nationales en matière de collecte et de traitement des données, découlant des différences entre les États membres en termes de systèmes administratifs, de solutions techniques et de modalités de fonctionnement, entravent la coopération transfrontière. L'identification et la suppression des obstacles à la coopération opérationnelle entre services répressifs - par exemple des fréquences radio incompatibles dans les zones frontalières, les barrières linguistiques ou la nécessité de compléter les bases juridiques existantes par des accords bilatéraux plus détaillés - constituent un autre défi. En cas d'urgence, les entités nationales peuvent ne pas avoir connaissance de l'éventail des solutions opérationnelles - qui sont fragmentées entre plusieurs instruments de l'UE - ni des canaux d'échange d'informations disponibles.

Il convient d'intensifier la coopération opérationnelle pluridisciplinaire entre les services répressifs, en mettant en place et en utilisant de nouvelles méthodes de collaboration et d'échange d'informations, tout en s'appuyant sur les nouvelles applications et les nouveaux outils technologiques. Parmi ces applications figurent par exemple les systèmes autonomes automatisés, les technologies de reconnaissance automatique des plaques d'immatriculation ou les interfaces de recherche unique pour les bases de données disponibles. Il existe manifestement une dynamique et des possibilités pour poursuivre et soutenir davantage cette évolution.

L'apprentissage et la formation tout au long de la vie sont encore plus importants pour exploiter toutes les possibilités existantes et se préparer aux défis à venir. La formation fournie par les agences de l'UE doit être utilisée de manière efficace. Dans le même temps, il convient de veiller à ce que les activités des agences de l'UE se complètent et à ce que les doubles emplois soient éliminés.

Nous devons tenir compte des différences régionales et des spécificités nationales, tout en visant à développer une culture commune en matière de répression parmi les services répressifs de l'UE. L'amélioration des compétences linguistiques, l'apprentissage mutuel des cultures et l'échange de bonnes pratiques permettent de mieux comprendre les différences régionales et culturelles et de soutenir l'objectif commun.

Les arrangements bilatéraux et multilatéraux restent importants pour la coopération locale et régionale et la flexibilité est nécessaire afin de garantir le respect de la diversité régionale et des différents intérêts opérationnels. Il convient de prendre en compte la définition de la répartition des responsabilités, des compétences et de la souveraineté dans toute évolution future.

Les agences JAI de l'UE continuent de jouer un rôle important dans le soutien des efforts déployés par les États membres dans le cadre de leurs mandats respectifs. Il est largement admis qu'une véritable coopération transfrontière entre les autorités des États membres, bénéficiant d'un soutien appuyé des agences de l'UE concernées, constitue le moyen le plus viable d'œuvrer à une union de la sécurité et de faire face de manière durable aux menaces existantes et nouvelles dans un environnement en constante évolution[5].

Les futures évolutions dans le domaine de la sécurité intérieure exigeraient donc que les agences continuent à jouer un rôle actif, allant de pair avec une augmentation attendue du volume des tâches existantes et de nouvelles responsabilités, découlant des besoins tant politiques qu'opérationnels. Compte tenu des limites en matière de ressources, il est nécessaire d'examiner le contexte dans lequel les agences peuvent apporter une valeur ajoutée le plus efficacement, par exemple les domaines dans lesquels les États membres pourraient avoir besoin d'avoir accès à des ressources ou des équipements techniques par la mise en commun de ressources, ceux dans lesquels les capacités d'analyse des données pourraient être renforcées et ceux dans lesquels un soutien opérationnel renforcé pourrait être fourni. Il convient d'établir des critères transparents pour déterminer dans quels domaines les États membres ont le plus besoin de soutien, compte tenu des avancées technologiques et des besoins matériels spécifiques ou d'autres ressources. Dans le cadre du développement du rôle des agences, l'objectif devrait être de parvenir à une solution équilibrée qui tienne compte des besoins des États membres. Il est essentiel d'appliquer une approche coordonnée et globale afin de renforcer l'expertise de base et les points forts de chaque agence ainsi que de générer de la valeur ajoutée d'une manière efficace au regard des coûts sans créer des chevauchements de tâches et de fonctions.

Il est nécessaire d'approfondir l'échange d'informations et la coopération fondée sur les agences, les menaces existantes et émergentes en matière de sécurité intérieure étant toujours plus complexes et transfrontières par nature. Il est également nécessaire d'assurer une interaction plus efficace avec les parties privées dans le cadre du partage d'informations. Il est en particulier nécessaire d'évaluer la base juridique d'Europol pour demander et recevoir des données à caractère personnel directement auprès de parties privées[6].

---

5 Le rôle des agences de l'UE a été abordé de manière spécifique lors des réunions informelles du COSI et du Conseil en juillet, WK 13271/19 et WK 13266/19, et a été un thème transversal dans l'ensemble des débats.

6 Des discussions sur la coopération d'Europol avec des parties privées ont eu lieu au sein du groupe "Application de la loi": documents 10494/19, 11832/19 et 12858/1/19.

Afin de renforcer l'approche pluridisciplinaire d'Europol en matière de répression à long terme, il convient de continuer de développer la coopération entre les autorités douanières et Europol en augmentant le nombre d'officiers de liaison des douanes au sein d'Europol, en promouvant l'utilisation de SIENA par les douanes dans tous les États membres de l'UE et en renforçant l'échange régulier et structuré d'informations entre les parties, y compris les informations en matière de gestion des risques et de renseignement. Un objectif à court terme devrait être le renforcement de la contribution et de l'intégration des douanes à la mise en œuvre des plans d'action opérationnels de l'EMPACT. Ces actions poursuivraient l'évolution positive de la coopération entre les douanes et Europol ces dernières années.

Il convient de relever les défis qui se posent dans le cadre de la coopération entre l'Union européenne et Europol. Il est important que les bases de données qui servent de sources principales d'information pour la coopération en matière répressive avec les pays tiers continuent à être utilisées efficacement par les autorités des États membres de l'UE à l'avenir. Dans le même temps, la législation applicable en matière de protection des données doit naturellement être pleinement respectée.

La présidence souligne qu'il est nécessaire de réexaminer le cadre juridique de la coopération transfrontière en matière de répression et le mandat d'Europol afin de l'adapter aux réalités actuelles et aux défis à venir. Il convient de continuer à soutenir le développement d'une culture commune en matière de répression parmi les services répressifs de l'UE.

4. Une approche globale en matière de sécurité

On peut s'attendre à ce qu'un certain nombre de tendances et d'évolutions se dessinent dans un avenir proche qui auront une incidence sur la situation en termes de menaces dans l'UE. La criminalité continue d'être induite par la demande, ainsi que par l'existence de possibilités d'agissements illicites. En outre, les changements en matière de sécurité qui sont intervenus dans les régions voisines et les différentes formes de radicalisation violente qui sont observées en Europe continuent de représenter une menace pour notre sécurité intérieure. Une approche globale en matière de sécurité s'accompagnant d'une coordination améliorée ainsi que de ressources et de capacités technologiques renforcées, requiert une meilleure connaissance de la situation et une meilleure préparation à toute une série de défis.

Les services répressifs, la protection civile et les autres autorités concernées devraient continuer à améliorer leur niveau de préparation en vue de faire face aux menaces hybrides. La coopération en matière de prévention des menaces hybrides et de lutte contre ce phénomène entre les autorités nationales concernées, sur la base de leurs mandats respectifs, ainsi que les institutions, organes et organismes de l'UE sur tous les aspects de l'interdépendance entre sécurité intérieure et sécurité extérieure, doit être constamment améliorée et intégrée dans les autres domaines d'action. Dans le même temps, il importe de renforcer les synergies et d'éviter les doubles emplois, y compris au moyen de méthodes de travail horizontales, d'un échange accru d'informations et de formations et d'exercices intersectoriels.

Il faut insister sur la nécessité de poursuivre les discussions sur la dimension interne des menaces hybrides, notamment en ce qui concerne le rôle des agences JAI dans le renforcement de la capacité de l'UE et des États membres à repérer les actions hybrides et leur origine.

En outre, une lutte efficace contre la désinformation passe par une approche globale. Dans le même ordre d'idées, la participation des services répressifs, y compris aux mécanismes existants de l'UE tels que le système d'alerte rapide, devrait être envisagée. Les services répressifs renforcent la résilience de l'UE et de ses États membres, et la lutte contre la désinformation doit être prise en compte[7]. La présidence insiste sur la nécessité de mieux utiliser les outils existants et de renforcer la coordination globale au niveau de l'UE. Le soutien qu'apportent les agences JAI aux États membres doit également être abordé dans ce contexte.

Le recours à la technologie et à l'internet pour orchestrer les activités criminelles continuera à se développer. Par exemple, l'utilisation de plateformes en ligne aussi bien sur le web visible que sur le dark web aux fins du commerce d'un large éventail de produits illicites devrait augmenter. En outre, la sphère en ligne peut être utilisée à mauvais escient à des fins de radicalisation, de recrutement et d'incitation à la violence. À cet égard, il convient de prévenir efficacement la diffusion en ligne de contenus terroristes et de contenus pédopornographiques et de supprimer rapidement les contenus en question.

---

7 Hybrid threats and internal security: Law Enforcement Strategic Communication and Tackling Disinformation (Menaces hybrides et sécurité intérieure: communication stratégique en matière répressive et lutte contre la désinformation) (doc. 11831/19).

Par ailleurs, on soulignera le rôle que joue la prévention de la radicalisation violente, qui fait partie intégrante d'une approche globale de la lutte contre le terrorisme. Dialoguer avec les praticiens de première ligne et les soutenir demeure essentiel pour prévenir l'extrémisme violent et lutter contre ce phénomène. L'extrémisme violent motivé par des considérations politiques ou idéologiques doit être traité sous toutes ses formes. Par conséquent, il faut continuer de mettre l'accent sur la prévention de l'extrémisme violent et du terrorisme et sur la lutte contre ces phénomènes, en s'appuyant sur une approche large, en tenant compte également des tendances émergentes dans l'extrémisme violent.

La menace que représente l'extrémisme violent et le terrorisme de droite doit être combattue en dressant un tableau plus précis de la situation, en procédant à un échange permanent de bonnes pratiques, en coopérant avec les pays tiers clés et en s'attaquant à la diffusion de contenus illégaux se rapportant à l'extrémisme de droite tant en ligne que hors ligne. Le défi que constitue le retour dans leur pays d'origine des combattants terroristes étrangers doit être relevé, y compris par une utilisation plus efficace du SIS.

La présidence insiste sur la nécessité de se doter en matière de sécurité d'une approche globale et pansociétale afin de faire face aux différentes menaces qui pèsent sur la sécurité intérieure. Elle souligne l'importance de travailler de manière plus stratégique, coordonnée et cohérente dans l'ensemble des domaines d'action pertinents.

ANNEXE

Subject	Meeting	Reference Number
Future Direction of internal security in the EU	Informal COSI meeting on 8-9 July 2019, The Hague	WK 13264/19
Hybrid threats and internal security	Informal COSI meeting on 8-9 July 2019, The Hague	WK 13265/19
Twenty Years of Europol - what next?	Informal COSI meeting on 8-9 July 2019, The Hague	WK 13266/19
The future of EU Internal Security	Informal Council meeting on 18-19 July 2019, Helsinki	WK 13271/19
The future direction of EU internal security: new technologies and internal security	JHA Council on 2 October 2019	12496/19
Hybrid threats and Internal Security	JHA Council on 2 October 2019	12495/19
Right-wing violent extremism and terrorism	JHA Council on 2 October 2019	12494/19
EU Information Management - Automation, access to, sharing of, and analysis of information	COSI meeting on 19 November 2019	13510/19
The future of EU law enforcement: Training for law enforcement	COSI meeting on 19 November 2019	13973/19