



Bundesministerium  
des Innern



MINISTÈRE DE L'INTÉRIEUR

**Initiative franco-allemande  
sur les enjeux clés de la coopération européenne dans le domaine  
de la sécurité intérieure**

**23 août 2016**

Plus que jamais, l'Europe se trouve confrontée à d'immenses défis. Surtout en temps de crise, nos concitoyens doivent pouvoir reconnaître la valeur ajoutée et les bénéfices de l'appartenance à l'Union européenne. La capacité à garantir la sécurité interne est d'une très grande importance. Ceci implique également une obligation de combattre la menace réelle et de plus en plus pressante du terrorisme islamiste international en Europe. Les attaques les plus récentes en France et en Allemagne illustrent une fois de plus les aspects perfides et barbares de ce nouveau fléau auquel l'Europe doit faire face. Par ailleurs, il est impératif d'intensifier nos efforts contre le crime organisé transfrontalier.

Aucun État membre ne pourra surmonter ces défis en agissant seul. À long terme, notre lutte intense contre le terrorisme et la criminalité ne pourra réussir qu'en unifiant nos forces et en renforçant notre sentiment d'appartenir à une communauté de démocraties prêtes à se défendre.

Nos mesures communes les plus urgentes doivent se focaliser sur l'intensification d'une coopération flexible et pratique. Les structures existantes de l'UE doivent être exploitées avec une plus grande efficacité. Nous devons réduire toute structure rigide qui y ferait obstacle. La souplesse et la visibilité de nos mesures doivent souligner notre détermination.

**1. Renforcer les contrôles à nos frontières externes**

Le règlement établissant une Agence européenne **de garde-frontières et de garde-côtes, sur lequel un accord a été trouvé, doit être formellement adopté et être mis en application dans les plus brefs délais.** Tous les États membres doivent fournir les moyens nécessaires. Ensemble, la France et l'Allemagne affecteront 395 personnels

(FRA : 170 + DEU : 225) au vivier de réaction rapide. Il conviendrait qu'un exercice de simulation de crise puisse avoir lieu avant la fin de l'année afin de vérifier la disponibilité nécessaire du personnel du vivier de réaction rapide.

Nous devons nous assurer que nos frontières externes sont dotées d'équipements adéquats faisant appel à la technologie la plus récente (par ex. systèmes de contrôle mobiles exploitant les bases de données de l'UE et les fichiers internationaux) afin de faciliter un contrôle efficace de chaque individu entrant ou sortant de l'espace Schengen.

Le **PNR européen** doit être mis en application **dans chaque État membre dans les plus brefs délais**, en y intégrant, comme il a été convenu, les vols charters et intra-européens.

Il est essentiel que tous les États membres mettent en œuvre très rapidement **la décision Prüm**.

Le périmètre du projet pilote **ADEP (Automation of the Data Exchange Process)** initié par la France et la Finlande avec un financement allemand, permettant une analyse automatisée entre services de police des antécédents judiciaires des individus, actuellement en cours de développement, **doit être étendu à tous les États membres, ainsi qu'à Europol**.

Nous devons cette année convenir d'un accord politique sur **les fondements d'un registre des entrées et sorties couvrant l'intégralité de l'UE** et nous devrions étudier la possibilité d'y inclure l'ensemble des citoyens de l'UE. Par ailleurs, nous devons nous accorder cette année sur la mise en place d'un **système européen d'information et d'autorisation de voyage (ETIAS)**.

Si l'on souhaite que nos contrôles soient efficaces, nous devons nous assurer que **tous les États membres** alimentent et exploitent **les bases de données internationales et européennes** tels que SIS II, SLTD, VIS, Eurodac ou Europol.

Afin d'améliorer la structure même de l'architecture actuellement fragmentée des bases de données, **il est nécessaire que l'UE crée un système européen unifié pour la gestion des identités. Il faut à cet effet améliorer l'interconnectivité des systèmes internationaux de sécurité et de gestion des frontières**. Une interface de recherche unique doit être mise en place le plus tôt possible et une meilleure exploitation de la biométrie pour toutes les bases de données concernées doit être assurée, notamment SIS II.

Pour les besoins des services répressifs, les autorités compétentes doivent pouvoir **accéder aux bases de données** (Eurodac par exemple) dans des conditions pratiques et efficaces. Les garde-frontières du vivier européen doivent aussi pouvoir consulter toutes les bases de données utiles aux contrôles aux frontières.

Nous devons renforcer la lutte contre la fraude documentaire. À cet effet, un programme de formation doit être mis en place au niveau européen sur la fraude documentaire par la nouvelle Agence européenne **de garde-frontières et de garde-côtes**.

Sur la base de la Communication de la Commission relative à la mise en place d'un **nouveau cadre de partenariat avec les pays tiers** dans le cadre de l'Agenda européen en matière de migration, nous devons aussi assurer une coordination plus étroite dans le domaine de l'assistance concernant les équipements et formations des services de police, et nous sommes favorables à la création de nouveaux partenariats entre polices européennes. L'objectif doit être clair : lutter contre le terrorisme et le trafic des êtres humains et des armes.

## **2. La sécurité au sein de l'espace Schengen**

Nous souhaitons maintenir la libre circulation des personnes et des biens. Pour ce faire, il sera nécessaire d'intensifier la coopération transfrontalière. Pour être à même d'appliquer des contrôles aux frontières qui soient adaptés à la situation tout en restant en dessous du seuil du contrôle frontalier exhaustif, nous avons besoin d'un instrument juridique qui permette de rétablir **les contrôles aux frontières selon des modalités plus flexibles** et mieux **adaptées à la menace terroriste**.

Une action concertée et décisive reste la clé de notre capacité à lutter efficacement contre des menaces intenses et réelles.

Il convient de doter Europol des moyens (financiers et humains) nécessaires **pour rehausser la coopération entre services de police**. Le Centre européen de contre-terrorisme (ECTC) joue déjà un rôle important dans la réponse européenne aux menaces terroristes. La « Taskforce Fraternité » créé à la suite des attentats de Paris est une réussite et peut servir d'exemple des bonnes pratiques pour les cas similaires.

**Les communications chiffrées entre terroristes constituent un défi lors d'enquêtes.** Il est nécessaire d'identifier des solutions permettant de mener des enquêtes efficaces en cas d'utilisation de données chiffrées liées à des actes à caractère terroriste, tout en tenant compte du besoin de protéger le droit à la vie privée numérique des citoyens, en assurant la disponibilité de systèmes cryptographiques hautement impénétrables et en respectant les exigences découlant des principes de nécessité et de proportionnalité, des droits fondamentaux et de l'État de droit. En assurant le partage de bonnes pratiques et d'idées innovantes sur le traitement des communications chiffrées liées à des actes à caractère terroriste, notre intention est de réduire les obstacles qui entraveraient la capacité de l'État à lutter contre les menaces terroristes. Par exemple, **tous les opérateurs, qu'ils soient fournisseurs d'accès à Internet ou de communi-**

**cations électroniques, doivent être sujets aux mêmes obligations en ce qui concerne la coopération judiciaire dans les pays où ils assurent leurs prestations** (indépendamment du pays où se situe leur siège juridique). À terme, il sera nécessaire d'étudier des recours efficaces à l'encontre des opérateurs qui ne s'y conformeraient pas. **La Commission européenne doit étudier la possibilité de proposer des mesures législatives sur cette question.** Nous appelons les États membres et les pays tiers qui ne l'auraient pas déjà fait à signer et à ratifier la **Convention de Budapest sur la cybercriminalité.**

Par ailleurs, nous devons préparer l'avenir et doter l'ECTC **d'une nouvelle composante pour lutter plus efficacement contre les menaces chimiques, biologiques, radiologiques et nucléaires (CBRN CoE).**

**Les services de renseignement doivent renforcer leur coopération,** notamment en soutenant les travaux du Groupe d'action contre le terrorisme (CTG) sur la création d'une plateforme dédiée destinée aux échanges multilatéraux d'informations en temps réel.

Pour ce qui est de la coopération dans les domaines de **la cybercriminalité et de la cybersécurité,** il est nécessaire de renforcer l'ensemble des institutions et instances qui favorisent la coopération entre États membres.

En dernier lieu, mais non des moindres, le **COSI doit être encore amélioré** afin d'assurer une coordination opérationnelle plus efficace dans le domaine de la sécurité.

### **3. Renforcer la lutte contre la radicalisation au niveau de l'UE**

Au sein d'Europol, nous voulons renforcer l'IRU (Internet Referral Unit) afin de mettre en place **un centre européen pour la lutte contre le terrorisme et la radicalisation sur Internet.** L'une des missions de ce centre sera d'identifier les contenus pertinents en partageant les informations et en s'assurant que les contenus déjà identifiés ne sont pas téléchargés à nouveau.

Nous devons également chercher à **restreindre le privilège des hébergeurs de contenus sur Internet** dans les cas où il est exploité pour la communication terroriste (« responsabilité de fait des produits »).

L'Allemagne et la France montrent le chemin et assurent une approbation réciproque des **demandes directes** adressées **aux fournisseurs d'accès à Internet** par les administrations répressives. Le but est de **créer une règle de ce type qui soit applicable à l'intégralité de l'Union européenne.** De plus, Europol et les services répressifs au niveau national doivent bénéficier de **la possibilité d'extraire des données d'inventaire des fournisseurs d'accès à Internet** sans être tenus de respecter des procédures judiciaires trop chronophages.

Nous devons également renforcer et revitaliser le RAN (Radicalisation Awareness Network), **le réseau de l'UE pour la prévention de la radicalisation et la déradicalisation**, en partageant les nombreuses initiatives déjà existantes au niveau national et en favorisant des échanges entre praticiens, scientifiques et acteurs publics. Dans cette perspective, il conviendrait que chaque État membre mette en place un réseau RAN au niveau national. Sur la base de ce réseau, un centre dédié devrait coordonner au niveau européen ces échanges d'expériences.

Dr. Thomas de Maizière, MdB  
Bundesminister des Innern

Bernard Cazeneuve  
Ministre de l'Intérieur