

**Conseil de sécurité**

Distr. générale
16 novembre 2023
Français
Original : anglais

**Lettre datée du 16 novembre 2023, adressée au Président
du Conseil de sécurité par la Présidente du Comité du Conseil
de sécurité créé par la résolution 1373 (2001) concernant la lutte
antiterroriste**

Au nom du Comité du Conseil de sécurité créé par la résolution 1373 (2001) concernant la lutte antiterroriste, j'ai l'honneur de me référer au rapport établi par la Direction exécutive du Comité contre le terrorisme en application du paragraphe 7 de la résolution 2617 (2021) du Conseil de sécurité.

Je vous serais reconnaissante de bien vouloir faire distribuer le présent texte comme document du Conseil de sécurité.

La Présidente du Comité du Conseil de sécurité
créé par la résolution 1373 (2001)
concernant la lutte antiterroriste
(Signé) Lana Zaki Nusseibeh



Application à l'échelle mondiale des dispositions des résolutions 2178 (2014) et 2396 (2017) du Conseil de sécurité appelant à redoubler d'efforts face à la menace évolutive que représentaient les combattants terroristes étrangers et à lutter contre les déplacements de terroristes, notamment grâce à la collecte, à l'utilisation et au partage des renseignements préalables concernant les voyageurs, des données des dossiers passagers et des données biométriques, et à l'établissement de listes de surveillance des terroristes connus ou présumés

I. Introduction

1. Dans sa résolution 2617 (2021), le Conseil de sécurité a demandé à la Direction exécutive du Comité contre le terrorisme d'évaluer l'application par les États Membres des dispositions de ses résolutions 2178 (2014) et 2396 (2017) appelant à un renforcement de l'action relative à la menace évolutive que représentent les combattants terroristes étrangers et à la lutte contre les déplacements de terroristes, notamment par la collecte, l'utilisation et le partage des renseignements préalables concernant les voyageurs, des données des dossiers passagers et des données biométriques, et par l'établissement de listes de surveillance des terroristes connus ou présumés, et de présenter un rapport sur la mise en œuvre de ces dispositions à l'échelle mondiale d'ici décembre 2022, en prenant note à cet égard des bonnes pratiques et des recommandations, y compris les Principes directeurs relatifs aux combattants terroristes étrangers (Principes directeurs de Madrid) (S/2015/939) et leur additif (2018) (S/2018/1177).

2. L'efficacité de la sécurité aux frontières et la diffusion rapide des données de renseignement aux niveaux national, régional et international sont essentielles si l'on veut empêcher les mouvements de terroristes, y compris de combattants terroristes étrangers, et de groupes terroristes et mettre en œuvre efficacement des mesures de lutte antiterroriste conformément à la résolution 1373 (2001) du Conseil de sécurité et aux autres résolutions pertinentes du Conseil.

3. Le maintien de la sécurité des frontières aériennes, terrestres et maritimes est un défi que doivent relever tous les États Membres, compte tenu en particulier de la rapide évolution de la situation en matière de sécurité. De nombreux États ne disposent pas des ressources financières et humaines, des équipements, des réglementations précises, des ressources humaines et des experts dotés de compétences spécialisées requis, ni des mécanismes de coopération à l'intérieur des institutions et entre eux qui leur permettraient de mettre en œuvre efficacement des mesures permettant de contrer la menace que représentent les combattants terroristes étrangers et de lutter contre les déplacements de terroristes. L'Équipe d'appui analytique et de surveillance des sanctions réitère que les données transmises par les systèmes de renseignements préalables concernant les voyageurs (RPCV) et les dossiers passagers (PNR) jouent un rôle essentiel pour ce qui est de l'efficacité de la procédure d'évaluation des risques et de contrôle des voyageurs reposant sur des observations factuelles. Toutefois, le fait de ne pas comparer systématiquement ces données aux listes de surveillance nationales et internationales, aux listes de sanctions des Nations Unies et aux informations contenues dans les bases de données pertinentes de l'Organisation internationale de police criminelle (INTERPOL) compromet leur utilité en tant qu'outils d'identification des terroristes et des combattants terroristes étrangers et de lutte contre l'utilisation d'itinéraires détournés. Plusieurs États Membres ont noté le risque croissant que des revenants et des relocalisés utilisent d'autres itinéraires associés à la criminalité organisée pour

regagner leur pays d'origine sans être détectés par les systèmes en place¹. La Direction exécutive a également identifié un risque similaire concernant le transit et la relocalisation de combattants terroristes étrangers dans d'autres régions où les terroristes et les combattants terroristes étrangers tirent parti des vulnérabilités des systèmes de contrôle aux frontières des États et se soustraient à la détection

4. La menace que représentent les combattants terroristes étrangers continue d'exiger des États Membres et de la communauté internationale qu'ils renforcent la sécurité aux frontières et comblent les lacunes en matière de sécurité résultant d'une moindre capacité d'utiliser les outils essentiels de contrôle aux frontières et les mécanismes d'échange d'informations. Après l'adoption par le Conseil de sécurité des résolutions 2178 (2014) et 2396 (2017), qui visent l'une et l'autre à endiguer le flux de combattants terroristes étrangers, le Comité contre le terrorisme et sa Direction exécutive ont encore renforcé leur mobilisation et leur analyse des capacités de lutte antiterroriste des États, notamment en ce qui concerne la sécurité aux frontières. Les évaluations et analyses menées par la Direction exécutive au nom du Comité contre le terrorisme continuent de révéler des lacunes majeures dans le respect par un certain nombre d'États des exigences en matière de sécurité aux frontières énoncées dans les résolutions 1373 (2001), 1624 (2005), 2178 (2014) et 2396 (2017), notamment l'élaboration de stratégies complètes et intégrées de gestion des frontières, l'analyse des données relatives aux passagers, le recoupement des informations par rapport aux listes de surveillance et aux bases de données, et l'utilisation de la biométrie dans le cadre des mesures de lutte contre le terrorisme. L'absence de systèmes informatisés est également problématique, les bases de données et les outils utilisés manuellement n'offrant pas le même niveau d'efficacité et ne permettant pas de garantir un accès rapide à l'information.

5. Depuis l'adoption des résolutions 2178 (2014) et 2396 (2017) du Conseil de sécurité, la nature de la menace terroriste n'a cessé d'évoluer, obligeant les États Membres à continuer d'adapter leurs politiques et leurs approches de manière à relever les défis et à combler les lacunes existantes dans leurs mesures de lutte contre le terrorisme, ainsi qu'à explorer les moyens de prévenir les menaces et les tendances nouvelles et émergentes et de les contrer.

6. Un certain nombre d'États ont fait des progrès quant au renforcement de la sécurité de leurs frontières et à la prévention des déplacements de combattants terroristes étrangers. La Direction exécutive continue de recenser les bonnes pratiques à cet égard, notamment l'amélioration de la sécurité des documents de voyage, l'introduction d'une obligation de visa de transit et l'utilisation plus efficace des bases de données d'INTERPOL pour effectuer des contrôles afin de repérer et d'identifier les combattants terroristes étrangers. Un nombre d'États non négligeable a également développé cette capacité à l'aide d'outils informatiques, en établissant des listes de surveillance et des bases de données, en recoupant des dossiers pénaux et en mettant en place des systèmes d'échange d'informations. Les États Membres ont fait quelques progrès dans le renforcement de la coopération et de la coordination en matière de sécurité et de répression du terrorisme, grâce à des mécanismes interinstitutions de mise en commun de l'information entre institutions ou à des cellules de fusion. Ils ont également adopté des plans d'action nationaux de prévention et de répression du terrorisme et renforcé la coopération internationale, notamment en élargissant au-delà des bureaux centraux nationaux l'accès au système mondial de communication policière I-24/7 de l'Organisation internationale de police criminelle (INTERPOL)²,

¹ Voir le trentième rapport de l'Équipe d'appui analytique et de surveillance des sanctions présenté conformément à l'annexe I de la résolution 2610 (2021) (S/2022/547).

² Voir www.un.org/securitycouncil/ctc/sites/www.un.org.securitycouncil.ctc/files/files/documents/.

désormais offert à d'autres entités nationales de répression, y compris les agents de première ligne.

7. En dépit des avancées réalisées à l'échelle mondiale, la longueur considérable des frontières de nombreux États, la complexité des terrains qu'elles traversent souvent, les zones non contrôlées qui se trouvent entre les points de passage frontaliers officiels et la technique des itinéraires de voyage fractionnés donnent à cet égard beaucoup de fil à retordre à la majorité des États Membres. L'une des plus grandes difficultés auxquelles font face les États s'agissant d'appliquer les dispositions de la résolution 1373 (2001) à cet égard est la nécessité de vérifier efficacement l'identité des voyageurs aux points d'entrée.

8. Les évaluations de la Direction exécutive continuent de révéler des écueils dans la mise en œuvre des mesures de sécurité de base telles que la coopération et l'échange d'informations au niveau national et entre les organismes nationaux concernés, des lacunes importantes dans l'accès aux informations essentielles, notamment aux bases de données d'INTERPOL, l'absence de protocoles de partage de données qui permettraient d'échanger des informations avec d'autres États et avec INTERPOL, notamment des données sur les combattants terroristes étrangers et des données biométriques, et l'inadéquation de la mise en œuvre des normes et pratiques recommandées existantes, telles que celles élaborées par l'Organisation de l'aviation civile internationale (OACI).

9. Pour établir le présent rapport, la Direction exécutive a recueilli des informations et des données provenant des évaluations auxquelles elle a procédé au nom du Comité contre le terrorisme, du dialogue qu'elle entretient avec les États Membres, de l'Enquête mondiale de 2021 sur la mise en œuvre par les États Membres de la résolution 1373 (2001) et d'autres résolutions pertinentes du Conseil de sécurité, du Programme de lutte contre les déplacements des terroristes dirigé par le Bureau de lutte contre le terrorisme et des initiatives en la matière menées dans le cadre du Pacte mondial des Nations Unies de coordination contre le terrorisme. En tant que principaux partenaires de mise en œuvre, le Bureau de lutte contre le terrorisme, l'OACI et INTERPOL ont été consultés au sujet des principales problématiques qui font l'objet du présent rapport.

10. Il convient de noter que les données disponibles concernant la collecte, l'utilisation et le partage de données de RPCV et de PNR et de données biométriques, ainsi que de données relatives à la liste de surveillance des terroristes connus ou présumés, varient considérablement. La mise en œuvre des quatre outils que les États Membres sont tenus d'utiliser n'a pas évolué au même rythme. Les variations tiennent dans une certaine mesure à la disponibilité de l'assistance technique et au renforcement des capacités, qui sont les plus avancés en ce qui concerne les RPCV et les PNR grâce au Programme de lutte contre les déplacements des terroristes. Il n'a pas été mis en place de programmes d'assistance technique similaires concernant les données biométriques et les listes de surveillance. Les informations relatives à l'état d'avancement de la mise en œuvre des systèmes de RPCV et de PNR sont par ailleurs plus méthodiquement communiquées et consignées³.

II. Gestion coordonnée des frontières

11. Bien que la menace du terrorisme ait une envergure mondiale, elle a des répercussions différentes selon les États, les régions et les sous-régions. La capacité

³ Par exemple, l'outil de suivi des données relatives aux systèmes de RPCV/PNR de l'Association du transport aérien international (IATA) (« API/PNR World Tracker ») permet de recueillir des informations sur l'utilisation de ces systèmes (non accessibles au public).

de tout État de gérer ses frontières et de contrer les déplacements des terroristes dépend fortement de facteurs tels que la situation géographique et les ressources, l'expertise et l'équipement disponibles. La porosité des frontières reste une préoccupation majeure, car elle peut permettre aux terroristes d'entrer dans un État sans passer par les points de passage officiels et de soustraire ainsi à un examen de leurs documents et la vérification des listes de surveillance ou des bases de données nationales et internationales. La surveillance de vastes espaces ouverts nécessite des ressources importantes. Les caractéristiques géologiques et climatiques de certains États compliquent encore les efforts déployés pour contrôler les personnes qui entrent sur leur territoire et en sortent. Le manque d'infrastructures nécessaires aux postes-frontières limite l'accès des agents aux bases de données pertinentes et est souvent aggravé par le fait que les agents d'un poste frontière peuvent être responsables de la surveillance de vastes zones au-delà des points de passage officiels.

12. La gestion coordonnée des frontières s'est avérée une bonne pratique pour gérer efficacement les frontières et permettre la coopération et la coordination de toutes les institutions de sécurité lorsque la sécurité des frontières ne peut être assurée par un seul organisme, afin de renforcer la sécurité globale des frontières et d'endiguer le flux de combattants terroristes étrangers. Une approche coordonnée de la gestion des frontières peut permettre aux États: a) de renforcer le contrôle et les services destinés à assurer la sécurité ; b) de clarifier les responsabilités et les axes de travail ; c) de rationaliser les opérations ; d) d'éviter les doublons ; e) de renforcer les flux de communication et l'échange d'informations ; f) de rationaliser l'utilisation des ressources humaines et financières ; g) d'apporter des réponses plus complètes et rapides face aux menaces émergentes ; h) de riposter plus rapidement et plus efficacement face aux menaces nouvelles⁴. L'élaboration et la mise en œuvre de stratégies globales de gestion des frontières restent une gageure pour de nombreux États. Les évaluations de la Direction exécutive continuent de donner à penser que, dans un certain nombre d'États, de telles stratégies n'existent pas et que la gestion des frontières n'est ni incluse ni prise en compte dans leurs stratégies nationales de lutte contre le terrorisme. Il est essentiel que les États continuent à se concentrer sur ces questions opérationnelles, notamment sur la nécessité que les informations sur les personnes et les marchandises entrant sur leur territoire et en sortant soient communiquées aux agents en poste aux points de passage des frontières et ailleurs sur leur territoire⁵.

13. Dans les résolutions 2178 (2014), 2322 (2016), 2396 (2017) et 2482 (2019) du Conseil, les États Membres sont encouragés, à utiliser régulièrement les bases de données d'INTERPOL pour contrôler les voyageurs dans les aéroports et aux points d'entrée terrestres et maritimes et à veiller à ce que leurs forces de l'ordre, leurs services de sécurité des frontières et leurs services de douanes soient connectés à ces bases de données par l'intermédiaire de leurs bureaux centraux nationaux ou grâce à un accès plus large au système mondial de communication policière I-24/7 d'INTERPOL, au-delà des bureaux centraux nationaux, y compris aux points de passage des frontières.

14. Dans le cadre des efforts déployés pour protéger les frontières aériennes, y compris dans le domaine de la sécurité des documents, la grande majorité des États a fait des progrès rapides s'agissant de satisfaire à la demande de l'Organisation de l'aviation civile internationale de mettre en place des documents de voyage lisibles à la machine. Au total, 165 États ont franchi une nouvelle étape en introduisant les

⁴ Voir www.un.org/securitycouncil/ctc/sites/www.un.org.securitycouncil.ctc/files/files/documents/2021/Jan/security-council-guiding-principles-on-foreign-terrorist-fig.pdf.

⁵ Voir le Guide technique pour la mise en œuvre de la résolution 1373 (2001) du Conseil de sécurité et d'autres résolutions pertinentes (S/2019/998, annexe).

passports électroniques, qui ajoutent une couche de sécurité aux passeports traditionnels non électroniques grâce à l'incorporation dans le livret d'une puce électronique stockant les informations biographiques visibles à la page 2 du passeport, ainsi qu'un élément de sécurité numérique. En outre, 92 États ont rejoint le système de l'OACI destiné à faciliter le partage d'informations entre les États, connu sous le nom de Répertoire OACI de clés publiques ; cet outil centralisé est une source en ligne indépendante, organisée, sûre et peu coûteuse d'informations actualisées sur les éléments de sécurité.

15. La base de données d'INTERPOL sur les documents de voyage volés ou perdus contient des informations mondiales sur les documents de voyage et d'identité qui ont été déclarés volés, perdus, révoqués ou invalides, ou qui ont été volés vierges, et qui devraient être retirés de la circulation. Elle est alimentée par les informations émanant des États membres d'INTERPOL et contient actuellement environ 99 millions d'entrées. Dans ses recommandations, la Direction exécutive encourage les États à redoubler d'efforts pour alimenter systématiquement les bases de données d'INTERPOL, notamment la base de données sur les documents de voyage volés ou perdus.

16. Le secteur maritime est particulièrement attrayant pour les terroristes car les ports, les navires et les voies de navigation sont des nœuds essentiels pour la livraison de biens et de services considérés comme vitaux pour le fonctionnement des économies des pays et communément appelés infrastructures critiques. Les bateaux à passagers sont également des cibles intéressantes en raison de leur capacité d'accueillir un grand nombre de personnes. En l'absence de procédures d'embarquement rigoureuses, les navires de croisière modernes peuvent devenir des cibles molles idéales pour les groupes terroristes désireux de causer un maximum de dégâts et de recevoir une large couverture médiatique en limitant la planification. Le secteur maritime reste une sphère difficile en termes de surveillance policière. L'absence de frontières matérielles et de postes de contrôle rend particulièrement difficile la surveillance de vastes espaces marins.

17. Les évaluations de la Direction exécutive laissent penser que les États doivent lier la sécurité maritime à l'ensemble de leur action antiterroriste et renforcer la sécurité des moyens maritimes en tant qu'éléments de leur infrastructure critique. La collaboration et la coordination entre les autorités responsables de la sécurité maritime ou les garde-côtes dans le cadre de l'architecture et des mesures de lutte contre le terrorisme prises par les États sont souvent insuffisantes.

18. La Direction exécutive promeut une approche de la sûreté maritime à l'échelle de l'ensemble de l'administration et fondée sur les risques et, lors de ses évaluations, examine la mise en œuvre par les États, le cas échéant, du Code international pour la sûreté des navires et des installations portuaires (code ISPS), qui contient un ensemble complet de mesures destinées à renforcer la sûreté des navires et des installations portuaires, élaboré sous les auspices de l'Organisation maritime internationale (OMI).

19. La Direction exécutive est membre du Groupe de travail de l'Organisation mondiale des douanes (OMD) sur la facilitation et le contrôle des passagers. Celui-ci élabore actuellement des directives sur les renseignements préalables concernant les voyageurs (RPCV) et aux renseignements relatifs aux réservations (également connus sous le nom de dossiers passagers (PNR) dans l'aviation) pour les voyages en bateau de croisière, devant être publié en 2023. Ces orientations sont basées sur les orientations relatives aux voyages en avion élaborées par le « comité de contact » de l'OMD, de l'Association internationale du transport aérien (IATA) et de l'OACI et ont été formulées en consultation avec l'Association internationale des lignes de croisière et l'OMI. L'élaboration de ces orientations est conforme aux résolutions [2178 \(2014\)](#), [2396 \(2017\)](#) et [2482 \(2019\)](#) du Conseil de sécurité et à la « Résolution

de Punta Cana » de l'OMD (2015). Les orientations portent sur la question du transfert des données de RPCV et des données liées aux renseignements relatifs aux réservations du système d'un opérateur à un organisme de contrôle des frontières et sur la gestion de ces données, y compris les dispositions relatives au stockage et à la protection.

20. La sécurité des frontières et le partage des informations et renseignements aux niveaux national, régional et international sont essentiels si l'on veut empêcher les mouvements de terroristes et de groupes terroristes et mettre en œuvre efficacement les mesures de lutte antiterroriste.

21. De nombreux États Membres ont pris des mesures pour renforcer la sécurité aux frontières et empêcher les déplacements de combattants terroristes étrangers. Ces mesures comprennent l'introduction de visas touristiques électroniques, de documents d'identité pour les marins et de procédures d'immigration biométriques sans passeport dans les aéroports.

22. La pièce d'identité des gens de mer délivrée conformément à la Convention (n° 185) sur les pièces d'identité des gens de mer (révisée) de 2003 de l'Organisation internationale du Travail, deviendra un document d'immigration officiel pour plus de 1,5 million de gens de mer travaillant et vivant sur des navires participant au commerce international. Ce document permet aux gens de mer de franchir les frontières sans visa, de monter à bord des navires et de débarquer dans les ports. Il est conçu selon une technologie proche de celle des passeports électroniques, en intégrant les normes de l'OACI, et permet d'assurer la sécurité dans les ports et aux frontières.

III. Dispositions pertinentes des résolutions 2178 (2014) et 2396 (2017) du Conseil de sécurité sur la collecte, l'utilisation et le partage des renseignements préalables concernant les voyageurs, des données des dossiers passagers et des données biométriques, ainsi que sur l'établissement de listes de surveillance des terroristes connus ou présumés

23. Dans sa résolution 2396 (2017), le Conseil de sécurité a décidé que, en application de la résolution 2178 (2014) et des normes pertinentes fixées par l'OACI, et aux fins de prévenir, de détecter et d'instruire les infractions terroristes et les voyages de terroristes, dans le plein respect des droits humains et des libertés fondamentales, les États Membres devraient mettre en place des systèmes de renseignements préalables concernant les voyageurs (RPCV) et exiger des exploitants d'aéronefs opérant sur leur territoire qu'ils communiquent à l'avance ces renseignements aux autorités nationales compétentes. Il a en outre demandé aux États de communiquer ces informations à l'État de résidence ou de nationalité des intéressés ou aux pays de destination, de transit ou de réinstallation et aux organisations internationales compétentes, selon qu'il convient, et de veiller à ce qu'elles soient analysées par toutes les autorités compétentes.

24. Le Conseil a également décidé que les États renforceraient leur capacité de collecter et de traiter les données des dossiers passagers (PNR) et de veiller à ce que ces données soient communiquées à toutes les autorités nationales compétentes et utilisées par celles-ci. Il a encouragé les États à communiquer ces données aux États concernés afin de détecter les combattants terroristes étrangers qui rentrent dans leur pays d'origine ou de nationalité, ou qui se rendent dans un pays tiers ou s'y réinstallent, en particulier toutes les personnes désignées par le Comité faisant suite

aux résolutions [1267 \(1999\)](#), [1989 \(2011\)](#) et [2253 \(2015\)](#) concernant l'État islamique d'Iraq et du Levant (Daech), Al-Qaïda et les personnes, groupes, entreprises et entités qui leur sont associés. Le Conseil a souligné que toutes ces mesures doivent être prises conformément au droit interne et aux obligations internationales et dans le plein respect des droits humains et des libertés fondamentales.

25. L'additif aux principes directeurs relatifs aux combattants terroristes étrangers (2018) contient le principe directeur 36, qui concerne la mise en œuvre des obligations relatives aux RPCV et au PNR et précise les éléments qui constituent des moyens liés à ces sources de données.

26. Dans sa résolution [2396 \(2017\)](#), le Conseil a décidé que les États Membres devaient élaborer et mettre en œuvre des systèmes de collecte de données biométriques, y compris aux ports d'entrée, qui pourraient comprendre la capture des empreintes digitales, la prise de photographies, la reconnaissance faciale, et d'autres systèmes de saisie de données biométriques, pour identifier de manière responsable et correcte les terroristes, y compris les combattants terroristes étrangers, dans le respect du droit interne et du droit international des droits de l'homme. Il a en outre demandé aux autres États et aux entités internationales, régionales et sous-régionales de fournir aux États Membres une assistance technique et des ressources et de renforcer leurs capacités afin qu'ils puissent mettre en place de tels systèmes et encouragé les États Membres à communiquer de manière responsable ces données aux États Membres concernés, selon qu'il conviendrait, ainsi qu'à INTERPOL et à d'autres organismes internationaux compétents.

27. L'additif aux principes directeurs relatifs aux combattants terroristes étrangers contient le principe directeur 38, qui concerne l'élaboration et l'utilisation responsable de systèmes biométriques. Il précise en outre les éléments qui constituent une utilisation et un échange responsables des données biométriques.

28. En ce qui concerne les informations biométriques, le Conseil, dans sa résolution [2322 \(2016\)](#), a invité les États à communiquer, selon qu'il conviendrait, des informations sur les combattants terroristes étrangers et d'autres terroristes et organisations terroristes, y compris leurs données biographiques et biométriques. Dans la même résolution, il a souligné qu'il importait d'inscrire ces informations dans les listes nationales de personnes à surveiller et les bases de données multilatérales de contrôle.

29. Dans sa résolution [2396 \(2017\)](#), le Conseil a décidé que les États Membres s'emploieraient à établir des listes de personnes à surveiller ou des bases de données de terroristes connus ou présumés, y compris de combattants terroristes étrangers, aux fins de leur utilisation par les forces de l'ordre, les services de sécurité des frontières, de douanes et de renseignement et les forces armées pour contrôler les voyageurs et procéder à des évaluations des risques et à des enquêtes, dans le respect du droit interne et du droit international, notamment du droit international des droits humains. Il a en outre encouragé les États Membres à échanger ces informations par l'intermédiaire de mécanismes bilatéraux et multilatéraux, dans le respect du droit interne et du droit international des droits de l'homme, et encourage également les États Membres et les organisations compétentes à faciliter le renforcement des capacités et l'assistance technique aux États Membres qui s'efforcent d'honorer cette obligation.

30. L'additif aux principes directeurs relatifs aux combattants terroristes étrangers contient le principe directeur 37, qui concerne l'élaboration de listes de surveillance et de bases de données et le partage d'informations au moyen de mécanismes bilatéraux et multilatéraux.

IV. État de la mise en œuvre à l'échelle mondiale des dispositions des résolutions 2178 (2014) et 2396 (2017) du Conseil de sécurité grâce à la collecte, à l'utilisation et au partage des renseignements préalables concernant les voyageurs, des données des dossiers passagers et des données biométriques, ainsi qu'à l'établissement de listes de surveillance des terroristes connus ou présumés

31. La Direction exécutive du Comité contre le terrorisme a intégré les questions relatives aux renseignements préalables concernant les voyageurs, aux PNR et à l'utilisation responsable des données biométriques et des listes de surveillance ou des bases de données dans ses évaluations, qui sont menées au nom du Comité, et dans les dialogues qu'elle tient avec les États Membres. Elle a en outre établi des partenariats avec un large éventail d'acteurs compétents dans ces domaines.

32. Dans sa résolution 2396 (2017), le Conseil a exhorté l'OACI à travailler avec ses États membres en vue d'établir une norme pour la collecte, l'utilisation, le traitement et la protection des données de PNR. Pour donner suite à cette demande, l'OACI a chargé une Équipe spéciale PNR d'examiner les normes et pratiques recommandées concernant les dossiers passagers (PNR) contenues dans l'annexe 9 de la Convention relative à l'aviation civile internationale (Convention de Chicago) et de présenter des propositions visant à l'élaboration de nouvelles normes. En conséquence, de nouvelles normes PNR ont été élaborées en tant qu'amendement 28 à l'annexe 9, intitulé « Facilitation ». Cet amendement a été adopté par le Conseil de l'OACI le 23 juin 2020 et est devenu applicable à compter du 28 février 2021. Les nouvelles normes PNR apportent aux États contractants de l'OACI et au secteur une certitude quant à la mise en œuvre des exigences PNR dans le monde entier, en établissant une approche internationale solide et cohérente et une base de référence s'agissant des garanties de protection des données qui régissent la collecte, l'utilisation, le traitement et la protection des données de PNR.

33. Il n'existe pas de normes communes et internationalement reconnues pour la mise en œuvre de systèmes biométriques, de listes de surveillance ou de bases de données⁶. L'accomplissement de ces obligations doit se faire dans le respect du droit national et du droit international des droits humains. Il convient également de noter qu'il s'agit pour les États Membres d'une entreprise extrêmement difficile, exigeant de vastes compétences ainsi que des connaissances et des ressources juridiques, techniques et opérationnelles.

34. Le domaine de la biométrie continue d'évoluer rapidement et les États Membres continuent de chercher de nouveaux moyens de développer leurs capacités biométriques, y compris le déploiement de nouvelles applications, qui s'est accéléré durant la pandémie de maladie à coronavirus (COVID-19). Il est largement établi que l'identification biométrique, lorsqu'elle est utilisée conformément aux normes et standards du droit international applicable, y compris le droit international des droits humains, est un outil efficace et puissant permettant d'identifier les terroristes et les criminels, et potentiellement d'interrompre leurs déplacements, et d'authentifier et vérifier les identités, grâce à des applications criminalistiques supplémentaires.

⁶ Certaines organisations ont élaboré des normes pertinentes dans ce domaine, à l'instar de l'Organisation internationale de normalisation (ISO), organisation internationale indépendante et non gouvernementale composée de 169 organismes nationaux de normalisation qui a élaboré des normes pertinentes favorisant, par exemple, la gestion de la qualité et la protection des données.

35. L'élaboration de listes de surveillance ou de bases de données est essentielle au traitement et à la vérification de l'identité des voyageurs et pour repérer les terroristes, y compris les combattants terroristes étrangers, les combattants terroristes étrangers qui retournent dans leur pays et ceux qui se relocalisent. Constituées de différents types de données, les listes de surveillance et les bases de données sont des systèmes d'alerte nationaux ou régionaux grâce auxquels sont lancés des alertes rapides et des procédures de contrôle qui facilitent la reconnaissance et l'identification des criminels et des terroristes présumés aux points de passage des frontières. L'application par les États Membres s'est améliorée depuis l'adoption de la résolution [2396 \(2017\)](#) du Conseil de sécurité, mais dans beaucoup d'entre eux, les organismes nationaux compétents gèrent toujours leurs propres listes de surveillance ou bases de données, souvent sans aucune interconnectivité ou sans partage d'informations ou accès mutuel. Il existe d'énormes différences entre les régions et les pays en ce qui concerne la mise en œuvre des dispositions pertinentes de la résolution [2396 \(2017\)](#).

<i>Région</i>	<i>Informations préalables sur les passagers et données des dossiers passagers</i>	<i>Biométrie</i>	<i>Listes ou bases de données de surveillance</i>
Afrique du Nord			
Algérie, Égypte, Libye, Maroc, Mauritanie, Tunisie	Il n'existe pas encore de systèmes de RPCV ou de PNR fonctionnels. Quatre États reçoivent les manifestes des passagers à l'avance (mais pas de manière systématique). En l'absence d'un cadre juridique et institutionnel approprié, notamment de centres de ciblage ou de services d'information sur les passagers, la capacité de détecter les éventuels terroristes à la frontière varie considérablement.	La plupart des États recueillent et stockent les données relatives à l'entrée et à la sortie des personnes qui franchissent la frontière, mais saisissent et vérifient rarement les données biométriques, telles que les empreintes digitales.	Un État a mis en place des équipes de ciblage et envoie des listes de terroristes, y compris de combattants terroristes étrangers, aux postes-frontières.
Afrique de l'Est			
Comores, Djibouti, Érythrée, Éthiopie, Kenya, Ouganda, République-Unie de Tanzanie, Rwanda, Somalie, Soudan, Soudan du Sud	Deux États bénéficient du Programme de lutte contre les déplacements des terroristes, qui a servi de feuille de route pour la mise en œuvre des capacités relatives aux RPCV et aux PNR dans chacun d'eux. Un autre État a mis en place un système de RPCV utilisable uniquement pour les passagers de sa compagnie aérienne nationale. Les huit autres États envisagent de mettre à jour leur système pour renforcer leurs capacités en matière de renseignements préalables concernant les voyageurs.	Informations insuffisantes.	Informations insuffisantes.
Afrique australe			
Afrique du Sud, Botswana, Lesotho, Madagascar, Malawi, Maurice, Mozambique, Namibie, Seychelles, Swaziland, Zambie, Zimbabwe	Un État s'est servi de son système de RPCV pour mettre en place un dispositif de contrôle général et un autre a entrepris de le faire. Aucun État n'applique actuellement des mesures liées aux PNR.	Informations insuffisantes.	Six États ont établi des listes de surveillance.

<i>Région</i>	<i>Informations préalables sur les passagers et données des dossiers passagers</i>	<i>Biométrie</i>	<i>Listes ou bases de données de surveillance</i>
Afrique de l'Ouest			
Bénin, Burkina Faso, Cabo Verde, Côte d'Ivoire, Gambie, Ghana, Guinée, Guinée-Bissau, Libéria, Mali, Niger, Nigéria, Sénégal, Sierra Leone, Togo ⁷	Bien qu'aucun système de RPCV fonctionnel ne soit encore en place dans les États de la sous-région, cinq États reçoivent l'assistance du Programme de lutte contre les déplacements des terroristes pour la mise en œuvre d'un système de RPCV/PNR. Quatre États reçoivent sporadiquement des manifestes passagers ou des RPCV.	Informations insuffisantes.	La capacité de détecter aux frontières des personnes qui pourraient être suspectées de terrorisme, y compris des combattants terroristes étrangers, reste limitée.
Afrique centrale			
Angola, Burundi, Cameroun, Cabo Verde, Congo, Gabon, Guinée équatoriale, République centrafricaine, République démocratique du Congo, Sao Tomé-et-Principe, Tchad	Cinq États sont dotés d'un système informatisé de gestion des entrées et sorties de voyageurs, système installé trouvant principalement dans les aéroports internationaux. Les postes de contrôle des frontières terrestres et maritimes continuent de s'appuyer sur des systèmes manuels, utilisant des versions papier. La mise en œuvre des systèmes de RPCV et de PNR est partielle et marginale. Dans le cas des deux États qui ont accès aux manifestes des passagers, les informations et la technologie disponibles ne permettent pas d'utiliser les systèmes de RPCV et de PNR.	Une politique de circulation sans visa a été approuvée par tous les États Membres de la Communauté économique et monétaire de l'Afrique centrale (CEMAC) en 2017. Toutefois, pour que la liberté de circulation soit pleinement mise en œuvre, les États membres de la CEMAC doivent introduire une technologie d'identification biométrique et assurer une coordination régionale entre les forces de police et de sécurité.	Informations insuffisantes.
Îles du Pacifique			
Fidji, Îles Marshall, Îles Salomon, Kiribati, Micronésie (États fédérés de), Nauru, Palaos, Papouasie-Nouvelle-Guinée, Samoa, Tonga, Tuvalu, Vanuatu	Aucun État n'utilise les systèmes de RPCV ou de PNR, mais quatre d'entre eux se sont dotés d'une législation qui impose aux aéronefs et embarcations à destination de leur territoire de les notifier au préalable de leur arrivée et de leur communiquer des renseignements sur l'ensemble de leurs passagers et membres d'équipage. Un État a officiellement adopté la	Informations insuffisantes.	Informations insuffisantes.

⁷ Le Cabo Verde est également inclus dans les perspectives régionales pour l'Afrique centrale.

<i>Région</i>	<i>Informations préalables sur les passagers et données des dossiers passagers</i>	<i>Biométrie</i>	<i>Listes ou bases de données de surveillance</i>
	stratégie du Programme OACI d'identification des voyageurs (Programme d'identification des voyageurs (TRIP), et la plupart des États se sont dotés d'une législation érigeant en infraction l'utilisation de documents de voyage frauduleux.		
Asie du Sud-Est			
Brunéi Darussalam, Cambodge, Indonésie, Malaisie, Myanmar, Philippines, République démocratique populaire lao, Singapour, Thaïlande, Timor-Leste, Viet Nam	Trois États utilisent des systèmes interactifs de RPCV RPCVi et de PNR (PNRi), et deux autres disposent de systèmes de RPCV et de PNR dans leurs principaux aéroports internationaux. Un État n'utilise qu'un système de RPCVi. Cinq États ne disposent d'aucun des deux systèmes. Un État a bénéficié du Programme de lutte contre les déplacements des terroristes.	Tous les États de cette région ont mis en place un système d'enregistrement des personnes qui franchissent leurs frontières. Certains d'entre eux utilisent des systèmes biométriques sophistiqués pour collecter et stocker en temps réel les informations relatives aux entrées et aux sorties des voyageurs, mais d'autres sont dotés de systèmes moins rigoureux. Deux États ont mis en place des systèmes de contrôle électronique aux frontières qui sont reliés au siège de plusieurs de leurs départements clés. Quatre États utilisent des systèmes biométriques plus ou moins perfectionnés aux principaux points d'entrée.	Les autorités de police des États exposés à un risque élevé de terrorisme établissent des listes de surveillance des terroristes et les communiquent à leurs agents de première ligne chargés des contrôles aux frontières afin d'endiguer les mouvements de terroristes, y compris les combattants terroristes étrangers
Asie du Sud			
Afghanistan, Bangladesh, Bhoutan, Inde, Maldives, Népal, Pakistan, Sri Lanka	Les États de la sous-région ont considérablement amélioré leur mise en œuvre des systèmes de RPCV et de PNR. Actuellement, un État dispose d'un système de RPCVi, et un autre devrait mettre le sien en place. Deux autres États ont mis en œuvre un tel système en 2020 et en 2021, respectivement. Un État a mis en place un système de PNR en 2021, et deux autres États prévoient de faire de même. Trois États n'ont pas encore introduit de législation exigeant la mise en œuvre d'un	Informations insuffisantes.	Informations insuffisantes.

<i>Région</i>	<i>Informations préalables sur les passagers et données des dossiers passagers</i>	<i>Biométrie</i>	<i>Listes ou bases de données de surveillance</i>
	système de RPCV, et quatre États n'exigent pas encore de système de PNR.		
Asie centrale et sud du Caucase			
Arménie, Azerbaïdjan, Géorgie, Kazakhstan, Kirghizistan, Ouzbékistan, Tadjikistan, Turkménistan	Aucun État n'a encore mis en place de système de RPCV, mais la plupart ont pris des mesures dans ce sens, notamment en faisant des demandes d'assistance technique, en procédant à des analyses comparatives des systèmes existants, en créant des groupes de travail interinstitutions, en entamant des révisions législatives et en mettant sur pied des procédures de passation de marchés. Dans plusieurs États, certains exploitants d'aéronefs fournissent volontairement des renseignements préalables concernant les voyageurs, mais il n'existe pas de cadre législatif adéquat. L'Organisation pour la sécurité et la coopération en Europe a activement aidé les États d'Asie centrale dans ce domaine. Au moins un État a confirmé sa volonté de recevoir une assistance dans le cadre du Programme de lutte contre les déplacements des terroristes.	Informations insuffisantes.	Informations insuffisantes.
Asie de l'Ouest			
Arabie saoudite, Bahreïn, Émirats arabes unis, Iran (République islamique d'), Iraq, Jordanie, Koweït, Liban, Oman, Qatar, République arabe syrienne, Yémen	Un État est passé à un système de RPCVi. Toutefois, peu d'autres États ont mis en place un système de RPCV. Certains États sont en train de développer un système de PNR, tandis que d'autres n'ont encore aucun système en place.	Informations insuffisantes	Informations insuffisantes

<i>Région</i>	<i>Informations préalables sur les passagers et données des dossiers passagers</i>	<i>Biométrie</i>	<i>Listes ou bases de données de surveillance</i>
Asie de l'Est			
Chine, Japon, Mongolie, République de Corée, République populaire démocratique de Corée	Quatre États utilisent des systèmes de RPCV et de PNR, dont deux emploient un système de RPCVi. Dans trois États, les agents chargés de l'immigration et de la sécurité aux frontières ont accès aux informations relatives aux RPCV. Dans l'un de ces trois États, les systèmes d'enregistrement des exploitants d'aéronefs dans les aéroports internationaux sont également connectés à un système de RPCV, tandis que dans un autre, le système de RPCV est également relié au système d'information automatisé des douanes pour faciliter la gestion des risques. Un État n'exige ni RPCV ni PNR	Trois États ont créé des bases de données biométriques sophistiquées pour enregistrer et stocker les données personnelles des visiteurs étrangers. Dans un État, une loi relative à l'administration des entrées et sorties du territoire autorise la collecte de données biométriques à la frontière et leur conservation pendant 90 jours.	Informations insuffisantes
Amérique centrale			
Belize, Costa Rica, El Salvador, Guatemala, Honduras, Mexique, Nicaragua, Panama	En 2019, un État a renforcé sa capacité à contrôler les personnes qui entrent sur son territoire, et il est actuellement le seul État de la sous-région qui utilise un système de RPCV et des données provenant du système de PNR. Six autres États mettent actuellement en place des systèmes de RPCV, et l'État restant prend des mesures pour se doter d'un tel système. Deux États ont autorisé le recours aux données de PNR, mais les systèmes en question n'ont pas encore été mis en place.	Informations insuffisantes.	Informations insuffisantes.
Caraïbes			
Antigua-et-Barbuda, Bahamas, Barbade, Cuba, Dominique, Grenade, Haïti, Jamaïque, République dominicaine, Sainte-Lucie, Saint-Kitts-et-Nevis, Saint-Vincent-et-	Tous les États de la sous-région ont mis en place des systèmes de RPCV et plusieurs d'entre eux ont adopté ou modifié des lois sur l'utilisation des données de PNR. Toutefois, la plupart des États ne disposent toujours pas de capacités opérationnelles dans ce domaine, notamment en ce qui concerne la collecte, le traitement et l'analyse des données de PNR.	Informations insuffisantes.	Un État a adopté une directive visant à assurer la gestion efficace de sa liste de personnes à surveiller établie aux fins de la lutte contre le terrorisme, pour que les

<i>Région</i>	<i>Informations préalables sur les passagers et données des dossiers passagers</i>	<i>Biométrie</i>	<i>Listes ou bases de données de surveillance</i>
les Grenadines, Trinité-et-Tobago	Les systèmes nationaux de gestion des frontières de la plupart des États de cette sous-région sont soutenus par des initiatives régionales plus efficaces telles que le système de RPCV, le système intégré de sécurité des frontières de la Communauté des Caraïbes (CARICOM) et son système automatique de liste de personnes à surveiller (CARIBSEC). Les États ont davantage utilisé la liste régionale du CARIBSEC pour faciliter la mise en commun et l'analyse des renseignements, notamment en ce qui concerne les passeports volés et perdus, les infractions pénales et les affiliations à des groupes terroristes.		services concernés s'en servent, en particulier les agents de l'immigration, de la sécurité des frontières et des services de renseignement chargés de la lutte contre le terrorisme. Quelques États, partagent, du moins en partie, des listes de surveillance nationales de terroristes connus et présumés, y compris des combattants terroristes étrangers, avec les services de police et les agents des frontières concernés afin de contrôler les voyageurs et de procéder à des évaluations des risques et à des enquêtes.
Amérique du Sud			
Argentine, Bolivie (État plurinational de), Brésil, Chili, Colombie, Équateur, Guyana, Paraguay, Pérou, Suriname, Uruguay et Venezuela (République bolivarienne du)	Cinq États utilisent des systèmes de RPCV et de PNR ; quatre autres États ne disposent que de systèmes de RPCV et n'exigent pas encore de données de PNR ; deux autres États ont autorisé la mise en place de systèmes de RPCV uniquement, et travaillent à leur mise en œuvre. Seul un État n'a autorisé aucun des deux systèmes. La plupart des États n'ont toujours pas la capacité juridique et opérationnelle de gérer les données provenant des PNR.	Informations insuffisantes.	Informations insuffisantes.

<i>Région</i>	<i>Informations préalables sur les passagers et données des dossiers passagers</i>	<i>Biométrie</i>	<i>Listes ou bases de données de surveillance</i>
Europe orientale			
Bélarus, Estonie, Fédération de Russie, Hongrie, Lettonie, Lituanie, Pologne, République de Moldova, Slovaquie, Tchéquie, Ukraine	La sécurité des frontières entre les États de cette sous-région qui sont membres de l'Union européenne est régie par une série de lois et de règlements de l'Union européenne. Tous les États de la sous-région qui font partie de l'espace Schengen disposent de systèmes de PNR. Trois des quatre États de la sous-région qui ne font pas partie de l'espace Schengen collectent également des données de RPCV, mais ils n'ont pas encore mis en place de système de PNR. Les capacités analytiques permettant de repérer des terroristes potentiels restent toutefois incertaines.	Les États de la sous-région qui sont membres de l'Union européenne mettront en œuvre le système de contrôle des entrées et des sorties, qui recueillera et enregistrera les données biométriques des personnes (empreintes digitales et images faciales). Le système d'entrée/sortie devrait être opérationnel en 2023.	Informations insuffisantes.
États d'Europe occidentale, États d'Amérique du Nord et autres États			
Allemagne, Andorre, Australie, Autriche, Belgique, Canada, Chypre, Danemark, Espagne, États-Unis d'Amérique, Finlande, France, Grèce, Irlande, Islande, Israël, Italie, Liechtenstein, Luxembourg, Malte, Monaco, Norvège,	Parmi les États d'Europe occidentale, 11 des 16 États qui sont membres de l'Union européenne dans cette sous-région ont mis en place des systèmes de RPCV et de PNR. Quatre États ont établi un « guichet unique » regroupant ces données, généralement par l'intermédiaire de leur service d'information sur les passagers, organe désigné pour recevoir, transmettre et analyser les données entrantes. Un État dispose d'un système de RPCV et met actuellement en place un système de PNR ; un	Cinq des six États du groupe des États d'Amérique du Nord et autres États ont mis au point un système biométrique de contrôle des entrées et des sorties ; deux d'entre eux procèdent à un contrôle intégral des passagers et un autre s'efforce actuellement d'établir une liste de surveillance assortie de données biométriques et d'instaurer une procédure de vérification en temps réel à la frontière. Parmi les États d'Europe occidentale, 18 mettront en œuvre le système d'entrée/sortie, qui permettra	Un État échange avec des partenaires internationaux des informations sur les terroristes connus ou présumés (y compris sur l'identité de combattants terroristes étrangers), l'objectif étant de faciliter les contrôles. Dans les

<i>Région</i>	<i>Informations préalables sur les passagers et données des dossiers passagers</i>	<i>Biométrie</i>	<i>Listes ou bases de données de surveillance</i>
Nouvelle-Zélande, Pays-Bas, Portugal, Royaume-Uni de Grande-Bretagne et d'Irlande du Nord, Saint-Marin, Suède, Suisse, Türkiye	État est doté d'un système de PNR mais ne dispose pas d'un système de RPCV ; et trois États ne sont dotés d'aucun de ces systèmes. L'envergure de la collecte des données de RPCV et PNR effectuée par les États membres de l'Union européenne varie. Certains États ne collectent ces données que pour les passagers voyageant en dehors de l'espace Schengen. Un petit nombre d'États de l'Union européenne ont également pris des mesures pour collecter des données de RPCV concernant les voyageurs qui se déplacent par d'autres moyens, notamment le bus, le rail et la mer. Ces mesures, qui vont au-delà des exigences strictes des résolutions du Conseil de sécurité, ont été saluées par le Comité parce qu'elles aidaient les États à détecter les itinéraires de voyage fractionnés. Seuls deux des autres États européens de ce groupe ont mis en place des systèmes avancés pour les données de RPCV et PNR ainsi qu'un « guichet unique » pour la réception et l'analyse de ces données. Deux autres ne collectent des données de RPCV que pour certains voyageurs et uniquement pour des vols en provenance de l'extérieur de l'espace Schengen et n'ont pas encore mis en place de systèmes de PNR. Cinq des six États du groupe des États d'Amérique du Nord et autres États sont dotés de systèmes de RPCV et de PNR qui sont mis en œuvre au moyen d'un « guichet unique », à savoir un centre destiné à la réception et à l'évaluation des données pertinentes. Un État a indiqué que la qualité des données reçues était variable et un autre a mis en place plusieurs garanties applicables au traitement et à l'utilisation des données de RPCV et PNR, dont le recours à des évaluations de l'impact sur le respect de la vie	de recueillir et d'enregistrer les données biométriques d'une personne (empreintes digitales et images faciales). Il devrait être opérationnel en 2023.	États d'Europe occidentale, les informations concernant l'établissement de listes de surveillance ou de bases de données sont insuffisantes.

<i>Région</i>	<i>Informations préalables sur les passagers et données des dossiers passagers</i>	<i>Biométrie</i>	<i>Listes ou bases de données de surveillance</i>
	privée. Un État a prévu de se doter d'un système de RPCV. Quatre États s'associent à des agents des services de répression d'autres pays et à des transporteurs commerciaux à l'étranger pour empêcher l'embarquement des passagers qui représentent une menace pour la sécurité. L'un d'eux a mis en place un programme de protection des passagers visant à faire obstacle aux déplacements aériens des personnes soupçonnées de représenter une menace.		
Europe du Sud-Est			
Albanie, Bosnie-Herzégovine, Bulgarie, Croatie, Macédoine du Nord, Monténégro, Roumanie, Serbie, Slovénie	En 2020, les quatre États de cette sous-région qui sont membres de l'Union européenne avaient mis en place des systèmes de RPCV et de PNR. Aucun autre État ne dispose d'un système de RPCV ou de PNR.	Deux États mettront en œuvre le système d'entrée/sortie, qui recueillera et enregistrera les données biométriques d'une personne (empreintes digitales et images faciales). Il devrait être opérationnel en 2023.	Informations insuffisantes.

V. Recommandations du Comité contre le terrorisme et facilitation des efforts de renforcement des capacités

36. L'état d'avancement de la mise en œuvre des dispositions des résolutions 2178 (2014) et 2396 (2017) varie considérablement d'une région à l'autre. En particulier, des difficultés persistent quant à la mise en œuvre des dispositions relatives aux données de RPCV et de PNR, ainsi qu'en ce qui concerne l'utilisation responsable des données biométriques et des listes ou bases de données de surveillance. Une mise en œuvre efficace exige que les États Membres adoptent des cadres juridiques et réglementaires aux fins de la collecte, du traitement, de l'utilisation, du transfert, du stockage et du partage des données à caractère personnel, et pour assurer la protection contre les ingérences illégales ou arbitraires dans la vie privée et garantir le respect des normes pertinentes en matière de protection des données, ainsi que des cadres similaires pour s'assurer que leurs systèmes et les mesures qui reposent sur eux fonctionnent conformément au droit national et aux obligations internationales, dans le plein respect des droits humains et des libertés fondamentales. Il est essentiel de renforcer les capacités juridiques, techniques et opérationnelles, ainsi que les compétences spécialisées, afin que les experts compétents en matière d'application de la loi et de sécurité des frontières, y compris en première ligne, puissent utiliser et gérer ces systèmes de données. Tous ces éléments devraient être inclus dans une stratégie nationale globale de gestion de la sécurité des frontières afin de garantir que tous les partenaires concernés soient inclus et disposent d'un cadre juridique pour réglementer l'échange d'informations.

Renseignements préalables concernant les voyageurs et dossiers passagers

37. La mise en œuvre des systèmes de PNR nécessite des moyens juridiques, opérationnels et techniques. Les évaluations de la Direction exécutive du Comité contre le terrorisme ont montré l'existence d'un besoin récurrent de cadres juridiques et réglementaires qui permettent aux États de réglementer la collecte, le traitement, l'utilisation, le transfert, le stockage et la protection des données relatives aux passagers, conformément aux normes internationales. Si la base juridique existe déjà, elle doit généralement être revue à la lumière de l'amendement 28 à l'annexe 9 de la Convention de Chicago afin de permettre une mise en œuvre cohérente et harmonisée des cadres normatifs en matière de RPCV et de PNR dans le monde entier.

38. Dans certains États, la législation relative à la protection des données et de la vie privée est inexistante ou ne garantit pas l'application de garanties appropriées à la collecte et à l'analyse des données de RPCV et PNR. Dans certains contextes, les cadres normatifs existants ou la législation sur la protection des données et de la vie privée ne sont pas pleinement mis en œuvre faute de ressources, de financement ou de formation, ou pour d'autres raisons. Les États devraient définir une approche de la réglementation du système de RPCV (et à plus long terme des données de PNR, dont la collecte et le traitement requièrent des garanties de protection plus complexes) et garantir une approche consultative et interinstitutions, examiner les lois et réglementations nationales pertinentes, y compris les cadres liés à la protection des droits humains et des données, et élaborer ou revoir leur cadre normatif relatif aux données concernant les passagers conformément aux normes internationales, aux droits humains et aux principes de protection des données, y compris les mécanismes de contrôle indépendants et les voies de recours.

39. La Direction exécutive et ses partenaires, dont l'OACI, ont identifié le principal obstacle à la mise en œuvre complète des systèmes de PNR par certains États : les lois d'un État sur la protection des données empêchent les exploitants d'aéronefs de se conformer, faute de certaines garanties en matière de protection des données, à

l'obligation imposée par un autre État de transmettre les données de PNR à ses autorités. C'est l'impact de cette divergence que la série de garanties de protection des données introduites dans l'amendement 28 à l'annexe 9 de la Convention de Chicago tente de minimiser. Toutefois, les États qui exigent de plus grandes garanties de protection des données telles qu'elles figurent à l'annexe 9 requièrent souvent des accords internationaux bilatéraux stipulant que ces garanties plus astreignantes de protection des données doivent être appliquées aux données de PNR transférées. En raison des débats nationaux et régionaux du moment sur la nécessité et la proportionnalité des modalités spécifiques de traitement des données de PNR, et des nombreuses affaires juridiques en cours, les États qui souhaitent que leur soient transmises les données de PNR des juridictions concernées doivent attendre, parfois pendant de nombreuses années, l'issue de ces débats juridiques et la conclusion ultérieure des négociations sur les accords bilatéraux de transfert de données de PNR. Durant cette période, il est fait obstacle aux transferts de données de PNR par les exploitants d'aéronefs, et des personnes potentiellement impliquées dans des infractions terroristes ou des crimes graves peuvent profiter des failles ainsi créées dans les dossiers passagers. En ce qui concerne les États membres de l'Union européenne, celle-ci a adopté en 2016 la directive établissant un registre d'enregistrement des noms des passagers, en vertu de laquelle les exploitants d'aéronefs sont tenus de transférer les données de PNR aux États membres de l'Union européenne afin d'identifier et de détecter les mouvements de terroristes et de grands criminels. En juin 2022, la Cour de justice de l'Union européenne, dans son arrêt dans l'affaire C-817/19, a posé des limites à la mise en œuvre de cette directive de plusieurs manières. Bien que les États membres de l'Union européenne soient encore en train d'évaluer la totalité des effets de l'arrêt, celui-ci pourrait les placer face à d'importants enjeux juridiques, opérationnels et techniques.

40. Un ciblage mieux défini pourrait bénéficier à l'architecture de sécurité des États Membres, y compris tous les services de police et de justice, leur structure et leurs compétences, ainsi que les bases de données disponibles. Dans certains États, un soutien politique supplémentaire et la mobilisation des organismes nationaux sont nécessaires pour garantir que l'approche à l'échelle de l'ensemble de l'administration est suivie dans la mise en œuvre d'un programme national. Un financement durable et une stratégie de collecte de fonds bien définie sont également requis, compte tenu en particulier du nombre croissant de bénéficiaires. L'approche à l'échelle de l'ensemble de l'administration exige la participation de toutes les entités à un programme national et l'intensification de l'échange en temps utile d'informations opérationnelles pertinentes, y compris de données de renseignement financier. À cet égard, les cellules de renseignement financier devraient également être des autorités compétentes engagées dans les efforts de renforcement des capacités nationales en matière de RPCV et de PNR. Les États doivent décider quels organismes seront associés au service d'information sur les passagers. Ils devraient également élaborer et mettre à l'essai des règles générales afin de constituer de tels services dotés du personnel, du budget et des installations requis.

41. En ce qui concerne l'approche globale et cohérente de la mise en œuvre des systèmes de RPCV et de PNR, les enjeux tiennent au fait que les risques rencontrés par les États ne sont pas uniquement liés aux passagers aériens. En effet, de nombreux criminels et terroristes changeront de méthode et fractionneront leurs itinéraires ou utiliseront plusieurs modes de transport. C'est pourquoi la Direction exécutive et d'autres partenaires du Programme de lutte contre les déplacements des terroristes ont déjà commencé à élargir celui-ci pour répondre à cet impératif. Tous les volets du Programme ont fait l'objet d'un examen complet afin d'y intégrer les données sur les passagers maritimes. Les activités de formation incluent désormais les données maritimes, et des orientations juridiques ont été élaborées à l'intention des États qui

veulent recueillir de telles données. Il est actuellement procédé à une mise à jour du système goTravel, la solution logicielle analytique du Programme, pour y inclure un module maritime. Une fois cette étape franchie, le Programme s'intéressera à d'autres domaines tels que les données routières et ferroviaires et les données de RPCVi, afin de prêter son concours aux États Membres dans ces domaines. À cet égard, certains États ont décidé de mettre en œuvre des systèmes de RPCV et de PNR au-delà des aéroports et d'inclure le domaine maritime, les chemins de fer internationaux et le transport par autobus afin de mieux détecter les itinéraires fractionnés et d'empêcher les terroristes et les criminels de profiter des failles résultant de l'absence d'enregistrements des données associées à ces voyages. En outre, dans de nombreux États, le manque de moyens techniques et opérationnels des experts compétents en matière de répression et de sécurité des frontières, y compris en première ligne, limite souvent l'utilisation des données de RPCV et PNR.

42. Les exploitants d'aéronefs sont des partenaires clés dans la mise en œuvre des systèmes de RPCV et de PNR, et l'établissement d'une connectivité entre les systèmes des exploitants d'aéronefs et les systèmes des services d'information sur les passagers peut s'avérer compliqué, chronophage et onéreux. Comme cela a été indiqué par l'OACI et pris en compte dans le cadre des consultations relatives au Programme de lutte contre les déplacements des terroristes menées par la Direction exécutive et des activités de mise en œuvre de celui-ci par l'OACI, de nombreux facteurs peuvent peser sur la capacité des États de mettre en œuvre leurs systèmes de RPCV et de PNR de manière efficace et efficiente. Les États présentent parfois aux exploitants d'aéronefs des calendriers de mise en œuvre ambitieux, en annonçant des exigences légales et des échéances avec lesquelles ceux-ci doivent composer dans un court laps de temps. Dans certains cas, ces demandes ne correspondent pas à la capacité de l'État de mettre en place les systèmes et moyens techniques nécessaires. Les exploitants d'aéronefs sont souvent confrontés à de multiples demandes concurrentes et simultanées de la part des États s'agissant de la mise en œuvre de systèmes de RPVC et de PNR. Par conséquent, des plans de mise en œuvre réalistes et flexibles sont nécessaires pour leur permettre de programmer et de déployer les ressources techniques et humaines nécessaires à la formation. Les États doivent mettre en place des canaux de communication appropriés pour dialoguer avec les exploitants d'aéronefs et les informer des projets.

43. Le respect des normes internationales est un autre enjeu. L'Organisation mondiale des douanes (OMD), l'IATA et l'OACI ont convenu de l'ensemble maximal de données de RPCV à incorporer dans le message PAXLST (EDIFACT-ONU) à utiliser pour la transmission des données de RPCV par les exploitants d'aéronefs aux organismes de contrôle aux frontières. Les États demandent parfois aux exploitants d'aéronefs de collecter et de transmettre des éléments de données non standards dans les messages contenant des données de RPCV. Il s'agit d'un problème particulier depuis le début de la pandémie de COVID-19, les États tentant d'imposer des exigences supplémentaires en matière d'informations liées à la COVID-19, telles que le statut vaccinal ou les résultats de tests, pour lesquelles il n'existe pas de format normalisé convenu, à inclure dans les messages transmettant des données de RPCV. Le respect des normes internationales convenues en matière de RPCV, telles qu'elles sont décrites dans les Directives sur les renseignements préalables concernant les voyageurs (RPCV) de l'OMD/IATA/ICAO, garantit une mise en œuvre efficace et efficiente. Si l'on s'écarte de ces normes et que l'on exige la collecte et la transmission d'éléments de données non standards, le temps nécessaire aux exploitants d'aéronefs pour se mettre en conformité, se connecter et fournir des données de RPCV peut passer d'environ six mois à plusieurs années.

44. La Direction exécutive, en tant que partenaire du Programme de lutte contre les déplacements des terroristes, facilite la fourniture d'une assistance technique aux États Membres qui souhaitent se doter de systèmes de RPCV et de PNR. Elle s'appuie sur l'enquête électronique détaillée sur la mise en œuvre (eDIS) et sur le bilan général de la mise en œuvre pour définir et comprendre la situation en matière de lutte contre le terrorisme dans chaque État, et se fonde aussi sur les visites d'évaluation, les recommandations et les rapports analytiques du Comité contre le terrorisme, concernant notamment les combattants terroristes étrangers, pour établir une liste prioritaire de pays ayant besoin d'une assistance technique, qui est ensuite soumise pour adoption à l'équipe de gestion du projet. La Direction exécutive consulte l'Office des Nations Unies contre la drogue et le crime, son équipe chargée du projet de communication aéroportuaire (AIRCOP), INTERPOL et le Bureau de lutte contre le terrorisme, et utilise l'expertise de l'OACI et de l'IATA, en particulier leur « API/PNR World Tracker ». La Direction exécutive prévoit différentes catégories de pays bénéficiaires ; chacune bénéficiera d'un niveau d'assistance différent et sur mesure en fonction de la capacité d'adaptation nationale⁸.

Biométrie

45. Les évaluations de la Direction exécutive ont révélé que, même si l'étendue de l'utilisation de la biométrie et de l'expertise en la matière varie considérablement et qu'une grande majorité d'États collectent ou recoupent des données biométriques, la biométrie est peu utilisée aux fins de la lutte antiterroriste. Les États Membres utilisent de plus en plus de technologies innovantes dans ce domaine, notamment des technologies plus sophistiquées pour saisir, collecter, traiter et analyser les données biométriques, comme la technologie de reconnaissance faciale. Toutefois, les données biométriques contenues dans les bases de données nationales existantes ne sont pas toujours recoupées avec les informations contenues dans d'autres bases de données pertinentes. À cet égard, l'existence d'informations biométriques dans les réseaux internationaux de police ne sera de la plus grande utilité que si la capacité d'exploiter ces informations existe en première ligne, ce qui n'est pas le cas dans le paysage mondial actuel. La Direction exécutive collabore activement avec INTERPOL et contribue à la promotion de ses bases de données d'empreintes digitales, d'images faciales et d'ADN. Elle met en avant les normes internationales élaborées par des organisations internationales spécialisées, telles que les mesures prises par l'OACI pour renforcer la sécurité des documents de voyage en incluant dans son programme d'identification des voyageurs (TRIP) des processus de vérification biométrique, de contrôle de la qualité, de gestion des erreurs et des anomalies, et de lecture correcte des documents de voyage biométriques à la frontière. Les projets de l'Organisation internationale pour les migrations en matière de gestion de l'identité sont par exemple axés sur l'aide à l'établissement de documents de voyage lisibles à la machine et

⁸ La Direction exécutive prend également en considération la situation des États Membres selon les critères suivants : a) RPCV et/ou PNR non viable(s) : États dans lesquels aucune mesure de mise en œuvre n'a été prise quant aux systèmes de RPCV et/ou de PNR ; b) RPCV et/ou PNR non encore autorisés : États dans lesquels le cadre législatif et réglementaire nécessaire existe mais n'est pas encore en vigueur, l'approbation des autorités et/ou la ratification parlementaire étant pendantes ; c) RPCV et/ou PNR prévu(s) : États dans lesquels le cadre législatif et réglementaire pour la mise en œuvre d'un système de RPCV et/ou de PNR est en place, mais où l'équipement technique et l'infrastructure nécessaires font défaut ; et d) RPCV et/ou PNR en vigueur : États dans lesquels les connaissances et l'expertise nécessaires à la mise en œuvre, à l'exploitation et à l'utilisation responsable des systèmes de RPCV et de PNR sont en place, mais où la solution logicielle nécessaire en matière d'informatique et de technologies des communications fait défaut. Les États doivent s'assurer de l'acquisition du matériel et de l'infrastructure informatique adéquats afin d'installer le logiciel goTravel.

assortis d'éléments biométriques, et sur l'examen de la législation et des pratiques institutionnelles.

46. La Direction exécutive a recensé des pratiques recommandées telles que l'adoption de cadres clairs fondés sur les droits humains pour l'utilisation de la technologie biométrique, qui prévoient l'utilisation de garanties procédurales, la bonne maintenance des bases de données biométriques et des protocoles de partage des données. Les données biométriques devraient être collectées, utilisées et partagées dans le plein respect des obligations internationales pertinentes et du droit international en matière de droits humains, en particulier le droit à la liberté de circulation, le droit au respect de la vie privée, les garanties relatives à la protection des données à caractère personnel, les garanties relatives aux droits de la défense et le principe de non-discrimination, et en tenant compte des questions de genre. L'utilisation de la technologie biométrique devrait être fondée sur un cadre juridique clair stipulant l'objectif et la portée de cette utilisation, y compris le traitement et la gestion des données. Les États devraient examiner à un stade précoce la manière dont la législation doit répondre aux enjeux du développement des technologies biométriques. Il est également important d'examiner attentivement toutes les conséquences de l'utilisation de la technologie biométrique qui ont un impact négatif sur les droits humains. En particulier, les parties prenantes concernées doivent être conscientes que le risque d'incidences négatives sur les droits humains peut être amplifié dans le cas de groupes et de personnes susceptibles d'être marginalisés ou victimes de discrimination, de membres de minorités et de groupes ethniques, religieux, raciaux et autres, et de personnes en situation de vulnérabilité, telles que les réfugiés et les demandeurs d'asile ou les personnes touchées par un conflit armé ou d'autres types de violence. Une approche mobilisant l'ensemble de la société, des partenariats et un dialogue entre les autorités publiques, le secteur de la biométrie et toutes les autres parties prenantes sont essentiels. L'absence de garanties empêchant l'utilisation abusive ou impropre des technologies et des données biométriques peut également avoir un impact négatif sur la coopération internationale, ce qui risque de compromettre les efforts internationaux de lutte contre le terrorisme.

47. La Direction exécutive, avec le Bureau de lutte contre le terrorisme et le Centre des Nations Unies pour la lutte contre le terrorisme, travaille en partenariat avec le Biometrics Institute sur une initiative conjointe à long terme. En juin 2018, le Recueil des pratiques recommandées applicables à l'utilisation et à l'échange responsables des données biométriques dans le contexte de la lutte contre le terrorisme a été lancé par le Groupe de travail sur la gestion des frontières et l'application de la loi dans le contexte de la lutte contre le terrorisme du Pacte mondial de coordination contre le terrorisme, en partenariat avec la Direction exécutive (qui préside le Groupe de travail), le Bureau de lutte contre le terrorisme/Centre des Nations Unies pour la lutte contre le terrorisme et le Biometrics Institute. À titre de suivi, la Direction exécutive et le Bureau de lutte contre le terrorisme/Centre des Nations Unies pour la lutte contre le terrorisme ont organisé avec les pays d'Asie du Sud-Est et d'Asie centrale des ateliers régionaux d'experts adaptés aux besoins, et des ateliers nationaux avec la Thaïlande et le Tadjikistan, au cours desquels le Recueil a été utilisé comme un outil de mise en œuvre pratique illustrant les mesures que les États doivent prendre pour appliquer efficacement la résolution [2396 \(2017\)](#) du Conseil et d'autres résolutions pertinentes, ainsi que les orientations énoncées dans l'additif aux principes directeurs relatifs aux combattants terroristes étrangers (2018) et conformément au droit national et au droit international relatif aux droits humains. Cette initiative conjointe de la Direction exécutive, du Bureau de lutte contre le terrorisme et du Centre des Nations Unies pour la lutte contre le terrorisme est appelée à être étendue à d'autres régions concernées dès que les fonds seront assurés. Elle est menée dans l'esprit de l'initiative Unité d'action des Nations Unies, qui bénéficie de l'expertise des entités

du Pacte mondial de coordination contre le terrorisme. Elle vise à procurer aux États bénéficiaires les outils et les ressources nécessaires pour mettre en place un système intégré de gestion des frontières et compléter les efforts nationaux et régionaux de contrôle des documents de voyage grâce à des procédures de contrôle faisant appel à la biométrie. Les ateliers ont été l'occasion de se pencher sur les pratiques nationales, les tendances, les lacunes et les besoins actuels et sur les récentes avancées technologiques et autres concernant l'utilisation responsable et le partage des données biométriques dans le contexte de la lutte contre le terrorisme.

48. La Direction exécutive entretient des relations suivies avec le Biometrics Institute qui, au cours des 20 dernières années, a mené le débat sur l'utilisation responsable et déontologique de la biométrie. Ce partenariat lui a permis de renforcer son engagement auprès du secteur de la biométrie, des fournisseurs de technologie jusqu'aux utilisateurs.

Listes de surveillance ou bases de données

49. Dans l'ensemble, la plupart des États ont établi une ou plusieurs listes de surveillance ou des bases de données distinctes pour lutter contre la criminalité. Souvent, cependant, ces listes de surveillance ou ces bases de données ne sont pas coordonnées ou interexploitables. Le nombre d'États disposant d'une liste de surveillance ou d'une base de données intégrée aux fins de la lutte contre le terrorisme reste faible. Il arrive souvent que tous les organismes compétents chargés de l'application de la loi et du contrôle des frontières n'aient pas accès à ces listes de surveillance ou à ces bases de données, mais qu'ils fonctionnent plutôt « à la demande ». Ces listes de surveillance ou bases de données sont également souvent classifiées en raison des données personnelles sensibles qu'elles contiennent. Les évaluations de la Direction exécutive ont révélé que dans de nombreux États les autorités compétentes ne partagent pas les informations contenues dans les listes de surveillance ou les bases de données nationales, y compris au niveau multilatéral. De nombreux cadres juridiques et réglementaires restent insuffisants, car ils ne prévoient pas de limites claires à l'utilisation et au partage des données contenues dans les listes de surveillance. La Direction exécutive a également constaté que certains États ne disposent pas de normes ou de protocoles clairs en matière d'échange d'informations.

50. La Direction exécutive a exhorté les États Membres à veiller à ce que l'élaboration de listes de surveillance soit conforme à toutes les obligations que leur impose le droit international, en particulier le droit international des droits humains, le droit international des réfugiés et le droit international humanitaire. Le respect des droits humains et des approches tenant compte des questions de genre devrait être intégré dès le départ dans le système de surveillance, car tout système de surveillance mal conçu ou mal utilisé est moins efficace et peut porter atteinte aux droits humains et, par conséquent, compromettre l'action antiterroriste. Dans le cadre des mesures de protection de la vie privée et des données, certains États ont doté leurs organismes nationaux de responsables des droits humains chargés de contrôler l'utilisation et le partage des données à caractère personnel. La Direction exécutive a relevé que les États doivent mettre en place des mécanismes de recours appropriés, efficaces et accessibles pour les personnes qui affirment que leurs droits ont été violés. Elle travaille en étroite collaboration avec les partenaires concernés afin d'améliorer la mise en œuvre des listes de surveillance ou des bases de données intégrées dans le respect des droits humains.

51. La Direction exécutive, en tant que présidente du Groupe de travail sur la gestion des frontières et l'application de la loi dans le contexte de la lutte contre le terrorisme, œuvre également avec toutes les entités internationales concernées à l'établissement de listes de surveillance. En 2019, le Forum mondial de lutte contre

le terrorisme a adopté le Mémorandum de New York sur les bonnes pratiques visant à empêcher les déplacements de terroriste, document non contraignant. Dans la foulée, une initiative relative à l'établissement de listes de surveillance a été lancée en 2020 pour améliorer la mise en œuvre et la gestion des listes de surveillance ou des bases de données antiterroristes afin d'appliquer les dispositions de la résolution [2396 \(2017\)](#) du Conseil, les principes énoncés dans l'additif aux principes directeurs relatifs aux combattants terroristes étrangers et ceux qui sont énoncés dans le Mémorandum de New York. Dans le cadre de cette initiative, six ateliers en ligne ont été organisés en 2020 et 2021, auxquels ont participé des représentants de gouvernements, d'organisations internationales et régionales, d'universités et de la société civile. Ce processus a conduit à l'élaboration de la Boîte à outils concernant les listes de surveillance dans le cadre de la lutte contre le terrorisme, codirigée par les États-Unis d'Amérique et le Bureau de lutte contre le terrorisme, avec le concours de la Direction exécutive. Ces mesures sont destinées à aider les États à tenir compte des implications juridiques, politiques et opérationnelles de l'élaboration de listes de surveillance ou de bases de données. Elles contiennent des informations sur les bonnes pratiques et les options possibles permettant aux États d'établir, de mettre en œuvre et de tenir à jour des listes de surveillance ou des bases de données nationales intégrées de terroristes connus et présumés, y compris de combattants terroristes étrangers. Elles ne sont pas contraignantes et invitent chaque État à en examiner les recommandations en tenant compte de sa propre situation, de ses lois et politiques nationales, ainsi que de ses obligations et engagements juridiques internationaux, notamment en vertu du droit international des droits humains. La Direction exécutive encourage l'établissement de listes de surveillance ou de bases de données en tant qu'outils et éléments essentiels parmi les moyens des États en matière de lutte contre le terrorisme. La mise en œuvre de listes de surveillance ou de bases de données est intégrée dans quelques projets et programmes de renforcement des capacités, notamment le Programme de lutte contre les déplacements des terroristes, le Programme de gestion de la sécurité des frontières du Centre des Nations Unies pour la lutte contre le terrorisme et l'initiative menée par la Direction exécutive, le Bureau de lutte contre le terrorisme et le Centre des Nations Unies pour la lutte contre le terrorisme dans le domaine de la biométrie. Il est toutefois nécessaire de fournir un soutien accru aux États Membres et de renforcer leurs moyens s'agissant d'élaborer, d'utiliser et de tenir à jour des listes de surveillance ou des bases de données aux fins de la lutte contre le terrorisme dans le respect du droit international en matière de droits humains.

VI. Observations et recommandations

52. Il est nécessaire de renforcer les approches coordonnées et globales de la gestion des frontières afin de répondre efficacement à l'évolution de la menace que représentent les combattants terroristes étrangers et de lutter contre les déplacements des terroristes. Cela suppose l'adoption d'un certain nombre de mesures par les États Membres et un effort à l'échelle de l'ensemble de l'administration.

53. Compte tenu de l'état d'avancement variable de l'établissement, au niveau mondial, des systèmes de RPCV et de PNR, des listes ou bases de données de surveillance et des systèmes biométriques, et des enjeux importants et variés avec lesquels les États Membres doivent composer pour appliquer efficacement les dispositions pertinentes de la résolution [2396 \(2017\)](#) du Conseil, il est essentiel que ces derniers restent déterminés à mettre en œuvre les résolutions du Conseil relatives à la lutte contre le terrorisme. Il est également essentiel que la Direction exécutive, au nom du Comité contre le terrorisme, continue d'évaluer la capacité des États de le faire et facilite l'assistance technique à l'appui de ces efforts. Les recommandations

découlant des évaluations du Comité contre le terrorisme concernant les systèmes de RPCV et de PNR, les listes ou bases de données de surveillance et les systèmes biométriques exigent des États qu'ils prennent des mesures aux niveaux politique, législatif, technique et opérationnel.

54. Il est clairement nécessaire d'accroître l'échange d'informations et de pratiques dans ces domaines entre toutes les parties prenantes, des décideurs politiques aux responsables opérationnels, et de renforcer la coopération entre les secteurs public et privé en associant la société civile, le monde universitaire et l'industrie. Il est également nécessaire de mieux comprendre les questions et les défis qui se posent au niveau opérationnel lors de la mise en œuvre pratique de ces capacités et d'étudier les moyens de parvenir à une approche globale plus cohérente. Il est essentiel que le Conseil de sécurité et le Comité contre le terrorisme, avec le concours de la Direction exécutive, continuent d'élaborer et de mettre en œuvre des approches et des outils propres à garantir une riposte mondiale efficace face à la menace permanente et évolutive que représentent les terroristes, en particulier les combattants terroristes étrangers, et leurs réseaux, en tenant compte des différents niveaux de capacité, d'expertise et de ressources auxquels les États Membres ont accès.

55. Le Conseil de sécurité et le Comité contre le terrorisme pourraient envisager de prendre les mesures suivantes et demander l'appui de la Direction exécutive afin de :

a) Continuer à promouvoir l'importance de la gestion coordonnée des frontières, notamment en resserrant la coordination entre les autorités compétentes au niveau national et en mettant en œuvre une approche coordonnée de la gestion des frontières grâce à des cadres juridiques et réglementaires et à des structures institutionnelles appropriés, en élaborant les procédures requises et en acquérant les ressources humaines, la formation, l'infrastructure et l'équipement nécessaires ;

b) Continuer à œuvrer aux côtés des États Membres, dans le cadre de visites d'évaluation, de dialogues et de consultations sur les capacités, afin d'identifier les moyens de renforcer et de promouvoir la mise en œuvre des dispositions pertinentes des résolutions [2178 \(2014\)](#) et [2396 \(2017\)](#), notamment en ce qui concerne les systèmes de RPCV et de PNR, les listes ou bases de données de surveillance et les systèmes biométriques, conformément aux obligations internationales, y compris le droit international des droits humains, et d'étudier les moyens de renforcer la mise en œuvre à l'échelle mondiale ;

c) Conserver leur rôle de facilitateur de l'assistance technique, œuvrer avec la communauté des donateurs, le Bureau de lutte contre le terrorisme et les entités chargées de la mise en œuvre, notamment dans le cadre du Pacte mondial de coordination contre le terrorisme, et intensifier les efforts en matière de renforcement des capacités et de sensibilisation pour que les États développent et améliorent encore leurs capacités et systèmes de gestion coordonnée des frontières ;

d) Collaborer avec les États et les organisations internationales et régionales afin de partager et promouvoir les pratiques efficaces et les lignes directrices internationales dans ces domaines et envisager d'élaborer de nouvelles orientations pour aider les États Membres à mettre effectivement en œuvre les dispositions pertinentes des résolutions [2178 \(2014\)](#) et [2396 \(2017\)](#) dans le respect du droit interne et du droit international, y compris le droit des droits humains, tout en ayant conscience des efforts requis pour développer les capacités juridiques et opérationnelles nécessaires, et explorer les synergies concernant l'intention d'élaborer un ensemble de principes directeurs non contraignants afin d'aider les

États Membres à contrer la menace que représente l'utilisation des technologies nouvelles et émergentes à des fins terroristes⁹ ;

e) Étudier les moyens de renforcer encore les partenariats avec les organisations internationales et régionales, le secteur privé, le monde universitaire, la société civile et le Réseau mondial de recherche dans le domaine de la lutte antiterroriste de la Direction exécutive, selon qu'il convient, afin de cerner les enjeux liés à la mise en œuvre de ces capacités et d'étudier les moyens d'aider les États Membres à trouver et à diffuser des solutions efficaces ;

f) Étudier les moyens de renforcer l'analyse des données relatives aux passagers et continuer à appuyer les travaux des organisations internationales spécialisées concernées, telles que l'OMI, l'OMD par l'intermédiaire de son groupe de travail sur la facilitation et le contrôle des passagers, et le Programme de lutte contre les déplacements des terroristes, afin d'introduire dans le secteur maritime le concept de RPCV et de PNR (renseignements relatifs aux réservations, dans le contexte maritime), d'abord en lien avec les navires de croisière puis avec les transbordeurs ;

g) Encourager les États à étendre l'analyse des données relatives aux passagers à d'autres modes de transport, tels que les chemins de fer et les bus, afin d'empêcher les terroristes et les combattants terroristes étrangers de recourir à la technique des itinéraires de voyage fractionnés.

⁹ Voir la Déclaration de Delhi sur la lutte contre l'utilisation des technologies nouvelles et émergentes à des fins terroristes, adoptée le 29 octobre 2022 par le Comité contre le terrorisme.