Nations Unies
Département des opérations de paix (DPO)
Réf. 2022.05

Lignes directrices

Partage d'informations issues du renseignement dans les opérations de maintien de la paix avec des entités n'appartenant pas au système des Nations Unies et avec des entités extérieures aux missions, et réception d'informations issues du renseignement provenant de ces entités

Document approuvé par :	Jean-Pierre Lacroix, Secrétaire général adjoint aux opérations de paix
Date d'entrée en vigueur :	*1er décembre 2022*
Service à contacter :	*DPO/OUSG/PICT*
Date de révision :	*1er décembre 2024*

LIGNES DIRECTRICES DU DÉPARTEMENT DES OPÉRATIONS DE PAIX RELATIVES AU PARTAGE D'INFORMATIONS ISSUES DU RENSEIGNEMENT DANS LES OPÉRATIONS DE MAINTIEN DE LA PAIX AVEC DES ENTITÉS N'APPARTENANT PAS AU SYSTÈME DES NATIONS UNIES ET DES ENTITÉS EXTÉRIEURES AUX MISSIONS, ET À LA RÉCEPTION D'INFORMATIONS ISSUES DU RENSEIGNEMENT PROVENANT DE CES ENTITÉS

Table des matières :

ANNEXES

A. OBJET ET CONTEXTE

1. Les présentes lignes directrices reviennent plus en détail sur les paragraphes 10.4. et 11.4. de la politique relative au renseignement dans les opérations de maintien de la paix ; elles expliquent les raisons qui peuvent amener les missions de maintien de la paix des Nations Unies à partager des produits issus du renseignement dans les opérations de maintien de la paix (ci-après, le « PKI ») avec des entités n'appartenant

pas au système des Nations Unies et des entités extérieures aux missions et à recevoir des produits issus du renseignement provenant d'entités non onusiennes, ainsi que les méthodes utilisées pour ce faire. Elles définissent les paramètres à respecter pour procéder à ce partage et à cette réception, et donnent un aperçu d'une structure de décision recommandée à cet effet. Elles ne concernent que le partage d'informations issues du PKI entre des missions de maintien de la paix des Nations Unies et des entités n'appartenant pas au système des Nations Unies et des entités extérieures aux missions, ainsi que la réception de produits de renseignement émanant de telles entités.

2. Parmi les entités n'appartenant pas au système des Nations Unies peuvent figurer, par exemple, le Ministère des relations extérieures de l'État hôte qui accueille une mission de maintien de la paix, des organisations régionales ou les missions qui en relèvent, des organisations non gouvernementales, ou encore des entités constituées au sein des États Membres, notamment pour les pays fournisseurs de contingents ou de personnel de police (forces armées, par exemple). Les entités onusiennes extérieures aux missions peuvent inclure les agences, fonds et programmes des Nations Unies, ou encore certaines entités du Secrétariat présentes dans le cadre d'une mission non intégrée. Celles qui ont leurs bureaux au Siège de l'Organisation des Nations Unies, comme le Département des opérations de paix (DOP), ne font pas partie de ces entités aux fins des présentes lignes directrices.

3. Promulguée en mai 2017, la « DPKO-DFS Policy on Peacekeeping Intelligence » a été mise à jour et rebaptisée « politique du DOP relative au renseignement dans les opérations de maintien de la paix » (ci-après, « la politique »), avec effet au 1er mai 2019. Dans son paragraphe 11.4. intitulé « Partage d'informations issues du PKI avec des entités extérieures aux missions et à l'ONU », ce document donne un aperçu des procédures relatives au partage d'informations issues du PKI avec les entités précitées. Au paragraphe 10.4, il fait état de la possibilité de recevoir des informations issues du renseignement provenant de tierces parties[1]. Les présentes lignes directrices visent à donner aux missions des orientations supplémentaires, plus détaillées, en la matière.

4. Dans ses contacts avec une tierce partie à des fins de partage et de réception d'informations, le personnel des missions est tenu d'agir dans la stricte observance du mandat de la mission ainsi que de l'ensemble des principes, règles et obligations de l'Organisation, notamment pour ce qui concerne la promotion et la protection des lois et normes internationales relatives aux droits humains. L'absence d'orientations suffisamment détaillées ou le non-respect de celles qui ont été données risque d'aboutir à des actes susceptibles de mettre en danger le personnel des missions, les populations locales ainsi que les personnes auprès desquelles les informations ont été recueillies, et de nuire à la réputation de l'Organisation.

B. CHAMP D'APPLICATION

5. Les présentes lignes directrices s'appliquent uniquement aux missions qui souhaitent ou doivent partager des informations issues du PKI avec des entités n'appartenant pas aux Nations Unies et/ou extérieures aux missions. Toutes les composantes des missions concernées par ce problème doivent obligatoirement s'y conformer. Les chefs

[1] Les entités non onusiennes, de même que celles extérieures aux missions des Nations Unies, sont toutes considérées comme des tierces parties aux fins des présentes lignes directrices.

de mission en particulier, mais aussi les autres membres du personnel d'encadrement ont un rôle essentiel à jouer pour garantir le respect de ces règles.

6. Les présentes lignes directrices concernent uniquement le partage d'informations issues du PKI et la réception d'informations provenant du renseignement ; l'échange et le traitement d'informations sensibles qui ne sont pas considérées comme relevant du renseignement ou du PKI demeureront régis par les documents d'orientation qui existent en la matière.

7. Les présentes lignes directrices s'appliquent à toutes les méthodes utilisées pour le partage d'informations issues du PKI et la réception d'informations provenant du renseignement, notamment lorsque ces informations sont réceptionnées oralement ou par d'autres moyens informels.

C. PROCÉDURES

- Les présentes lignes directrices sont réparties en deux sections. La première décrit les procédures relatives au partage d'informations issues du PKI, tandis que la seconde explique celles qui ont trait à la réception d'informations provenant du renseignement.

- La première section est subdivisée en deux parties, qui portent, l'une, sur le partage d'informations issues du PKI avec des entités n'appartenant pas au système des Nations Unies et, l'autre, sur le partage de telles informations avec des entités des Nations Unies extérieures aux missions.

- Les informations issues du renseignement/PKI sont généralement classées comme stratégiques ou opérationnelles/tactiques, selon l'origine de la demande. Sont qualifiées de stratégiques celles livrées à la suite d'une instruction émise par le (la) chef de mission ; sont qualifiées d'opérationnelles/tactiques celles qui résultent d'un ordre émanant du sous-quartier général ou du bureau local. Pour plus de détails sur chacun de ces points, prière de se reporter au chapitre « F. Définitions ».

- Tout au long des processus de partage et de réception des informations, les responsables chargés de coordonner la gestion de l'information ou d'autres membres du personnel dûment formés et habilités à cet effet sont appelés à jouer un rôle central en facilitant et coordonnant le partage des informations issues du PKI[2]. Ils devront de préférence être installés dans le bureau du chef d'état-major de la mission ou dans un bureau similaire, commun ou central, qui ne soit pas directement rattaché à une composante ou à un bureau spécifique. Dans certaines missions, la gestion de l'information peut relever de la compétence de l'unité d'analyse de la Cellule d'analyse conjointe de la mission ou du Centre d'opérations conjoint.

---

[2] L'expérience et le niveau d'instruction requis des responsables chargés de coordonner la gestion de l'information doivent être comparables à ceux exigés des spécialistes de la gestion de l'information de grade P3 (https://iseek.un.org/departmental_page/gjp-information-management-0). Les formations susceptibles de compléter les exigences imposées en termes d'expérience et d'instruction susmentionnées figurent à l'adresse suivante : https://iseek.un.org/system/files/data_and_analytics_curriculum.pdf. D'autres formations devraient être proposées à mesure que le Secrétariat définira de nouvelles orientations en la matière.

- Il incombera notamment aux responsables chargés de coordonner la gestion de l'information :
  a. d'indiquer au personnel concerné comment filtrer les informations issues du PKI avant de les partager, selon que de besoin[3] ;
  b. de contacter la ou les entités concernées pour tout ce qui a trait aux évaluations et examens[4], ce qui permet d'apprécier et d'atténuer, de manière structurée, les risques liés au partage d'informations issues du PKI et à la réception d'informations provenant du renseignement. On trouvera en annexe des exemples des quatre types d'évaluations et examens existants ;
  c. d'enregistrer les produits issus du PKI qui ont été partagés et les produits de renseignement réceptionnés dans les systèmes officiels de gestion de l'information des Nations Unies, en ce compris les informations communiquées oralement ;
  d. de tenir les registres et de les réactualiser régulièrement afin de pouvoir dégager d'éventuelles tendances au fil du temps.
  Les responsables chargés de coordonner la gestion de l'information devront consulter le Conseiller juridique principal ou d'autres juristes de la mission s'ils se heurtent à des problèmes susceptibles d'avoir des conséquences juridiques dans leur travail.

- Les entités en charge du renseignement dans les opérations de maintien de la paix pourront en outre, en fonction des besoins et des ressources disponibles, souhaiter nommer des responsables de la coordination au niveau des composantes, qui devront travailler en étroite collaboration avec leurs homologues en poste au niveau des missions.

- Les registres représentent un outil essentiel et indispensable pour gérer les informations issues du PKI qui ont été partagées et les informations provenant du renseignement qui ont été réceptionnées.
  a. **Toutes les missions devront constituer et tenir à jour un registre central dans lequel seront systématiquement consignées les données factuelles relatives aux informations susmentionnées, telles que la date et l'heure auxquelles elles ont été partagées ou réceptionnées, leur degré de sensibilité, les personnes auxquelles elles ont été communiquées ou dont elles émanent, ainsi que la façon dont elles ont été partagées ou obtenues**. D'autres informations, telles que les résultats de l'évaluation des risques liés au partage d'informations ou de l'examen rapide d'informations réceptionnées, ainsi que les mesures auxquelles ils auraient éventuellement donné lieu, devront également y figurer.
  b. Les procédures relatives à l'enregistrement des informations issues du PKI qui ont été partagées ou des informations provenant du renseignement qui ont été réceptionnées devront être détaillées dans le plan d'appui au PKI de la mission.

---

[3] Le filtrage consiste à retirer les informations sensibles d'un document afin qu'il puisse être diffusé à un public plus large, notamment tous les détails confidentiels figurant dans les informations recueillies qui pourraient permettre d'en retrouver la source ou le moyen d'acquisition et les compromettre, ou de rendre identifiables d'éventuels témoins ou victimes ayant un lien avec ces informations.

[4] Il existe quatre types d'évaluations et examens : 1) Évaluation d'une entité aux fins du partage d'informations, 2) Évaluation des risques liés au partage d'informations, 3) Évaluation d'une entité aux fins de la réception d'informations, 4) Examen rapide d'information provenant du renseignement à leur réception.

c. Tous les registres devront être gérés en toute sécurité et n'être accessibles qu'au personnel concerné. Les responsables chargés de coordonner la gestion de l'information devront s'acquitter de cette tâche au jour le jour.
d. Tous les registres devront être pleinement accessibles au Bureau des services de contrôle interne ainsi qu'à d'autres mécanismes de contrôle pertinents, si nécessaire.

8. Partage d'informations issues du renseignement dans les opérations de maintien de la paix avec des entités n'appartenant pas au système des Nations Unies et avec des entités extérieures aux missions

- Compétence en matière de partage des informations
  a. La compétence relative au partage des informations, dévolue au (à la) chef de mission, doit être déléguée comme il convient. Une fois arrêtée, la décision de déléguer devra être clairement indiquée dans le plan d'appui au PKI de la mission. Les chefs de mission peuvent souhaiter déléguer ce pouvoir à différents membres du personnel en fonction du classement d'un produit du PKI en termes de sécurité, ainsi que des personnes avec lesquelles il sera partagé. Ils devront veiller à ce que celles et ceux qui se sont vus déléguer cette compétence aient parfaitement connaissance des principes et paramètres régissant le partage d'informations issues du PKI avec des entités n'appartenant pas aux Nations Unies et avec des entités extérieures aux missions.
  b. Les processus propres à la délégation de compétence en fonction du destinataire[5], ainsi que du degré de sécurité et de la nature des informations (stratégiques ou opérationnelles/tactiques) devront être déterminés par chaque mission de façon à être adaptés au mieux à leur situation respective. S'agissant du partage d'informations issues du PKI revêtant un caractère stratégique, il est recommandé de déléguer cette compétence au (à la) président(e) du mécanisme de coordination du renseignement dans les missions de maintien de la paix.

8.1. *Partage d'informations issues du renseignement dans les opérations de maintien de la paix avec des entités n'appartenant pas au système des Nations Unies*

8.1.1. Avant qu'une mission ne partage des informations issues du PKI avec une entité n'appartenant pas au système des Nations Unies, une évaluation de l'entité aux fins du partage d'informations et une évaluation des risques liés au partage d'informations devront être menées à bien afin de déterminer les conséquences préjudiciables qui pourraient en résulter pour la mission ou pour son mandat[6].

8.1.2. L'évaluation de l'entité avec laquelle il est envisagé de partager le produit du PKI se compose de deux parties : 1) un aperçu des informations pertinentes concernant l'entité et 2) une évaluation de l'entité sous l'angle des droits humains. Dans le cadre de la première partie, les missions devront déterminer le champ d'action de l'entité avec laquelle elles ont

[5] Partage d'un produit de PKI avec une entité onusienne extérieure aux missions ou avec une entité n'appartenant pas à l'ONU, notamment une force de sécurité, par exemple.
[6] Une évaluation d'une entité aux fins du partage d'informations ne devra être réalisée qu'à la condition que cela n'a pas encore été fait ou que l'évaluation existante est jugée obsolète (voir le point 8.1.2.3.).

l'intention de partager des informations, afin qu'il n'y ait pas d'ambiguïté quant à l'application du principe de la « maîtrise de l'information par son auteur » (voir le point 8.1.5.). Si l'entité est une force de sécurité n'appartenant pas aux Nations Unies, telle que définie dans la politique de diligence voulue en matière de droits humains, en ce comprises les autorités civiles qui en sont directement responsables, la partie de l'évaluation relative aux droits humains devra correspondre à l'évaluation des risques PDVDH[7] ; pour les entités civiles autres que les forces de sécurité, ladite évaluation des risques devra être adaptée en fonction de ce qu'aura décidé la mission[8]. On trouvera à l'annexe A un exemple d'évaluation d'une entité aux fins du partage d'informations.

8.1.2.1. Les missions devront déterminer quelle composante/unité est la mieux placée pour réaliser la première partie de l'évaluation en fonction de la nature des informations issues du PKI (stratégiques ou opérationnelles/tactiques) et de la personne qui a procédé à leur analyse. La deuxième partie devra être effectuée par la composante Droits humains de la mission, en concertation avec les autres composantes concernées ; elle devra suivre, le cas échéant, les procédures spécifiquement prévues pour la réalisation des évaluations des risques PDVDH. Si une mission ne dispose pas de composante Droits humains, elle devra s'adresser au (à la) Haut(e)-Commissaire des Nations Unies aux droits de l'homme par l'intermédiaire de son responsable en charge de la coordination des questions relatives aux droits humains.

8.1.2.2. L'évaluation des risques PDVDH ou une évaluation adaptée des risques PDVDH (selon le cas) devra faire état, si nécessaire, des mesures d'atténuation envisagées pour minimiser les risques avant tout partage d'informations. L'entité qui partage les informations devra veiller à ce que des mesures d'atténuation soient mises en œuvre par l'entité à laquelle elles sont destinées.

8.1.2.3. Une fois réalisées, les évaluations des entités aux fins du partage d'informations devront être régulièrement revues et mises à jour, de manière à pouvoir être réutilisées pour de nouveaux partages d'informations. Une surveillance active des faits nouveaux ou incidents pertinents est particulièrement importante pour la mise à jour de ces évaluations lorsqu'elles portent sur des forces de sécurité n'appartenant pas aux Nations Unies. Les évaluations devront, au minimum, être

[7] Un modèle d'évaluation des risques figure à l'annexe 1 de la Note d'orientation sur la politique de diligence voulue en matière de droits de l'homme dans le contexte de l'appui que l'ONU fournit aux forces de sécurité non onusiennes (2015), et des indications précises quant aux modalités à suivre pour mener cette évaluation sont fournies aux pages 18 à 24 de ce même document. Si l'entité des Nations Unies dispose d'une instruction permanente pour la mise en œuvre de la politique susmentionnée, elle devra procéder à l'évaluation des risques conformément à la procédure qui y est définie.

[8] À l'exception des autorités civiles nationales directement responsables de la gestion, de l'administration ou du commandement et du contrôle de forces de sécurité n'appartenant pas aux Nations Unies, pour lesquelles l'évaluation des risques PDVDH devra être effectuée conformément à la politique en la matière.

réexaminées après un laps de temps déterminé par la mission (tous les trois mois au moins, par exemple).

8.1.3. Le produit du PKI appelé à être partagé devra faire l'objet d'une évaluation des risques liés au partage d'informations. Contrairement aux évaluations des entités, celles relatives aux risques devront être réalisées pour chaque produit qui sera partagé (à l'exception des produits du PKI faisant régulièrement l'objet d'un partage – voir le point 8.1.8.). On trouvera à l'annexe B un exemple d'évaluation des risques liés au partage d'informations.

8.1.3.1. Il appartiendra aux missions de déterminer quelle composante/unité est la mieux placée pour réaliser l'évaluation des risques liés au partage d'informations en fonction de la nature des informations issues du PKI (stratégiques ou opérationnelles/tactiques) et de la personne qui a procédé à leur analyse. La composante Droits humains devra, au besoin, être consultée.

8.1.3.2. En cas de partage d'informations opérationnelles/tactiques issues du PKI avec des entités n'appartenant pas aux Nations Unies, le bureau/l'unité qui a obtenu ces informations devra être consulté(e) pour approbation.

8.1.4. Le partage d'informations issues du PKI pourra avoir lieu une fois que la mission aura procédé aux deux évaluations (entité et risques liés au partage) et qu'elle aura conclu que le risque est acceptable.

8.1.5. Lors du partage d'un produit du PKI, les entités n'appartenant pas aux Nations Unies devront s'engager par écrit :

- à reconnaître et respecter rigoureusement le principe de « maîtrise de l'information par son auteur ». **Si l'entité concernée souhaite partager un produit du PKI avec une autre entité, il lui faudra d'abord obtenir l'accord écrit explicite de la mission ;**
- à accepter, conformément aux principes régissant le PKI, que toute utilisation ultérieure de produits du PKI qui ont été partagés[9] :
  - soit strictement limitée aux activités ou opérations relatives à la sûreté et à la sécurité du personnel des Nations Unies, à l'appréciation de la situation et à la protection des civils ; ou
  - soit d'une portée définie par la mission plus restreinte que celle décrite ci-dessus ;
- à accepter de ne pas utiliser des produits du PKI qui ont été partagés pour inciter à commettre des violations des droits humains, des violations du droit international humanitaire ou tout autre crime international, ni à faciliter la commission de tels actes ;

[9] Voir le point 9.4. Domaines d'application au regard de la politique relative au renseignement dans les opérations de maintien de la paix.

- à accepter que des produits du PKI qui ont été partagés conservent leur classification de sécurité[10] ;
- à accepter que les produits classifiés du PKI soient traités et sécurisés selon des normes identiques à celles qu'applique l'entité réceptrice aux produits issus du renseignement d'un niveau de classification équivalent, ou selon une autre norme que la mission puisse accepter.

8.1.6. Les missions pourront également décider de partager partiellement des informations issues du PKI. Il leur faudra cependant se conformer à toutes les conditions susmentionnées.

8.1.7. S'il s'avère nécessaire de partager des produits du PKI en urgence, les étapes 8.1.1 à 8.1.4 n'en devront pas moins être respectées, mais il incombera au personnel de les mettre en œuvre **en priorité absolue**. Les missions pourront prévoir des procédures destinées à alerter le personnel concerné de l'urgence de la demande et à indiquer clairement la nécessité de la traiter en priorité en précisant le délai imparti. Toutes les conditions énumérées au point 8.1.5. demeureront de rigueur.

8.1.8. Si des produits du PKI font régulièrement l'objet d'un partage, les missions pourront prévoir une procédure d'autorisation normalisée à cet effet. Il pourra ainsi être envisagé de dresser et tenir à jour une liste d'entités pré-autorisées auxquelles ces produits peuvent être communiqués. Mais, même en pareil cas, tous les produits partagés devront être transmis au (à la) responsable chargé(e) de coordonner la gestion de l'information, qui devra veiller à ce qu'ils soient correctement consignés dans le registre ; la liste des entités devra être revue périodiquement (tous les trois mois au minimum, par exemple).

8.1.9. Si des informations issues du PKI ont été partagées par des voies informelles (oralement, par exemple), le personnel devra donner au (à la) responsable chargé(e) de coordonner la gestion de l'information un maximum de précisions afin que celles-ci puissent être consignées dans le registre.

8.1.10. En cas de non-respect ou de forte suspicion de non-respect des conditions énoncées au point 8.1.5, tout partage de produits du PKI devra être suspendu dans l'attente des résultats de l'enquête interne menée par la mission, conformément à la politique de diligence voulue en matière de droits de l'homme ; les activités de partage pourront reprendre dès lors que les conclusions de l'enquête sont positives et sous réserve que les risques et avantages de la poursuite des contacts entre les services de renseignement/de PKI et l'entité concernée soient réévalués. S'il est envisagé de reprendre le partage d'informations issues du PKI, la mission pourra décider de le faire à un moindre niveau et/ou au cas par cas dans un premier temps.

---

[10] Les niveaux de classification conférés aux produits du PKI devront être conformes à la circulaire ST/SGB/2007/6 relative au classement et maniement des informations sensibles et confidentielles, ainsi qu'à toutes les autres lignes directrices et instructions édictées par l'Organisation des Nations Unies en la matière.

8.1.11. Toutes les décisions relatives au partage d'informations issues du PKI sont prises au cas par cas, conformément aux présentes lignes directrices et aux éventuelles orientations données en la matière par les missions. Les résultats des deux évaluations devront également être soigneusement pris en compte. Les missions devront par ailleurs mettre en balance leur « besoin de partager » ces informations et le « besoin d'en savoir » de la contrepartie ; elles devront en outre s'assurer du respect de certains critères et vérifier notamment que l'entité : 1) intervient dans la zone d'opérations de la mission ou à proximité immédiate de celle-ci, 2) dispose d'une structure organisationnelle capable d'adapter ses opérations ou ses activités en fonction des informations nouvellement réceptionnées et 3) opère dans le cadre d'un mandat cohérent avec celui de la mission. Si des forces de sécurité n'appartenant pas aux Nations Unies sont concernées, leurs antécédents en matière de respect de la politique de diligence voulue en matière de droits de l'homme devront également être passés au crible.

8.1.12. Toute partie d'un produit du PKI qui, combinée avec d'autres données, pourrait permettre d'en retrouver la source ou le moyen d'acquisition, ou de rendre identifiables d'éventuels témoins ou victimes, devra être filtrée de manière appropriée avant d'être partagée[11]. Les responsables chargés de coordonner la gestion de l'information pourront être amenés, le cas échéant, à donner des conseils sur ce processus.

8.1.13. On trouvera à l'annexe C un logigramme représentant l'ensemble du processus.

8.2. *Partage d'informations issues du renseignement dans les opérations de maintien de la paix avec des entités des Nations Unies extérieures aux missions*

8.2.1. Les informations issues du PKI pourront être partagées avec des entités des Nations Unies extérieures aux missions dans les conditions suivantes :

- les informations stratégiques issues du PKI devront être partagées avec le (la) chef de bureau de l'entité ou de son équivalent ;
- les informations opérationnelles/tactiques issues du PKI devront être partagées avec le (la) plus haut(e) responsable du DSS en poste sur le lieu d'affectation, ainsi qu'avec le (la) responsable désigné(e) pour la sécurité. Il conviendra de suivre ce même processus dans les missions intégrées[12] ;
- si les informations issues du PKI portent sur des menaces affectant la protection des civils, la composante qui les a réceptionnées devra en outre avertir le (la) responsable hiérarchique le (la) plus haut placé(e)

[11] En outre, conformément à la circulaire ST/SGB/2007/6, aucune information ne devra être divulguée si elle risque : i) de mettre en danger la sécurité d'une personne, ii) de contrevenir à un devoir de confidentialité que l'ONU a envers un tiers, iii) de compromettre la confidentialité du processus décisionnel interne de l'Organisation, ou iv) d'entraver le bon déroulement des opérations actuelles ou futures de l'ONU.

[12] Le (la) responsable du DSS désigné(e) pour la sécurité devra ensuite partager ces informations avec les entités des Nations Unies concernées extérieures à la mission, conformément aux présentes lignes directrices.

en charge de la protection des civils et/ou le (la) représentant(e) désigné(e) comme tel(le).

Les responsables susmentionnés partageront ensuite les informations issues du PKI avec les membres du personnel concernés, selon les principes du « besoin de partager » pour les premiers et du « besoin d'en savoir » pour les seconds.

8.2.2. Tout partage d'informations issues du PKI avec des entités des Nations Unies extérieures aux missions devra être systématiquement consigné dans le registre *ad hoc* par le (la) responsable chargé(e) de coordonner la gestion de l'information, selon des modalités identiques à celles régissant le partage d'informations avec des entités n'appartenant pas au système des Nations Unies.

8.2.3. **Le principe de la « maîtrise de l'information par son auteur » s'appliquera également au partage d'informations issues du PKI avec des entités des Nations Unies extérieures aux missions**. Plus précisément, si l'entité concernée souhaite partager un produit du PKI avec une autre entité, il lui faudra d'abord obtenir l'accord écrit explicite de la mission.

8.2.4. Conformément aux principes régissant le PKI, l'entité devra s'engager à accepter que toute utilisation ultérieure de produits du PKI qui ont été partagés[13] :

- soit strictement limitée aux activités ou opérations relatives à la sûreté et à la sécurité du personnel des Nations Unies, à l'appréciation de la situation et à la protection des civils ; ou
- soit d'une portée définie par la mission plus restreinte que celle décrite ci-dessus.

8.2.5. Toute partie d'un produit du PKI qui, combinée avec d'autres données, pourrait permettre d'en retrouver la source ou le moyen d'acquisition, ou de rendre identifiables d'éventuels témoins ou victimes, devra être filtrée de manière appropriée avant d'être partagée. Les responsables chargés de coordonner la gestion de l'information pourront être amenés, le cas échéant, à donner des conseils sur ce processus.

8.2.6. Le marquage de sécurité des produits du PKI devra être conservé, traité et protégé de manière appropriée en fonction de leur niveau de classification correspondant.

9. <u>Réception d'informations issues du renseignement provenant d'entités extérieures aux Nations Unies</u>

- Compétence en matière de réception des informations
  a. Après vérification des informations réceptionnées, il conviendra d'attribuer comme il se doit la compétence relative aux modalités de leur diffusion au sein de la mission en fonction du niveau de classification de sécurité du

[13] Voir le point 9.4. Domaines d'application au regard de la politique relative au renseignement dans les opérations de maintien de la paix.

produit, de la source des informations et de la nature de ces dernières (stratégiques, opérationnelles/tactiques).

b. Les processus propres à l'attribution de la compétence en fonction de l'entité qui a partagé le produit[14], du degré de sécurité et de la nature des informations (stratégiques ou opérationnelles/tactiques) devront être déterminés par chaque mission de façon à être adaptés au mieux à leur situation respective. S'agissant des informations issues du renseignement revêtant un caractère stratégique, il est recommandé de confier cette compétence au (à la) président(e) du mécanisme de coordination du renseignement dans les opérations de maintien de la paix.

9.1. Dès réception d'un produit de renseignement, il conviendra de déterminer s'il concerne une menace évidente et imminente visant le personnel des Nations Unies et/ou des civils.

9.2. À supposer qu'il en soit ainsi, les étapes 9.4 à 9.7. n'en devront pas moins être respectées lors de la réception des informations mais il incombera au personnel de les mettre en œuvre **en priorité absolue**. Les missions pourront prévoir des procédures destinées à alerter le personnel concerné de la réception d'une telle information et à indiquer clairement la nécessité de la traiter en priorité en précisant le délai imparti.

9.3. La composante qui réceptionne les informations devra également en avertir le (la) commandant(e) de la force et/ou le (la) chef de la police civile, le ou les responsables chargés de coordonner la gestion de l'information ainsi que le DSS, afin qu'ils soient prêts à réceptionner les résultats de l'évaluation de l'entité aux fins de la réception d'informations et de l'examen rapide des informations recueillies, et déterminer s'il y a lieu de les faire suivre au (à la) chef de mission. Si les informations issues du renseignement portent sur des menaces affectant la protection des civils, la composante qui les a réceptionnées devra en outre avertir le (la) responsable hiérarchique le (la) plus haut placé(e) en charge de la protection des civils et/ou le (la) représentant(e) désigné(e) comme tel(le) par la mission.

9.4. Dès réception d'un produit de renseignement, il conviendra de procéder à une évaluation de l'entité aux fins de la réception d'informations et à un examen rapide des informations issues du renseignement[15].

9.5. L'évaluation de l'entité aux fins de la réception d'informations se compose de deux parties : 1) un aperçu des informations pertinentes concernant l'entité dont elles proviennent et 2) un examen rapide de l'entité sous l'angle des droits humains. On trouvera à l'annexe D un exemple d'évaluation d'une entité aux fins de la réception d'informations.

9.5.1. En principe, c'est la composante/l'unité qui a réceptionné les informations qui réalisera la première partie de l'évaluation, à moins que la mission ne décide qu'une autre composante/unité est mieux placée pour ce faire. La

[14] Entité des Nations Unies extérieure à la mission, entité n'appartenant pas au système des Nations Unies ou force de sécurité non onusienne, par exemple.

[15] L'évaluation de l'entité aux fins de la réception d'informations ne devra être réalisée qu'à la condition que cela n'a pas encore été fait ou que l'évaluation existante est jugée obsolète (voir le point 9.5.2.).

deuxième partie devra être effectuée par la composante Droits humains de la mission, en concertation avec les autres composantes concernées ; elle devra suivre, le cas échéant, les procédures spécifiquement prévues pour la réalisation des évaluations des risques PDVDH.

9.5.2. Une fois réalisées, les évaluations des entités aux fins de la réception d'informations devront être régulièrement revues et mises à jour, de manière à pouvoir être réutilisées pour la réception d'autres informations provenant des mêmes entités. Une surveillance active des faits nouveaux ou incidents pertinents est particulièrement importante pour la mise à jour de ces évaluations lorsqu'elles portent sur des forces de sécurité n'appartenant pas aux Nations Unies. Les évaluations devront, au minimum, être réexaminées après un laps de temps déterminé par la mission (tous les trois mois au moins, par exemple).

9.6. Le produit de renseignement qui a été réceptionné devra faire l'objet d'un examen rapide. Contrairement à l'évaluation de l'entité aux fins de la réception d'informations, cet examen devra être réalisé pour chaque produit réceptionné (à l'exception des produits de renseignement réceptionnés de manière régulière – voir le point 9.10.). On trouvera à l'annexe E un exemple d'examen rapide d'informations issues du renseignement à leur réception.

9.6.1. En principe, c'est la composante/l'unité qui a réceptionné les informations qui réalisera cet examen, à moins que la mission n'en décide autrement. La composante Droits humains devra également être consultée à cette occasion.

9.7. Une fois que l'évaluation de l'entité aux fins de la réception d'informations et l'examen rapide d'informations issues du renseignement à leur réception ont été effectués et que le produit de renseignement est autorisé à être utilisé par la mission, il appartiendra à l'autorité compétente de déterminer comment le diffuser, en fonction du besoin d'en connaître du personnel de la mission. Toutes les décisions relatives à la diffusion et à l'utilisation de produits de renseignement devront être prises au cas par cas, conformément aux présentes lignes directrices et aux éventuelles orientations données par les missions.

9.8. Lorsqu'elles réceptionnent des informations issues du renseignement, les missions devront en principe :

- respecter le principe de la « maîtrise de l'information par son auteur ». Si elles souhaitent partager un produit de renseignement avec une autre entité, elles devront d'abord obtenir l'accord écrit explicite de celle dont émanent ces informations ;
- traiter et sécuriser les informations recueillies, en respectant des normes identiques à celles applicables aux informations issues du PKI à un niveau de sécurité équivalent[16].

Si l'entité qui partage les informations issues du renseignement a prévu des normes spécifiques pour leur traitement et leur préservation, la mission devra,

[16] Ces normes devront être conformes à la circulaire ST/SGB/2007/6 relative au classement et maniement des informations sensibles et confidentielles, ainsi qu'à toutes les autres lignes directrices et instructions édictées par l'Organisation en la matière.

préalablement à leur réception, s'assurer qu'elle dispose des ressources et capacités nécessaires pour s'y conformer.

9.9. Le (la) chef de mission devra en outre faire officiellement savoir à ses homologues que les Nations Unies n'accepteront pas de recevoir des informations issues du renseignement qui auraient été obtenues sous la torture ou par d'autres agissements constituant de graves violations des droits humains ou du droit international humanitaire ; s'il existe un réel risque de cet ordre, les missions ne devront ni accepter ni solliciter de telles informations. La composante Droits humains devra être immédiatement avertie de la situation.

9.10. Si des produits de renseignement, en particulier des informations opérationnelles/tactiques, sont régulièrement fournis par une entité à une mission, celle-ci pourra prévoir une procédure d'autorisation normalisée à cet effet. Il pourra ainsi être envisagé de dresser et tenir à jour une liste d'entités pré-autorisées auprès desquelles ces produits peuvent être obtenus. Mais, même en pareil cas, tous les produits réceptionnés devront être transmis au (à la) spécialiste de la gestion de l'information, qui devra veiller à ce qu'ils soient correctement consignés dans le registre ; la liste devra être revue périodiquement (tous les trois mois au minimum, par exemple).

9.11. Si les informations issues du renseignement ont été réceptionnées par voies informelles (oralement, par exemple), le personnel devra donner au (à la) responsable chargé(e) de coordonner la gestion de l'information les informations nécessaires afin que celles-ci puissent être dûment consignées dans le registre.

9.12. Dans l'hypothèse où l'entité qui a partagé les informations est jugée peu fiable, ou à supposer que l'examen rapide détecte l'existence de l'un ou l'autre signal d'alerte fixé par la mission, des mesures supplémentaires devront être prises :

- une attention accrue devra être portée aux recoupements du produit en question avec d'autres informations issues du renseignement, du PKI ou autres ;
- si le produit est diffusé, il devra l'être en signalant clairement en quoi elles pourraient poser problème.

Les spécialistes de la gestion de l'information devront en faire état dans le registre afin de pouvoir déterminer comment évolue cette situation au fil du temps.

9.13. Lors de la réception d'un produit de renseignement, qu'il soit stratégique ou opérationnel/tactique, provenant d'entités qui n'appartiennent pas aux Nations Unies, il faudra en outre tenir dûment compte de ce qui suit :

- même si des évaluations des entités aux fins de la réception d'informations et des examens rapides des informations réceptionnées ont été effectués, tous les membres du personnel concernés n'en devront pas moins analyser soigneusement chaque produit de renseignement auquel ils ont accès, certains détails pouvant avoir été omis ou déformés à dessein ;
- toutes les informations issues du renseignement qui auront été réceptionnées devront être utilisées conjointement avec d'autres produits de renseignement et du PKI, ainsi qu'avec les autres informations dont dispose la mission ; elles ne devront jamais constituer le seul et unique élément à l'origine d'un acte ou d'une décision que la mission est amenée à prendre ;
- afin de s'assurer de l'exactitude et de la fiabilité des informations réceptionnées, les spécialistes de la gestion de l'information devront veiller à tenir à jour le registre central et à faire régulièrement le point sur son

contenu. En cas de réception répétée d'informations douteuses émanant d'une entité particulière, il conviendra d'en faire mention dans le registre et de prendre les mesures qui s'imposent ;

- les règles et procédures susmentionnées devront également s'appliquer au traitement de produits de renseignement obtenus auprès d'entités des Nations Unies extérieures aux missions mais provenant d'entités n'appartenant pas au système des Nations Unies.

9.14. On trouvera à l'annexe F un logigramme représentant l'ensemble du processus.

E. FONCTIONS ET ATTRIBUTIONS

- Chef de mission
  Le (la) chef de mission est chargé(e) de la mise en œuvre globale des présentes lignes directrices et doit veiller à ce que toutes les composantes de la mission soient pleinement informées de la façon dont elles procèdent. Il (elle) peut décider de déléguer la compétence en matière de partage des produits du PKI. Les chefs de mission sont tenus de prendre des mesures immédiates dès qu'ils ont connaissance d'informations issues du renseignement faisant état de menaces imminentes visant les Nations Unies et/ou des civils.

- Président(e) du mécanisme de coordination du renseignement dans les missions de maintien de la paix
  La tâche qu'il est recommandé de confier au (à la) président(e) de ce mécanisme consistera à déterminer si un produit stratégique du PKI peut être partagé avec une entité extérieure à la mission, et à qui devront être communiquées des informations stratégiques issues du renseignement émanant d'une entité extérieure à la mission.

- Composante Droits humains
  La composante Droits humains de la mission est chargée de contribuer à toutes les évaluations et à tous les examens pertinents pour ce qui concerne les droits humains, tant dans le cadre du partage d'informations issues du PKI que de la réception de produits de renseignement. C'est à elle qu'il reviendra également de réaliser les évaluations des risques PDVDH pour les évaluations décrites aux points 8.1.2 et 8.1.3. Si la mission ne dispose pas d'une telle composante, il faudra consulter le HCDH.

- Responsable chargé de coordonner la gestion de l'information
  Les responsables chargés de coordonner la gestion de l'information doivent consigner dans un registre central tous les produits du PKI qui sont partagés ainsi que les produits de renseignement réceptionnés. Il leur incombera également de conserver en lieu sûr les produits du PKI et produits de renseignement, ainsi que les examens dont ils ont fait l'objet, et de faciliter d'une manière générale les processus internes décrits dans les présentes lignes directrices pour ce qui est du partage d'informations issues du PKI ou de la réception d'informations issues du renseignement.

- Bureau des affaires juridiques de la mission
  Le Bureau des affaires juridiques veille à ce que tous les documents signés en rapport, par exemple, avec la réception d'informations issues du renseignement, ainsi que toutes les directives opérationnelles élaborées à la suite des présentes

lignes directrices, soient conformes à la Charte des Nations Unies, aux principes fondamentaux du maintien de la paix, au mandat de la mission et à d'autres règles et réglementations pertinentes relatives au PKI.

- Personnel des missions participant aux processus
  Tout membre du personnel de la mission qui participe aux processus de réception d'informations issues du renseignement ou de partage d'informations issues du PKI avec des entités extérieures est tenu de respecter ou de faire respecter les présentes lignes directrices, ainsi que les directives opérationnelles correspondantes.

F. DÉFINITIONS

- Mécanisme de coordination du renseignement dans les missions de maintien de la paix – Mécanisme établi au sein de la mission pour diriger et superviser son cycle du PKI. Doivent y participer les entités constitutives de la mission chargées d'acquérir, de compiler et d'analyser les informations en vue d'atteindre les objectifs des activités de PKI menées au sein de la mission, à savoir le Centre d'analyse conjointe de la mission, les composantes compétentes dans le domaine militaire et de la police, ainsi que le DSS. Le Centre d'opérations conjoint devrait également être un membre permanent du mécanisme, étant donné qu'il intervient dans la fourniture d'un ensemble d'informations permettant d'apprécier la situation. D'autres sections de la mission, notamment le Bureau des affaires juridiques de la mission, la Division des affaires civiles ou la composante Droits humains, peuvent être invitées à participer au mécanisme de manière permanente ou ponctuelle.

- Renseignement dans les opérations de maintien de la paix (PKI) – Voir le point 9 de la politique relative au renseignement dans les opérations de maintien de la paix pour ce qui concerne les principes sur lesquels il repose.

- Renseignement/PKI opérationnel ou tactique – Renseignement ou PKI obtenu en réponse à une instruction donnée au niveau opérationnel ou tactique, et visant à éclairer, au sein d'une mission, la prise de décisions concernant des opérations ou activités menées au niveau du sous-quartier général. Il requiert généralement une action plus rapide et plus dynamique que le renseignement/PKI stratégique, et son périmètre géographique est plus limité. Les produits de renseignement/PKI qui font régulièrement l'objet d'un partage entre une mission et une entité extérieure entrent généralement dans cette catégorie.

- Renseignement/PKI stratégique – Renseignement ou PKI obtenu en réponse à une instruction donnée par le (la) chef de mission ou en son nom, et visant à éclairer sa prise de décisions et celle d'autres hauts responsables de la mission. Ce type de produit offre une perspective à moyen ou plus long terme, et son périmètre géographique couvre généralement l'ensemble de la zone de la mission, voire au-delà.

G. RÉFÉRENCES

Références normatives

- Politique du DOP relative au renseignement dans les opérations de maintien de la paix (2019)

Procédures ou directives connexes

- Politique de diligence voulue en matière de droits de l'homme en cas d'appui de l'ONU à des forces de sécurité non onusiennes (2011)
- Note d'orientation relative à la politique de diligence voulue en matière de droits de l'homme en cas d'appui de l'ONU à des forces de sécurité non onusiennes (2015)
- Lignes directrices relatives aux opérations de police menées dans le cadre des opérations de maintien de la paix et des missions politiques spéciales de l'Organisation des Nations Unies (2016)
- Joint Mission Analysis Centre Field Handbook (2018)
- Manuel du renseignement dans les opérations de maintien de la paix (2019)
- OICT SOP on Sharing Information with External Partners (2020)
- Politique relative aux cellules d'analyse conjointe des missions (2020)
- Circulaire du Secrétaire général ST/SGB/2007/6 – Informations sensibles ou confidentielles : classification et maniement (2007)

H. SUIVI DE L'APPLICATION

8. Le (la) chef de mission est chargé(e) de veiller à ce que celle-ci respecte les présentes lignes directrices et mette en place des mécanismes ou procédures efficaces permettant de s'en assurer. Si tous les membres du personnel des missions qui participent au système de PKI doivent rendre compte, *via* leur hiérarchie, de la façon dont ils se conforment à ces lignes directrices, le (la) chef d'état-major de la mission, le chef du Bureau des affaires juridiques et le ou les spécialiste(s) de la gestion de l'information ont chacun des attributions essentielles pour ce qui concerne leur application effective. Il peut être procédé à des évaluations régulières de la mise en œuvre des présentes lignes directrices afin de déterminer dans quelle mesure elles sont respectées.

I. SERVICE À CONTACTER

9. Pour tout ce qui concerne les présentes lignes directrices, le service à contacter est l'Équipe de coordination du renseignement dans les opérations de maintien de la paix du Bureau du (de la) Secrétaire général(e) adjoint(e) aux opérations de paix du Département des opérations de paix.

J. HISTORIQUE

10. Le présent texte constitue la première version de ces lignes directrices.

SIGNATURE :

Jean-Pierre Lacroix
Secrétaire général adjoint
aux opérations de paix

DATE D'APPROBATION :

ANNEXE A : EXEMPLE D'ÉVALUATION D'UNE ENTITÉ AUX FINS DU PARTAGE D'INFORMATIONS ISSUES DU RENSEIGNEMENT (pour chaque entité)

PARTIE 1 : Aperçu des informations pertinentes concernant l'entité

- Informations relatives à une entité n'appartenant pas au système des Nations Unies (Organisation, département/unité, point(s) de contact, fonctions, coordonnées, etc.)
- Questions suggérées
  - De quel mandat l'entité est-elle investie ?
  - Le mandat de l'entité est-il compatible avec celui de la mission ?

PARTIE 2 : Évaluation des risques sous l'angle des droits humains[17]

- Un modèle d'évaluation des risques PDVDH figure à l'annexe 1 de la note d'orientation relative à la politique de diligence voulue en matière de droits de l'homme en cas d'appui de l'ONU à des forces de sécurité non onusiennes (2015). Des indications précises quant aux modalités à suivre pour mener cette évaluation sont fournies aux pages 18 à 24 de ce même document.
- Conformément au point 11.4.4. de la politique, s'il est envisagé de partager des informations issues du PKI avec des forces de sécurité n'appartenant pas aux Nations Unies, en ce comprises les autorités civiles qui en sont directement responsables, l'évaluation des risques PDVDH devra a priori être effectuée par la composante Droits humains de la mission ou, à défaut, par le HCDH. En ce qui concerne les entités civiles, l'évaluation devra être adaptée en fonction de ce qu'aura décidé la mission, sauf pour les autorités civiles nationales directement responsables de la gestion, de l'administration, du commandement ou du contrôle de forces de sécurité n'appartenant pas aux Nations Unies, pour lesquelles l'évaluation des risques devra être effectuée conformément à la politique en la matière.

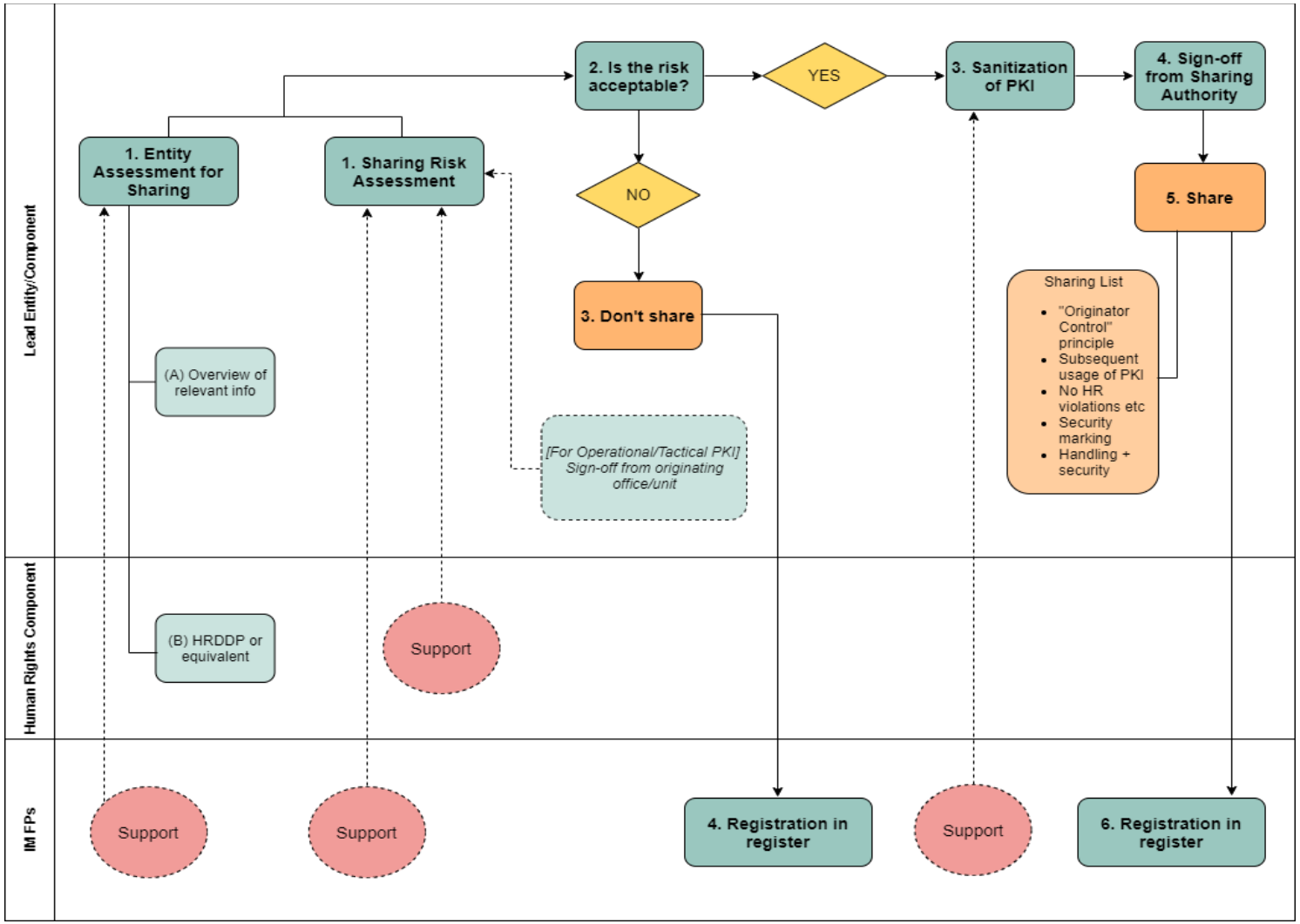
[17] Si le partage d'informations issues du PKI avec l'une des sous-composantes d'une entité est jugé inacceptable, les missions peuvent décider qu'il ne se fera qu'à la condition que cette sous-composante en soit exclue.

ANNEXE B : EXEMPLE D'ÉVALUATION DES RISQUES LIÉS AU PARTAGE D'INFORMATIONS ISSUES DU RENSEIGNEMENT (pour chaque produit du PKI)

Questions suggérées

- Le partage de ce produit du PKI est-il conforme au mandat de la mission ?
- Le partage de ce produit du PKI est-il conforme à la Charte des Nations Unies, aux règles et réglementations de l'Organisation des Nations Unies, ainsi qu'à tout accord bilatéral ou multilatéral applicable à [dénomination de la mission] ?
- Le produit de renseignement/du PKI a-t-il été « filtré » pour en retirer toute donnée/information qui, combinée avec d'autres données, pourrait permettre d'en retrouver la source ou le moyen d'acquisition et de les compromettre, ou de rendre identifiables d'éventuels témoins ou victimes ayant un lien avec ces informations ?
- Le service qui a initialement acquis les informations a-t-il été consulté et a-t-il approuvé leur partage ?
- Que peut-on raisonnablement attendre que l'entité fasse du produit du PKI ?
- Le partage d'informations issues du PKI avec cette entité a-t-il déjà posé problème ?
- Peut-on raisonnablement escompter que le partage de ce produit du PKI avec cette entité ne portera pas préjudice aux Nations Unies ou à [dénomination de la mission], à son personnel ou à son mandat ?
- Existe-t-il de sérieux motifs de croire que les informations issues du PKI qui devraient être partagées pourraient être utilisées pour inciter à commettre des violations des droits humains, des violations du droit international humanitaire ou tout autre crime international ou à faciliter la commission de tels actes ?
- Quel est le niveau de classification du produit du PKI pour l'ONU ?
- L'entité dispose-t-elle des ressources et capacités nécessaires pour traiter et sécuriser les produits classifiés du PKI selon des normes identiques à celles qu'elle applique aux produits issus du renseignement d'un niveau de classification équivalent, ou selon une autre norme que la mission puisse accepter ?

ANNEXE C : LOGIGRAMME DU PROCESSUS DE PARTAGE D'INFORMATIONS ISSUES DU PKI



ANNEXE D : EXEMPLE D'ÉVALUATION D'UNE ENTITÉ AUX FINS DE LA RÉCEPTION D'INFORMATIONS ISSUES DU RENSEIGNEMENT (pour chaque entité)

PARTIE 1 : Aperçu des informations pertinentes concernant l'entité

- Informations relatives à l'entité (Organisation, département/unité, point(s) de contact, fonctions, coordonnées, etc.)
- Questions suggérées
  - De quel mandat l'entité est-elle investie ?
  - En quoi l'entité est-elle concernée par la situation actuelle ?
  - Quels sont les intérêts et motivations possibles de l'entité par rapport à la situation actuelle ?
  - Pourquoi l'entité souhaite-t-elle partager des produits de renseignement avec [dénomination de la mission] ?
  - L'entité a-t-elle fait savoir ce qu'elle attend que l'ONU fasse au vu des informations qu'elle a partagées ?
- Une note de fiabilité devra être attribuée à l'aide du tableau ci-dessous à toutes les entités qui fournissent des informations.

Tableau : Notation de la fiabilité de l'entité

Fiabilité de l'entité		
Notation	**Évaluation**	**Observations**
A	Fiable	Absence totale de doute quant à l'authenticité, la crédibilité ou la compétence de l'entité, qui s'est révélée totalement fiable par le passé
B	Généralement fiable	Existence d'un léger doute quant à l'authenticité, la crédibilité ou la compétence de l'entité, qui a fourni par le passé des informations généralement valables
C	Généralement peu fiable	Doute important quant à l'authenticité, la crédibilité ou la compétence de l'entité, qui a cependant déjà fourni des informations valables par le passé
D	Non fiable	Manque d'authenticité, de crédibilité et de compétence de l'entité, qui a fourni par le passé des informations non valables
E	Ne peut être appréciée	Absence d'éléments permettant d'évaluer la fiabilité de la source.

PARTIE 2 : Examen rapide d'une entité sous l'angle des droits humains

- Quel est le bilan de l'entité en matière de droits humains (respecte-t-elle ou non le droit international humanitaire, le droit international des droits humains et le droit international des réfugiés) ?
- L'entité a-t-elle des antécédents spécifiques de « violations graves » du droit international humanitaire, du droit international des droits humains ou du droit international des réfugiés, telles que définies au point 12 de la politique de diligence voulue en matière de droits de l'homme ?[18]
- L'entité est-elle connue pour détenir arbitrairement du personnel auprès desquelles des informations ont pu être obtenues, ou est-elle soupçonnée de le faire ?

[18] Les antécédents pris en considération devront remonter aussi loin que la mission le juge utile pour pouvoir éventuellement anticiper un comportement futur.

- L’entité est-elle connue pour utiliser des techniques d’interrogatoire de détenus non conformes au droit international humanitaire, au droit international des droits humains et au droit international des réfugiés, ou est-elle soupçonnée de le faire ?
- L’entité dispose-t-elle de mécanismes de contrôle et de sanction appropriés et efficaces en cas de violation des droits humains ?
- L’entité a-t-elle des préjugés notoires à l’encontre de groupes spécifiques, tels que les minorités ethniques/religieuses, les femmes, les jeunes, les groupes politiques, les personnes handicapées et les personnes LGBTQIA+ ?

ANNEXE E : EXEMPLE D'EXAMEN RAPIDE D'INFORMATIONS ISSUES DU RENSEIGNEMENT À LEUR RÉCEPTION (pour chaque produit de renseignement)

Questions suggérées

- Le produit qui a été réceptionné contient-il des informations issues du renseignement qui concernent une menace imminente pour le personnel des Nations Unies et/ou des civils ?
- Les informations issues du renseignement qui ont été réceptionnées sont-elles de nature stratégique ou opérationnelle/tactique ?
- Existe-t-il des raisons de penser que les informations issues du renseignement qui ont été réceptionnées ont été obtenues par le biais de moyens constituant des violations graves du droit international humanitaire, du droit international des droits humains ou du droit international des réfugiés ?
- Pourquoi le produit de renseignement a-t-il été partagé ?
- Existe-t-il des raisons de penser que le produit de renseignement réceptionné pourrait être utilisé à des fins politiques ?
- Quel est le niveau de classification de sécurité du produit de renseignement ?

Une note de fiabilité devra être attribuée à l'aide du tableau ci-dessous aux informations issues du renseignement.

Tableau : Notation des informations issues du renseignement réceptionnées

Crédibilité des informations		
Notation	**Évaluation**	**Observations**
1	Confirmée	Information confirmée par d'autres sources indépendantes, intrinsèquement logique et cohérente avec d'autres informations ou informations issues du renseignement ou du PKI sur le même sujet.
2	Probablement vraie	Information non confirmée, mais intrinsèquement logique et cohérente avec d'autres informations ou informations issues du renseignement ou du PKI sur le même sujet.
3	Douteuse	Information non confirmée, possible mais non logique, et pour laquelle il n'existe pas d'autres informations ou informations issues du renseignement ou du PKI sur le même sujet.
4	Improbable	Information non confirmée, dénuée de toute logique intrinsèque, et en contradiction avec d'autres informations ou informations issues du renseignement ou du PKI sur le même sujet.
5	Ne peut être appréciée	Absence d'éléments permettant d'évaluer la validité de l'information ou de l'information issue du renseignement ou du PKI.

ANNEXE F : LOGIGRAMME DU PROCESSUS DE RÉCEPTION D'INFORMATIONS ISSUES DU RENSEIGNEMENT