



Politique

Renseignement dans les opérations de maintien de la paix (PKI)

Document approuvé par : Secrétaire général adjoint aux opérations de paix
Date d'entrée en vigueur : 1^{er} mai 2019
Service à contacter : Équipe de coordination du renseignement dans
les opérations de maintien de la paix du
Département des opérations de paix
Date de révision : 1^{er} mai 2021

**POLITIQUE DU DÉPARTEMENT DES OPÉRATIONS DE PAIX SUR
le renseignement dans les opérations de maintien de la paix**

Table des matières :

- A. Objet et contexte**
 - B. Champ d'application**
 - C. Politique**
 - D. Fonctions et attributions**
 - E. Définitions**
 - F. Références**
 - G. Suivi de l'application**
 - H. Service à contacter**
 - I. Historique**
-

ANNEXES

- A. Cadre général relatif au renseignement dans les opérations de maintien de la paix
 - B. Principaux membres du mécanisme de coordination du renseignement dans les missions de maintien de la paix
 - C. Modèle de plan d'appui au renseignement dans les missions de maintien de la paix
-

A. OBJET ET CONTEXTE

1. La présente politique expose les motifs qui président au recueil, à la compilation, à l'analyse, à la diffusion, à l'utilisation, à la protection et à la gestion des informations obtenues à l'appui des missions que mènent sur le terrain les opérations de maintien de la paix des Nations Unies, et indique les méthodes utilisées à cet effet. Elle établit un cadre qui définit une approche cohérente et fondée sur des principes concernant le renseignement dans les opérations de maintien de la paix, aide à tirer parti des ressources aussi efficacement que possible, met en place un système rigoureux de supervision, de responsabilité et de constante amélioration, et prévoit des mécanismes facilitant l'application d'une stratégie efficace, intégrée et sûre axée sur l'ensemble d'une mission.
2. À l'image des mandats et contextes opérationnels des missions de maintien de la paix des Nations Unies, les capacités, processus et procédures qu'exigent la collecte et l'analyse des informations changent. Face à des situations tendues, complexes et périlleuses caractérisées par des menaces asymétriques et transnationales qui font courir aux soldats de la paix et aux civils de graves dangers et entravent l'exécution des tâches qui leur sont assignées, les responsables des missions de maintien de la paix se doivent de mieux comprendre l'environnement et le contexte dans lesquels ils interviennent, d'avoir une vue d'ensemble stratégique de leur évolution, d'anticiper les menaces spécifiques et de saisir les possibilités qui s'offrent pour permettre aux soldats de la paix de s'acquitter avec efficacité de leur mandat.
3. Ces exigences nouvelles ont conduit le Conseil de sécurité, les États Membres et le Secrétariat à considérer de plus en plus le PKI comme un moyen essentiel de faire en sorte que les missions puissent être menées de manière sûre et efficace. Dans sa résolution 1894 de 2009, le Conseil de sécurité a demandé au Secrétariat de donner « la priorité dans les décisions qui organisent, aux fins de l'accomplissement des mandats, l'emploi des moyens et des ressources disponibles, y compris en matière d'information et de renseignement » à la protection des civils. Il a depuis souligné, notamment

dans sa résolution 2295 de 2016, la nécessité de doter la MINUSMA de capacités en matière de renseignement, compte tenu des conditions de sécurité complexes dans lesquelles elle opère.

4. Le Comité spécial des opérations de maintien de la paix (Comité des 34) s'est également dit conscient qu'il importait de renforcer les capacités de collecte et d'analyse de l'information. Dans son rapport de 2018 (A/72/19), il a convenu « que certaines missions de maintien de la paix [étaient] déployées dans des contextes d'insécurité et d'instabilité politique et [devaient] faire face à des menaces asymétriques et complexes ». Il a rappelé, dans ce contexte, « qu'[...] il avait demandé au Secrétariat de mettre au point un système d'appréciation de la situation qui soit plus cohérent et mieux intégré à l'échelle du système des Nations Unies [...] ». Aux paragraphes 71 à 77 de ce même rapport, le Comité spécial a notamment mis en avant l'importance d'une complémentarité avec d'autres approches en matière de sûreté et de sécurité, fait valoir que les politiques et pratiques en matière de PKI devaient respecter les principes de la Charte des Nations Unies et les principes fondamentaux du maintien de la paix, plaidé pour que soit garanti le respect de la souveraineté des États hôtes et des États voisins, et souligné que la sécurité et la confidentialité des informations sensibles devaient être gérées avec soin.
5. L'objectif fondamental du renseignement dans les opérations de maintien de la paix des Nations Unies s'inscrit dans le droit fil des résolutions pertinentes du Conseil de sécurité et du rapport susmentionné du Comité des 34 : il vise à permettre aux missions de prendre des décisions sur les mesures à prendre pour mieux apprécier la situation et améliorer la sûreté et la sécurité du personnel de l'Organisation, et à éclairer les activités et interventions liées à la protection des civils. Le renseignement a pour but, en l'espèce :
 - 5.1. d'appuyer une situation opérationnelle commune – Des informations exactes et à jour en matière de maintien de la paix contribuent à dresser un bilan opérationnel cohérent en temps réel de la zone de la mission et de le tenir à jour, de manière à faciliter la planification et l'exécution des activités ;
 - 5.2. de lancer rapidement l'alerte en cas de menace imminente – Le renseignement permet de lancer rapidement l'alerte en cas de menace imminente pour la vie des personnes, de risque de destructions majeures de biens, de restrictions importantes à la circulation, etc., afin que la mission puisse agir de manière appropriée, conformément à son mandat ;
 - 5.3. de repérer les risques à éviter et les possibilités à exploiter – Le renseignement peut donner aux responsables de la mission une compréhension plus fine de l'évolution du contexte opérationnel et stratégique, ainsi que des risques à éviter et des possibilités à exploiter, en ce qui concerne la sûreté et la sécurité du personnel des Nations Unies et du personnel associé, ainsi que la protection des civils.

B. CHAMP D'APPLICATION

6. La présente politique décrit les principes généraux, les processus et les paramètres sur lesquels repose la gestion des besoins en matière de renseignement dans les opérations de maintien de la paix des Nations Unies. Des orientations quant aux outils et activités des différentes composantes d'une mission, ainsi que des informations relatives aux fonctions des bureaux du Département des opérations de paix au Siège en matière de soutien, de coordination et d'appui aux systèmes de renseignement dans les opérations de maintien de la paix d'une mission, seront fournies dans les politiques opérationnelles et instructions permanentes secondaires. La présente politique devra être lue en parallèle avec ces informations et orientations (voir l'annexe A).

7. La présente politique s'applique aux opérations et activités de missions dont il a été établi, soit par les bureaux du DPO au Siège durant la phase initiale de planification de la mission, soit ultérieurement lors d'une consultation entre le Siège et la mission, que des capacités et moyens de renseignement leur étaient nécessaires. Des besoins et exigences spécifiques seront recensés au cours du processus de planification de la mission ou durant son cycle de vie en fonction d'un certain nombre de considérations, notamment – sans que cette énumération soit limitative – le mandat de la mission, la nature des menaces pesant sur le personnel, les biens et les programmes des Nations Unies, la nature des menaces pesant sur les civils, ainsi que le contexte politique et sécuritaire dans lequel la mission est déployée. Le respect des principes fondamentaux, des paramètres et des limites applicables à la gestion du PKI tels que décrits dans la présente politique est impératif et vaut pour tout le personnel en charge de ces activités.
 8. La présente politique concerne uniquement les données, informations et produits recueillis et gérés dans le cadre du cycle du renseignement dans les opérations de maintien de la paix, par opposition aux autres informations communiquées. La communication de routine et le partage d'informations sont distincts du renseignement, même si l'analyse de certaines informations peut s'appuyer sur la communication de routine, et quand bien même cette dernière peut parfois renfermer des informations sensibles. La présente politique ne modifiera ni ne limitera les pratiques habituelles en matière de gestion, de communication et de partage des informations, conformément aux orientations existant dans ces domaines, et s'appuiera sur ces pratiques pour encadrer les activités de renseignement dans les opérations de maintien de la paix.
-

C. POLITIQUE

9. Principes du renseignement dans les opérations de maintien de la paix (PKI)

- 9.1. La présente section expose les principes généraux qui doivent guider toutes les activités des opérations de maintien de la paix des Nations Unies à tous les stades de la gestion du renseignement. Toutes les orientations et directives, tous les plans et toutes les opérations connexes devront être conformes à ces principes et les appliquer.
- 9.2. **Respect des règles** – Toutes les activités liées au PKI seront menées dans le droit fil des mandats définis par le Conseil de sécurité pour les opérations de maintien de la paix, en parfaite conformité avec la Charte des Nations Unies. Elles devront être cohérentes avec le cadre juridique général régissant les opérations de maintien de la paix des Nations Unies, notamment les principes fondamentaux en la matière et l'ensemble des normes et obligations juridiques ainsi que des dispositions relatives aux droits humains. Elles devront être exécutées dans le plein respect des droits humains, en ce compris le droit à la vie privée, le droit à la liberté d'expression, le droit de réunion pacifique et le droit d'association, en veillant tout particulièrement à n'exposer aucune source d'information existante ou potentielle à un quelconque danger.
- 9.3. **Non-clandestinité** – Les activités clandestines, à savoir celles qui visent à acquérir des informations ou renseignements en faisant en sorte de les tenir secrètes ou de les dissimuler en raison de leur caractère illicite ou contraire au cadre juridique ainsi qu'aux principes, politiques et mandats des opérations de maintien de la paix des Nations Unies, vont au-delà des limites fixées pour le PKI et ne doivent pas être menées par les entités participant à la mission. Afin de renforcer ce principe, il conviendra d'organiser périodiquement des formations théoriques et pratiques, notamment une formation préalable au déploiement destinée à l'ensemble du personnel participant aux différentes composantes du PKI, et de veiller à ce que ces activités fassent régulièrement l'objet d'audits et de mesures de supervision.

NON CLASSIFIÉ

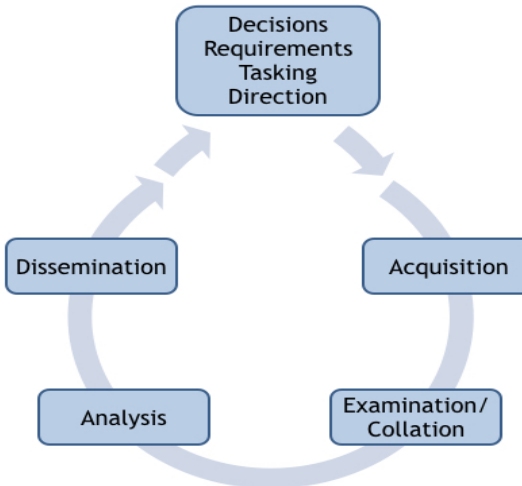
- 9.4. **Portée** – L’acquisition et la gestion d’informations ou de renseignements effectuées dans le cadre des opérations de maintien de la paix des Nations Unies auront pour but de permettre au personnel de l’Organisation de mieux apprécier la situation et d’améliorer sa sûreté et sa sécurité ; elles viendront également guider les opérations et activités liées à la protection des civils inscrites dans les mandats du Conseil de sécurité.
- 9.5. **Respect de la souveraineté des États** – La souveraineté des États, y compris de l’État hôte et des États voisins, doit être respectée.
- 9.6. **Indépendance** – Les activités liées au PKI seront menées de manière totalement autonome et indépendante à tous égards d’un quelconque système national de renseignement ou d’autres opérations, et conserveront leur caractère exclusivement international. Les missions pourront se mettre en rapport avec des entités extérieures, notamment les États hôtes, afin de recevoir des informations et de partager des renseignements spécifiques sur le maintien de la paix, à condition de le faire dans les conditions et selon les paramètres décrits dans le présent document et dans les orientations connexes.
- 9.7. **Responsabilisation, moyens et habilitation** – Les personnes habilitées à prendre des décisions concernant les activités liées au PKI doivent disposer de moyens appropriés pour exercer ces fonctions et continueront à rendre compte de leur bonne exécution au sein de leurs chaînes de commandement respectives, devant le (la) chef de mission et, en dernier ressort, devant le (la) Secrétaire général(e). Le (la) chef de mission est responsable du fonctionnement du système de PKI. Il lui appartient de veiller à ce que les membres du personnel qui s’occupent des produits de renseignement ou les utilisent respectent la présente politique et les orientations y relatives, en mettant en place des procédures de gouvernance, des formations et des pratiques efficaces.
- 9.8. **Sécurité et confidentialité** – Les produits du PKI doivent être stockés et partagés de manière sécurisée, tout en garantissant l’accès aux personnes qui en ont besoin à des fins de prise de décisions et de planification des opérations. Les missions doivent mettre en place, en s’appuyant sur une évaluation des risques et en concertation avec le Département des opérations de paix et le Département de l’appui opérationnel au Siège, des procédures, outils technologiques et mesures de sécurité physique visant à garantir la sécurité de la gestion de l’information et des communications dans le cadre du système du renseignement. Les produits de renseignement confidentiels liés au maintien de la paix doivent être partagés et diffusés selon les principes du « besoin d’en connaître » ou du « besoin de partager », au titre desquels le renseignement doit être divulgué au personnel de la mission si, et uniquement si, l’accès audit renseignement est indispensable pour qu’il puisse mener à bien ses fonctions officielles. Pour ce faire, une délégation de pouvoirs écrite de la personne ou du membre du personnel ayant décidé du niveau de classification est nécessaire. Il en résulte que les informations issues du PKI ne peuvent être partagées qu’avec des personnes de confiance, l’objectif étant de faire en sorte que leur diffusion reste limitée, en particulier lorsqu’elle est susceptible de porter atteinte à la sûreté ou à la sécurité d’une personne ou d’un groupe, ou d’entraîner une violation des droits ou de la vie privée. Ce faisant, les missions s’efforceront d’établir et de maintenir un niveau de confiance élevé auprès de tous leurs interlocuteurs quant à leur capacité à acquérir, protéger et gérer de manière appropriée des informations liées au PKI.

10. Processus : le cycle du renseignement pour le maintien de la paix

- 10.1. La présente section décrit le cycle du renseignement pour le maintien de la paix, c’est-à-dire le processus par lequel les informations sont acquises, examinées ou compilées, analysées et diffusées selon des besoins clairement définis en la matière. Les normes, outils, techniques et procédures permettant aux différentes composantes de la mission de mener à bien chaque

étape du cycle de manière efficace et rationnelle feront l'objet d'orientations et conseils opérationnels connexes.

Figure 1. Cycle du renseignement pour le maintien de la paix



- 10.2. Orientation, besoins et répartition des tâches – L'orientation désigne le processus visant à déterminer les questions auxquelles il faut répondre, à préciser les « besoins en information ou renseignement pour le maintien de la paix » liés à ces questions qui n'ont pas été satisfaits, et à rechercher ces informations par divers moyens. L'orientation permet d'être au cœur-même du cycle du renseignement pour le maintien de la paix, en établissant un lien entre les besoins de la ou du chef de la mission et de son équipe de direction et la gestion du PKI. C'est sur elle que reposent les besoins en renseignement. L'ordre de priorité des tâches et les délais y afférents sont déterminés par les mécanismes de gestion du renseignement dans les opérations de maintien de la paix mis en place au sein de la mission. Les décisions relatives au PKI doivent être prises sous l'autorité et la responsabilité du (de la) chef de mission ou dans les limites des pouvoirs que celle-ci ou celui-ci délègue.
- 10.3. Acquisition – L'acquisition désigne le processus d'obtention de données et d'informations qui seront ensuite analysées. Le ciblage et la planification sont nécessaires pour que les activités d'acquisition soient menées efficacement et les ressources utilisées au mieux pour répondre aux besoins en renseignement. Il s'agit notamment d'affecter les moyens en fonction des besoins en renseignement et des capacités, de s'assurer que les données et les informations sont communiquées en temps voulu et de mettre en place des mécanismes permettant de corroborer ou de vérifier l'exactitude des informations et des données, le cas échéant. Les paramètres d'une acquisition efficace, responsable et déontologique de données et d'informations seront décrits dans le plan d'appui au PKI de la mission (voir la section 12.8 et l'annexe C). Outre le fait qu'il doit être conforme à la présente politique et aux autres politiques et orientations des Nations Unies, ce plan décrit les outils, techniques et procédures acceptables et inacceptables d'acquisition d'informations par la mission, les obligations juridiques applicables et les éléments à prendre en compte lors de l'acquisition de PKI, en fonction des moyens dont dispose la mission et conformément aux orientations et conseils opérationnels attachés à la présente politique.
- 10.4. Outre que la mission peut acquérir des informations grâce aux moyens qui lui sont attribués à cet effet, elle peut également obtenir des renseignements fournis volontairement par les États Membres ainsi que par d'autres entités extérieures à la mission ; elle devra donc mettre en place des mécanismes destinés à faciliter la réception et le traitement sécurisés de ces données.

Lorsqu'il est en contact avec des tierces parties pour l'acquisition d'informations, le personnel de la mission doit respecter pleinement le mandat de la mission ainsi que tous les principes et toutes les règles et obligations de l'Organisation, notamment en ce qui concerne la promotion et la protection des textes de loi et des normes internationales en matière de droits humains, et agir conformément à ceux-ci. Les liens avec des entités extérieures à la mission à des fins du partage de PKI peuvent également être régis par des accords écrits conclus entre l'Organisation des Nations Unies et ces parties, dans le cadre de paramètres plus larges.

- 10.5. Examen et compilation – Les données et informations recueillies par les missions sont enregistrées et conservées de manière à pouvoir être aisément comparées, évaluées, appréciées, retrouvées, analysées et communiquées. Les entités participant à la mission utilisent des outils normalisés pour la compilation de données et d'informations, notamment des bases de données communes, des taxonomies, ainsi que des outils d'indexation et des menus programmés. Le DPO devra concevoir et mettre en place, en consultation avec les missions, des outils communs et, le cas échéant, spécialisés, qui devront faire l'objet d'une formation.
- 10.6. Analyse – L'analyse désigne le processus consistant à décomposer méthodiquement l'information pour en extraire les éléments constitutifs, à examiner chacun d'entre eux afin d'établir des corrélations et à appliquer un raisonnement pour déterminer la signification et la pertinence des différents éléments et de l'ensemble qu'ils forment. Lors de la récupération des informations acquises grâce aux moyens affectés aux différentes entités de la mission, les analystes du PKI appliquent des processus de raisonnement, d'intégration et d'interprétation, en utilisant des méthodes à la fois qualitatives et quantitatives. L'analyse du PKI est un processus qui concerne l'ensemble de la mission et tire pleinement profit de toutes les ressources dont celle-ci dispose en fonction de leurs avantages comparatifs – connaissance de la situation, des langues et des cultures locales, capacités d'analyse du PKI des forces armées et de la police, techniques d'analyse des informations relatives aux menaces pesant sur la sécurité.
- 10.7. Diffusion¹ – La diffusion désigne le processus de transmission du PKI à celles et ceux qui dirigent la mission et à d'autres membres du personnel concernés. Les produits élaborés dans le cadre du cycle du PKI peuvent être diffusés directement par les différentes entités participant à la mission à leurs responsables respectifs (voir l'annexe B), ou conjointement par l'intermédiaire du mécanisme de coordination du renseignement dans les missions de maintien de la paix. La délégation de pouvoir pour la diffusion des produits du PKI doit être clairement définie dans le plan d'appui au PKI de la mission ou dans les orientations internes destinées aux entités participant à la mission. Cette diffusion se fait dans le respect des concepts de « besoin d'en connaître et besoin de partager », ainsi que des impératifs institutionnels évoqués ci-après en matière de classification, de sécurité, de traitement, de propriété et de partage de l'information. Le (la) chef de mission est responsable en dernier ressort de la décision concernant la diffusion de tous les produits du PKI.

11. Classification, sécurité, traitement et partage des informations

- 11.1. La présente section aborde la question de la gestion du PKI par les missions sous l'angle de la politique des Nations Unies relative à la sécurité, au traitement et au partage des informations sensibles. Elle recense les pratiques, les instances et les mécanismes de contrôle qui doivent être mis en place pour assurer un traitement efficace et un partage rapide, cohérent et sûr des informations obtenues grâce au PKI. La classification, la sécurisation et le traitement des informations obtenues grâce au PKI doivent veiller à préserver la sûreté et la sécurité des sources, à limiter au maximum le risque de diffusion ou de divulgation non autorisée, à défendre les intérêts

¹ Certains documents d'orientation relatifs à la gestion de l'information de l'Organisation des Nations Unies, du DPO et du DOS utilisent également le terme « distribution ».

NON CLASSIFIÉ

de l'Organisation des Nations Unies et à respecter les obligations qu'impose le droit international pour le partage des produits issus du renseignement dans le domaine des opérations de paix.

11.2. Classification et sécurité des informations

11.2.1. Les données et informations acquises, stockées et partagées dans le cadre du cycle du PKI sont considérées comme la propriété de l'Organisation des Nations Unies et doivent être traitées dans le strict respect de la circulaire du Secrétaire général sur la classification et le maniement des informations sensibles ou confidentielles (ST/SGB/2007/6) et de tout autre instrument d'orientation adopté ultérieurement à ce sujet. Les informations sensibles doivent donc être qualifiées de « strictement confidentielles » et de « non classifiées » par celle ou celui qui les a recueillies, sous la supervision de sa chaîne de commandement ou de sa direction. Sont notamment visées ici les informations dont la divulgation est susceptible de mettre en péril la sécurité d'un individu ou d'un groupe d'individus, de violer les droits des intéressés ou de porter atteinte à la vie privée. Il convient toutefois de noter qu'en matière de diffusion d'informations au sein des missions, en ce compris les produits issus du PKI, l'approche par défaut doit consister à autoriser le partage d'informations ; celles-ci ne devraient porter la mention « confidentiel » ou « strictement confidentiel » qu'à titre exceptionnel et uniquement si les critères énoncés dans la circulaire ST/SGB/2007/6 l'exigent.

11.2.2. Le (la) chef de mission ou les chefs des composantes peuvent, en concertation avec les bureaux du DPO au Siège et les États Membres qui fournissent des unités à la mission le cas échéant, définir des mesures supplémentaires pour leur permettre d'exécuter les tâches qui leur incombent concernant le cycle du PKI de la mission afin d'assurer la sécurité, la confidentialité et la traçabilité des informations, en s'appuyant pour ce faire sur une analyse des risques et des facteurs de vulnérabilité propres à la mission en matière de sécurité de l'information. Au nombre de ces mesures peuvent notamment figurer, sans que cette liste soit limitative, le recours à des systèmes fermés dédiés à la gestion des informations ainsi qu'aux dispositifs de sécurité physique nécessaires pour protéger lesdits systèmes (contrôles d'accès, mesures de protection des câbles, ordinateurs et serveurs, par exemple), l'utilisation d'outils de communication cryptés, le paramétrage individualisé du matériel informatique visant à empêcher la duplication ou le transfert non autorisé d'informations, l'agencement des bureaux en espaces compartimentés équipés de dispositifs de contrôle d'accès, et l'obligation pour l'ensemble du personnel technique participant à la maintenance des outils technologiques auxquels fait appel le PKI de suivre une formation.

11.2.3. Les mesures supplémentaires relatives à la sécurité des informations qui seront éventuellement déployées devront être dûment documentées et s'appuyer sur les orientations, le savoir-faire, les moyens et la formation nécessaires à leur mise en œuvre efficace ; il faudra notamment prévoir une définition claire des fonctions et attributions, fixer des règles faisant expressément état de la gravité d'un partage non autorisé d'informations issues du PKI dans le cadre de la déontologie et de la discipline propres aux missions de maintien de la paix et instaurer un régime prévoyant que tout comportement fautif engage la responsabilité de son auteur.

11.3. Traitement, partage et utilisation d'informations tirées du PKI Les informations provenant du PKI doivent être traitées, conservées et partagées conformément aux règles, règlements, politiques et procédures de l'Organisation des Nations Unies, ainsi qu'aux orientations y afférentes, et utilisées exclusivement dans les conditions indiquées dans le présent document. S'agissant des unités en tenue attachées au système de PKI de la mission (les unités de renseignement, de surveillance et de reconnaissance, par exemple), toutes les informations qu'elles-mêmes et leurs

NON CLASSIFIÉ

contingents pourraient acquérir devront être traitées en conséquence. Le cas échéant, l'Organisation des Nations Unies conclura avec les fournisseurs de contingents ou de personnel de police des accords précisant les procédures à suivre pour le traitement des données recueillies par des capteurs afin de respecter ce principe. Ces procédures devront être d'un niveau au moins équivalent et conformes à celles prescrites dans les orientations et instructions permanentes pertinentes de l'ONU. De même, tous les outils d'acquisition de données que l'Organisation se sera procurée aux termes de contrats passés avec des fournisseurs devront être couverts par des dispositions indiquant clairement que les données ainsi recueillies seront la propriété exclusive de l'ONU et fixant les conditions dans lesquelles ces données pourront être stockées, gérées et partagées. Les normes par lesquelles ces accords seront régis devront figurer dans les instructions permanentes y relatives.

11.3.2. La diffusion de produits confidentiels issus du PKI au sein des missions de maintien de la paix devra reposer sur 1) les concepts de « besoin d'en connaître/besoin de partager » afin de limiter autant que faire se peut le risque de divulgation non autorisée, et 2) une évaluation des risques associés à la divulgation de ces produits. La question de la gestion de l'accès aux informations et de leur diffusion est abordée dans les instructions permanentes du DPO et du DOS relatives à l'accès aux informations, qui doivent être appliquées dans le cadre de la mise en œuvre des processus de diffusion du PKI. Nonobstant ce qui précède, toute information provenant du cycle du PKI qui pourrait avoir une incidence sur la sûreté et la sécurité du personnel des Nations Unies (tant le personnel de la mission que celui d'autres entités opérant dans la zone de cette dernière) devra être communiquée en temps utile au plus haut représentant du DSS présent (ou à son représentant désigné).

11.3.3. Afin de garantir la sécurité de la conservation et du traitement des informations tirées du PKI, les missions devront mettre en place deux mécanismes : 1) un registre dans lequel sont enregistrées de manière systématique la réception et la diffusion de produits du PKI classifiés et 2) une matrice de contrôle d'accès permettant d'enregistrer les documents confidentiels relatifs au PKI que devraient pouvoir examiner les organes de supervision, et d'en guider la diffusion.

11.4 Partage d'informations issues du PKI avec des entités extérieures aux missions et à l'ONU

11.4.1. La décision de partager des informations issues du PKI avec des entités des Nations Unies ne faisant pas partie de la mission (par exemple, des membres de l'équipe de pays des Nations Unies) ou des entités ne faisant pas partie de l'ONU (l'État hôte, par exemple) est du ressort du (de la) chef de mission, en sa qualité de fonctionnaire habilité(e) par le (la) Secrétaire général(e), en consultation, le cas échéant, avec le Siège de l'Organisation. Si le (la) chef de mission choisit de déléguer plus largement le pouvoir de décision en la matière au personnel agissant sous sa responsabilité, cette délégation devra être documentée et assortie d'orientations relatives aux principes et paramètres du partage d'informations tirées du PKI avec les partenaires.

11.4.2. Conformément à la politique des Nations Unies relative au cadre de responsabilités applicable au système de gestion de la sécurité des Nations Unies, les dispositions relatives au partage des informations tirées du PKI avec d'autres entités de l'Organisation doivent couvrir les cas où les informations concernent la sûreté et la sécurité du personnel, des locaux et des biens des Nations Unies ainsi que du personnel associé, et intéressent donc l'ensemble des organismes des Nations Unies opérant dans la zone de la mission. Ces informations devront être transmises au plus haut représentant du DSS [ou à son (sa) représentant désigné(e)] et au (à la) responsable

NON CLASSIFIÉ

désigné(e) de la sécurité. Les dispositions susmentionnées devront figurer dans le plan d'appui au PKI de la mission.

11.4.3. Les missions peuvent partager des informations issues du PKI avec des entités qui n'en font pas partie et sont extérieures au système des Nations Unies, telles que les forces de sécurité de l'État hôte ou les unités chargées d'opérations de sécurité parallèles, dans la mesure où leur mandat les y autorise et où cette pratique est conforme aux règles, règlements, politiques et procédures des Nations Unies en vigueur. Les informations partagées avec ces entités devront être assorties de dispositions écrites garantissant à ceux qui les ont transmises un contrôle sur leur utilisation ou leur application ultérieure. Tout partage d'informations tirées du PKI devra être enregistré au niveau central par des agents habilités à le faire et formés à cet effet ; il devra être motivé, justifié au regard du mandat et approuvé par le (la) chef de mission ou l'autorité déléguée. Les dispositions relatives au processus décisionnel et à la tenue de registres concernant le partage de ce type d'informations devront être précisées dans le plan d'appui au PKI de la mission.

11.4.4. Toutes les décisions concernant le partage de produits du PKI avec des entités extérieures à la mission doivent être conformes aux règles, règlements et politiques de l'Organisation des Nations Unies. Lorsque des informations tirées du PKI peuvent être partagées, directement ou indirectement, avec des forces de sécurité extérieures à l'Organisation, 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 doit s'appliquer. Cette politique met en place les mécanismes, structures et processus nécessaires pour en garantir le respect. Si des dispositions techniques prévoyant le partage permanent d'informations sensibles entre la mission et des forces de sécurité non onusiennes ont été prises, il pourra être procédé à une évaluation générale et préliminaire des risques qui devra toutefois être régulièrement réexaminée ; qui plus est, toute décision visant à partager des informations touchant au maintien de la paix devra être arrêtée au cas par cas. Si le partage de produits du PKI avec des tierces parties risque de poser problème au regard du mandat de la mission, de la Charte des Nations Unies, des règles et règlements de l'Organisation et de tout arrangement ou accord bilatéral conclu avec des parties non onusiennes, l'avis du conseiller juridique principal de la mission pourra être sollicité. Par ailleurs, il sera possible de consulter le Siège de l'Organisation des Nations Unies, notamment le Bureau des affaires juridiques.

11.5 Conservation et suppression des informations

11.5.1. Tous les produits du PKI sont réputés présenter un intérêt durable et devront être conservés à des fins d'alimentation de la mémoire institutionnelle. La planification, la conception des programmes, les listes de diffusion et les produits de renseignement liés aux opérations de maintien de la paix doivent être conservés et transférés chaque semestre aux archives des Nations Unies tout au long du cycle de vie de la mission et après sa clôture. La conservation et la suppression des informations devront s'effectuer conformément à la circulaire ST/SGB/2007/5 sur la gestion des dossiers et des archives de l'Organisation des Nations Unies, à la Politique du Département des opérations de maintien de la paix et du Département de l'appui aux missions sur la gestion des documents à valeur d'archives et au plan d'archivage des opérations de maintien de la paix.

12. Outils de gestion du cycle du renseignement dans les opérations de maintien de la paix

- 12.1. La présente section présente les principaux mécanismes auxquels il doit être fait appel pour la gestion du PKI dans les missions. Les besoins et capacités en matière de gestion du PKI étant très différents selon le contexte propre à chaque mission, les mécanismes, l'encadrement et les outils nécessaires à la mise en œuvre de la présente politique peuvent eux aussi varier. L'application de ces outils aux systèmes de renseignement des missions devra de ce fait être adaptée comme il se doit aux conditions propres à la mission.
- 12.2. Mécanisme de coordination du renseignement dans les missions de maintien de la paix – Outre les entités chargées de l'acquisition, de la compilation et de l'analyse des informations, les missions de maintien de la paix doivent se doter d'un mécanisme de coordination du renseignement dont le rôle consistera à diriger et superviser leur cycle du PKI. Participeront à ce mécanisme les entités constitutives de la mission chargées d'acquérir, de compiler, d'analyser et de diffuser les informations en vue d'atteindre les objectifs des activités de PKI menées au sein de la mission, à savoir les Centres 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 et de faciliter les discussions en cas de crise. D'autres sections de la mission, notamment la Division des affaires politiques, le Bureau du Conseiller juridique ou la Division des droits de l'homme, peuvent être invitées à participer au mécanisme de manière permanente ou ponctuelle et devront être consultées en tant que de besoin (voir l'annexe B).
- 12.3. La fonction du mécanisme est de rendre possible la centralisation du contrôle du système de renseignement dans les opérations de maintien de la paix de la mission et des orientations à définir en la matière, grâce à l'établissement de liens étroits entre les activités d'acquisition et d'analyse menées par toutes les entités participant à la mission et les besoins des hauts responsables de la mission, tout en instituant un système approprié de contrôle et de responsabilité dans les processus de gestion du PKI de la mission. Le mécanisme ne procède à aucune analyse et ne dispose pas, au demeurant, de capacités analytiques propres.
- 12.4. Les fonctions du mécanisme devront de préférence être coordonnées par le (la) chef d'état-major de la mission en sa qualité de président(e) du mécanisme, selon les dispositions énoncées au paragraphe 15.1. Dans certaines missions, les fonctions du mécanisme de coordination peuvent être assumées par le Centre d'analyse conjointe de la mission, conformément à la description qui en est donnée au paragraphe 27 a) de la Politique du Département des opérations de paix et du Département de l'appui aux missions relative aux cellules d'analyse conjointe des missions. Il peut parfois s'avérer nécessaire de créer une fonction indépendante.
- 12.5. Dans tous les cas, le mécanisme doit disposer de moyens spécifiques, fussent-ils ponctuels, aux fins de la coordination ; ces moyens **devront être distincts de ceux alloués à la mission pour la collecte et l'analyse d'informations**.
- 12.6. Les principales fonctions et responsabilités des membres du mécanisme de coordination du renseignement dans les missions de maintien de la paix sont énoncées ci-après.
- 12.6.1. Gestion des besoins de PKI – Grâce à ses liens directs avec les hauts responsables de la mission, le mécanisme de coordination du renseignement dans les missions de maintien de la paix s'enquiert de leurs besoins et traduit les décisions à prendre en la matière en une liste des besoins en renseignement, qui va influencer les besoins des différentes composantes de la mission.

NON CLASSIFIÉ

- 12.6.2. Planification et coordination des acquisitions – Sur la base des besoins en renseignement, le mécanisme charge le Centre d'analyse conjointe de la mission de mener à bien l'élaboration d'un Plan d'acquisition d'informations de la mission en collaboration avec les membres du mécanisme plus particulièrement concernés. Dans la mesure où il est chargé de valider ce plan, le mécanisme peut contrôler le processus et s'assurer que ses différents éléments concourent effectivement à l'acquisition et à l'analyse des informations afin de répondre à tous les besoins en la matière. Le plan permet en outre au mécanisme de faire en sorte que les moyens et les sources soient utilisés de manière efficace et que les acquisitions faisant double emploi servent uniquement à des fins de confirmation et de corroboration.
- 12.6.3. Attribution au Centre d'analyse conjointe de la mission d'une tâche consistant à encadrer l'établissement du plan d'appui au PKI de la mission, en collaboration avec les membres du mécanisme de coordination plus particulièrement concernés. Il appartiendra ensuite au mécanisme de valider le plan, en concertation avec les hauts responsables de la mission et en coordination avec le Siège de l'Organisation des Nations Unies, afin de définir les paramètres d'acquisition des informations et de déterminer les devoirs et responsabilités quant à l'orientation à donner au cycle du renseignement ainsi qu'à l'acquisition et au partage des informations tirées du renseignement dans les opérations de maintien de la paix.
- 12.6.4. Sensibilisation aux moyens d'acquisition et d'analyse des informations, aux priorités du moment, aux domaines d'intervention, aux avantages comparatifs et à la charge de travail des membres du mécanisme de coordination ou des entités participant à la mission.
- 12.6.5. Affectation, coordination et harmonisation, au sein du mécanisme, des activités visant à obtenir des informations à des fins de PKI.
- 12.6.6. Selon que de besoin, réalisation d'analyses conjointes faisant intervenir deux membres du mécanisme de coordination ou plus, et élaboration de produits de renseignement conjoints.
- 12.6.7. Définition d'orientations relatives à la coordination opérationnelle entre et parmi les membres du mécanisme, quant aux moyens permettant de faciliter le partage horizontal des informations à tous les niveaux et de formuler, le cas échéant, des instructions permanentes.
- 12.6.8. Définition d'orientations relatives aux niveaux appropriés de classification, aux procédures de partage des produits de renseignement et à l'application des politiques des Nations Unies en matière de gestion, de traitement et de classification des informations.
- 12.6.9. Établissement et tenue d'un registre central, d'une liste de diffusion et d'accès, ainsi que d'archives sur les données ou documents classifiés issus du PKI. Mise en place de plans d'archivage de tous les moyens d'acquisition des informations, en ce comprises la supervision du transfert de fichiers présentant un intérêt durable et la destruction de documents, le cas échéant.
- 12.6.10. Selon que de besoin, sollicitation de conseils auprès du conseiller juridique principal de la mission et, si nécessaire, de l'Équipe de coordination du renseignement dans les opérations de maintien de la paix du DPO et du Bureau des affaires juridiques du Siège de l'Organisation des Nations Unies, sur des questions liées aux activités de

NON CLASSIFIÉ

renseignement, notamment leur conformité au regard du cadre juridique régissant l'Organisation et la mission.

- 12.7. Plan d'acquisition d'informations de la mission – Le plan d'acquisition d'informations de la mission traduit en besoins en renseignement tangibles les orientations stratégiques données par les hauts responsables de la mission et les besoins exprimés par les personnes en charge de la planification opérationnelle ; il contient également la feuille de route à respecter pour répondre à ces besoins grâce au travail d'acquisition ciblée et d'analyse que mènent les entités participant à la mission. Le plan dresse la liste des différentes catégories de renseignement nécessaires, énumère les principaux acteurs de la mission appelés à intervenir pour que ces besoins soient satisfaits et fixe les principales échéances y afférentes. Il sert de base à l'élaboration, par les entités participant à la mission, de plans plus spécifiques (plan d'acquisition d'informations militaires ou policières, par exemple) qui intégreront les besoins en renseignement de leur principal client (voir l'annexe C). Ce document peut être classé « confidentiel » ou « strictement confidentiel » si le (la) président(e) du mécanisme de coordination du renseignement dans les missions de maintien de la paix, en concertation avec le (la) chef de mission, l'estime opportun.
- 12.8. Plan d'appui au renseignement dans les missions de maintien de la paix – Le plan d'appui décrit les limites dans lesquelles le cycle du renseignement devra être mis en œuvre et détermine les principaux facteurs qui devront être pris en considération lorsque des orientations seront données quant au cycle du renseignement ou que des tâches seront exécutées dans le cadre dudit cycle (voir l'annexe C pour un modèle de plan d'appui au renseignement dans les missions de maintien de la paix). Ce document peut être classifié si le (la) président(e) du mécanisme de coordination du renseignement dans les missions de maintien de la paix, en concertation avec le (la) chef de mission, l'estime opportun. Le plan d'appui devra être établi en étroite collaboration avec les bureaux du DPO au Siège et comporter les éléments ci-après, sans que cette liste soit limitative.
- 12.8.1. Les méthodes que pourront ou non utiliser les entités participant à la mission pour l'acquisition de données et d'informations portant spécifiquement sur les capacités qu'offrent les moyens mis à la disposition de la mission.
- 12.8.2. Les éléments spécifiques à prendre en compte lors de l'exécution d'activités d'acquisition d'informations (respect des normes internationales en matière de droits humains, notamment les droits de l'enfant, considérations relatives à la vie privée, normes et critères de justice pénale, lois et normes nationales et internationales et autres obligations découlant de la Charte des Nations Unies, etc.).
- 12.8.3. Les outils et mesures touchant à la gestion du renseignement, à la gestion de l'information et à la sécurité qui devront venir s'ajouter à ceux décrits dans les politiques des Nations Unies et du DPO et DOS (instructions relatives à l'utilisation d'un système d'information ou de communication sécurisé, aménagement d'espaces à accès sécurisé ou contrôlé, conseils en matière de conservation des données, etc.).
- 12.8.4. Les dispositions et paramètres qui concernent la mise en commun d'informations tirées du PKI avec des entités des Nations Unies ne faisant pas partie de la mission et des entités non onusiennes, telles que l'État hôte ou des forces armées. Il s'agit notamment de mesures visant à garantir, le cas échéant, l'application de la politique de diligence voulue en matière de droits de l'homme, à partager des informations pertinentes issues du PKI avec des entités des Nations Unies intégrées à l'équipe de coordination du dispositif de sécurité, et à donner toutes autres indications quant au partage

NON CLASSIFIÉ

d'informations de ce type avec des entités ne faisant pas partie de la mission, dès lors que ce pouvoir a été délégué par le (la) chef de mission.

12.9. Besoins en renseignement dans les opérations de maintien de la paix – Les besoins en renseignement sont liés à un manque total ou partiel de connaissances concernant un problème réel ou potentiel qu'il convient de régler pour faire en sorte que le mandat de la mission puisse être exécuté avec efficacité, de manière rationnelle ou en toute sécurité. Généralement exprimés sous forme de questions, ces besoins constituent la base du Plan d'acquisition d'informations d'une mission, lequel permet aux responsables de cette dernière, ainsi qu'aux membres du mécanisme de coordination, de s'assurer que le processus d'acquisition des informations a bien été lancé pour tous les besoins qui ont été formulés et que les ressources sont utilisées comme il se doit, efficacement et selon un ordre de priorité. Les besoins en renseignement et le Plan d'acquisition d'informations de la mission devront être réexaminés périodiquement, au moins une fois par an. Des tâches ponctuelles, n'entrant pas dans le cadre du plan, pourront également être prescrites en réponse à des besoins urgents.

12.10. Registre des documents classifiés et matrice de contrôle d'accès – Dans le droit fil de ce que prévoit le cycle du PKI décrit dans la section 10, toute réception et diffusion de produits de renseignement classifiés concernant les opérations de maintien de la paix devront être consignées dans un registre. Une matrice de contrôle d'accès devra être mise en place et constamment actualisée afin de servir de guide de référence pour la diffusion desdits produits.

13. Soutien, coordination, supervision et appui de la part des bureaux du DPO au Siège

13.1. Si le cycle du PKI s'occupe essentiellement de répondre aux besoins des opérations de maintien de la paix, les bureaux du DPO au Siège assument quant à eux un certain nombre de fonctions en matière de gestion du renseignement, qui sont présentées ci-après et seront précisées dans une directive connexe.

13.1.1. Planification stratégique – Les bureaux du DPO au Siège peuvent utiliser les produits issus du cycle du PKI pour éclairer les processus de planification stratégique et de prise de décision qu'il dirige au sein de la mission, ou auxquels il participe. L'utilisation qu'il fait du PKI doit être principalement dictée par la situation sur le terrain et avoir exclusivement pour but d'appuyer et de faciliter concrètement la planification, le déploiement de la stratégie et l'exécution des opérations dont est chargé le Siège de l'Organisation des Nations Unies et d'aider la mission à s'acquitter de son mandat. La coordination de ces activités doit être assurée par l'Équipe de coordination du renseignement dans les opérations de maintien de la paix du DPO.

13.1.2. Appui, soutien et supervision – Dans le cadre des fonctions d'orientation stratégique globale intégrée et de supervision qui incombent aux bureaux du DPO au Siège, les différents bureaux qui le composent sont chargés d'apporter un appui aux entités participant à la mission (le Centre des Nations Unies pour les opérations et la gestion des crises apportant ainsi son concours au Centre d'analyse conjointe de la mission, le Bureau des affaires militaires aux U2 (entités spécialisées dans le renseignement militaire opérant au niveau des états-majors des forces), la Division de la police (Bureau de l'état de droit et des institutions chargées de la sécurité) aux composantes Police, le mécanisme régional unique (DPPA/DPO) aux responsables de la mission, le Bureau des affaires juridiques au conseiller juridique principal, etc.). Ce sont eux aussi qui seront les principaux points de contact au Siège de l'Organisation des Nations Unies pour la formulation d'orientations techniques et stratégiques, l'élaboration de lignes directrices connexes ainsi que de modèles de stratégies et de produits, la détermination des besoins en solutions technologiques à l'échelle de l'entité et le pilotage du

développement de ces outils, avec le soutien technique du Service des technologies de l'information et des communications du DOS. Au Siège de l'ONU, la coordination des activités de soutien, d'appui et de supervision sera assurée par l'Équipe de coordination du renseignement dans les opérations de maintien de la paix du DPO ; cette même Équipe apportera également son concours pour ce qui concerne le Cadre général relatif au renseignement dans les opérations de maintien de la paix.

- 13.1.3. Réception de produits de renseignement provenant des États Membres – L'Équipe de coordination du renseignement dans les opérations de maintien de la paix est le principal point de contact aux bureaux du DPO au Siège pour la réception des produits de renseignement fournis par les États Membres de manière volontaire. Il tient un registre central des produits ainsi réceptionnés ainsi qu'une liste de diffusion et d'accès. Les produits communiqués aux bureaux du DPO au Siège par les États Membres ou d'autres entités sont systématiquement transmis par l'Équipe précitée à la ou aux missions concernées, conformément aux normes de traitement et de classification des informations en vigueur.

D. FONCTIONS ET ATTRIBUTIONS

14. Chef de mission/Représentant(e) spécial(e) du (de la) Secrétaire général(e)

- 14.1. Le (la) chef de mission est le principal client du cycle de renseignement dans les opérations de maintien de la paix ; il (elle) est aussi le plus important usager du mécanisme de coordination du renseignement dans les missions de maintien de la paix. Son rôle consiste à donner au mécanisme de coordination des orientations stratégiques susceptibles d'être traduites en besoins en renseignement qui serviront à piloter le cycle du PKI.
- 14.2. Le (la) chef de mission assume la responsabilité des décisions relatives au partage des données, informations et produits issus du PKI, que ce soit au sein de la mission ou avec les entités extérieures, conformément au cadre juridique de l'ONU, notamment la Charte des Nations Unies, le mandat de la mission, les règles et règlements de l'Organisation, la politique de diligence voulue en matière de droits humains et les accords conclus avec des tiers, et ce en concertation avec le conseiller juridique principal de la mission et, le cas échéant, l'Équipe de coordination du renseignement du DPO ainsi que le Bureau des affaires juridiques au Siège de l'ONU.
- 14.3. Le (la) chef de mission rend compte en dernier ressort au (à la) Secrétaire général(e), par l'intermédiaire du (de la) Secrétaire général(e) adjoint(e) aux opérations de paix, de l'exécution du cycle du PKI, conformément aux paramètres décrits dans la présente politique, aux orientations pertinentes de l'ONU et du DPO, ainsi qu'au plan d'appui au PKI de la mission.

15. Présidence du mécanisme de coordination du renseignement dans les missions de maintien de la paix

- 15.1. Le (la) chef de mission nomme à la présidence du mécanisme de coordination du renseignement dans les missions de maintien de la paix une personnalité civile – de préférence le (la) chef d'état-major de la mission –, qui sera le principal intermédiaire chargé de faire le lien entre les processus décisionnels des hauts responsables et le cycle du PKI de la mission. Si, conformément au paragraphe 12.4, la fonction du mécanisme de coordination est assurée par le Centre d'analyse conjointe de la mission, c'est le (la) chef de celui-ci qui en sera nommé(e) président(e). Il (elle) rendra compte au (à la) Représentant(e) spécial(e) du (de la) Secrétaire général(e). Le (la) président(e), secondé(e) par un personnel formé à cet effet qui assurera le

NON CLASSIFIÉ

secrétariat du mécanisme de coordination, rendra compte au (à la) chef de mission et sera chargé(e) des tâches ci-après.

- 15.1.1. Organiser les réunions du mécanisme de coordination du renseignement dans les missions de maintien de la paix, diriger ses activités et veiller à l'exécution de toutes les fonctions décrites à la section 12.6.
- 15.1.2. Superviser la conformité des opérations au regard de la présente politique, des orientations pertinentes de l'ONU et du DPO, ainsi que du plan d'appui au PKI de la mission.
- 15.1.3. Se tenir en permanence au fait de tous les moyens d'acquisition et d'analyse dont dispose la mission, notamment de leurs capacités, domaines d'intervention, avantages comparatifs et charges de travail.
- 15.1.4. Jouer le rôle de principal interlocuteur au niveau opérationnel entre la mission et le Siège de l'ONU pour ce qui est de la gestion et du partage des produits du PKI, sous l'autorité du (de la) chef de mission.

16. Entités participant à la mission

- 16.1. Le mécanisme de coordination du renseignement dans les missions de maintien de la paix est composé des entités participant à la mission visée qui sont chargées, dans le cadre du cycle du PKI y afférent, de l'acquisition, de la compilation et de l'analyse des informations ainsi que de la diffusion des produits de renseignement (voir l'annexe B). Les fonctions assignées à ces entités sont énumérées ci-après.
 - 16.1.1. Recenser les besoins en renseignement permanents et ponctuels des principaux responsables des missions (le (la) commandant(e) de la force pour l'U2 ou le (la) chef de la police civile pour la composante Police).
 - 16.1.2. Traduire le plan d'acquisition d'informations de la mission et les besoins en renseignement des principaux clients en plans d'acquisition pour leurs composantes respectives (plan d'acquisition d'informations militaires ou plan d'acquisition d'informations policières, par exemple).
 - 16.1.3. S'assurer du respect de la présente politique, des orientations opérationnelles pertinentes ainsi que du plan d'appui au renseignement de la mission.
 - 16.1.4. Attribuer les activités des moyens d'acquisition de la composante, les coordonner et désamorcer les situations conflictuelles en la matière.
 - 16.1.5. Tenir à jour, individuellement ou en coordination avec d'autres composantes, une base de données contenant les informations tirées du renseignement qui ont été enregistrées et compilées grâce aux moyens d'acquisition de la composante, assurer la sécurité de ces outils et organiser le contrôle de leur accès.
-

E. DÉFINITIONS

17. Cadre du renseignement dans les opérations de maintien de la paix – Orientations normatives et opérationnelles régissant collectivement les activités de PKI. Ce cadre comprend la présente politique ainsi que les orientations connexes fixées par le Siège de l'Organisation et la mission afin de la concrétiser.
18. Cycle du renseignement dans les opérations de maintien de la paix – Processus suivi pour déterminer les besoins en renseignement et y répondre, afin de pouvoir étayer les décisions incombant aux hauts responsables de la mission.
19. Données – Éléments factuels ou informations ponctuelles sous leur forme la plus atomisée, indépendamment du format ou de la structure du fichier.
20. Entité extérieure à la mission – Tout intervenant ne faisant pas partie de la structure de la mission. Il peut s'agir de membres de l'équipe de pays des Nations Unies, d'États Membres, d'organisations de la société civile, etc. Aux fins de la présente politique, le DSS est considéré comme une entité de la mission en raison de la responsabilité qu'il a, le cas échéant, de superviser la sécurité d'une mission.
21. Entité participant à la mission – Élément de la mission exerçant des activités dans le cadre du cycle du PKI. Ces entités font généralement partie du mécanisme de coordination du renseignement dans les missions de maintien de la paix. D'autres entités, qui peuvent ou non être attachées à une mission, ne sont pas concernées par le cycle du PKI. Des passerelles ont toutefois été prévues dans la présente politique, pour faire en sorte que le signalement de menaces, l'analyse de tendances et le partage d'informations puissent alimenter le cycle du PKI.
22. Information – Toute connaissance susceptible d'être communiquée ou tout document, indépendamment de son format ou de ses caractéristiques physiques, qui appartient à l'Organisation des Nations Unies, est produit par ou pour elle ou est sous son contrôle. On entend par « contrôle » le pouvoir qu'a le service, le bureau ou la mission à l'origine de l'information, ou son successeur dans la fonction, d'en réglementer l'accès.
23. Moyen d'acquisition – Toute ressource chargée, par une entité participant à la mission ou lui apportant son appui, de recueillir, dans le cadre d'un plan d'acquisition d'informations, les données ou informations nécessaires pour répondre aux besoins en matière de PKI. Il peut s'agir de systèmes faisant appel à des moyens technologiques tels que des capteurs aériens, de capacités associées à des compétences spécifiques telles que l'analyse médico-légale, ou d'une source humaine.
24. Produit du PKI – Résultat de la phase d'analyse du cycle du PKI, qui permet de traiter les informations et d'en tirer des conclusions. Ces produits peuvent se présenter sous diverses formes, telles que des évaluations écrites, des présentations orales et visuelles, des analyses de données, voire des comptes rendus informels présentés oralement. Les produits de renseignement à caractère confidentiel sont diffusés aux clients du cycle du PKI selon les principes du « besoin d'en connaître et besoin de partager ».
25. Protection du PKI – Ensemble des efforts visant à définir et mettre en œuvre des mesures destinées à protéger le PKI contre les risques menaçant l'efficacité, la continuité, la confidentialité et la sécurité opérationnelle du cycle du PKI et des informations qu'il génère.
26. Système de renseignement dans les opérations de maintien de la paix de la mission – Structures, outils et activités qui permettent, en se conjuguant, de mener à bien le cycle du PKI au sein de la mission. Il s'agit notamment des mécanismes de coordination chargés de piloter le cycle, des entités participant à la mission et de leurs moyens d'acquisition respectifs, des politiques et plans régissant

les activités de PKI, ainsi que de l'infrastructure en charge de la gestion de l'information et des communications qui traite les données et informations dans le cadre dudit cycle.

F. RÉFÉRENCES

Références relatives à l'Assemblée générale et au Conseil de sécurité

Rapport du Comité spécial des opérations de maintien de la paix sur les travaux de sa session de fond de 2018 (A/72/19)

Rapport du Comité spécial des opérations de maintien de la paix sur les travaux de sa session de fond de 2017 (A/71/19)

Rapport du Comité spécial des opérations de maintien de la paix sur les travaux de sa session de fond de 2016 (A/70/19)

Résolution 2295 (2016) du Conseil de sécurité

Résolution 1894 (2009) du Conseil de sécurité

Références normatives

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 (A/67/775–S/2013/110)

Circulaire du Secrétaire général ST/SGB/2007/6 – Informations sensibles ou confidentielles : classification et maniement (2007)

Circulaire du Secrétaire général ST/SGB/2007/5 – Gestion des dossiers et des archives de l'Organisation des Nations Unies (2007)

Circulaire du Secrétaire général ST/SGB/2004/15 sur l'utilisation des moyens et des données informatiques et télématiques (2004)

Politique du Département des opérations de maintien de la paix et du Département de l'appui aux missions sur la gestion des documents à valeur d'archives (2016.19)

Instructions permanentes du Département des opérations de maintien de la paix et du Département de l'appui aux missions sur le marquage, l'archivage et le nettoyage des informations (2016.20)

DPKO/DFS on Access and Declassification of Archives and Non-current Records (SOP 2006.3) (2^e modification)

Politiques connexes

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 (2015)

Politique et manuel relatifs aux cellules d'analyse conjointe des missions (2015/2018)

Politique et lignes directrices du Département des opérations de paix relatives aux centres d'opérations conjoints (2019)

NON CLASSIFIÉ

Instruction permanente sur l'établissement de rapports intégrés des missions sur le terrain dirigées par le DOMP, destinés au Siège de l'Organisation des Nations Unies (2012)

Standard Operating Procedure on Access to Information (2010)

Directive politique sur l'utilisation des techniques de détection et de surveillance par les missions extérieures et Procédures opérationnelles permanentes sur l'utilisation des techniques de contrôle et de surveillance dans les missions (2010)

Information Sensitivity Toolkit (2010)

Autorité, commandement et contrôle dans les opérations de maintien de la paix des Nations Unies (2008)

G. SUIVI DE L'APPLICATION

27. Le (la) chef de mission est tenue(e) de veiller à ce que celle-ci respecte la présente politique et mettre en place des mécanismes ou procédures efficaces permettant de s'en assurer. 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 cette politique.
-

H. SERVICE À CONTACTER

28. Équipe de coordination du renseignement dans les opérations de maintien de la paix, Bureau du (de la) Secrétaire général(e) adjoint(e), DPO
-

I. HISTORIQUE

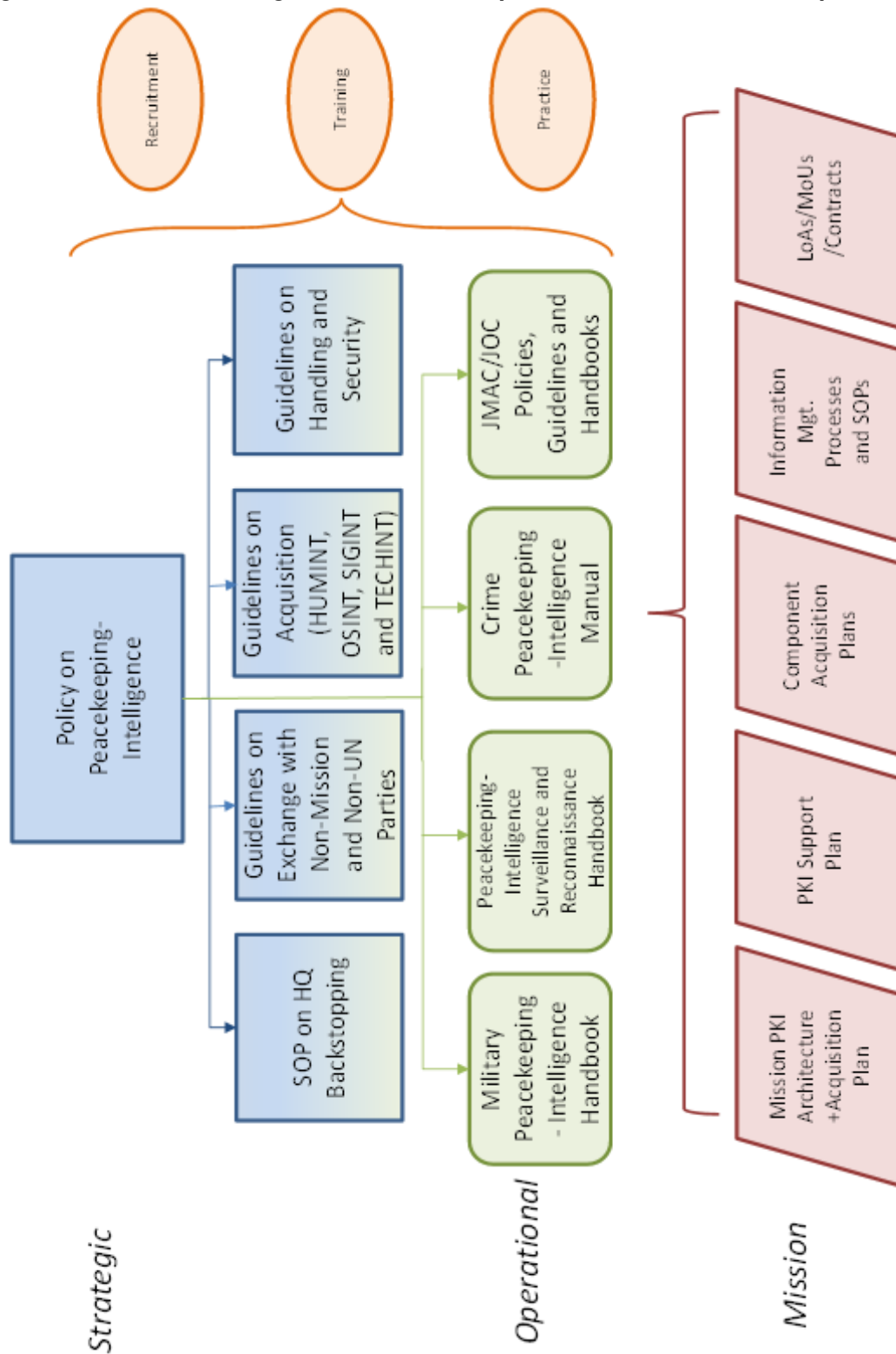
29. Le présent texte constitue la deuxième version de cette politique.
-

SIGNATURE :

DATE D'APPROBATION :

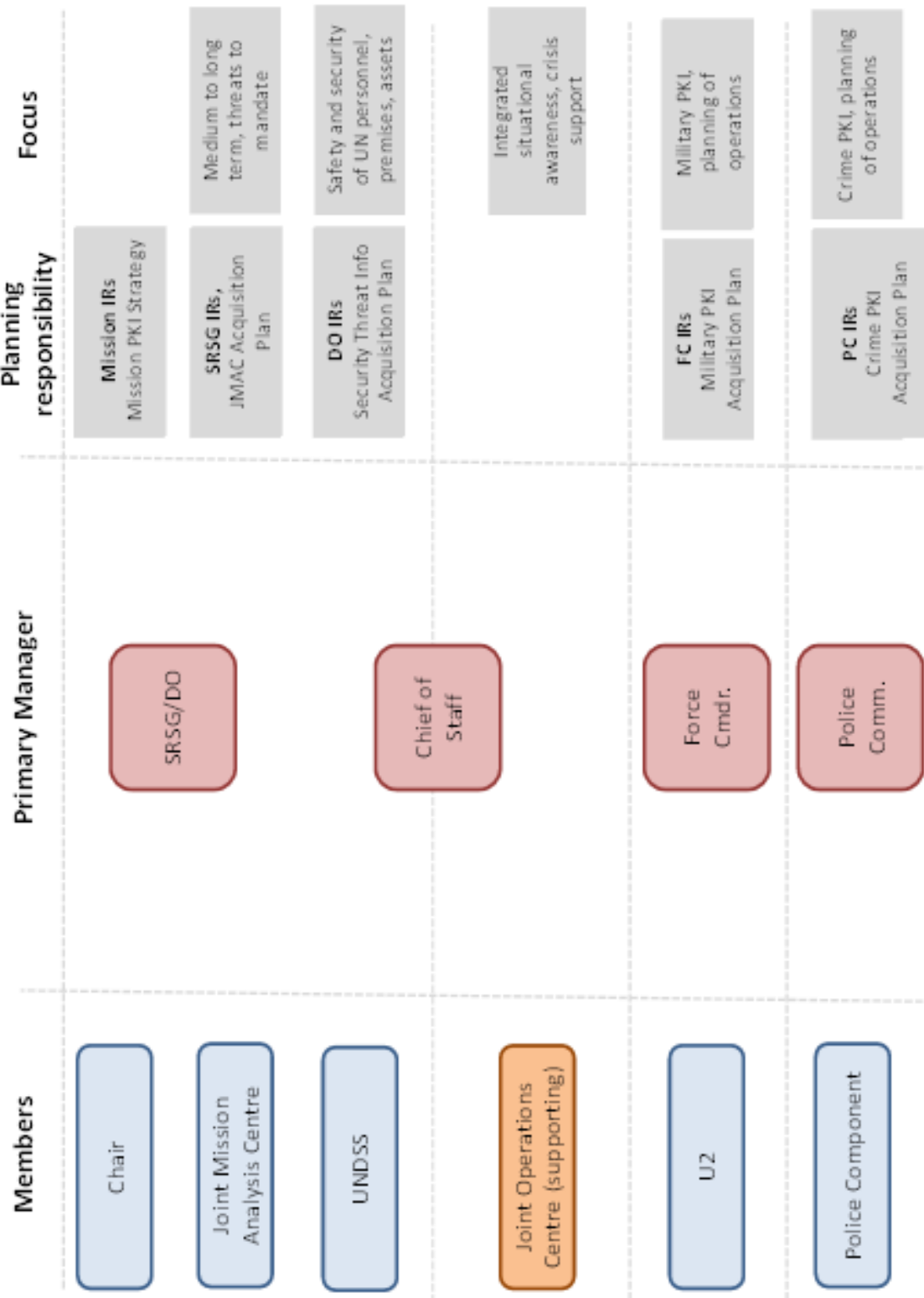
ANNEXE A

Cadre général relatif au renseignement dans les opérations de maintien de la paix



ANNEXE B

Principaux membres du mécanisme de coordination du renseignement dans les missions de maintien de la paix



ANNEXE C

Modèle de plan d'appui au renseignement dans les missions de maintien de la paix

Contexte

1. Le contexte permet de préciser les circonstances qui ont conduit à l'élaboration du plan d'appui au renseignement dans les missions de maintien de la paix et donne un certain nombre d'informations essentielles sur le concept des opérations auquel il apporte son concours. Le plus souvent, il n'excède pas un ou deux paragraphes.

Objectif

2. Le plan d'appui a pour but de décrire le système de PKI mis en place pour épauler la mission et de définir les fonctions qui peuvent être affectées à la mission ou lui prêter main-forte en termes de moyens stratégiques, opérationnels et tactiques de renseignement.

MISSION

3. Il s'agit ici d'exposer les objectifs du système de PKI de la mission tels qu'ils découlent du mandat de cette dernière, du concept des opérations et d'autres documents de planification.

EXÉCUTION

Domaine d'intérêt du PKI

4. Précise le domaine auquel s'intéresse le PKI.

Concept de l'appui au PKI

5. Énumère les faits et hypothèses essentiels sur lesquels repose le plan.

6. Fournit toutes autres informations pertinentes selon que de besoin.

Mécanisme du système de PKI

7. Précise le mécanisme et les fonctions d'appui au PKI sur le plan tactique, opérationnel et stratégique.

8. Indique la structure et la composition du mécanisme de coordination du renseignement dans les missions de maintien de la paix.

9. Présente un diagramme linéaire situant les différentes composantes du système de PKI, ainsi que leurs liens avec la hiérarchie et le commandement.

Fonctions et attributions du PKI

10. Donne des informations sur les fonctions et attributions des acteurs ci-après :

- a) mécanisme de coordination du PKI ;
- b) entités participant à la mission présentes au Siège (membres du mécanisme de coordination) ;
- c) états-majors de secteur, chefs de bureau et autres responsables de haut rang ;
- d) personnel participant au cycle du PKI.

Gestion des besoins et des acquisitions

11. Explique les processus de gestion des besoins et des acquisitions.

12. Précise les méthodes qui seront utilisées dans le cadre de la procédure d'acquisition d'informations, ainsi que celles jugées totalement inacceptables pour les composantes de la mission.

13. Indique les facteurs dont devra tenir compte le personnel des missions dans la gestion des moyens d'acquisition et dans la prise de décisions concernant les activités y relatives.

14. La structure à respecter pour la demande d'information/de PKI est présentée dans une annexe.

Production et diffusion du PKI

15. Dresse la liste des postes ayant pour fonction de générer et diffuser des produits par différents canaux, en précisant notamment les autorités responsables de leur diffusion au sein et en dehors de la mission.

16. Précise les médias et les technologies de l'information auxquels il sera recouru, ainsi que les systèmes de gestion et de communication utilisés pour diffuser les produits du PKI.

Commandement et contrôle du PKI

17. Répertorie les mesures de contrôle technique et les dispositifs de liaison.

Appendices (Ne figurent pas dans ce modèle ; il s'agit uniquement d'un exemple de ce qu'elles devraient comporter.)

- 1. Structure de la demande d'information/de PKI
- 2. Plan relatif aux informations et services géospatiaux
- 3. Autres éléments, selon que de besoin