

NON CLASSIFIÉ



Nations Unies
Département des opérations de paix
Réf. 2022.03

Lignes directrices

Renseignement d'origine sources ouvertes dans les opérations de maintien de la paix

Document approuvé par : Jean-Pierre Lacroix,
Secrétaire général adjoint
aux opérations de paix

Date d'entrée en vigueur : *1^{er} mars 2022*

Service à contacter : *DPO/OUSG/PICT*

Date de révision : *1^{er} mars 2026*
(ou selon les besoins)

LIGNES DIRECTRICES DU DÉPARTEMENT DES OPÉRATIONS DE PAIX RELATIVES AU RENSEIGNEMENT D'ORIGINE SOURCES OUVERTES DANS LES OPÉRATIONS DE MAINTIEN DE LA PAIX

Table des matières :	A. Objet
	B. Champ d'application
	C. Contexte
	D. Lignes directrices
	E. Fonctions et attributions
	F. Définitions
	G. Références
	H. Service à contacter
	I. Historique

ANNEXES

A. Ressources et outils

A. OBJET

1. Les présentes lignes directrices ont pour objet d'encadrer et de faciliter l'acquisition sûre et efficace d'informations d'origine sources ouvertes à des fins de renseignement dans les opérations de maintien de la paix (ROSO, ci-après « renseignement de sources ouvertes »). Elles s'inscrivent dans le cadre relatif au renseignement dans les opérations de maintien de la paix et doivent être lues conjointement avec la politique du Département des opérations de paix (DPO) relative au renseignement dans les opérations de maintien de la paix¹ (ci-après « la Politique »). Ni ces lignes directrices ni la Politique ne sont des supports de formation.
-

B. CHAMP D'APPLICATION

2. Le présent document d'orientation s'applique à tous les membres en activité des opérations de maintien de la paix des Nations Unies affectés à l'appui à l'acquisition d'informations de sources ouvertes à des fins de renseignement dans les opérations de maintien de la paix. Les présentes lignes directrices revêtent un caractère obligatoire².
 - 2.1. Les principes qui régissent les activités de renseignement dans les opérations de maintien de la paix doivent être respectés à la lettre. Ces principes sont les suivants :

¹ Politique relative au renseignement dans les opérations de maintien de la paix (*Policy on peacekeeping-intelligence*, 2019.08)

² Ces orientations ne s'appliquent qu'aux données, informations et produits recueillis et analysés dans le cadre du cycle du renseignement dans les opérations de maintien de la paix. Les pratiques courantes de gestion, de communication et de diffusion de l'information qui ne sont pas liées au renseignement dans les opérations de maintien de la paix demeurent encadrées par les orientations applicables en vigueur.

- 2.2. **Respect des règles** : toute activité de renseignement dans les opérations de maintien de la paix doit être menée conformément aux mandats définis par le Conseil de sécurité, dans le plein respect de la Charte des Nations Unies. Ces activités doivent s'inscrire dans le cadre juridique général qui régit les opérations de maintien de la paix des Nations Unies, notamment les principes fondamentaux du maintien de la paix et toutes les normes et obligations en matière de droit et de droits humains. Les activités de renseignement dans les opérations de maintien de la paix doivent être menées dans le respect strict des droits humains, y compris, en particulier, le droit à la vie privée et la liberté d'expression, de réunion pacifique et d'association, en veillant tout particulièrement à ne pas exposer les sources d'information actuelles ou futures à un quelconque préjudice.
- 2.3. **Non-clandestinité** : les activités clandestines, définies comme l'acquisition d'informations ou de produits de renseignement effectuée dans le secret ou dans le but de dissimuler des activités illicites ou incompatibles avec le cadre juridique, les principes, les politiques et les mandats des opérations de maintien de la paix des Nations Unies, sortent du cadre des activités de renseignement dans les opérations de maintien de la paix et doivent être exclues par les entités de la mission. L'application de ce principe sera renforcée par des formations et séances d'information régulières, notamment la formation normalisée préalable au déploiement de tous les membres du personnel menant des activités de renseignement dans les opérations de maintien de la paix, et par l'audit et le contrôle réguliers du processus d'exécution des tâches liées au renseignement dans ces opérations.
- 2.4. **Domaines d'application** : l'acquisition et la gestion des informations ou du renseignement par les opérations de maintien de la paix des Nations Unies doivent être menées en vue d'améliorer la perception de la situation et la sûreté et la sécurité du personnel des Nations Unies, et afin d'éclairer les opérations et les activités liées aux missions de protection des civils prévues dans le cadre des mandats confiés par le Conseil de sécurité.
- 2.5. **Respect de la souveraineté des États** : la souveraineté des États, en particulier des États hôtes et des États voisins, doit être respectée.
- 2.6. **Indépendance** : les activités de renseignement dans les opérations de maintien de la paix doivent être entièrement autonomes et indépendantes à tous égards de tout système de renseignement national ou autre opération menée à ce niveau, et conserveront leur caractère exclusivement international. Les missions peuvent se mettre en rapport avec des entités extérieures à la mission afin d'obtenir des produits de renseignement et peuvent à leur tour transmettre certains produits de renseignement liés au maintien de la paix à ces dernières, y compris à des États hôtes, sous réserve de le faire dans les conditions et les limites décrites dans le présent document et les orientations connexes.
- 2.7. **Responsabilité, capacités et prérogatives** : les personnes habilitées à prendre des décisions concernant les activités de renseignement dans les opérations de maintien de la paix doivent disposer de capacités adaptées à l'exercice de ces fonctions et demeurent responsables de l'exécution effective de ces tâches au sein de leurs chaînes de commandement respectives, devant le (la) Chef de la mission et, en dernier ressort, devant le (la) Secrétaire général(e). Au sein de la mission, le (la) Chef de la mission doit répondre du fonctionnement du système de renseignement dans les opérations de maintien de la paix. Il lui incombe, au

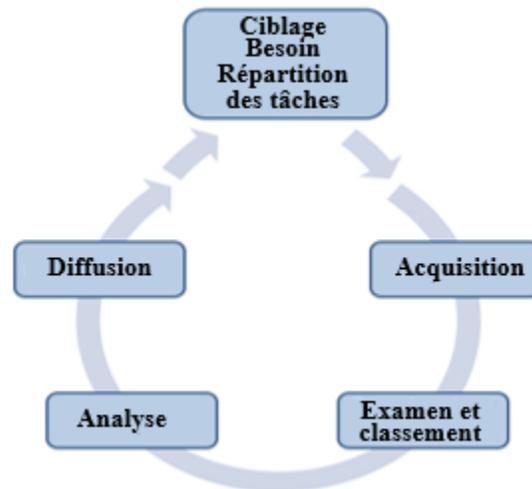
moyen de procédures de gouvernance, de formations et de pratiques efficaces, de veiller au respect des présentes lignes directrices et des orientations connexes par le personnel qui est en contact avec les produits de renseignement et qui les utilise.

- 2.8. **Sécurité et confidentialité** : le renseignement dans les opérations de maintien de la paix doit être stocké et partagé de manière sécurisée, tout en en garantissant l'accès aux personnes qui en ont besoin aux fins de prise de décisions et de planification des opérations. Après avoir estimé les risques, les missions doivent mettre en place des outils en matière de procédure, de technologie et de sécurité physique, en concertation avec le Département des opérations de paix et le Département de l'appui opérationnel (DOS), afin de garantir la sécurité de la gestion de l'information et des communications au sein du système de renseignement. Les produits de renseignement confidentiels doivent être partagés et diffusés sur la base des notions du « besoin d'en connaître » et du « besoin de partager », au titre desquelles le renseignement dans les opérations de maintien de la paix 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. Cette divulgation nécessite également une délégation de pouvoir écrite de la part de l'auteur(trice) du rapport ou du membre du personnel ayant décidé du niveau de classification. Le renseignement dans les opérations de maintien de la paix ne peut donc être partagé qu'avec des personnes de confiance, l'objectif étant de faire en sorte que sa diffusion reste limitée, en particulier lorsqu'il 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 vis-à-vis de tous leurs interlocuteurs en ce qui concerne leur capacité d'acquérir, de protéger et de gérer comme il se doit les produits de renseignement dans les opérations de maintien de la paix.

C. CONTEXTE

3. La Politique « expose les raisons pour lesquelles les opérations de maintien de la paix des Nations Unies acquièrent, classent, analysent, diffusent, utilisent, protègent et gèrent le renseignement dans les opérations de maintien de la paix et les moyens qui leur permettent d'y parvenir ». L'acquisition d'informations fait référence à la deuxième étape du cycle de renseignement dans les opérations de maintien de la paix (fig. 1).

Figure 1. Le cycle du renseignement dans les opérations de maintien de la paix



4. Dans la Politique, l'étape de l'acquisition est définie comme suit : « **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 matière de renseignement. Il s'agit notamment d'affecter les moyens en fonction des besoins en matière de 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** ».
5. Il est également énoncé dans la Politique que « les paramètres d'acquisition efficace, responsable et éthique de renseignement dans les opérations de maintien de la paix doivent être décrits dans le plan d'appui renseignement de la mission. Ce dernier, qui doit être conforme à la présente politique et aux autres politiques et orientations de l'ONU, doit également contenir une description des outils, techniques et procédures acceptables et inacceptables d'acquisition d'informations par la mission, des obligations juridiques applicables et des considérations à prendre en compte lors de l'acquisition de renseignement de cette nature, en fonction des moyens dont dispose la mission et conformément aux orientations opérationnelles subordonnées à la présente politique ».
6. Dans le cadre des opérations de maintien de la paix des Nations Unies, le renseignement de sources ouvertes est celui qui est issu de l'acquisition, du classement et de l'analyse d'informations accessibles au public en vue de répondre aux besoins en renseignement. Les informations accessibles au public, quelle que soit leur forme, sont l'ensemble des informations ou documents librement accessibles qui sont mis en ligne sur Internet (dont les médias sociaux), publiés, diffusés à la radio et à la télévision ou mis à la disposition du public. Il peut également s'agir d'informations accessibles au public par voie commerciale moyennant paiement. Lorsqu'ils paient pour des informations accessibles au public, les utilisateurs doivent s'assurer qu'ils respectent toutes les règles et réglementations de l'ONU, les principes encadrant la collecte de renseignement dans les opérations de maintien de la paix et les lignes directrices qui s'y rapportent.

7. L'acquisition d'informations de sources ouvertes est généralement divisée en trois catégories, selon la méthode de collecte employée.
 - 7.1. **Collecte non ciblée et informelle** : ce type de collecte consiste à obtenir des informations auprès de sources ouvertes, sans répondre à un besoin précis de renseignement. À titre d'exemple, on peut citer les informations obtenues grâce à un tour d'horizon prospectif général, en se contentant de lire le journal ou de faire défiler les mots-clés en « Tendances » sur Twitter. Cette acquisition est dite « passive ».
 - 7.2. **Collecte ciblée, mais non clandestine** : cette catégorie renvoie au même type de méthodes d'acquisition que le point 7.1., mais dans le cadre du cycle du renseignement dans les opérations de maintien de la paix. Autrement dit, les informations sont délibérément découvertes et acquises en réponse aux besoins de renseignement définis au niveau de la mission et seront traitées en suivant les étapes du cycle du renseignement dans les opérations de maintien de la paix. Ce mode d'acquisition nécessite l'emploi de méthodes de recherche particulières afin d'obtenir les informations recherchées et peut nécessiter de payer pour des informations accessibles par voie commerciale (voir le paragraphe 6). L'acquisition classée dans cette catégorie peut être aussi bien active que passive.
 - 7.3. **Collecte ciblée ou non ciblée et clandestine : cette méthode d'acquisition est strictement interdite par la Politique (voir paragraphe 2.3) et peut avoir des conséquences graves, tant pour le membre du personnel concerné (militaire, policier et civil) que pour le système des Nations Unies dans son ensemble. Si cette méthode est mentionnée ici, c'est dans le seul but d'énoncer ce qu'il ne faut pas faire.** Une acquisition de renseignements de sources ouvertes dans les opérations de maintien de la paix est dite « clandestine » lorsqu'elle est menée de façon à cacher la nature de l'opération. Les activités sont menées dans le secret avec une volonté de dissimulation, par exemple en se présentant sous une fausse identité ou en ne disant pas la vérité sur son emploi à l'Organisation des Nations Unies dans les interactions sur des plateformes comme les médias sociaux et les blogs, ainsi que dans les échanges visant à établir des relations avec des entités en ligne.
 8. Seule la variante ciblée (paragraphe 7.2) qui est menée dans le cadre du cycle de renseignement dans les opérations de maintien de la paix peut être considérée comme du renseignement de sources ouvertes dans les opérations de maintien de la paix. Les entités de la mission autres que les membres principaux du mécanisme de coordination du renseignement dans les missions de maintien de la paix², telle que décrites à l'annexe B de la Politique, peuvent également être amenées à utiliser des sources ouvertes en vue d'acquérir des informations, mais le font de manière non ciblée et informelle.
 9. Les entités principales du mécanisme de coordination du renseignement dans les missions de maintien de la paix qui utilisent des renseignements de sources ouvertes sont tenues de respecter les présentes lignes directrices.
 10. Directement inspirées des paramètres susmentionnés, les présentes lignes directrices ont été élaborées en vue de fournir des orientations aux opérations de maintien de la paix quant à la manière de procéder à l'acquisition de renseignements de sources ouvertes.
-

D. Lignes directrices

11. Règles générales et caractéristiques

11.1. **L'acquisition de produits de renseignement dans les opérations de maintien de la paix est essentiellement fondée sur des sources ouvertes et doit être la méthode de collecte d'informations privilégiée du fait de sa simplicité, du faible risque qu'elle représente, de son faible coût et de sa rapidité d'exécution. On envisagera d'autres sources lorsque le renseignement de sources ouvertes est jugé inadapté ou s'est avéré vain ou incomplet.** Les autres sources de renseignement dans les opérations de maintien de la paix conservent donc toute leur légitimité. Les produits de renseignement dans les opérations de maintien de la paix les plus fiables sont fondés sur des informations provenant de sources multiples, et le renseignement de sources ouvertes doit être validé, souvent au moyen d'autres méthodes d'acquisition.

11.2. Toutes les activités de renseignement de sources ouvertes dans les opérations de maintien de la paix seront menées dans le strict but d'améliorer la perception de la situation et la sécurité du personnel des Nations Unies, ainsi que d'éclairer les opérations et les activités liées aux missions de protection des civils énoncées des mandats du Conseil de sécurité.

11.3. Toutes les activités de renseignement de sources ouvertes dans les opérations de maintien de la paix seront menées conformément à la Charte des Nations Unies, aux principes fondamentaux du maintien de la paix, au droit international des droits humains, au droit international humanitaire, aux décisions pertinentes des organes intergouvernementaux de l'Organisation et aux autres cadres juridiques applicables.

11.4. Le renseignement de sources ouvertes peut être utilisé pour répondre à de nombreux types de besoins de renseignement au sein d'une opération de maintien de la paix. Exemples :

11.4.1. Le personnel chargé du renseignement qui surveille l'actualité peut utiliser les flux d'informations en direct et les médias sociaux pour suivre l'évolution des situations de crise.

11.4.2. Les informations culturelles relatives aux perceptions, aux sentiments, aux intentions et aux capacités des entités locales peuvent éclairer les visites ou les opérations sur le terrain.

11.4.3. Les données encyclopédiques peuvent alimenter le renseignement, permettant à la mission d'acquérir une compréhension de base essentielle de l'environnement opérationnel complexe.

11.4.4. Le renseignement de sources ouvertes peut fournir des données permettant d'analyser la manière dont les acteurs locaux réagissent aux activités de la mission dans certaines zones.

11.4.5. Dans le cadre du renseignement géospatial, le renseignement de sources ouvertes peut donner accès à d'énormes quantités d'images, de sons et de vidéos souvent géolocalisés.

11.5. Le renseignement de sources ouvertes est un terme générique qui recouvre un large éventail de sources possibles et pas uniquement les informations provenant de sources en ligne.

11.5.1. Enceintes de prise de parole en public. Événements ouverts au public, où ni l'orateur(trice) ni le (la) participant(e) ne s'attendent au respect des règles de confidentialité. À titre d'exemple, citons les manifestations politiques, les sermons religieux, les débats universitaires, les conférences pédagogiques, les conférences de presse et les expositions.

11.5.2. Documents publics. Les documents publics sont notamment les livres, les journaux, les brochures, les affiches, les revues professionnelles, les cartes, les manuels, les photographies et les registres de biens publics. Leur suivi systématique peut, au fil du temps, permettre de dégager des tendances utiles.

11.5.3. Émissions publiques. Elles peuvent être suivies sur Internet, à la radio et à la télévision. Elles constituent une source d'informations actuelles sur la situation dans les sociétés. Les émissions animées par des médias et le commentaire journalistique entrent dans cette catégorie, qui englobe aussi la propagande et la publicité commerciale.

11.5.4. Internet.

11.5.4.1. Le **Web** n'est qu'un des nombreux services disponibles sur Internet. Il permet de consulter un ensemble de contenus reliés entre eux grâce à un code normalisé (HTML), et l'on y fait des recherches à l'aide de moteurs grand public. Pour autant, le Web n'est pas réglementé, ce qui signifie que n'importe qui peut y télécharger des informations. Trouver l'origine d'un site Web ou d'un article peut relever de la gageure, mais s'avère essentiel pour la vérification de l'information. Le renseignement de sources ouvertes peut fournir aux analystes les outils nécessaires à l'évaluation de la véracité des sources.

11.5.4.2. Le **deep Web** est la partie du Web qui n'est pas accessible via un moteur de recherche grand public mais qui est codé en HTML. Il regroupe notamment des sites Web privés qui nécessitent une inscription ou un mot de passe. Les sites Web de bibliothèques, de courrier électronique et de banques en sont quelques exemples. Les missions de maintien de la paix des Nations Unies peuvent utiliser le deep Web quand et où il existe un besoin légitime et une possibilité d'accès légal au contenu. **Le piratage de sites Web n'est pas autorisé dans le cadre du renseignement de sources ouvertes dans les opérations de maintien de la paix.**

11.5.4.3. Le **dark Web** est une partie du deep Web qui n'est pas accessible via un navigateur Internet classique et qui est utilisée pour préserver l'anonymat et la confidentialité des activités sur Internet. Les sites Web du dark Web se terminent en «.onion » au lieu d'une extension plus connue du Web visible comme «.com », «.gov » et «.org ». L'utilisation du dark Web pouvant présenter un danger à la fois pour le personnel qui y accède et pour l'Organisation :

11.5.4.3.1 tout accès au dark Web grâce à du matériel appartenant à l'ONU, aux fins du renseignement dans les opérations de maintien de la paix, doit avoir été autorisé au préalable par le Siège (Équipe de coordination du renseignement dans les opérations de maintien de la paix, Bureau de l'informatique et des communications).

11.5.4.3.2 Les membres du personnel des Nations Unies qui accèdent au dark Web grâce à leur matériel personnel doivent en assumer les risques et la responsabilité.

11.5.4.3.3 Une information obtenue sur le dark Web grâce à du matériel personnel ne peut être utilisée à des fins de renseignement dans les opérations de maintien de la paix.

11.5.4.3.4 Le Siège de l'ONU surveille le dark Web afin de détecter toute menace pesant sur les Nations Unies (y compris pour la sûreté et la sécurité des soldats de la paix) et toute information d'intérêt est communiquée sans délai à la mission de maintien de la paix concernée.

11.5.5. « Médias sociaux » est le terme général employé pour désigner les plateformes Internet où se déroulent les interactions entre personnes (pour la plupart) au sein de communautés virtuelles, telles que les réseaux sociaux et d'autres services de communication à distance. Ils permettent de mettre en ligne des blogs et des microblogs, de publier des messages sur les réseaux sociaux et professionnels et de participer au partage de vidéos (vlogs), de contenus audio (podcasts), de photos et de favoris.

11.5.5.1. Les médias sociaux sont souvent utilisés pour organiser des manifestations et diffuser rapidement des messages. Ce faisant, ils peuvent considérablement influencer la dynamique d'une société.

11.5.5.2. Outre les particuliers, les médias sociaux sont désormais largement utilisés par les organisations politiques, les

gouvernements, les entreprises commerciales et les groupes d'intérêt.

11.5.5.3. Avant d'exploiter des informations provenant des médias sociaux, il est primordial de ne pas perdre de vue que les comptes des médias sociaux sont la source d'informations informelles non contrôlées par excellence. Il est souvent difficile de savoir qui se cache vraiment derrière un compte (s'agit-il de personnes physiques ? De robots ? De trolls ? Des autorités ? D'une entité commerciale ? D'une autre entité ?) et l'objectif qu'ils ou elles poursuivent en publiant certaines informations, parfois montées de toutes pièces. La désinformation et la mésinformation sont très répandues et parfois difficiles à repérer.

11.5.6. La documentation grise fait référence aux documents non classifiés qui sont accessibles en respectant la légalité et l'éthique, mais qui ne sont pas contrôlés par des éditeurs commerciaux ou des organismes d'abonnement. Leur consultation nécessite de passer par des canaux spécialisés. Il peut s'agir de plans, d'ensembles de données, d'images commerciales, de documents de travail, de rapports techniques, d'annuaires universitaires, de thèses, etc.

11.6. Les médias constituent l'une des principales sources de renseignement de sources ouvertes dans les opérations de maintien de la paix. Ils prennent de nombreuses formes : journaux ; sites Web d'information ; télévision ; radio ; plateformes de médias sociaux. Il importe de prendre en compte le fait que de nombreux médias d'information sont engagés dans une compétition commerciale qui vise à capter l'attention du public. Afin de se distinguer, ils doivent donc proposer des sujets vendeurs et être réactifs. Cette priorité est un frein au traitement de fond qui limite la précision de l'information. De nombreux journalistes sont des généralistes couvrant un large éventail de sujets dont les reportages peuvent présenter des lacunes dans la compréhension d'événements particuliers et de points précis, du fait d'attentes irréalistes, d'interprétations erronées et d'un manque de contexte (« conclusions hâtives »). Les médias d'information, comme les médias sociaux, peuvent être utilisés pour diffuser de la désinformation (informations fausses ou inexactes). Le fait de recourir à la mésinformation dans l'intention de tromper est considéré comme de la désinformation.

11.7. La radio est souvent la première source d'information dans de nombreuses zones rurales et dans un grand nombre de pays en développement. Elle mérite donc que l'on s'y intéresse au titre des activités de renseignement de sources ouvertes dans les opérations de maintien de la paix.

11.8. Dans leurs interactions avec des entités en ligne, lors de la publication de commentaires ou de billets de blog ou dans le suivi de comptes de médias sociaux et le partage de contenu, **les spécialistes du renseignement de sources ouvertes dans les opérations de maintien de la paix ne sont pas autorisés à utiliser de faux comptes et à dissimuler le fait qu'ils sont**

employés par l'Organisation des Nations Unies. La mission peut autoriser la création et l'utilisation de comptes de médias sociaux institutionnels mentionnant la qualité professionnelle de l'opérateur afin de protéger l'identité du membre du personnel tout en indiquant qu'il travaille pour l'ONU. Cette pratique doit être prévue dans le plan d'appui renseignement de la mission mais doit être limitée et contrôlée³.

- 11.9. **L'utilisation d'un réseau privé virtuel (réseau VPN) sur du matériel appartenant à l'ONU, aux fins du renseignement de sources ouvertes, est soumise à l'autorisation du Siège (Équipe de coordination du renseignement dans les opérations de maintien de la paix, Bureau de l'informatique et des communications).** Le personnel des Nations Unies utilisant un réseau VPN sur son matériel personnel doit en assumer les risques et la responsabilité, et aucune information acquise au moyen d'un réseau VPN depuis du matériel personnel ne peut être utilisée en tant que renseignement de sources ouvertes dans les opérations de maintien de la paix.
- 11.10. Étant donné que la méthode d'acquisition d'informations dans les enceintes de prise de parole en public relève essentiellement de l'observation directe (présence), le caractère ostensible de l'opération doit faire l'objet de précautions particulières de la part de la personne concernée. Si la prudence s'impose, l'utilisation d'une fausse identité n'est pas autorisée. La sûreté et la sécurité du personnel de la mission doivent à tout moment être prioritaires.
- 11.11. Toutes les opérations de renseignement de sources ouvertes dans les opérations de maintien de la paix seront menées dans le strict respect du Plan d'acquisition d'informations de la mission et conformément au plan d'appui renseignement.
- 11.12. **Les spécialistes du renseignement de sources ouvertes dans les opérations de maintien de la paix ne doivent pas se livrer à la gestion de sources en ligne. Ces activités relèvent du renseignement de source humaine virtuel ou en ligne et sont régies par des lignes directrices propres.** Aussi, lors d'interactions en ligne (par exemple avec des utilisateurs de médias sociaux, des journalistes ou d'autres personnes privées), aucune somme d'argent ne sera versée, ni aucun cadeau offert, en rémunération d'une information.
- 11.13. Les exceptions au paiement concernent les **informations accessibles par voie commerciale** (p. ex., articles de journaux, images commerciales, analyses, abonnements) qui seront probablement considérées comme essentielles dans le cadre des activités de renseignement de sources ouvertes dans les opérations de maintien de la paix. Il convient de procéder à une analyse approfondie des sources et des informations et de l'actualiser régulièrement, ainsi que

³ Les spécialistes du renseignement de sources ouvertes autorisés à utiliser un compte institutionnel ne doivent pas perdre de vue le fait que le moindre de leur agissements en ligne a des répercussions pour l'Organisation dans son ensemble. Il est donc IMPÉRATIF que l'activité en ligne (comme les commentaires, la publication de blogs et le partage de contenu) à partir d'un compte institutionnel fasse l'objet d'une délégation de pouvoir explicite.

d'envisager l'affectation d'un budget adéquat, dans les missions, afin de tenir compte de ces dépenses.

- 11.14. Dans la mesure du possible, les activités de renseignement de sources ouvertes dans les opérations de maintien de la paix doivent être menées par du personnel formé dans ce domaine, dont les compétences et l'expérience lui permettent d'être efficace et rapide dans la recherche des informations requises. Autant que faire se peut, l'intégration de spécialistes du renseignement de sources ouvertes dans les entités de renseignement des composantes de la mission est vivement encouragée⁴.
- 11.15. Le renseignement de sources ouvertes dans les opérations de maintien de la paix est généralement moins gourmand en ressources que les autres méthodes d'acquisition de renseignement. Les plateformes et le matériel sont moins coûteux et les opérations sont généralement moins dangereuses pour l'opérateur(trice) et pour la source, par rapport au renseignement de source humaine, par exemple. Les informations obtenues grâce aux activités de renseignement de sources ouvertes ne sont pas intrinsèquement moins précieuses que d'autres sources d'information sous prétexte qu'elles sont accessibles à tous.
- 11.16. Conformément à la Politique, le (la) Chef de la mission ou un(e) fondé(e) de pouvoir est autorisé(e) à communiquer des renseignements, y compris d'origine sources ouvertes, à des acteurs non onusiens. L'échange de renseignement, y compris de sources ouvertes, avec des forces de sécurité non onusiennes, doit être conforme à la politique de diligence voulue en matière de droits humains en cas d'appui de l'ONU à des forces de sécurité non onusiennes. **Certaines informations provenant de sources ouvertes et traitées dans le cadre du cycle du renseignement dans les opérations de maintien de la paix seront classifiées.** La sûreté et la sécurité du personnel des Nations Unies, de la mission et de la population sont primordiales, et ces considérations doivent éclairer toute prise de décision relative à la communication de produits de renseignement.
- 11.17. Étant donné que les rapports de renseignement de sources ouvertes sont établis à partir d'informations accessibles au public, ils peuvent la plupart du temps être diffusés plus largement que les rapports de renseignement obtenu grâce à d'autres méthodes d'acquisition. Si l'accès aux informations avait un caractère commercial, leur diffusion pourrait être limitée⁵.
-

⁴ Cellule d'analyse conjointe de la mission, Département de la sûreté et de la sécurité (DSS) de l'Organisation des Nations Unies, Centre d'opérations conjoint (appui), U2 de la Force, groupe de la police des Nations Unies chargé du renseignement criminel.

⁵ Certaines informations accessibles par voie commerciale peuvent être soumises à des droits d'auteur et leur diffusion doit donc être limitée.

E. Fonctions et attributions

12. Ciblage

- 12.1. Le (la) Chef de la composante de la mission⁶ doit vérifier les besoins de renseignement et s'assurer que l'attribution des tâches est conforme aux capacités et aux limites de son entité.
- 12.2. Toutes les activités de renseignement de sources ouvertes dans les opérations de maintien de la paix seront menées à l'appui de la mission et des plans d'acquisition d'informations des composantes.

13. Acquisition ou activités de renseignement de sources ouvertes dans les opérations de maintien de la paix

- 13.1. Toutes les activités de renseignement de sources ouvertes sont planifiées, délibérées et décidées en fonction du temps imparti, du champ d'application et des capacités et ressources disponibles.
- 13.2. Les ressources nécessaires à l'acquisition de publications imprimées et d'abonnements commerciaux doivent être planifiées et budgétisées par la mission.
- 13.3. Avant de se lancer dans l'acquisition, il convient d'analyser le risque de manque d'objectivité, de mésinformation et de désinformation, ainsi que la probabilité que des entités hostiles surveillent et décèlent les activités de collecte de renseignement.
- 13.4. Du fait de la quantité massive d'informations disponibles à partir de sources ouvertes, les activités de renseignement en la matière doivent être soigneusement planifiées en fixant des priorités et en élaborant des stratégies de recherche tenant compte des outils de traitement disponibles.
- 13.5. En ce qui concerne les informations acquises qui révèlent l'existence d'une menace imminente pour la sûreté et la sécurité du personnel des Nations Unies ou des civils, veuillez vous reporter au paragraphe 16.1.
- 13.6. Les algorithmes en ligne « apprennent » des activités des utilisateurs. Ce point est à prendre tout particulièrement en compte sur les réseaux de médias sociaux et les moteurs de recherche. Il convient d'être attentif aux bulles de filtre qui ne font ressortir que des résultats correspondant à ses recherches ou activités antérieures.

14. Classement et examen

- 14.1. La grande quantité de données qui seront acquises grâce au renseignement de sources ouvertes nécessite de systématiser la réception, le regroupement, l'enregistrement et le classement de toutes les informations acquises. L'une des

⁶ Cellule d'analyse conjointe de la mission, DSS, Centre d'opérations conjoint (appui), Force, composante Police.

raisons de procéder ainsi est d'éviter la diffusion circulaire. La gestion des données est essentielle.

14.2. Étant donné que les activités de renseignement de sources ouvertes dans les opérations de maintien de la paix sont menées grâce à un large éventail de sources, il importe de tenir compte, pour chaque information, de l'allégeance, de l'avantage personnel, des objectifs et des intérêts de l'auteur, de l'entreprise, du site Web, du parti politique, de l'organisme, etc., qui a publié l'information afin de déterminer le risque de partialité, de mésinformation, de désinformation, de propagande et d'information fallacieuse (infox).

14.3. Une forme de validation des sources s'impose. Afin de valider la source, on peut adopter un système semblable à celui qui est utilisé pour le renseignement de source humaine. Dans le renseignement de sources ouvertes, l'évaluation portera sur l'auteur (ou le locuteur ou le site Web d'origine) et sur le contenu de l'information.

Tableau 1 Détermination du degré de fiabilité de la source

Fiabilité de la source		
Note	Évaluation	Observations
A	Fiable	Aucun doute sur l'authenticité, la fiabilité ou la compétence ; a toujours été complètement fiable.
B	Habituellement fiable	Léger doute quant à l'authenticité, à la fiabilité ou à la compétence ; dans le passé, a communiqué des éléments d'information valides la plupart du temps.
C	Généralement pas fiable	Il existe des doutes significatifs quant à l'authenticité, à la fiabilité ou à la compétence, mais la source a fourni des éléments d'information valides dans le passé.
D	Non fiable	L'authenticité, la fiabilité et la compétence font défaut ; a fourni des éléments d'information non valides dans le passé.
E	Impossible de formuler un jugement	Aucun élément ne permet d'évaluer la fiabilité de la source.

Tableau 2 Évaluation de la crédibilité de l'information

Crédibilité de l'élément d'information		
Note	Évaluation	Observations
1	Confirmé	Confirmé par d'autres sources indépendantes ; logique en soi ; cohérent par rapport aux autres éléments d'information dont on dispose sur le sujet.
2	Probablement vrai	Non confirmé ; logique en soi ; cohérent par rapport aux autres éléments d'information dont on dispose sur le sujet.
3	Doute quant à la véracité	Non confirmé ; possible mais pas logique ; on ne dispose d'aucun autre élément d'information sur le sujet.
4	Improbable	Non confirmé ; pas logique en soi ; contredit d'autres éléments d'information dont on dispose sur le sujet.
5	Impossible de formuler un jugement	Rien ne permet d'évaluer la validité de l'élément d'information.

15. Analyse

- 15.1. Un(e) spécialiste ou une cellule chargé(e) du renseignement de sources ouvertes dans les opérations de maintien de la paix peut procéder à une analyse reposant sur une source unique afin d'organiser et de structurer les informations disponibles et d'éviter de surcharger les analystes d'informations à traiter, à intégrer et à interpréter ; le renseignement de sources ouvertes fondé sur une source unique doit être signalé comme tel.

16. Diffusion

- 16.1. Les informations acquises par un(e) spécialiste du renseignement de sources ouvertes dans les opérations de maintien de la paix qui laissent présager une menace imminente pesant sur le personnel des Nations Unies ou les populations civiles doivent être immédiatement transmises à la composante chargée du renseignement concernée⁷ par les moyens les plus rapides. La composante alerte alors **immédiatement** tous les autres membres du mécanisme de coordination du renseignement dans les missions de maintien de la paix, y compris le (la) Chef d'état-major de la mission.
- 16.2. De même, les informations acquises par un(e) spécialiste du renseignement de sources ouvertes dans les opérations de maintien de la paix relatives à une présomption d'activité criminelle peuvent également être transmises à la composante chargée du renseignement concernée par les moyens les plus rapides⁸. La composante alertera alors le groupe de la police des Nations Unies chargé du renseignement criminel de la mission⁹.
- 16.3. Les principes de diffusion suivants doivent être suivis :
 - 16.3.1. **Rapidité** – Les informations acquises doivent être fournies dans les meilleurs délais afin que les spécialistes de la planification et les décideurs puissent agir plutôt que de réagir.
 - 16.3.2. **Pertinence** – On détermine la pertinence en fonction des besoins des destinataires tels que définis dans le plan d'acquisition d'informations applicable (à la mission ou à la composante).
 - 16.3.3. **Concision** – Les rapports doivent être aussi concis que possible mais contenir toutes les informations dont les destinataires ont besoin.
 - 16.3.4. **Interprétation** – Dans la mesure du possible, tous les faits doivent être évalués comme il se doit, en évaluant leur portée avant de les diffuser.

⁷ Cellule d'analyse conjointe de la mission, DSS, Centre d'opérations conjoint (appui), U2, composante Police.

⁸ Cellule d'analyse conjointe de la mission, DSS, Centre d'opérations conjoint (appui), U2, composante Police.

⁹ Dans le cadre de ses mandats non exécutifs actuels, la police des Nations Unies n'est pas toujours en mesure d'agir sur la base de ces informations, mais peut informer ses homologues locaux des infractions graves (telles que définies par les lois locales).

- 16.4. Un(e) spécialiste ou une cellule chargé(e) du renseignement de sources ouvertes dans les opérations de maintien de la paix peut choisir de mettre ses informations à la disposition d'un public plus large au moyen d'un tableau de bord intégrant plusieurs flux de renseignement de sources ouvertes.
- 16.5. La diffusion du renseignement de sources ouvertes doit être fondée sur une base légale : la majorité de ces renseignements, en particulier les informations accessibles par voie commerciale, sont protégés par les lois sur les droits d'auteur. Ces lois doivent être prises en compte et ce type d'information ne peut être diffusé qu'à l'appui de la mission.
-

F. DÉFINITIONS

17. Le (la) **spécialiste du renseignement de sources ouvertes dans les opérations de maintien de la paix d'une composante** est un(e) militaire, un(e) policier(ère) ou un membre du personnel civil préalablement formé(e) et doté(e) d'une expérience dans le domaine du renseignement de sources ouvertes dans les opérations de maintien de la paix ou du renseignement d'origine sources ouvertes (ROSO), qui est chargé(e) de mener des activités de renseignement de sources ouvertes dans le cadre d'opérations de maintien de la paix des Nations Unies.
18. La **désinformation** est l'acte qui consiste à publier une information fausse ou erronée dans l'intention de tromper. Elle résulte d'informations délibérément mensongères ou partiales, de récits ou de faits manipulés et d'actes de propagande. L'origine de l'information peut être dissimulée, l'information peut être diffusée clandestinement et l'intention et les bénéficiaires de la campagne de désinformation ne sont pas toujours clairs. Elle est considérée comme une sous-catégorie de la mésinformation.
19. Les **bulles de filtre** sont un état d'isolement intellectuel ou idéologique qui peut résulter d'un filtrage algorithmique, c'est-à-dire d'algorithmes qui fournissent aux destinataires des informations auxquelles ils sont sensibles et avec lesquelles ils sont d'accord, sur la base de son comportement passé et de son historique de recherche, ce qui peut fausser sa perception de la réalité du fait d'une surexposition à une vision et une sous-exposition à d'autres.
20. La **mésinformation** fait référence à la publication d'informations fausses ou inexactes, qu'il y ait ou non une intention de tromper ou d'induire en erreur.
21. Le **renseignement de sources ouvertes dans les opérations de maintien de la paix** est le renseignement qui est issu de l'acquisition, du classement et de l'analyse d'informations accessibles au public à partir de sources ouvertes en vue de répondre aux besoins en renseignement d'une mission.
22. Une **activité de renseignement de sources ouvertes dans les opérations de maintien de la paix** consiste à planifier et à exécuter avec efficacité une opération, dans le cadre d'une mission de maintien de la paix, visant à rechercher, trouver et extraire des informations accessibles au public d'une manière sûre, légale et non clandestine. Cette activité peut être menée physiquement et en ligne.

23. L'acronyme « **VPN** » désigne un réseau privé virtuel. Il s'agit d'un service qui permet à l'utilisateur de protéger sa vie privée et de préserver son anonymat en ligne. Un réseau VPN masque l'adresse du protocole Internet (IP) de l'appareil, de sorte que les actions en ligne sont pratiquement intraquables. La connexion à un serveur VPN sécurisé permet de faire circuler les données dans un tunnel souvent crypté sur les sites Internet publics.
-

G. RÉFÉRENCES

Assemblée générale et Conseil de sécurité

- Rapport du Comité spécial des opérations de maintien de la paix sur les travaux de sa session de fond de 2020 (A/74/19)

Références normatives

- Politique du Département des opérations de paix relative au renseignement dans les opérations de maintien de la paix, 2019
- Politique du Département des opérations de paix et du Département de l'appui opérationnel relative aux cellules d'analyse conjointe des missions, 2020

Directives connexes

- Manuel consacré aux cellules d'analyse conjointe des missions (*Joint Mission Analysis Centres Handbook*), 2017
 - Manuel du renseignement militaire dans les opérations de maintien de la paix des Nations Unies, 2019
 - Manuel du renseignement, de la surveillance et de la reconnaissance dans les opérations de maintien de la paix des Nations Unies, 2020
 - Directives du Département des opérations de paix relatives à l'acquisition d'informations auprès de sources humaines aux fins du renseignement dans les opérations de maintien de la paix (*Guidelines on acquisition of information from human sources for peacekeeping-intelligence*), 2020
-

H. SUIVI DE L'APPLICATION

24. Au sein des missions, le (la) Chef de la mission répond du respect des présentes lignes directrices par la mission et doit mettre en place des mécanismes ou des procédures permettant de contrôler efficacement leur application. Tous les membres du personnel des missions qui participent aux activités de renseignement sont responsables, via leur chaîne de commandement ou leur voie hiérarchique, du respect de la Politique et des présentes lignes directrices.
-

I. SERVICE À CONTACTER

25. Le service à contacter en ce qui concerne les présentes lignes directrices est l'Équipe de coordination du renseignement dans les opérations de maintien de la paix [au sein du DPO/Bureau du (de la) Secrétaire général(e) adjoint(e)].
-

J. HISTORIQUE

26. Le présent texte constitue la première version des lignes directrices.

SIGNATURE :

**Jean-Pierre Lacroix,
Secrétaire général adjoint aux opérations de paix**

DATE D'APPROBATION :

Annexe A

Ressources et outils

Outils publics

Alexa.com (Amazon)

Outil de recherche par mots-clés, de consultation de statistiques de fréquentation de sites Web et de recherche de sites analogues

Datawrapper (datawrapper.de)

Création de graphiques, de cartes et de tableaux avec ses propres données

EO Browser (apps.sentinel-hub.com/eo-browser)

Consultation et comparaison de données et d'images satellitaires en haute résolution provenant de nombreux satellites

Forensically Beta (29a.ch/photo-forensics/)

Analyse forensique d'images numériques (détection de clones, extraction de métadonnées, etc.)

Looker Studio (<https://lookerstudio.google.com/navigation/reporting>)

Recherche, visualisation et partage de données

Google Earth (google.com/earth/)

Navigation sur des cartes et des images, import et export de données du système d'information géographique, création de cartes

Google Trends (trends.google.com)

Exploration par région des thèmes d'actualité, des articles récents et des tendances

In Vid (invid-project.eu)

Détection, authentification et vérification de la fiabilité et l'exactitude des fichiers vidéo

News Explorer d'IBM Watson (news-explorer.mybluemix.net)

Exploration des tendances en matière de requêtes et d'associations et des actualités immédiates

Open Refine (openrefine.org)

Exploration de jeux de données, nettoyage et transformation de formats de données, associations de jeux de données

Tin Eye (tineye.com)

Recherche d'images inversée aux fins de l'identification, de la vérification, du suivi et de la reconnaissance d'images

RAWGraphs (rawgraphs.io)

Système de visualisation de données

TweetDeck (tweetdeck.twitter.com)

Suivi et organisation en temps réel des engagements sur Twitter

TwitterAudit (twitteraudit.com)

Détermination de l'authenticité des comptes Twitter (vrais ou faux)

Abonnements de l'ONU

Dataminr (dataminr.com)

Outil d'intelligence artificielle appliqué aux jeux de données publiques. Dataminr fournit à l'ONU un accès à First Alert

Jeux de données publiques

ACLEDD (acleddata.com)

Données en temps réel sur les lieux, les dates, les acteurs, les pertes et les types d'événements

Global Peace Index (visionofhumanity.org)

Tour d'horizon des facteurs de paix par pays

Health Map (<https://healthmap.org/fr/>)

Surveillance des épidémies et des menaces pesant sur la santé publique fondée sur des sources informelles en ligne

Indice des États fragiles (fragilestatesindex.org)

Tableaux de bord par pays, analyse comparative, analyse des tendances

Organisation internationale pour les migrations (migrationdataportal.org)

Statistiques sur les migrations : flux, vulnérabilité, politique, opinion publique, etc.

Uppsala Conflict Data Program (ucdp.uu.se)

Données sur la violence organisée