PROTECTION international

Nouveau Manuel de Protection pour les Défenseurs des Droits Humains

Recherche et texte par Enrique Eguren et Marie Caraj

Nouveau Manuel de Protection

pour

Les Défenseurs des Droits Humains

Recherche et texte par Enrique Eguren et Marie Caraj

Protection International (PI)

Publié par Protection International

Publié par Protection International 2009
Rue de la Linière, 11
B-1060 Bruxelles, Belgique.
3ème édition

Des exemplaires du Nouveau manuel peuvent être commandés à:

Protection International
Rue de la Linière, 11. B-1060 Bruxelles (Belgique)
Tel: +32(0)2 609 44 05 / +32(0)2 609 44 07 / Fax: +32(0)2 609 44 06
pi@protectioninternational.org

Il peut être téléchargé gratuitement depuis **www.protectionline.org**
Prix des exemplaires:
Organisations du sud: gratuit
Organisations du nord: 20 Euros plus frais de port et d'emballage (remises pour des commandes importantes)

Ce Nouveau manuel édité par Protection International existe en anglais (version originale), en espagnol ainsi que dans d'autres langues.

ISBN: 978-2-930539-07-2

Avant-propos d'Hina Jilani (Première édition)

Au cours de mon travail en tant que représentante spéciale du secrétaire général chargée des défenseurs des droits humains, j'ai remarqué, avec une profonde inquiétude, l'augmentation du nombre de rapports sur des violations graves des droits humains perpétrées à l'encontre des défenseurs ainsi qu'un changement visible de la gravité de ces violences qui est passée de l'intimidation et du harcèlement à de plus sérieuses exactions comme des attaques et des menaces contre l'intégrité physique des défenseurs. En 2004, nous avons travaillé sur les rapports d'au moins 47 défenseurs tués en raison de leur travail.

Il est évident que l'obligation de protéger les défenseurs des droits humains incombe au premier chef aux gouvernements, comme l'établit la Déclaration sur les défenseurs des droits humains de l'ONU.[1] *Nous devons poursuivre nos efforts afin d' inciter les Etats et les gouvernements à respecter leurs obligations en la matière et à adopter les mesures appropriées pour garantir la protection des défenseurs des droits humains.*

Cependant, la gravité des risques encourus au quotidien par les défenseurs des droits humains est telle que leur protection ne pourrait être renforcée sans stratégies additionnelles. À cet égard, j'espère que ce manuel de protection aidera les défenseurs des droits humains à élaborer leurs propres plans de sécurité et mécanismes de protection. De nombreux défenseurs des droits humains se vouent corps et âme à la protection des autres au point d'en oublier leur propre sécurité. Il est essentiel pour nous qui oeuvrons en faveur des droits humains de prendre conscience de l'importance de la sécurité pour nous-mêmes et pour les personnes avec qui et pour qui nous travaillons.

Hina Jilani

Ex Représentante spéciale du Secrétaire général des Nations unies sur la situation des défenseurs des droits de l'homme (2000-2008)

[1] Déclaration sur le droit et la responsabilité des individus, groupes et instances de la société pour la promotion et le respect des droits humains et des libertés fondamentales universellement reconnus.

Les membres de PI ont plus de 25 ans d'expérience en matière de protection des défenseurs des droits humains et d'autres groupes vulnérables.[2]

Le but de PI est de contribuer au respect des obligations nationales et internationales en matière de protection des défenseurs des droits humains. Plusieurs ONG et institutions travaillent déjà sur les questions des droits humains et des défenseurs. PI se propose de collaborer à cette activité.

La stratégie globale de PI pour la protection des défenseurs comprend les points suivants:

Développement des capacités en protection et sécurité - Formation

- Evaluation du risque et gestion de la sécurité / protection
- Transmission de connaissances et d'outils méthodologiques.
- Publication de manuels, parmi lesquels ce Nouveau manuel (et son édition précédente)[3]
- Formation: entre 2004 et 2008, plus de 1700 défenseurs ont participé à des ateliers de développement de capacités en protection et sécurité, améliorant leurs compétences en gestion de leur propre sécurité et de la protection d'autrui.

Recherche en matière de protection

- Recherche et élaboration d'outils méthodologiques et opérationnels de protection / sécurité.
- Publication d'informations basées sur les leçons apprises et les bonnes pratiques.

Promotion de la protection

- Distribution d'informations sur la protection aux défenseurs des droits humains, aux personnes déplacées (Internally Displaced Persons -IDPs), aux institutions de l'UE et à ses Etats membres sous la forme de recommandations de rapports et de communiqués de presse ainsi que de documentaires.

[2] À compter du 25 octobre 2007 et par décret du Service public fédéral de Justice, le bureau européen de Peace Brigades International, est devenu par le biais de l'amendement de ses statuts publiés dans le Journal officiel de Belgique "Protection International", une association à but non lucratif international.

[3] Avec le soutien financier de Front line et de Development Cooperation of Ireland.

- Rappel aux autorités nationales et internationales de leurs obligations internationales quant à la protection des défenseurs des droits humains, des déplacés internes, des réfugiés et d'autres acteurs sociaux.
- Promotion des débats et initiatives ayant pour but de protéger les défenseurs des droits humains; d'impliquer les parlements, syndicats et médias.
- Lutte contre l'impunité des exactions contre les DDH, comprenant l'observation internationale de procès et plaidoyer en ce sens.

Vidéos de protection (plaidoyer par vidéo)

- Réalisation de portraits de défenseurs des droits humains.

Mise en place de bureaux de protection (en anglais Protection Desk - PD) dédiés aux défenseurs des droits humains

- En partenariat avec des réseaux locaux de défenseurs des droits humains, les bureaux de protection sont mis en place pour servir de centres régionaux et nationaux pour la gestion de la protection et de la sécurité des défenseurs.
- Remise progressive aux Protection Desks du processus entier de la gestion de la sécurité / protection (l'appropriation fait partie de ce processus).

Site Protectionline (Protection en ligne)

- www.protectionline.org est un site Internet unique fait par/avec/pour les défenseurs des droits humains et ceux qui cherchent à contribuer à la protection des défenseurs des droits humains.
- PI procède à la mise à jour régulière des informations, et à la publication de documents, témoignages, actions urgentes et outils conçus pour promouvoir la protection des défenseurs des droits humains.

Cadre normatif:

PI se conforme à toutes les normes internationales en matière de droits humains et au droit international humanitaire. PI utilise les dispositions de la Déclaration sur les défenseurs des droits humains des Nations Unies (1998) et des Lignes directrices sur les défenseurs des droits humains (2004), ainsi que les résolutions sur les défenseurs adoptées par les Etats membres de l'UE tels que l'Espagne, la Belgique et l'Allemagne et les diffuse.

Ateliers de PI sur la sécurité et le développement de capacités

De 2004 à 2007, un total de 1747 défenseurs des droits humains ont participé aux ateliers de PI sur la sécurité et le développement de capacités

- En Amérique de Sud et Centrale: 558 défenseurs des droits humains (Bolivie, Brésil, Colombie, Guatemala, Honduras, Mexique, Pérou)
- En Asie: 650 défenseurs des droits humains (Birmanie, Indonésie, Népal, Thaïlande)
- En Afrique: 441 défenseurs des droits humains (Kenya, Ouganda, République Démocratique du Congo)
- En Europe: 98 défenseurs des droits humains (Allemagne, Belgique, Irlande, Serbie, République d'Ingouchie)

Les défenseurs des droits humains protègent souvent les autres en négligeant leur propre sécurité. Il y a plusieurs raisons à cela. La formation qu'offre PI en matière de sécurité et de protection aborde ces raisons et donne l'occasion et le temps de réfléchir aux risques et menaces auxquels sont exposés les défenseurs des droits humains. La formation que propose PI permet d'analyser et de décomposer les risques et d'acquérir le savoir-faire et le raisonnement nécessaires pour intégrer la sécurité dans le travail des défenseurs des droits humains. Pendant la formation, la sécurité est subdivisée en ses différentes composantes pour mieux les analyser, réfléchir a des théories et scénarios possibles, ainsi qu'aux conséquences de choix spécifiques. Ceci permet de voir l'option dont les défenseurs pensent pouvoir gérer les conséquences, tout en sachant qu'ils ne peuvent s'attendre avec certitude à des résultats précis.

Dans tous les cas, il n'y a pas de solution miracle qui s'appliquerait à toutes les éventualités; la formation vise à ce que les défenseurs des droits humains acquièrent les compétences nécessaires à la sécurité: l'analyse, la prévision des conséquences, la gestion et la mise à jour du processus. Ils doivent le faire à un niveau individuel, organisationnel et inter-organisationnel tout en prenant en compte au moins l'aspect politique, psychosocial et physique.

Préface

Après plus d'une décennie de formations, de recherche et de rencontres avec des défenseurs des droits humains et d'autres parties prenantes responsables de la protection des défenseurs des droits humains, nous, l'équipe de Protection International, renouvelons notre hommage aux défenseurs et avons décidé d'inclure une fois de plus leurs contributions dans ce nouveau manuel de protection écrit avec, par et pour tous les défenseurs des droits humains.

Ces trois dernières années, Protection International a étendu ses formations et ses recherches, bénéficiant de l'expérience sur le terrain et du retour d'information des défenseurs des droits humains.

Dans ce nouveau manuel, Protection International met en avant une méthodologie et une logique de gestion pouvant être reprises dans des structures et des environnements d'organisations différents mais aboutissant au même résultat: l'intégration d'un plan de sécurité dans la planification du travail. Il n'y a pas de formule magique ni universelle, seulement des choix et des conséquences à gérer. Cet objectif peut être atteint par un brainstorming,[4] en appliquant différentes méthodes, en posant les bonnes questions, en procédant à des évaluations du risque de la sécurité de l'organisation et de ses membres, en élaborant des plans et des processus participatifs...

Ce nouveau manuel vise l'appropriation par les défenseurs des droits humains de l'ensemble de la logique et du processus de sécurité et de protection. L'appropriation est une composante de la sécurité elle-même. Le nouveau manuel contribue à l'autonomie de la sécurité et de la protection des défenseurs des droits humains et à les rendre durables.

Bien qu'il n'existe pas de plan de sécurité miracle et universel - applicable à tous les cas de figure et tous les contextes - le nouveau manuel transcende les différences -issues des contextes locaux, culturelles, sociales, religieuses et organisationnelles en ce qu'il fournit une méthodologie. Elle peut donc être facilement utilisée par les défenseurs des droits humains pour une gestion sur mesure de leur sécurité et de leur protection, dans la mesure où nous sommes bien sûr conscients qu'ils détiennent seuls "la matière première", c'est à dire la connaissance et l'expérience de leur propre contexte.

Protection International traite de la gestion de la sécurité du défenseur des droits humains par lui-même d'une part, et de la protection du défenseur des droits humains par les acteurs de protection.

[4] Brainstorming: technique de travail en groupe permettant de susciter des idées originales en faisant appel aux suggestions individuelles. (Larousse).

Remerciements:

♦ La nouvelle version et édition mise à jour et étendue du manuel est le fruit de la contribution de:

• tous les défenseurs des droits humains qui ont suivi les formations à la gestion de la sécurité et de la protection de Protection International. Il est impossible d'en faire la liste complète ici. Ils se trouvent en Bolivie, au Brésil, en Birmanie, en Colombie, dans la République Démocratique du Congo, au Guatemala, au Honduras, en Indonésie, en Ingouchie, au Kenya, au Mexique, au Népal, au Pérou, en Serbie, au Sri Lanka, en Thaïlande, en Ouganda.

• des anciens membres et les actuels de PI: Pascale Boosten, Soledad Briones, Shaun Kirven, Christoph Klotz, Olivier Richard, Michael Schools...

• des anciens collaborateurs et les actuels de PI: Ana Cornide, Jérôme Hieber, Eric Juzen, María Martín, Thomas Noirfalisse, Sheila Pais, Flora Petrucci, Sophie Roudil, Catherine Wielant, Jabier Zabala...

• de Carmen Díez Rozas et Montserrat Muñoz qui toutes les deux ont consacré un soin remarquable au design et à la mise en page des éditions précédentes et actuelles du manuel. Thomas Noirfalisse a contribué en réalisant le design du logo de PI et en proposant des idées pour la mise en page de la couverture.

Nous avons ici une pensée affectueuse pour Brigitte Scherer.

Nous sommes reconnaissants du soutien apporté par le Bundeministerium für Wirtschaftliche Zusammenarbeit und Entwicklung (le ministère allemand de la coopération et du développement) et le Service public fédéral Affaires Etrangères de Belgique.

Le "Nouveau manuel de protection pour les défenseurs des droits humains" met à jour et développe le premier "Manuel de protection des défenseurs des droits humains" (auteur: Luis Enrique Eguren © 2005 PI anciennement PBI-BEO) qui a été publié avec le soutien financier de Front Line et de Development Cooperation of Ireland, l'organisme irlandais de coopération en matière de développement.

La première épreuve du premier manuel a été commentée par Arnold Tsunga (Zimbabwe, avocat spécialisé dans les droits humains), Sihem Bensedrine (Tunis, Conseil National pour les Libertés en Tunisie), le père Bendan Forde (Colombie, franciscains itinérants), Indai Sajor (Philippines, ancien directeur du Centre asiatique des droits humains), James Cavallaro (Brésil, directeur associé du Human Rights Programme - Harvard Law School), Nadejda Marques (Brésil, consultant et chercheur - Global Justice) et Marie Caraj (PI anciennement PBI BEO).

D'autres collègues ont contribué avec leur propre travail: José Cruz et Iduvina du SEDEM (Guatemala), Jaime Prieto (Colombie), Emma Eastwood (Royaume-Uni) et Cintia Lavandera du programme pour les défenseurs des droits humains d'Amnesty International à Londres.

Le programme des défenseurs des droits humains d'Amnesty International à Londres et le Indonesia Project de PBI ont respectivement financé la traduction

de la première édition du manuel en portugais et en indonésien. La Commission Internationale de Juristes l'a fait traduire en thai, et PBI en népalais.

Le chapitre 1.11 est basé sur le travail de Robert Guerra, Katitza Rodriguez et Caryn Madden de Privaterra (Canada).

Remerciements de l'auteur: Luis Enrique Eguren

Comme de nombreuses autres personnes ont contribué à la collecte des informations de fond nécessaires à l'écriture de ce manuel, il est impossible d'en faire la liste complète ici. J'aimerais néanmoins mentionner quelques noms, comme par exemple:

toutes les personnes de PBI, et spécialement mes anciens collègues du projet Colombie comme Marga, Elena, Francesca, Emma, Tomás, Juan, Mikel, Solveig, Mirjam, Jacobo et tant d'autres...

Danilo, Clemencia et Abilio et leurs collègues de la Comision Intereclesial de Justicia y Paz en Colombie. Ils m'ont appris comment vivre au coeur des gens.

Aux habitants de Santa Marta au Salvador, et à ceux de Cacarica, Jiguamiando et San José de Apartado en Colombie. Ils m'ont appris, parmi d'autres choses, la dignité de la vie des gens de la campagne.

À Irma Ortiz, ma collègue formatrice dans de nombreux ateliers, et à tous les autres collègues de Pensamiento y Acción Social (PAS) en Colombie.

Remerciements aussi pour le conseil et le savoir initial fourni par REDR (Londres) Koenraad van Brabant (Belgium).

Et aux nombreux défenseurs rencontrés au Salvador, au Guatemala, en Colombie, au Pérou, en Birmanie, au Sri Lanka, en Croatie, en Serbie, au Kosovo, au Rwanda, en République Démocratique du Congo, en Ingouchie, etc.

Un océan de conversations, de larmes, de sourires, d'apprentissage et d'engagement...

En dernier lieu, rien n'aurait été possible sans l'amour, le dévouement et le soutien de Grisela et Iker et de mes parents.

Avec toute mon affection.

Remerciements du co-auteur: Marie Caraj

Je ressens de l'admiration, du respect, de la solidarité, de l'empathie et de la gratitude pour tous les défenseurs des droits humains que j'ai rencontrés, que je vais rencontrer et que je ne rencontrerai jamais. Ils ont changé ma vie. Les jours passés ensemble ont, de manière imperceptible, noué un lien entre nous.

Je suis partagée entre la colère envers les violateurs des droits humains et l'espoir qu'ils comprennent un jour que les défenseurs des droits humains

ne les discriminent pas et qu'ils peuvent, sans crainte, rejoindre ce mouvement qui œuvre pour qu'un jour l'ensemble des droits humains soit respecté et que les défenseurs puissent jouir d'une vie normale.

À Leze Gegaj, ma mère, la première femme défenseur des droits humains que j'ai rencontrée.

À tous mes amis et collègues pour leur soutien tacite ou explicite. La plupart d'entre eux ont partagé les histoires que j'ai ramenées et m'ont aidée à recharger les piles.

Nous remercions tous ceux cités plus haut pour leur apport, et le nombre bien plus important de défenseurs des droits humains avec lesquels nous avons travaillé et qui nous ont beaucoup appris. Les erreurs éventuelles dans ce nouveau manuel (bien que nous ayons fait tout notre possible pour qu'il n'y en ait pas !) sont entièrement attribuables à notre relecture imparfaite. Nous espérons que le nouveau manuel soit un outil utile pour améliorer la protection et la sécurité des défenseurs des droits humains, tout en étant conscients qu'il n'offre aucune garantie de résultat et que dans ce domaine, c'est à chacun d'assumer sa responsabilité en dernier lieu. Nous sommes impatients de connaître votre opinion et votre retour sur ce manuel.

Protection International

Avril 2009

Clause de non responsabilité

Le contenu de ce manuel ne représente pas nécessairement la position de Protection International.

Ni les auteurs, ni l'éditeur ne garantissent que l'information contenue dans la présente publication soit complète ou juste et ils déclinent toute responsabilité pour tout dommage résultant de son utilisation. Aucune partie de ce manuel ne peut être prise pour norme ou pour garantie absolue; être utilisée sans les critères nécessaires à une évaluation du risque et des problèmes de sécurité auxquels un défenseur des droits humains pourrait être confronté.

Nouveau manuel de sécurité et de protection pour les défenseurs des droits humains

Les défenseurs des droits humains en danger

Les droits humains sont garantis par le droit international, mais les défendre ainsi que défendre les personnes dont les droits ont été violés peut s'avérer une activité dangereuse dans le monde entier. Les défenseurs des droits humains représentent souvent la seule force entre les gens ordinaires et le pouvoir sans frein de l'État. Ils sont essentiels à la mise en place de processus et d'institutions démocratiques, à la lutte contre l'impunité, à la défense et au respect des droits humains.

Les défenseurs des droits humains sont souvent victimes de harcèlement, de détention, de torture, de diffamation, de licenciements abusifs, d'entraves à leur liberté de mouvement et d'entraves à la reconnaissance juridique de leurs associations. Dans certains pays, ils sont assassinés, enlevés ou "portés disparus".

Au cours des dernières années, on a constaté une prise de conscience accrue des risques énormes auxquels les défenseurs des droits humains sont confrontés dans l'exercice de leur travail. Ce risque est facile à identifier lorsque les défenseurs des droits humains travaillent dans un milieu hostile, par exemple lorsque la loi d'un pays condamne les personnes menant des activités de défense des droits humains. Cependant, les défenseurs sont également en danger lorsque la loi autorise pleinement toute activité liée aux droits humains, mais qu'en même temps elle néglige de punir ceux qui menacent ou agressent des défenseurs. En situation de conflit armé, le danger est encore plus grave.

Hormis certains moments chaotiques où la vie des défenseurs des droits humains peut par exemple reposer entre les mains de soldats à un poste de contrôle, les actes de violence (agressions) commis contre des défenseurs des droits humains ne peuvent être qualifiés de fortuits. Dans la plupart des cas, les agressions violentes sont une réponse délibérée et soigneusement organisée à l'activité des défenseurs et obéissent à des intérêts politiques ou militaires concrets.

Ces défis exigent que les défenseurs des droits humains mettent en œuvre des stratégies de sécurité globales et dynamiques dans leur travail quotidien. Donner

des conseils bien intentionnés aux défenseurs ou leur recommander de "faire bien attention" ne suffit pas. Une meilleure gestion de la sécurité est capitale. Ce manuel n'offre pas de solutions "type" qui s'appliquent indifféremment à tous les scénarios. Cependant, il s'efforce de proposer une méthodologie et un ensemble de stratégies visant à améliorer la gestion de la sécurité des défenseurs des droits humains.

Les leçons de sécurité les plus efficaces proviennent des défenseurs des droits humains eux-mêmes, de leurs expériences quotidiennes, des tactiques et des stratégies qu'ils ont adoptées au fil des ans pour protéger autrui et leurs propres cadres de travail. Ce manuel doit par conséquent être compris comme un projet évolutif à mettre à jour et à adapter à mesure que nous recevons davantage de contributions de la part des défenseurs.

Il y a également des enseignements à tirer des ONG humanitaires internationales qui depuis peu ont commencé à élaborer leurs propres règles et procédures pour préserver la sécurité de leur personnel.

Il faut savoir que le principal risque pour les défenseurs réside dans le fait qu'une menace se concrétise en agression réelle. Cela se produit lorsque les agresseurs ont la volonté, les moyens et quand ils jouissent de l'impunité nécessaire pour mettre leurs menaces à exécution. Le meilleur outil de protection des défenseurs est donc l'action politique face au seul grand problème persistant: l'obligation pour les gouvernements et la société civile de faire pression et d'agir contre ceux qui, jour après jour, menacent, harcèlent et assassinent les défenseurs des droits humains. Les conseils donnés dans ce manuel n'entendent en aucun cas délester les gouvernements de leur responsabilité effective de protéger les défenseurs des droits humains.

Ceci dit, les défenseurs des droits humains peuvent sensiblement améliorer leur sécurité en respectant des règles et procédures ayant fait leurs preuves.

Ce manuel représente une contribution modeste au but commun que poursuivent de nombreuses organisations différentes et qui consiste à défendre le travail extrêmement précieux des défenseurs des droits humains. Ces derniers sont les principales parties prenantes comme les principaux protagonistes de ce manuel.

Le manuel

Ce manuel est le fruit de 25 ans d'expérience cumulée des membres de Protection International (PI) acquise, dans le cadre du droit international humanitaire et des droits humains, lors de la protection des défenseurs des droits humains et d'autres groupes vulnérables. L'expérience des membres de PI puise sa source dans leur engagement préalable et leur participation à Peace Brigades International (PBI), dans ses missions sur le terrain et sa structure internationale. Des centaines de défenseurs nous ont permis de partager leurs expériences et connaissances sur le terrain, lors d'ateliers, de réunions et de débats sur la sécurité. L'essentiel du manuel a déjà été appliqué dans les activités de protection ou lors d'ateliers de formation avec les défenseurs.

Ce manuel est né de tous ces échanges et nous adressons aux défenseurs participants nos plus profonds remerciements.

La sécurité et la protection sont des domaines complexes. Elles se fondent sur des connaissances factuelles mais dépendent aussi de comportements individuels et du fonctionnement d'une organisation. L'un des messages clé de ce manuel est qu'il faut accorder à la question de la sécurité, le temps et la place qu'elle mérite, en dépit de programmes de travail surchargés, du stress extrême et de la peur qu'endurent tous les défenseurs et leurs organisations. Cela signifie qu'il est nécessaire de passer outre l'expérience individuelle de la sécurité et d'évoluer vers une culture de l'organisation dont la sécurité est inséparable.

Avoir une connaissance suffisante d'un scénario de conflit et comprendre la logique politique locale sont également indispensables pour une gestion adéquate de la sécurité des défenseurs. Ce manuel contient un cadre de référence général ainsi qu'un système détaillant la gestion de la sécurité point par point pour établir un plan de sécurité (produit) et pour gérer la sécurité (processus). Il comprend également des considérations sur des notions fondamentales comme le risque, la vulnérabilité et les menaces, et quelques conseils pour améliorer et augmenter la sécurité des défenseurs dans leur travail au quotidien. Nous espérons que les sujets abordés permettront aux ONG et défenseurs de mieux répondre aux défis croissants de sécurité posés par la défense des droits humains.

Cela dit, nous souhaitons en premier lieu faire prendre conscience que les défenseurs des droits humains sacrifient leur bien-être et risquent leur vie et que c'est une question sérieuse. Parfois, la seule façon de sauver une vie est de se mettre à l'abri et puis de fuir. Pour nous, les techniques et conseils de ce manuel ne sont en aucun cas la seule façon de penser la sécurité des défenseurs. Ce manuel a été rédigé en toute bonne foi mais n'offre malheureusement aucune garantie de résultat.

Améliorons ensemble ce manuel ...

Le risque change. Ce manuel est un projet en évolution conçu pour être approfondi, amélioré et retouché au fil du temps. Votre réaction en tant que défenseur à tout élément de ce manuel serait inestimable.

Veuillez nous écrire vos commentaires ou avis, surtout s'ils portent sur l'utilisation du manuel dans votre travail. Grâce à vous, nous pouvons faire de ce manuel un outil de plus en plus utile pour les défenseurs partout dans le monde.

Adressez vos courriels à:

pi@protectioninternational.org

Et votre courrier à PI:

Protection International. Rue de la Linière, 11 - 1060 Bruxelles (Belgique)
Tel: + 32 (0) 2 609 44 05, +32 (0) 2 609 44 07
Fax: +32 (0) 2 609 44 06

www.protectioninternational.org
www.protectionline.org

Une brève introduction aux défenseurs des droits humains

Par "défenseurs des droits humains" on désigne des personnes qui, seules ou en association avec autrui, participent à la promotion, défense et à la protection des droits humains. Les défenseurs des droits humains se reconnaissent avant tout par ce qu'ils font, et le terme peut être expliqué au mieux en décrivant leurs activités et certaines circonstances dans lesquelles ils travaillent.

Le travail des défenseurs des droits humains est légal et légitimé par la société civile qu'ils représentent. Chaque jour à travers le monde, le travail de centaines de défenseurs des droits humains est exposé à la violence politique parce qu'ils luttent pour protéger les droits d'autrui. En risquant leur intégrité physique et mentale, ils aspirent à mettre un terme à l'impunité concernant les violations des droits humains et contribuent à promouvoir la paix et la justice sociales.

En 1998, l'assemblée générale des Nations unies a adopté la "Déclaration sur le droit et la responsabilité des individus, groupes et organes de la société de promouvoir et protéger les droits de l'homme et les libertés fondamentales universellement reconnus", (ci-après déclaration sur les défenseurs des droits humains de l'ONU). Autrement dit, cinquante ans après la Déclaration universelle des droits de l'homme, et au terme de vingt ans de négociations sur le projet de déclaration sur les défenseurs des droits humains, les Nations unies ont finalement reconnu ce qui est une réalité, c'est-à-dire que des milliers de personnes militent pour les droits humains et contribuent à les défendre de par le monde. Il s'agit d'une déclaration exhaustive qui honore le nombre et la diversité des personnes qui font avancer et défendent les droits humains.

Le représentant spécial du Secrétaire général des Nations unies sur la situation des défenseurs des droits de l'homme a pour mandat de "recueillir, recevoir, étudier et répondre aux informations sur la situation et les droits de toute personne, militant individuellement ou en groupe, pour faire avancer et défendre les droits humains et les libertés fondamentales".

Les lignes directrices de l'Union Européenne (UE) sur les défenseurs des droits humains (2004) ont non seulement intégré la déclaration des Nations Unies sur les défenseurs des droits humains dans son intégralité mais ont de plus effectué des recommandations spécifiques à l'égard États membres (EM) de l'UE.

Le travail des défenseurs des droits humains est légal et légitimé par les communautés internationales et nationales. PI souscrit à la définition d'un défenseur des droits humains telle qu'elle est précisée dans la déclaration des Nations unies sur les défenseurs des droits humains et réitérée dans les lignes directrices de l'UE sur les défenseurs des droits humains:

> "Le terme 'défenseur des droits humains' est utilisé pour décrire des personnes qui, individuellement ou en collaboration avec d'autres personnes, agissent pour promouvoir ou protéger les droits humains. Les défenseurs des droits humains se définissent en premier lieu par leurs actions et c'est par la description de leurs actions et d'une partie des contextes dans lesquels ils opèrent que le terme est expliqué de la meilleure manière."[5]

(voir l'annexe à la fin du manuel pour plus de renseignements sur la déclaration des NU sur les DDH et sur les lignes directrices de l'UE sur les DDH).

[5] Défenseurs des droits humains: Protéger le Droit de défendre les droits humains. Fact Sheet 29. www.unhchr.ch

Qui est responsable de la protection des défenseurs des droits humains?

La déclaration sur les défenseurs des droits humains souligne que c'est l'État qui est responsable au premier chef de la protection des défenseurs des droits humains. Elle reconnaît aussi "le travail précieux des individus, groupes et associations dans leur contribution à l'élimination réelle de toute violation des droits humains et des libertés fondamentales" et "le lien qui existe entre la paix et la sécurité internationales, et la jouissance des droits humains et des libertés fondamentales."

Cependant, selon Hina Jilani, ex représentante spéciale du Secrétaire général des Nations unies sur les défenseurs des droits humains,[6] "dénoncer les violations des droits humains et exiger réparation dépend largement du degré de sécurité dont jouissent les défenseurs des droits humains."[7] Il suffit de regarder n'importe quel rapport sur les défenseurs des droits humains à travers le monde pour découvrir des cas de torture, de disparitions, d'assassinats, de menaces, de vols, d'effractions dans les bureaux, de harcèlements, de détentions illégales, d'activités d'espionnage et de surveillance, etc. Malheureusement, c'est le lot quotidien des défenseurs et non un cas isolé.

Lectures supplémentaires conseillées

Pour en savoir plus sur les défenseurs des droits humains, cliquez sur:

- www.unhchr.ch/defender/about1.htm (Le bureau du Haut Commissaire des Nations unies aux droits de l'homme).
- www.protectionline.org (Protection International).
- L'observatoire pour le respect des défenseurs des droits humains, projet conjoint de la fédération internationale sur les droits humains (FIDH; www.fidh.org) et de l'organisation mondiale contre la torture (OMCT; www.omct.org).
- Amnesty International sur: www.amnesty.org et http://web.amnesty.org/pages/hrd-index-eng
- www.ishr.ch, sous HRDO (le bureau des défenseurs des droits humains du service international pour les droits humains de Genève).
- www.frontlinedefenders.org (Front Line, The International Foundation for Human Rights Defenders - Fondation internationale pour les DDH).

Pour plus d'informations sur les instruments juridiques internationaux en vigueur et la déclaration sur les défenseurs des droits humains de l'ONU, cliquez sur:

- www.unhchr.ch: le site internet du Bureau du Haut Commissaire des Nations unies aux droits de l'homme.
- www.protectionline.org (Protection International).
- www.ishr.ch/index.htm (Service international pour les droits humains, Genève), pour un recueil des instruments régionaux et internationaux relatifs à la protection des défenseurs des droits humains.

6 Margaret Sekaggya (Ouganda) a succédé à Hina Jilani en 2008 en qualité de Rapporteur Spécial sur la situation des DDH, nommée par le Conseil de l'ONU des Droits de l'Homme.

7 Rapport sur les défenseurs des droits humais, 10 sept. 2001 (A/56/341)

Première Partie

Risque, Évaluation des Menaces et Outils Méthodologiques

Introduction:

Dans la première partie de ce manuel, nous aborderons les concepts fondamentaux de sécurité, quelques outils pratiques et des approches de sécurité quant à certains cas spécifiques.

Ces concepts devront tous être intégrés au plan de sécurité et au manuel de sécurité de l'organisation.

Contenu de la première partie:

1.1 Prendre des décisions fondées de sécurité et de protection

1.2 Évaluer les risques

1.3 Comprendre et évaluer les menaces

1.4 Incidents de sécurité: définition et analyse

1.5 Prévenir les agressions et y réagir

1.6 Élaborer une stratégie de sécurité globale

1.7 Préparer un plan de sécurité

1.8 Améliorer la sécurité au travail et au domicile

1.9 La sécurité et les femmes défenseurs des droits humains

1.10 La sécurité dans les zones de conflits armés

1.11 Sécurité, communication et technologie de l'information

CHAPITRE 1.1

Prendre des décisions fondées de sécurité et de protection

Objectifs

Prendre conscience de l'importance d'une analyse de votre contexte de travail pour des raisons de sécurité

Apprendre différentes méthodes pour effectuer les analyses du contexte et des parties prenantes

Contexte de travail des défenseurs des droits humains

Les défenseurs des droits humains travaillent en général dans des cadres complexes, où interagissent des protagonistes variés qui sont influencés par des procédures décisionnelles profondément politiques. Beaucoup d'événements se déroulent simultanément et chaque événement a une répercussion sur un autre. L'évolution de chaque acteur, ou partie prenante, aura un impact important sur ses relations avec les autres acteurs, ou partie prenante. Les défenseurs des droits humains ont donc besoin d'informations non seulement sur les questions relatives à leurs actions mais aussi sur les fonctions des principaux acteurs et des parties prenantes.

Un premier exercice simple serait de mettre en place un groupe de réflexion afin d'essayer d'identifier et d'établir une liste de tous les acteurs sociaux, politiques et économiques qui pourraient éventuellement influencer les conditions de sécurité dans lesquelles vous évoluez.

Analyse du contexte de travail

Il est très important de connaître et de comprendre autant que possible le contexte dans lequel vous travaillez. Une bonne analyse du contexte permet de prendre des décisions en connaissance de cause sur les règles ou procédures de sécurité à adopter. Il est aussi important d'imaginer d'éventuels scénarios pour prendre des mesures préventives lorsque cela est possible.

Cependant, une simple analyse des conditions de travail ne suffit pas. Il faut aussi penser à la façon dont chaque intervention peut influencer la situation ainsi qu'à la réaction de chaque intervenant. Il est important de considérer l'étendue

d'un espace de travail. Vous pouvez mener une analyse de la situation d'ensemble en étudiant un pays ou une région, cependant il vous faut par la même occasion comprendre comment ces dynamiques globales fonctionnent à l'intérieur de la zone plus spécifique dans laquelle vous travaillez, c'est-à-dire les dynamiques à petite échelle. Par exemple, les forces paramilitaires d'une zone spécifique peuvent agir bien différemment de ce que faisait apparaître votre analyse de la région ou du pays. Vous devez connaître ces caractéristiques particulières. Il est également crucial d'éviter d'avoir une idée arrêtée du contexte de travail puisque les situations évoluent et changent. Les analyses devraient ainsi être revues régulièrement.

Poser des questions, analyser les forces en présence et **analyser les parties prenantes** constituent trois méthodes utiles pour l'analyse du contexte de travail.

Poser des questions

Vous pouvez mieux comprendre votre contexte de travail en vous posant simplement les bonnes questions. Il s'agit-là d'un moyen utile qui entraîne des discussions en petit groupe, mais qui ne peut fonctionner que si les questions sont formulées de manière à trouver facilement une solution.

Prenons, par exemple, le problème du harcèlement par les autorités locales. Si vous formulez votre question de cette façon: "que pourrait-on faire pour réduire ce harcèlement?", il se peut que la réponse obtenue ne soit qu'une solution à un symptôme: c'est-à-dire au harcèlement.

Par contre, si vous formulez la question de façon à l'orienter vers une solution, il se peut que vous trouviez une vraie solution. Par exemple, si votre question est: "notre cadre sociopolitique est-il assez sûr pour travailler?", le nombre de réponses est ainsi limité au nombre de deux: un oui ou un non.

Si la réponse est oui, alors d'autres questions seront nécessaires pour identifier et comprendre les éléments cruciaux en jeu pour le maintien de la sécurité. Si, après avoir longuement considéré toutes les activités possibles, tous les projets et toutes les informations, et après avoir étudié la législation, les négociations possibles et fait des comparaisons avec d'autres défenseurs des droits humains de la région, etc., la réponse est non, alors vous aurez-là une solution à votre problème de sécurité.

Mettre en pratique la méthode des questions:

- Cherchez des questions qui vous aideront à identifier et à comprendre les éléments cruciaux en jeu pour le maintien de votre sécurité.
- Formulez des questions privilégiant la solution.
- Répétez ce processus autant de fois que possible (en créant une discussion).

Questions utiles à poser:

- Quels sont les problèmes majeurs en jeu dans l'arène sociopolitique et économique?
- Qui sont les principaux acteurs liés à ces problèmes majeurs?

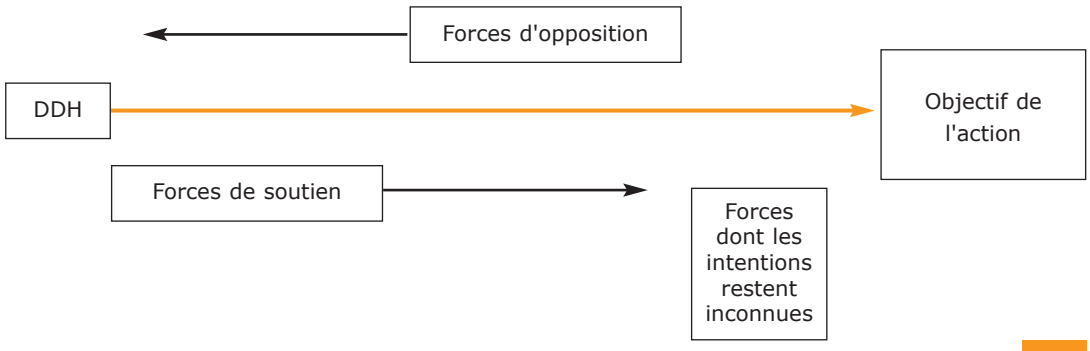
- Comment nos actions peuvent-elles influencer de manière positive ou négative les intérêts de ces acteurs principaux?
- Quelle serait notre réaction si nous devenions, à cause de nos actes, la cible d'un de ces protagonistes?
- Notre cadre sociopolitique est-il assez sûr pour nous permettre de mener nos actions à bien?
- Comment les autorités locales ou nationales ont-elles réagi face à des actions similaires d'autres défenseurs des droits humains?
- Quelle fut la réaction des principales parties prenantes face aux activités précédentes ou similaires des défenseurs des droits humains ou d'autres personnes dans le même domaine?
- Comment les médias et la communauté ont-ils réagi dans des circonstances identiques?
- Etc.

Analyse des forces en présence

L'analyse des forces en présence est une technique qui permet d'identifier visuellement comment les différentes forces favorisent ou empêchent la réussite des actions. Elle identifie les forces de soutien et d'opposition et elle suppose que des problèmes de sécurité sont induits par les forces d'opposition, et que vous pouvez tirer profit des forces de soutien. Cette technique peut être appliquée par une seule personne, cependant elle est plus efficace lorsqu'elle est utilisée par un groupe diversifié avec un objectif de travail clairement défini ainsi qu'une méthode pour y parvenir.

Commencez par tracer une flèche horizontale pointant vers une case (c'est vous, en déplacement vers votre objectif). Dans cette case, résumez l'objectif de l'action. Vous obtenez ainsi un point de référence permettant l'identification des forces de soutien et d'opposition. Dessinez ensuite une autre case au-dessus de la flèche centrale. Faites la liste de toutes les forces éventuelles qui pourraient vous empêcher d'atteindre votre objectif dans cette case. Dessinez une case identique pour les forces éventuelles de soutien au-dessous de la flèche. Pour finir, tracez une case contenant les forces dont les intentions restent incertaines ou méconnues.

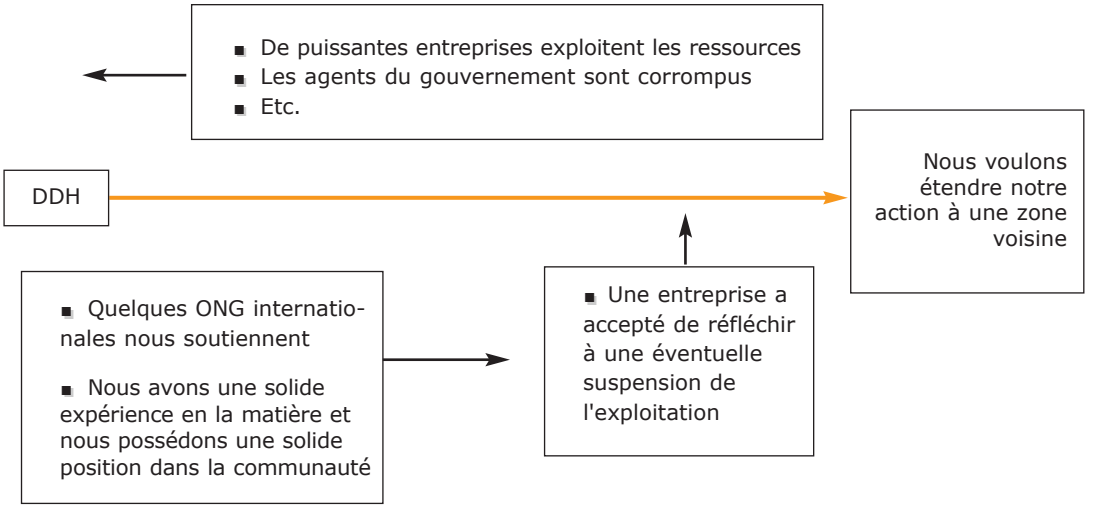
Schéma 1: Analyse des forces en présence pour faire le point sur le contexte de travails



Après avoir réalisé le schéma, il convient d'évaluer les résultats. L'analyse des forces opérationnelles vous aide à visualiser clairement les forces auxquelles vous avez affaire. Le but est de trouver des solutions pour éliminer ou réduire les risques générés par les forces d'opposition, en partie grâce à l'aide éventuelle des forces de soutien. En ce qui concerne les forces aux intentions inconnues, vous devrez décider de si tenter de les rallier à votre cause ou de les surveiller constamment afin de déceler les signes d'une opposition ou d'un soutien.

Par exemple:

Imaginez que vous appartenez à une organisation s'occupant du droit des populations autochtones d'accéder aux ressources naturelles de leur pays. Nombre de conflits existent entre les différents acteurs qui se disputent l'exploitation de ces mêmes ressources. Vous voulez à présent étendre votre action à une zone voisine où les problèmes sont similaires



Analyse des acteurs (ou des parties prenantes)

L'analyse des parties prenantes représente un moyen important pour disposer de davantage d'informations lors de la prise de décision sur la protection. Cela suppose d'identifier et de décrire les différentes parties prenantes impliquées et les rapports entre elles, leurs caractéristiques et leurs intérêts en jeu dans le problème de protection en question.

Est considérée comme partie prenante à la protection toute personne, groupe ou institution qui a un intérêt, ou qui est impliqué dans le résultat d'une politique de protection.[8]

8 Adaptation des *Sustainable Livelihoods Guidance Sheets* No.5.4 (2000).

Les parties prenantes en matière de protection peuvent être classées de la façon suivante:

Les **parties prenantes principales**. Dans un contexte de protection, il s'agit des **défenseurs des droits humains eux-mêmes**, et de **ceux avec qui ou pour qui ils travaillent**, puisqu'ils ont tous un intérêt primordial dans leur propre protection.

Les **détenteurs des obligations, qui sont responsables de la protection des défenseurs des droits humains**, comme par exemple:

- Les gouvernements ou les institutions de l'État (y compris les forces de sécurité, les juges, les législateurs…).
- Les organes internationaux dotés d'un mandat de protection, comme les organes de l'ONU, les forces de maintien de la paix, les organisations intergouvernementales régionales, etc.
- Les acteurs armés de l'opposition (ils sont tenus de ne pas attaquer les défenseurs des droits humains -en leur qualité de civils-, plus particulièrement lorsque ces acteurs contrôlent le territoire).

Les parties prenantes-clés, qui influencent d'une manière significative la protection des défenseurs des droits humains. Elles peuvent avoir une influence politique ou la capacité d'exercer une pression sur les détenteurs d'obligations qui ne remplissent pas leurs responsabilités (comme les gouvernements, les organes des Nations Unies etc.) et en retour quelques-uns d'entre eux peuvent être de près ou de loin impliqués dans des agressions ou des pressions à l'encontre des défenseurs des droits humains (comme les entreprises privées, les médias ou les autres gouvernements, etc.). Tout dépend du contexte, des intérêts et des stratégies de chacune de ces parties prenantes-clés. Une liste non exhaustive peut inclure:

- Les organes des Nations Unies (autres que ceux ayant un mandat "Protection des défenseurs des droits humains").
- Le CICR (le comité international de la Croix Rouge).
- Les autres gouvernements et institutions multilatérales (à la fois les donateurs et les décideurs).
- Les autres acteurs armés.
- Les ONG (nationales ou internationales).
- Les églises et institutions religieuses.
- Les entreprises privées.
- Les médias.

Lors de la mise au point de stratégies et d'actions, l'une des difficultés majeures relève du fait que les relations entre ces différentes parties prenantes ne sont pas explicites, voire parfois inexistantes. De plus, nombre de détenteurs d'obligations, et plus particulièrement les gouvernements, les forces de sécurité et les forces armées de l'opposition, créent ou contribuent aux violations des droits de l'homme et à une absence de protection des défenseurs des droits humains. En outre, certaines parties prenantes, qui partagent en principe les mêmes préoccupations de protection, peuvent avoir des conflits d'intérêts, comme d'autres gouvernements, des organes de l'ONU et des ONG. Ces facteurs, aux côtés de facteurs inhérents aux scénarios de conflit, esquissent une vision d'ensemble complexe du contexte de travail.

Analyse des parties prenantes, des structures et procédures changeantes

Les parties prenantes **ne sont pas** des acteurs **statiques**. Elles entretiennent des rapports entre elles à différents niveaux, ce qui engendre un réseau dense de relations. Il est important de faire attention à ces relations qui forment et transforment les besoins de protection des individus.

Les structures sont étroitement liées au secteur public, à la société civile ou aux organes privés. On s'y intéressera du point de vue de la protection. À l'intérieur du secteur public, le gouvernement peut être envisagé comme un ensemble d'acteurs avec, soit une stratégie unique, soit des stratégies internes divergentes. Par exemple, des différences d'opinion peuvent apparaître entre le ministre de la Défense et celui des Affaires Etrangères lorsqu'ils discutent des mesures politiques relatives aux défenseurs des droits humains, ou entre le bureau de l'ombudsman (protecteur du citoyen) et l'armée. Les structures peuvent comporter des constituants variés; par exemple, le cas d'une commission intersectorielle (composée de membres du gouvernement, d'ONG, de l'ONU et du corps diplomatique) créée pour suivre la situation de protection d'une organisation spécifique de défenseurs des droits humains.

Les procédures sont les chaînes de décisions et d'actions prises par une ou plusieurs structures dont l'objectif est d'améliorer la situation en matière de protection d'un groupe précis. Les procédures peuvent être juridiques, culturelles et politiques. Toutes les procédures ne permettent pas d'obtenir une amélioration de la protection. À plusieurs occasions les procédures de protection peuvent être contradictoires ou s'annuler. Par exemple, les personnes supposées être sous protection peuvent ne pas vouloir accepter une procédure de protection politique proposée par le gouvernement qu'elles considèrent comme une manœuvre déguisée pour les déplacer. L'ONU et les ONG peuvent apporter leur appui à ces personnes lors de cette procédure.

L'analyse des parties prenantes est essentielle pour comprendre:

- Qui peut être considéré comme partie prenante et dans quelles circonstances sa participation intervient.
- Les liens entre les parties prenantes et la protection, leurs caractéristiques et leurs intérêts.
- Comment seront-elles concernées par les activités de protection?
- La volonté de chaque partie prenante à prendre part à ces activités de protection.

Il existe différentes méthodes pour faire l'analyse des parties prenantes. La suivante adopte une méthodologie directe, source de bons résultats dans l'analyse et dans les procédures de décision.

Lors de l'évaluation des processus de protection, il est important de s'accorder un temps de réflexion et d'avoir en tête les intérêts et les objectifs des parties prenantes impliquées.

Analyse des parties prenantes en quatre étapes:

1. Identifiez le contexte plus large de protection, par exemple la situation sur la sécurité des défenseurs des droits humains dans une région précise à l'intérieur d'un pays.

2. Qui sont les parties prenantes? (Plus précisément, quelles sont les institutions, les groupes et les individus pour qui la protection représente une responsabilité ou un enjeu?) Identifiez et faites la liste de toutes les parties prenantes liées au problème de protection, à travers des séances de réflexion ou des discussions.

3. Recherchez et analysez les caractéristiques des parties prenantes, leurs attributs particuliers, comme leurs responsabilités en matière de protection, leur influence sur les situations de protection, leurs objectifs, leurs stratégies, leur légitimité et leurs intérêts (y compris leur volonté de participer à la protection).

4. Recherchez et analysez les rapports entre les parties prenantes.

Après avoir fait cette analyse, il sera peut-être utile d'utiliser la matrice suivante:

Placez-y la liste de toutes les parties prenantes relatives à la question clairement définie de la protection (voir le schéma 2). Inscrivez cette liste des parties prenantes dans la première colonne et la première ligne du tableau. Le tableau offre ainsi deux possibilités d'analyse. Ensuite:

- Pour analyser les attributs de chaque partie prenante (objectifs, intérêts, stratégies, légitimité et pouvoir), remplissez les cases sur la diagonale formée par l'intersection de chaque partie prenante avec elle-même:

Par exemple:

Placez les objectifs, les stratégies et les intérêts des groupes d'opposition armés dans la case A.

- Pour analyser les rapports entre les parties prenantes, remplissez les cases qui définissent les relations les plus importantes en matière de sécurité. Par exemple, dans la case B, les relations entre l'armée et le Haut Commissaire aux réfugiés des Nations unies se rejoignent, et ainsi de suite.

Après avoir rempli les cases les plus pertinentes, vous obtiendrez une vue d'ensemble des objectifs, des stratégies, des intérêts et de l'interaction entre les principales parties prenantes à l'égard du problème de protection.

Schéma 2: Système de matrice pour l'analyse des parties prenantes

	Gouvernement	Armée	Police	Groupes d'opposition armés	ONG nationales de droits humains	Églises	Autres gouvernements	Agences de l'ONU	ONG internationales
Gouvernement	Partie prenante								
Armée		Partie prenante							
Police			Partie prenante						
Groupes d'opposition armés									
ONG nationales de droits humains					Partie prenante				
Églises						Partie prenante			
Autres gouvernements							Partie prenante		
Agences de l'ONU								Partie prenante	
ONG internationales									Partie prenante

A

B

Case **A**

Pour chaque partie prenante:

- Leurs objectifs et leurs intérêts
- Leurs stratégies
- Leur légitimité
- Leur pouvoir

Case **B**

Relations entre parties prenantes:

Relations en rapport avec la question de protection et en rapport avec les intérêts stratégiques pour chaque partie prenante.

En résumé

- Tous les défenseurs des droits humains sont exposés à des risques.
- Les défenseurs des droits humains ne sont pas égaux face aux risques.
- Les risques dépendent du contexte politique.
- Le contexte politique change, il est dynamique.
- Par conséquent, le risque est dynamique.

Ceci est l'hypothèse sur laquelle nous basons l'importance de découvrir des informations-clé en se posant les bonnes questions.

Ensuite, schématisez et analysez les parties prenantes avec toutes leurs composantes jusqu'à leurs éléments constitutifs les plus profonds.

Déterminez comment elles interagissent toutes au vu des questions de sécurité et comment ces dernières ont un rapport aux enjeux stratégiques des parties prenantes.

Trouvez des intérêts convergents et divergents, des alliances, des méthodes opérationnelles, etc.

Observez quelles sont les structures sous-jacentes et les processus.

Vous serez en mesure de déterminer les différentes forces (d'opposition, de soutien et celles dont les intentions sont inconnues).

Mettre en application les points cités ici exige sans doute un effort la première fois. Par la suite, si votre analyse est actualisée régulièrement, cela devient beaucoup plus facile.

Ceci vous aidera à prendre des décisions fondées en matière de sécurité et de protection.

CHAPITRE 1.2

Évaluer les risques: les menaces, les vulnérabilités et les capacités

Objectifs:

Comprendre les concepts de menace, de vulnérabilité et de capacité en terme de sécurité

Apprendre à évaluer un risque

L'analyse des risques et les besoins de protection

Le travail des défenseurs des droits humains peut avoir des répercussions négatives sur les intérêts d'acteurs spécifiques, ce qui en retour peut mettre le défenseur en danger. Il est donc important de souligner que, dans certains pays, **le risque fait partie du quotidien des défenseurs.**

La question du risque peut se découper de la façon suivante:

> Analyser les principaux intérêts et stratégies des parties prenantes ⇨ Évaluer l'impact des actions des défenseurs des droits humains sur ces intérêts et stratégies ⇨ Évaluer les menaces contre les défenseurs des droits humains ⇨ Évaluer les vulnérabilités et capacités des défenseurs des droits humains ⇨ Établir le risque.

En d'autres termes, votre activité de défenseur peut vous exposer à un risque plus élevé.

- **L'objet** de votre activité peut engendrer des menaces
- Le **lieu**, le **moment** et la **manière** d'exercer votre activité soulèvent la question de vos vulnérabilités et capacités.

Il n'y a pas de définition largement acceptée du terme "risque"; cependant, on peut dire que le risque renvoie aux événements potentiels, quoique incertains, pouvant porter préjudice.

Dans quelque circonstance que ce soit, toute personne travaillant sur les droits humains peut être exposée à un certain risque. Cependant, tous les défenseurs ne sont pas également vulnérables du fait qu'ils se trouvent au même endroit. La vulnérabilité, la possibilité qu'un défenseur ou qu'un groupe soient victimes d'une agression, varie suivant plusieurs facteurs, comme nous allons le voir maintenant.

Exemple:

Il existe des pays dans lesquels le gouvernement constitue une menace générale pour n'importe quelle action des défenseurs. Cela signifie que tout défenseur est susceptible d'être en danger. De plus, certains défenseurs sont plus confrontés au danger que d'autres. Par exemple, une grande ONG, bien établie et située dans la capitale du pays, ne devrait pas être aussi vulnérable qu'une petite ONG locale. Cela semble aller de soi, mais il peut s'avérer intéressant d'en connaître les raisons afin de mieux comprendre et de mieux répondre aux problèmes de sécurité des défenseurs.

Le niveau de risque auquel doivent faire face les défenseurs augmente avec les **menaces** reçues, leurs **vulnérabilités** et leurs **capacités** face à ces menaces, comme le présente l'équation[9] suivante:

$$\textbf{RISQUE} = \frac{\textbf{MENACES} \quad \textbf{X} \quad \textbf{VULNÉRABILITÉS}}{\textbf{CAPACITÉS}}$$

On entend par menaces la possibilité que quelqu'un porte atteinte à l'intégrité physique, morale ou aux biens d'une autre personne par un acte délibéré et souvent violent.[10] L'évaluation d'une menace est l'analyse de la **probabilité de l'exécution** d'une menace.

Les défenseurs sont confrontés à différentes menaces dans un scénario de conflits, notamment au ciblage, aux crimes de droit commun et aux menaces indirectes.

Le type le plus commun de menace, le ciblage, vise à entraver le travail d'un groupe ou à le modifier, ou encore à influencer les comportements des personnes concernées. Les menaces de ciblage sont en général étroitement liées au travail des défenseurs en question, tout comme aux intérêts et besoins des personnes opposées au travail des défenseurs.

Les **menaces inhérentes à la situation de conflit** sont notamment constituées par le fait:

- De se trouver dans des **zones de combat de conflits armés** ('être au mauvais endroit au mauvais moment').

Résumé des différents types de menaces:

- Le ciblage (menaces directes, déclarées ou indirectes): menaces dues aux activités.
- Les menaces d'agressions criminelles ordinaires.
- Les menaces contingentes: dues au fait de travailler dans des zones de conflits armés.

[9] Adapté de *Van Brabant* (2000) et REDR.
[10] Dworken (1999).

- D'être exposé à des **agressions de droit commun** (cachant souvent une agression politique) surtout si le travail des défenseurs les mène dans des zones à risque. Mais attention, beaucoup de cas de ciblage sont effectués sous couvert d'incidents criminels 'ordinaires'.

Le ciblage (menaces ciblées) peut, lui aussi, être nuancé: Les défenseurs des droits humains peuvent être sujets à des menaces **directes (déclarées)**, par exemple lorsqu'ils reçoivent des menaces de mort (voir le chapitre 3 sur l'évaluation des menaces ouvertes). Il y a aussi des cas de menaces **indirectes**, par exemple lorsqu'un défenseur proche de vous a été menacé et que tout porte à croire que vous serez la prochaine personne à être menacée.

Les vulnérabilités

La vulnérabilité est le degré d'exposition à une perte, un dommage, une souffrance ou une mort en cas d'agression. Cela peut varier d'un défenseur à un autre, et changer avec le temps. La vulnérabilité est toujours relative, parce que toutes les personnes et les groupes sont vulnérables dans une certaine mesure. Cependant, chacun a son propre degré et type de vulnérabilité, selon les circonstances. Voici quelques exemples:

- La vulnérabilité est pour partie liée à la situation géographique: un défenseur est plus vulnérable par exemple lorsqu'il ou elle se trouve en mission sur le terrain que lorsqu'il ou elle se trouve dans un bureau bien connu où il est fort probable que des témoins assistent à l'agression.
- La vulnérabilité peut comprendre l'absence d'accès à un téléphone, à un transport sûr ou à de bons verrous sur les portes d'une maison. Mais les vulnérabilités sont aussi liées à l'absence de contacts et de solutions partagées entre défenseurs.
- La vulnérabilité peut avoir un lien avec le travail en équipe et la peur: un défenseur qui reçoit une menace peut avoir peur et son travail peut en être affecté. Si cette personne n'a pas les moyens de faire face à cette peur (quelqu'un à qui parler, une équipe de bons collègues…) alors elle prendra peut-être des décisions ou fera des erreurs qui l'exposeront à encore plus de problèmes de sécurité.

(Vous trouverez une liste des vulnérabilités potentielles et des capacités à la fin de ce chapitre.)

Les capacités

Les capacités sont les forces et les ressources auxquelles un groupe ou un défenseur peut avoir accès pour mettre en place un niveau raisonnable de sécurité. Des exemples de capacités pourraient être la formation à des questions de sécurité ou des sujets juridiques, un groupe travaillant en équipe, l'accès à un téléphone et à des moyens de transport sûrs, à de bons réseaux de défenseurs et à une bonne stratégie pour faire face à la peur, etc.

Dans la plupart des cas, les vulnérabilités et les capacités correspondent aux deux faces d'une même médaille.

Exemple:

Ne pas connaître suffisamment son travail et le contexte de travail engendre une vulnérabilité, tandis que la connaissance de ceux-ci constitue une capacité. Idem lorsqu'on a accès ou non à des moyens de transport sûrs ou qu'on a affaire à de bons réseaux de défenseurs.

Cependant, le comportement est un facteur déterminant.

Exemple:

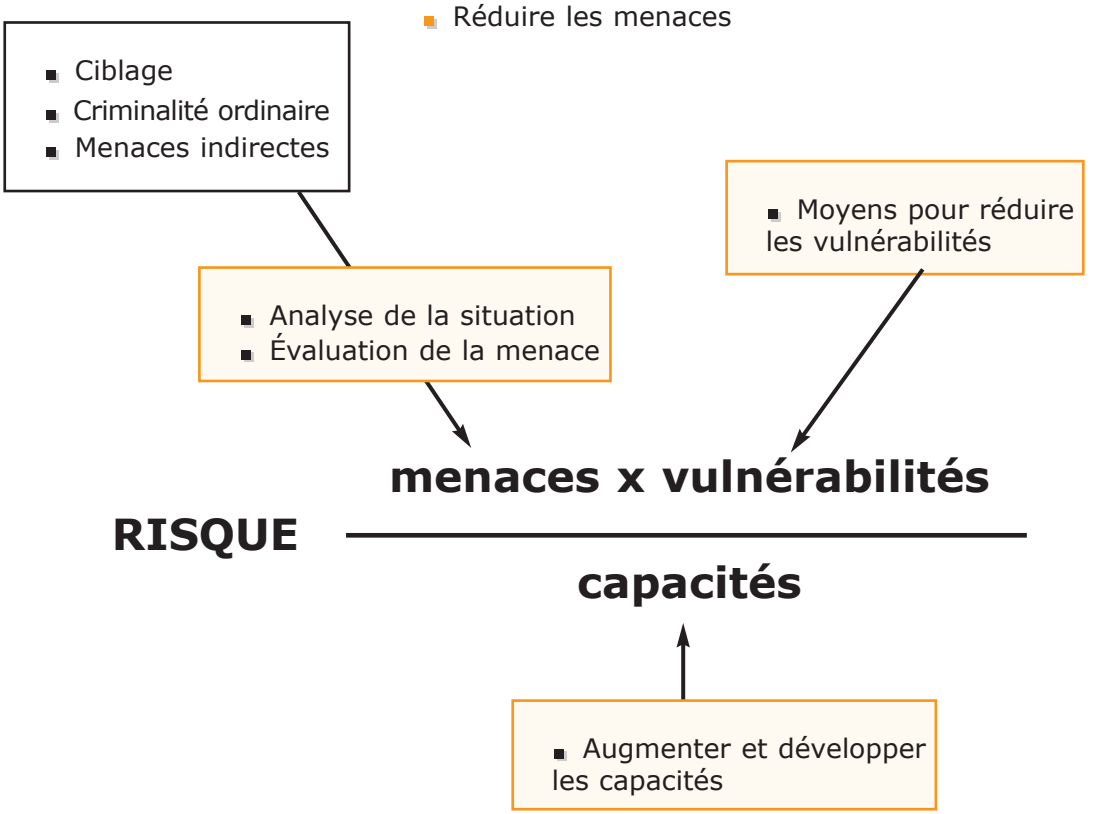
Disposer d'un téléphone peut potentiellement constituer à la fois une vulnérabilité et une capacité, selon l'usage qui en est fait. Si on l'utilise sans discrétion et que des informations confidentielles sont communiquées à haute voix, c'est une vulnérabilité. S'il est utilisé avec discrétion et que les informations confidentielles sont codées, c'est une capacité.

(À la fin de ce chapitre se trouve une liste de vulnérabilités et de capacités potentielles)

En résumé

afin de réduire le danger à des niveaux acceptables et d'assurer la protection, vous devez:

- Réduire les facteurs de vulnérabilité
- Augmenter les capacités de protection
- Réduire les menaces



Le risque est un concept dynamique qui varie avec le temps et avec les changements de nature des menaces, des vulnérabilités et des capacités. Cela signifie que le risque doit être évalué périodiquement, particulièrement si votre contexte de travail, les menaces ou les vulnérabilités changent. Par exemple, les vulnérabilités peuvent augmenter si un changement de direction met le groupe de défenseurs dans une position plus faible qu'avant. Le risque s'accroît de façon dramatique lorsque la menace est précise et réelle; dans une telle situation, il n'est pas prudent d'essayer de réduire le risque en augmentant les capacités puisque cela prend du temps.

Prendre des mesures de sécurité, telles qu'effectuer des formations juridiques ou poser des barrières de protection, peuvent réduire le risque en réduisant les facteurs de vulnérabilité. Cependant, de telles mesures ne s'attaquent pas à la source principale de risques, les menaces, ni à la volonté de les mettre à exécution, surtout dans des situations où les exécutants savent qu'ils ne courent pas le risque d'être punis. Toutes les interventions majeures en terme de protection devraient donc viser à réduire les menaces, tout en réduisant les vulnérabilités et en augmentant les capacités.

Exemple:

Un petit groupe de défenseurs travaille sur des questions de propriété terrienne dans une ville quelconque. Lorsque leur travail commence à affecter les intérêts des propriétaires locaux, ces défenseurs reçoivent des menaces de mort très claires. Si vous appliquez l'équation du risque à leur situation de sécurité, vous remarquerez que le risque encouru par les défenseurs est très élevé, en premier lieu à cause de cette menace de mort. Si vous voulez réduire ce risque il est probable que ce ne soit pas le moment voulu pour commencer à changer les verrous de la porte d'un bureau (puisque le risque ne provient pas d'une effraction éventuelle dans le bureau), ni le moment pour acheter un téléphone portable à chaque défenseur (même si communiquer représente une importante question de sécurité, il est presque certain qu'un téléphone ne soit pas suffisant lorsque quelqu'un a décidé de vous tuer). Dans ce cas précis, une stratégie plus adéquate serait d'établir des contacts et d'obtenir des réponses politiques afin de faire face directement à la menace (et si cela s'avère ne pas être une réponse efficace rapide, la meilleure solution est de réduire l'exposition au risque des défenseurs, peut-être par un déplacement provisoire. Être capable de se déplacer vers un endroit sûr constitue une capacité).

Prendre une telle décision et la réaliser suppose la capacité psychosociale du défenseur à considérer que battre en retraite n'équivaut pas à de la lâcheté ou à une défaite... Se retirer peut permettre la réflexion et la reprise du travail dès que le défenseur sera mieux équipé.

Les vulnérabilités et les capacités, tout comme certaines menaces, peuvent varier selon le genre et l'âge. À vous d'effectuer vos recherches en conséquence.

Évaluation des vulnérabilités et des capacités

Analyser les vulnérabilités et les capacités d'un groupe particulier (ou d'une personne) exige que le groupe se définisse lui-même (en tant que communauté, coopérative, ONG, individus, etc.), et qu'il définisse la région physique où il opère et la période concernée (votre profil de vulnérabilité évoluera et changera au cours du temps). Pour faire l'analyse des vulnérabilités et des capacités dans les grandes lignes, utilisez le **tableau 3** à la fin de ce chapitre.

À noter: cette analyse doit être vue comme une activité régulière permettant de se baser sur les informations existantes pour connaître précisément une situation en constante évolution. Lors de l'analyse des capacités, il faudrait d'abord dresser l'inventaire des capacités réelles à un moment donné pour dégager les capacités potentielles et souhaitables. Par la suite, vous devrez mettre en place un processus pour les acquérir.

Tableau 3:

Informations nécessaires à l'évaluation des vulnérabilités et des capacités d'un groupe.

(À noter: en règle générale, l'information contenue dans la colonne de droite montre soit une vulnérabilité soit une capacité de chaque composant)

Vulnérabilités et capacités	Informations nécessaires à l'analyse des vulnérabilités ou capacités des défenseurs pour chacun des composants
Composants liés à des aspects géographiques, physiques et techniques	
L'exposition	Besoin de rester ou de circuler dans des zones dangereuses comprenant des acteurs menaçants, dans le cadre d'activités quotidiennes ou occasionnelles.
Les structures physiques	Les caractéristiques des bâtiments (bureaux, maisons, refuges...); matériaux de construction, portes, fenêtres, pla-cards. Barrières de protection. Veilleuses / Eclairage?
Les bureaux et locaux ouverts au public	Bureaux ouverts au grand public? Existe-t-il des zones strictement réservées au personnel? A-t-on affaire à des visiteurs inconnus?
Les lieux de refuge et itinéraires de fuite	Y-a-t-il des endroits pour vous cacher? Sont-ils faciles d'accès (distance physique) et qui y a accès (individus spécifiques ou groupe entier)? Est-il possible de quitter la région si nécessaire?
L'accès à la région	Quelle est la difficulté pour les visiteurs extérieurs (fonctionnaires du gouvernement, ONG etc.) d'accéder à cette région, par exemple dans un voisinage dangereux? Quelle est la facilité d'accès pour les agresseurs potentiels?
Le transport et le logement	Les défenseurs ont-ils accès à des moyens de transport sûrs (publics ou privés)? Est-ce que ceux-ci ont des avantages ou des inconvénients particuliers? Les défenseurs ont-ils accès à des logements sûrs lorsqu'ils voyagent?
Les communications	Existe-t-il des réseaux dec ommunication en place (radio, téléphone)? Les défenseurs y ont-ils un accès facile? Ces réseaux fonctionnement-ils correctement en permanence? Peuvent-ils être coupés par les auteurs des menaces avant une agression?

Composants liés au conflit	
Liens avec les parties en conflit	Les défenseurs ont-ils des liens avec les parties en conflit (liens de parentèle), viennent-ils de la même région, partagent-ils des mêmes intérêts? Ces liens pourraient-ils être utilisés injustement contre ces derniers?
Les activités des défenseurs affectant les parties au conflit	Le travail des défenseurs affecte-t-il directement les intérêts d'un acteur? (par exemple en défendant des ressources naturelles précieuses, le droit à la terre, ou d'autres cibles potentielles pour des acteurs puissants). Travaillez-vous sur un problème particulièrement sensible pour des acteurs puissants (comme par exemple la propriété terrienne)?
Transport d'objets et d'informations écrites	Les défenseurs des droits humains ont-ils des objets, des biens ou des informations pouvant s'avérer précieux aux yeux de groupes armés, ce qui va par conséquent accroître le risque d'être pris pour cible (essence, aide humanitaire, batteries, manuels sur les droits humains, manuels sur la santé, etc.)?
Connaissance des zones de conflit et des zones minées	Les défenseurs disposent-ils des informations sur les zones de conflit et sur les zones de sécurité pour les aider à garantir leur propre sécurité? Possèdent-ils des informations fiables sur les zones minées?
Composants liés au système judiciaire et politique	
Accès aux autorités et au système judiciaire pour revendiquer vos droits	Les défenseurs des droits humains peuvent-ils entamer des procédures judiciaires pour défendre leurs droits? (accès à une représentation juridique, présence physique aux procès ou aux entretiens, etc). Les défenseurs des droits humains peuvent-ils bénéficier d'une assistance appropriée de la part des autorités compétentes en vue de leurs actions et de leurs besoins de protection?
Capacité à obtenir des résultats du système judiciaire et des autorités	Les défenseurs des droits humains sont-ils juridiquement autorisés à revendiquer leurs droits? Sont-ils sujets à des lois nationales de répression? Peuvent-ils obtenir assez d'influence pour que les autorités prennent en compte leurs revendications?
Enregistrement, capacité de tenir des comptes et normes juridiques	Les défenseurs des droits humains se voient-ils privés d'un statut juridique ou doivent-ils se soumettre à de longs délais? Leur organisation est-elle capable de tenir des comptes et de satisfaire les normes juridiques nationales? Utilisez-vous des logiciels informatiques piratés?
Composants liés à la gestion des informations	
Sources et précision des informations	Les défenseurs possèdent-ils des informations fiables sur lesquelles ils peuvent baser leurs accusations? Les défenseurs rendent-ils publique l'information avec la précision et les méthodes nécessaires?
Garder, envoyer et recevoir des informations	Les défenseurs ont-ils la possibilité de garder les informations dans des lieux sûrs? Ces informations pourraient-elles être volées? Ces informations sont-elles protégées d'éventuels virus et de pirates de l'informatique? Pouvez-vous envoyer et recevoir des informations en toute sécurité? Les défenseurs sont-ils capables de distinguer différents degrés de confidentialit? Les défenseurs ont-ils des informations les uns sur les autres en dehors des heures de travail?

Être témoin ou détenir des informations essentielles	Les défenseurs sont-ils des témoins cruciaux dans des affaires qui mettent en cause des acteurs puissants? Les défenseurs ont-ils des informations pertinentes et uniques sur une affaire ou une procédure particulière?
Avoir une explication cohérente et acceptable sur ses actions et ses objectifs	Les défenseurs possèdent-ils une explication claire, viable et cohérente de leurs actions et objectifs? Cette explication est-elle acceptable, ou tout au moins tolérable, pour la plupart ou toutes les parties prenantes (et tout particulièrement les groupes armés)? Tous les membres du groupe sont-ils capables de fournir cette explication lorsque c'est nécessaire - comme à un poste de contrôle par exemple?
Composants liés à des aspects sociaux et d'organisation	
Existence d'une structure de groupe	Le groupe est-il structuré ou organisé d'une façon particulière? Cette structure fournit-elle un niveau acceptable de cohésion au groupe?
Capacité à prendre des décisions communes	La structure du groupe reflète-t-elle des intérêts particuliers ou représente-t-elle l'ensemble du groupe? Est-ce que les responsabilités majeures et la prise de décision reviennent à une ou plusieurs personnes? Existe-t-il une procédure de suppléance pour la prise de décision et de responsabilités? Jusqu'à quel niveau la prise de décision reste-t-elle participative? Est-ce que la structure du groupe aboutit à: a) des prises de décision et mises en application en commun, b) la discussion des problèmes en commun, c) des réunions sporadiques et inefficaces, d) aucune des trois solutions ci-dessus?
Plans et procédures de sécurité	Existe-il des règles et procédures de sécurité en place? Existe-il une bonne compréhension et une adhésion aux procédures de sécurité? Le personnel respecte-t-il ces règles? (Pour plus de détails, consulter le chapitre 8)
Gestion de la sécurité en dehors du travail (famille et temps libre)	Comment les défenseurs emploient-ils leur temps libre (famille et passe-temps)? L'alcool et la drogue représentent de grandes vulnérabilités. Les relations sociales peuvent aussi entraîner des vulnérabilités (tout comme des atouts). À quel point les familles et les amis sont-ils impliqués dans les activités du défenseur?
Conditions de travail	Les contrats de travail sont-ils en règle pour tous? Avez-vous accès à des fonds d'urgence? A des assurances?
Recrutement du personnel	Y-a-t'il des procédures appropriées pour recruter le personnel, les collaborateurs et les membres? Y -a-t'il une procédure de sécurité spécifique pour les volontaires temporaires (tels que les étudiants, par exemple) ou visiteurs?
Travail avec des gens ou avec des organisations - interface	Le travail comprend-il des entretiens directs avec les personnes? Ces personnes, sont-elles bien connues des défenseurs/organisations? Le travail avec ses personnes se déroule-t-il en avec une organisation interface?
S'occuper des témoins et des victimes avec qui nous travaillons	Evaluez-vous le risque encouru par les victimes et les témoins, etc, est-il évalué lors de travail sur des cas précis? les défenseurs appliquent-ils des mesures de sécurité précises lorsque ils rencontrent ces personnes dans les bureaux ou à l'extérieur? S'ils sont menacés, comment doit-on réagir?
Voisinage et environnement social	Les défenseurs sont-ils bien intégrés socialement dans le voisinage? Certains groupes sociaux perçoivent-ils le travail des défenseurs positivement ou comme préjudiciable? Les défenseurs sont-ils entourés de gens potentiellement hostiles (voisins agissant comme informateurs, par exemple)? Est-ce que les voisins bien intentionnés participent au système d'alarme du défenseur?
Capacité à mobiliser	Les défenseurs sont-ils capables de mobiliser des personnes pour des actions publiques?

Composants liés à l'impact psychosocial (groupe/individus)	
Capacité à gérer le stress et la peur	Est-ce que les individus principaux, ou le groupe, ont confiance en leur travail? Les membres de la communauté/groupes expriment-ils ouvertement leur sentiment d'appartenance à un groupe et d'adhésion à des objectifs communs (à la fois à travers les mots et les actions)? Est-ce que le niveau de stress nuit à la bonne communication et aux relations entre les membres du personnel? Les gens ont-ils accès à un soutien psychologique à l'extérieur ou/et ont-ils acquis des compétences psychosociales intérieures?
Sentiments profonds de pessimisme et de persécution	Les sentiments de "déprime" et de perte d'espoir sont-ils ouvertement exprimés (à la fois à travers les mots et les actions)?
Composants liés à la société, la culture et à la religion	
Discrimination	Est-ce qu'il y a discrimination à l'encontre des défenseurs (à l'intérieur et à l'extérieur de l'organisation) en raison de leur sexe, appartenance ethnique, religion ou orientation sexuelle? Y a t-il confusion entre les droits humains, sociaux, économiques, droits à l'identité, culturelle et religieuse?
Composants liés aux ressources de travail	
Capacité à comprendre le contexte de travail et les risques	Les défenseurs ont-ils accès à des informations précises sur leurs conditions de travail, sur les parties prenantes et leurs intérêts? Sont-ils capables de traiter ces informations et d'obtenir une compréhension des menaces, des vulnérabilités et des capacités?
Capacité à définir des plans d'action	Les défenseurs peuvent-ils définir et, en particulier, mettre en place des plans d'action? Existe-il des exemples préalables?
Capacité à obtenir des conseils de sources bien informées	Est-ce que le groupe peut obtenir des conseils sûrs? De sources légitimes? Le groupe peut-il faire des choix indépendants sur les sources à utiliser? Les défenseurs ont-ils accès à des organisations particulières ou à un statut de membre qui améliore leurs capacités de protection?
Personnel et charge de travail	Est-ce que les personnes ou le personnel couvrent la masse de travail nécessaire? Peut-on planifier des visites sur le terrain en groupe (au moins deux personnes)?
Ressources financières	Dispose-t-on de moyens financiers nécessaires pour assurer la sécurité? Peut-on manier de l'argent en toute sécurité?
Connaissance des langues et des lieux	Parle-t-on les langues nécessaires au travail dans la région? A-t-on une bonne connaissance de la région? (routes, villages, téléphones publics, centres de santé, etc.)
Composant liés à des contacts nationaux et internationaux ainsi qu'aux médias	
Accès aux réseaux nationaux et internationaux	Les défenseurs ont-ils des contacts nationaux ou internationaux? Pour visiter les délégations, les ambassades, les autres gouvernements, etc? Avec les leaders des communautés, les leaders religieux, et autres personnes d'influence? Les défenseurs ont-ils accès à d'autres groupes pour publier des "actions/appels urgents"? Ont-ils accès à des organisations particulières ou à un statut de membre qui augmente les capacités de protection des défenseurs?
Accès aux médias et possibilité d'obtenir d'eux des résultats	Est-ce que les défenseurs ont accès aux médias (nationaux ou internationaux)? Aux autres médias (indépendants)? Est-ce que les défenseurs savent comment entretenir de bonnes relations avec les médias?

La balance des risques: une autre façon de comprendre le risque

Une balance fournit un autre moyen de compréhension du concept de risque. On pourrait appeler cela "le risque-mètre". Si nous prenons deux boîtes, l'une avec nos menaces et vulnérabilités et l'autre avec nos capacités, et que nous les plaçons sur les deux plateaux de la balance, on peut alors remarquer comment nos risques augmentent ou diminuent:

Fig. 1

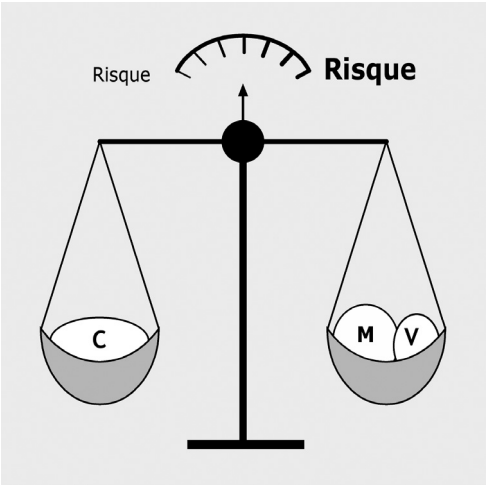
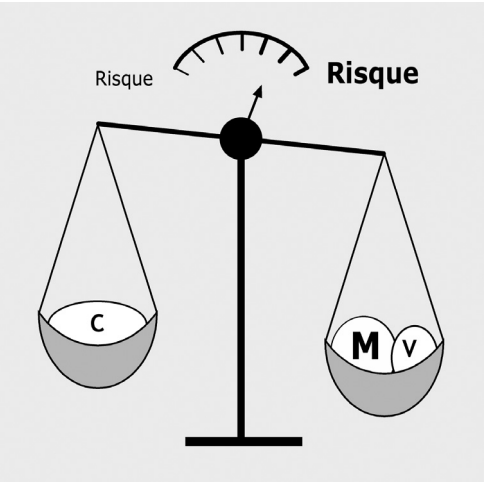
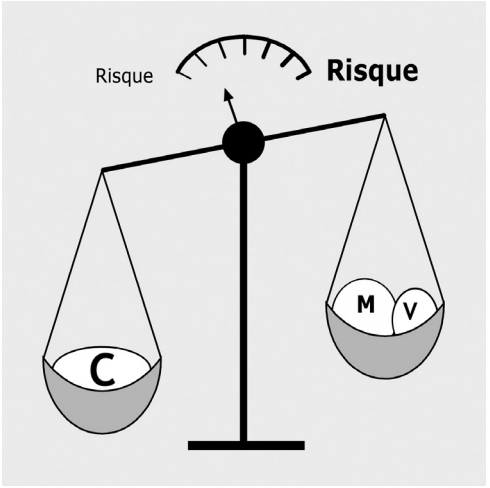


Fig. 2



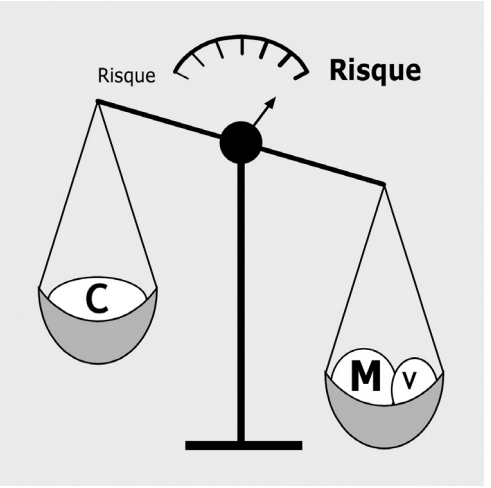
plus nous sommes confrontés à des menaces et plus nous possédons de vulnérabilités, plus le risque est grand.

Fig. 3



plus nous possédons de capacités, moins nous sommes confrontés à des risques. Afin de réduire les risques, nous pouvons réduire les menaces et nos vulnérabilités tout en augmentant nos capacités.

Fig. 4



mais… regardez ce qui arrive si nous sommes confrontés à des menaces importantes: rien ne sert d'essayer d'augmenter nos capacités à ce moment-là, la balance montrera de toute façon un niveau de risque élevé.

En résumé

$$\text{RISQUE} = \frac{\text{Menaces x Vulnérabilités}}{\text{Capacités}}$$

Les vulnérabilités et les capacités sont des variables **internes** (les défenseurs peuvent influer sur elles).

Les menaces sont des variables **externes** (A noter que des menaces peuvent être proférées même si elles ne sont pas réalisables).

1 • Influer sur la vulnérabilité et les capacités réduira la faisabilité des menaces. Faites l'inventaire de vos vulnérabilités et capacités.

2 • Différenciez-les par composants globaux puis par composants spécifiques.

3 • Fixez vos capacités souhaitables: travaillez à les atteindre et considérez le processus nécessaire à leur obtention.

Souvent, une même série d'actions peut résoudre plusieurs éléments d'un même composant.

4 • La marche à suivre ci-dessus aura comme effet une réduction de la faisabilité de la menace, et donc la réduction du risque.

Bien que certains composants puissent être liés à l'environnement, les composants peuvent être considérés comme des variables internes sur lesquels le défenseur peut influer: une zone dangereuse par exemple est bien sûr "externe" et cependant, le défenseur peut développer les compétences ("internes") pour les gérer.

Une menace est externe et quoi que l'on fasse, la personne à l'origine des menaces peut continuer à menacer. Le défenseur peut "seulement" travailler à réduire la probabilité de l'exécution de la menace sans pouvoir l'éliminer, à moins que le contexte politique ne change.

CHAPITRE 1.3

Comprendre et évaluer les menaces

Objectif:

Acquérir une connaissance approfondie des menaces et des moyens d'y réagir.

L'évaluation des menaces: comprendre les menaces de manière approfondie

La répression des défenseurs des droits humains est une affaire de psychologie. Les menaces visent surtout à ce que les défenseurs se sentent vulnérables, anxieux, désemparés et impuissants. En dernière analyse, la répression vise aussi à briser les organisations et à miner la confiance des défenseurs en leurs dirigeants et collègues. Les défenseurs doivent concilier à la fois une gestion soignée et efficace des menaces et le maintien d'un sentiment de sécurité dans leur travail. C'est également l'objectif principal de ce chapitre.

Au chapitre deux, nous avons défini les menaces comme "la possibilité qu'une personne porte atteinte à l'intégrité physique et morale d'une autre personne ou de ses biens par un acte délibéré et souvent violent". Nous avons aussi abordé les menaces **probables (indirectes)** (lorsqu'un défenseur lié à votre travail est menacé et qu'il y a des raisons fondées de croire que vous serez menacé(e) à votre tour) et les menaces **déclarées (directes)** (comme par exemple recevoir une menace de mort). Nous allons à présent examiner les moyens de gérer les **menaces déclarées**.

Une menace déclarée est l'annonce ou l'indication de l'intention d'infliger un dommage, de punir ou de blesser, généralement afin de parvenir à une fin concrète. Les défenseurs des droits humains reçoivent des menaces à cause de l'impact de leur travail, et la plupart des menaces ont pour but avoué de mettre fin aux activités des défenseurs, ou de les forcer à faire quelque chose.

La menace a toujours **une origine,** c'est-à-dire la personne ou le groupe qui est mis en cause par le travail du défenseur et qui menace. Une menace **a aussi un objectif**, qui dépend de l'impact du travail du défenseur, et un **moyen d'expression**, autrement dit la manière dont elle se manifeste au défenseur.

Les menaces sont complexes. Nous pourrions dire avec une pointe d'ironie que les menaces sont "écologiques" car elles ont pour but d'obtenir des résultats

maximaux avec un investissement minimal d'énergie. La personne qui menace a choisi ce moyen plutôt que de passer à l'acte, ce qui exigerait un investissement d'énergie plus important. Il peut y avoir de nombreuses raisons à cela, qui méritent d'être signalées dans ce contexte:

- L'auteur de la menace dispose de la capacité d'agir mais s'inquiète dans une certaine mesure du coût politique d'une action au grand jour contre un défenseur des droits humains. Des menaces anonymes peuvent être proférées pour les mêmes raisons.
- L'auteur de la menace n'a qu'une capacité limitée d'action et veut obtenir le même résultat en cachant ses moyens défaillants par une menace. Cette capacité limitée peut être seulement passagère, en raison d'autres priorités, ou permanente; cependant, les choses peuvent changer dans les deux cas et entraîner une agression directe du défenseur à une date ultérieure.

Une menace est toujours une expérience personnelle, et elle n'est jamais sans effet. Pour l'exprimer autrement, les menaces affectent toujours les personnes visées de quelque façon que ce soit. Un défenseur a dit un jour: "Les menaces ont toujours un effet, ne serait-ce que parce que nous en parlons". En fait, toute menace peut produire un effet double, émotionnel et sécuritaire. Nous nous concentrerons sur la sécurité dans ce qui suit, mais nous ne devons pas oublier l'aspect émotionnel dans toute menace ni les conséquences des émotions sur la sécurité.

Nous savons qu'une menace est généralement due à l'impact de notre travail. Recevoir une menace représente donc une réaction à la façon dont notre travail touche une personne donnée. De ce point de vue, une menace est une source inestimable d'informations qui devrait être analysée minutieusement.

"Emettre" une menace par opposition à "constituer" une menace

Les personnes émettent des menaces contre les défenseurs des droits humains pour de multiples raisons et seules certaines ont l'intention ou la capacité de commettre une agression. Cependant, certains individus peuvent constituer une menace sérieuse sans jamais l'exprimer. La distinction entre le fait d'émettre et le fait de constituer une menace est importante:

- Certains **émettent** des menaces et constitueront en fin de compte une menace.
- Beaucoup **émettent** des menaces mais **ne constituent pas** de menace.
- Certaines personnes qui n'**émettent** jamais de menace **constituent** pourtant une menace.

Une menace n'est crédible que si elle indique que son auteur dispose des moyens de s'en prendre à vous. Elle doit être la preuve d'un degré minimum de force ou un élément menaçant conçu dans le but d'instiller la peur.

La personne à l'origine de la menace peut donner la preuve de sa capacité à agir par un acte simple, par exemple en laissant une menace écrite à l'intérieur d'une voiture fermée à clé, même si vous ne l'avez laissée garée que quelques minutes, ou en vous téléphonant à la minute où vous êtes arrivé à votre domicile pour que vous sachiez qu'on vous surveille.

On peut tenter de vous faire peur en incluant des éléments symboliques dans une menace, par exemple en vous envoyant une invitation à votre propre enterrement ou en déposant un animal mort sur le seuil de votre domicile ou sur votre lit.

Beaucoup de menaces sont un mélange des caractéristiques ci-dessus. Il est important de les distinguer, car certains auteurs de menaces feignent de disposer des moyens d'agir en recourant à des éléments symboliques et effrayants.

N'importe qui peut émettre une menace, mais n'importe qui ne constitue pas une menace.

En fin de compte, il vous faut déterminer si la menace peut être mise à exécution. Si vous êtes suffisamment sûr que c'est improbable, votre démarche ne sera pas la même que si vous pensez que la probabilité d'une menace est réelle.

Les trois objectifs principaux lors de l'évaluation d'une menace sont:

- l'obtention d'autant d'informations que possible sur le but et l'origine de la menace (tous deux auront un lien avec l'impact de votre travail).
- l'aboutissement à une conclusion raisonnée et raisonnable quant à la probabilité d'une mise à exécution d'une menace.
- une décision quant à la marche à suivre.

Cinq étapes pour évaluer une menace

1 • **Établissez les faits concernant la ou les menaces.** Il est important de connaître exactement les faits. Vous pouvez le faire en menant des entretiens ou en interrogeant des individus-clés, et quelquefois grâce à des rapports pertinents.

2 • **Établissez le modèle de menaces au fil du temps.** Si plusieurs menaces sont faites à la suite (comme cela arrive souvent), il est important d'en rechercher les caractéristiques, tels que les moyens employés pour menacer, le moment où les menaces se produisent, les symboles, la forme (information écrite à la main ou communication verbale), etc. Il n'est certes pas toujours possible d'établir de tels modèles, mais ils sont cependant importants pour une évaluation correcte des menaces.

3 • **Établissez le but de la menace.** Puisqu' une menace a habituellement un but clairement lié à l'impact de votre travail, suivre la piste de cet impact pourrait vous aider à établir le but de la menace.

4 • **Établissez l'origine de la menace.** (Ceci n'est possible qu'après avoir suivi les trois premières étapes). Essayez d'être aussi précis que possible et de distinguer entre le commanditaire et l'exécutant: par exemple, vous pourriez dire que le "gouvernement" vous menace. Comme tout gouvernement est un acteur complexe, il est plus utile de chercher quelle partie du gouvernement pourrait être à l'origine de la menace. Des acteurs tels que "les forces de sécurité" ou les "groupes

armés" sont également des acteurs complexes. Souvenez-vous que même si elle est signée, une menace peut s'avérer irréalisable. Ceci peut être un bon moyen pour l'auteur des menaces d'éviter un coût politique tout en parvenant à sa fin d'effrayer le défenseur et de l'empêcher de poursuivre son travail.

5 • **Arrivez à une conclusion raisonnée et raisonnable sur la probabilité que la menace puisse être mise à exécution ou non.** La violence est conditionnelle. Vous ne pouvez jamais savoir avec certitude si une menace sera mise - ou non - à exécution. Etablir des prévisions en matière de violence revient à affirmer que dans certaines circonstances précises, il existe un risque qu'un individu ou qu'un groupe particulier use de violence contre une cible donnée.

Les défenseurs ne sont pas devins et ne peuvent pas prétendre savoir ce qui surviendra. Cependant, vous pouvez arriver à une conclusion raisonnable sur la probabilité qu'une certaine menace soit mise à exécution ou non. Vous pouvez ne pas avoir obtenu assez d'informations sur la menace aux quatre premières étapes et pouvez ne pas aboutir à une conclusion. Vous pouvez aussi avoir des avis divergents sur ce qu'est une menace "réelle". De toute façon, vous devez partir du scénario-catastrophe (principe de précaution).

Exemple:

Des menaces de mort ont été émises à l'encontre d'un défenseur des droits humains. Le groupe analyse les menaces et aboutit à deux conclusions divergentes, toutes deux partant d'un raisonnement solide. Certains disent que la menace est une imposture complète, tandis que d'autres pensent qu'il y a des indices inquiétants que les menaces soient mises à exécution. En fin de réunion, le groupe opte pour le scénario-catastrophe, c'est-à-dire qu'il estime que la menace peut se concrétiser et prend donc les mesures nécessaires.

Cette évaluation de la menace évolue de faits concrets (1e étape) vers un raisonnement spéculatif. La 2e étape introduit une légère interprétation des faits que l'on approfondit progressivement dans les 3e, 4e et 5e étapes. Il y a des raisons fondées pour lesquelles il convient d'observer l'ordre des étapes. Si vous commencez directement par la 2e ou la 4e étape, par exemple, vous vous privez d'informations plus concrètes découlant des étapes précédentes.

Le suivi et la clôture d'un cas de menace

Une menace ou un incident de sécurité peut inquiéter un groupe de défenseurs, mais il est souvent difficile de faire durer la conscience d'un danger pendant toute la durée de la menace. En raison de la pression extérieure constante sur les défenseurs et leurs activités, tirer les sonnettes d'alarme d'une organisation trop souvent pourrait amener les membres à perdre l'intérêt et, par conséquent, à baisser la garde.

Donner l'alerte au sein d'un groupe ne devrait se produire qu'en cas de preuves fiables et devrait être directement lié à un événement anticipé précis. Elle doit être prévue de façon à motiver le groupe à agir, et à exiger la mise en œuvre d'un ensemble concret de mesures. Afin d'être la plus efficace possible, l'alerte ne devrait susciter qu'une motivation relative. Si la motivation est trop faible, elle ne pousse pas les personnes à agir, en revanche lorsqu'elle est trop intense, elle provoque une surcharge d'émotions. Si la menace est susceptible de se prolonger dans le temps, il est essentiel de procéder à un débriefing et à des activités de suivi une fois l'alerte initiale donnée, afin de corriger les fausses informations, de modifier les recommandations peu judicieuses, et également de renforcer la confiance des membres dans les efforts communs du groupe.

En conclusion, si la menace n'est pas mise à exécution, une explication devrait être fournie et le groupe devrait être informé que la menace est moindre ou qu'elle a cessé.

Vous pouvez envisager de clore le dossier lorsque vous estimez que l'agresseur potentiel ne constitue plus une menace. Idéalement, pour être sûr de pouvoir clore un cas de menace en connaissance de cause, vous devriez être en mesure de justifier la décision au préalable. Il faudrait également s'interroger sur les circonstances changeantes qui pourraient pousser l'auteur des menaces à passer à un acte violent.

Réagir aux menaces du point de vue de la sécurité

- Une menace peut être considérée comme un incident de sécurité. Pour plus d'informations sur les réponses aux incidents de sécurité, reportez-vous au chapitre 1.4.
- Une évaluation des menaces déclarées peut vous amener à craindre une agression. Lisez le chapitre consacré à la prévention des attaques, chapitre 1.5.

En résumé

Les menaces peuvent être inhérentes à la situation de conflit ou non. Elles peuvent être directes (déclarées) ou indirectes (non déclarées).

Une menace déclarée est une déclaration ou une indication d'intention à l'encontre de quelqu'un pour atteindre quelque chose.

Cinq étapes aideront à déterminer la faisabilité d'une menace afin de prendre une décision quant à la marche à suivre:

1 • Déterminez les faits

2 • Déterminez le modèle de menace étalé dans le temps

3 • Déterminez l'objectif

4 • Déterminez l'origine

5 • Aboutissez à une conclusion raisonnée et raisonnable concernant la faisabilité (probabilité de mise à exécution) de la menace.

Évitez des conclusions hâtives et "évidentes" et essayez d'être aussi précis que possible en posant autant de scénarios que les faits et schémas indiquent. Développez-les aussi loin que des éléments fondés le permettent.

CHAPITRE 1.4

Incidents de sécurité: définition et analyse

Objectif:

Apprendre à reconnaître et à réagir aux incidents de sécurité.

Qu'est-ce qu'un incident de sécurité?

En termes simples, un incident de sécurité peut être défini comme tout **acte ou événement dont vous pensez qu'il pourrait mettre en cause votre sécurité personnelle ou la sécurité de votre organisation.**

Les incidents de sécurité peuvent être dus à une situation donnée, ou bien provoqués intentionnellement ou involontairement.

Les exemples d'incidents de sécurité pourraient inclure le fait de voir le même véhicule suspect stationné devant votre bureau ou votre maison durant plusieurs jours, le téléphone qui sonne en pleine nuit sans que quelqu'un vous réponde, une personne qui pose des questions sur vous dans une ville ou un village proche, une effraction à votre domicile, etc.

Or, tout ce que vous remarquez ne constituera pas toujours un incident de sécurité. Vous devriez donc le consigner par **écrit**, et ensuite **l'analyser**, idéalement avec vos collègues, pour établir s'il est réellement susceptible de porter atteinte à votre sécurité. À ce moment-là, vous pouvez **réagir** à l'incident. La marche à suivre est celle-ci:

> Vous remarquez quelque chose ⇨ vous vous rendez compte qu'il peut s'agir d'un incident de sécurité ⇨ vous le consignez ou en informez vos collègues ⇨ vous l'analysez ⇨ vous établissez qu'il s'agit d'un incident de sécurité ⇨ vous réagissez de façon appropriée.

S'il y a urgence, la marche à suivre doit néanmoins être respectée, mais beaucoup plus rapidement pour éviter de perdre du temps (voir ci-dessous).

Distinguer les incidents de sécurité des menaces:

Si vous attendez le bus et qu'une personne à côté de vous vous menace à cause de votre travail, cela - indépendamment du fait d'être une menace - constitue un incident de sécurité. Cependant, si vous découvrez que la police surveille votre bureau depuis une voiture garée sur le trottoir d'en face ou que votre téléphone portable a été volé, il s'agira alors d'incidents de sécurité mais pas nécessairement de menaces. Toutefois, tandis que les incidents de sécurité découlant

de la situation et/ou involontaires (se retrouver dans la foule et/ou avoir perdu ses clefs) peuvent être clairement distingués des menaces, rappelez-vous que les incidents de sécurité délibérés ont un objectif, qui n'est pas nécessairement le même que celui des menaces (voir chapitre 1.2). L'objectif minimum d'un incident de sécurité délibéré est de collecter des informations concernant les défenseurs, indépendamment du fait qu'elles soient utilisées contre eux ou non.

Il est important d'établir une distinction nette ne serait-ce que pour la santé mentale des défenseurs.

Toutes les menaces sont des incidents de sécurité, mais tous les incidents de sécurité ne constituent pas forcément des menaces.

Pourquoi les incidents de sécurité sont-ils si importants?

Les incidents de sécurité sont cruciaux pour la gestion de la sécurité car ils fournissent des **informations vitales sur l'impact de votre travail, et sur des actions éventuelles qui peuvent se préparer ou avoir lieu à votre encontre**. De même, ces incidents vous permettent de modifier votre comportement ou vos activités et d'éviter des endroits qui pourraient s'avérer dangereux, ou plus dangereux que d'habitude. Les incidents de sécurité peuvent donc être vus comme des indicateurs du niveau de sécurité local. Si vous étiez privés de la possibilité de déceler de tels changements, il serait difficile de prendre les mesures nécessaires et opportunes pour protéger votre sécurité.

Par exemple, vous pourrez vous rendre compte que vous êtes sous surveillance après avoir remarqué plusieurs incidents de sécurité. Vous êtes alors en mesure de réagir à cette surveillance.

Les incidents de sécurité représentent "l'unité de base" de mesure de la sécurité et sont les indicateurs de la résistance à vos activités et de la pression qu'elles suscitent. Ne les laissez pas passer inaperçus!

Quand et à quoi remarquez-vous des incidents de sécurité?

Cela dépend du degré de visibilité de l'incident. S'il peut potentiellement passer inaperçu, votre aptitude à le reconnaître dépendra de votre formation à la sécurité, de votre expérience et de votre conscience du risque.

Meilleures sont votre vigilance et votre formation, moins les incidents échapperont à votre attention.

Les incidents de sécurité sont parfois négligés ou remarqués brièvement puis écartés, ou à l'inverse, les défenseurs peuvent parfois dramatiser ce qu'ils croient être des incidents de sécurité.

Pourquoi un incident de sécurité peut-il échapper à notre attention?

Exemple:

Un défenseur vit un incident de sécurité, mais l'organisation pour laquelle il travaille ne réagit pas du tout. Pourquoi?

- Le défenseur n'est pas conscient qu'un incident de sécurité a eu lieu.
- Le défenseur en est conscient mais n'en tient pas compte parce qu'il l'estime sans importance.
- Le défenseur n'a pas informé son organisation (il ou elle a oublié, estime que ce n'est pas nécessaire ou décide de le taire parce que l'incident a eu lieu en raison d'une erreur de sa part).
- L'organisation, a évalué l'incident au sein du groupe après que le défenseur l'ait consigné dans le cahier, mais a jugé qu'une action n'était pas nécessaire.

Pourquoi les personnes réagissent-elles parfois de manière excessive aux incidents de sécurité?

Exemple:

Un collègue raconte constamment des histoires à propos de l'un ou l'autre incident de sécurité, mais après examen, elles s'avèrent sans fondement ou ne pas mériter la qualification d'incident de sécurité. L'incident de sécurité réel dans ce cas de figure est constitué par le fait que votre collègue souffre d'un problème qui lui fait voir des incidents de sécurité inexistants. Il ou elle ressent peut-être une grande peur, ou souffre de stress, et il faudrait lui proposer alors de l'aide pour pouvoir résoudre son problème.

N'oubliez pas que bien trop souvent, on ne s'aperçoit pas des incidents de sécurité ou qu'on ne les prend pas au sérieux. Soyez attentifs!

Gérer les incidents de sécurité

Vous pouvez gérer les incidents de sécurité en suivant ces trois étapes élémentaires:

1 • **Consignez-les.** Tous les incidents de sécurité (n'oubliez pas les évènements ou changements bizarres) remarqués par un défenseur doivent être signalés, soit dans un cahier personnel ordinaire, soit dans un cahier accessible à tout le groupe.

2 • **Analysez-les.** Tous les incidents de sécurité consignés doivent faire l'objet d'une analyse en bonne et due forme, que ce soit immédiatement après ou régulièrement. Il vaut mieux les analyser en groupe plutôt que par soi-même car cela réduit le risque d'omettre un élément. Quelqu'un devrait être responsable de veiller à la réalisation de cette tâche.

Il conviendra de décider s'il faut ou non révéler aux autres certains incidents (comme pour les menaces). Est-il moral et pertinent de taire une menace face à des collègues ou d'autres collaborateurs? Il n'y a pas de règle unique s'appliquant à toutes les situations, mais il est cependant souvent conseillé d'être aussi franc que possible en matière d'échange d'informations, de gestion des problèmes logistiques, ainsi que de craintes.

3 • **Réagissez-y.** Étant donné que les incidents de sécurité sont le baromètre de l'impact de vos activités, ils peuvent générer:

- Une réaction à l'incident lui-même.
- Des **retours d'information**, en termes de sécurité, à propos de votre manière de travailler, de vos programmes ou de vos **stratégies** de travail. Ainsi:

Exemple d'un incident qui génère un **retour d'information** permettant d'améliorer la sécurité dans vos activités:

Pour la troisième fois un membre de votre organisation a rencontré des problèmes lors du passage à un poste de contrôle de la police, car cette personne oublie fréquemment de se munir des documents d'identité obligatoires. Vous décidez par conséquent d'élaborer une liste de contrôle (checklist) que tous les membres doivent consulter avant de quitter la ville. Vous déciderez peut-être aussi de modifier l'itinéraire de tels déplacements.

Exemple d'un incident qui vous permet d'avoir un retour d'information et donc de **planifier** les mesures nécessaires à la sécurité:

Au même poste de contrôle de la police, vous êtes retenu pendant une demi-heure et on vous dit que votre travail est tenu en piètre estime. Des menaces à peine voilées sont formulées. Lorsque vous demandez une explication au quartier général de la police, la scène se répète. Vous convoquez une réunion de groupe pour réexaminer les activités prévues car il semble évident que des changements sont nécessaires si vous voulez continuer votre travail. Vous organisez une série de rencontres avec les fonctionnaires du ministère de l'Intérieur pour que les agents de police du poste de contrôle cessent de vous harceler; vous modifiez une partie des activités prévues et prévoyez des réunions hebdomadaires pour suivre l'évolution de la situation.

Exemple d'un incident qui génère un retour d'information qui vous permet d'élaborer votre **stratégie** de sécurité.

Lorsque que lancez vos activités de défenseur dans une nouvelle région, vous recevez immédiatement des menaces de mort et l'un de vos collègues est agressé physiquement. Vous n'aviez pas imaginé une telle opposition à votre travail, et n'avez pas prévu de réponse dans votre stratégie globale. Vous aurez donc à modifier votre stratégie afin de faire grandir (d'accroître?) la tolérance locale à l'égard de votre travail et de dissuader davantage les agressions et menaces. Pour ce faire, vous devrez interrompre vos activités provisoirement, quitter la région et réexaminer le projet entier.

Réagir d'urgence à un incident de sécurité

Il existe beaucoup de façons de réagir rapidement à un incident de sécurité. Les étapes ci-dessous ont été formulées en fonction du moment et de la forme de la réaction, à partir du moment où l'incident a été signalé, pendant sa survenance et après qu'il se soit passé.

1e étape. Signalez l'incident.

- Qu'est-ce qui est en train de se passer / que s'est-il passé? (essayez de vous concentrer sur les faits réels)
- Où et quand cela s'est-il passé?
- Qui était impliqué (si vous êtes en mesure de le déterminer)?
- Y a-t-il eu des blessures et dommages infligés à des personnes (membres), à la propriété ou aux biens?

Étape 2. Décidez du moment d'agir. Il y a trois possibilités:

- Une **réaction immédiate** s'impose afin de porter des secours aux personnes blessées ou pour arrêter/prévenir une agression.
- Une **réaction rapide** (dans les heures ou les jours qui suivent) est nécessaire pour éviter que de nouveaux incidents de sécurité se produisent (l'incident est clos).
- Une **action de suivi** (après quelques jours, semaines, ou mois): si la situation s'est stabilisée, une réaction immédiate ou rapide peut ne pas être nécessaire. Cependant, tout incident de sécurité exigeant une réaction immédiate ou rapide doit donner lieu à une action de suivi afin de rétablir ou réexaminer le contexte de votre travail.

Étape 3. Décidez de la manière de réagir et de vos objectifs.

- Quand la réaction doit être immédiate, les objectifs sont clairs: soigner les blessures et/ou empêcher la poursuite de l'agression ou une nouvelle agression.
- Quand la réaction doit être rapide, les objectifs seront établis par une équipe de crise (ou assimilée) et viseront à rétablir la **sécurité nécessaire pour les personnes touchées par l'incident.**

Les réactions ultérieures découleront des mesures fixées selon les procédures de décision habituelles de l'organisation, et viseront à rétablir un cadre extérieur sûr pour vos activités, à revenir sur les procédures d'organisation internes et à prévoir de meilleures réactions face aux incidents de sécurité futurs.

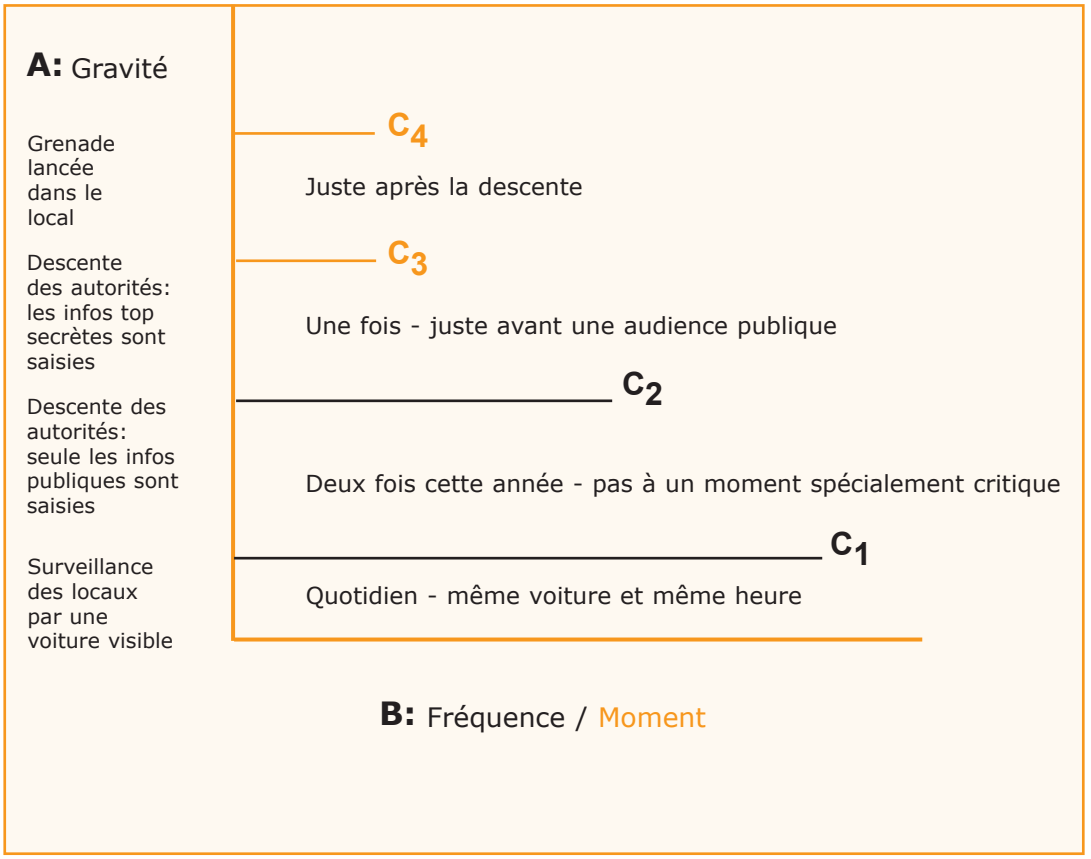
Toute réaction doit prendre en compte la sécurité et la protection des autres personnes, organisations ou institutions avec lesquels vous entretenez des relations de coopération.

Fixez vos objectifs avant d'agir.
Si la rapidité de votre action compte,
il est cependant important de savoir pourquoi vous agissez.
En définissant d'abord le but recherché (vos objectifs),
vous pourrez décider du moyen de le réaliser
(la marche à suivre).

Par exemple:

Si des défenseurs travaillant ensemble sont informés qu'une de leurs collègues n'est pas arrivée comme prévu à sa destination en ville, ils pourront réagir d'abord en téléphonant à un hôpital et à leurs contacts au sein d'autres ONG, puis à une représentation locale des Nations unies et à la police. Mais avant de lancer ces appels, il est très important de définir ce que vous souhaitez obtenir et ce que vous direz. Dans le cas contraire, vous alarmeriez d'autres personnes sans raison (imaginez que le défenseur soit simplement arrivé en retard parce qu'il ou elle a manqué un bus et qu'il ou elle ait oublié de prévenir le bureau) ou pourriez provoquer une réaction opposée à celle voulue.

Consigner les incidents de sécurité (et les menaces) permet de les analyser dans la perspective d'être à même, à un moment donné, de les anticiper. Par exemple, si il apparaît que des incidents de sécurité surviennent pendant les périodes pré-électorales, il est probable que d'autres interviendront durant la période pré-électorale suivante. Consigner les incidents permet également d'évaluer les similitudes des actions contre les DDH par un agresseur potentiel, ou, en cas d'incidents de sécurité dus à la négligence des DDH, d'évaluer comment la sécurité est gérée par les DDH eux-mêmes.



C: Probabilité d'une action imminente plus grave à l'encontre d'un DDH par un agresseur potentiel.

C1: TRES BAS (A1: surveillance des locaux par une voiture visible + B1: Quotidien - même voiture et même heure).

C2: BAS (A2: Descente des autorités, seule les infos publiques sont saisies + B2: Deux fois cette année - pas à un moment spécialement critique).

C3: ELEVE (A3: Descente des autorités, les infos top secrètes sont saisies (les listes top secrètes de noms de témoins) + B3: Une fois - juste avant une audience publique.

C4: TRES ELEVE (A4: Grenade lancée dans le local + B4: Juste après une descente C3).

(...)

En résumé

Un incident de sécurité est tout fait ou événement dont vous pensez qu'il pourrait affecter votre sécurité personnelle ou celle de votre organisation.

Les incidents de sécurité peuvent découler de la situation ou provoqués intentionnellement ou involontairement.

Les incidents de sécurité permettent de mesurer la sécurité et l'impact du travail des défenseurs sur les intérêts d'autrui.

Tous les défenseurs ont des incidents de sécurité. Le contraire implique que:

- l'impact du travail des défenseurs est insignifiant soit parce que le travail n'est pas effectué correctement et/ou parce que personne ne voit ses intérêts affectés. En d'autres termes: personne ne s'intéresse à eux.

- l'agresseur potentiel a déjà toutes les informations nécessaires concernant les défenseurs et n'a pas besoin de se déranger: les défenseurs n'ont alors pas été capables de percevoir les incidents de sécurité provoqués (surveillance, recueil d'informations…).

Un incident de sécurité n'est pas une menace; il requiert cependant de l'attention.

Voici trois étapes à respecter pour faire face aux incidents de sécurité:

1 • Notez-les

2 • Analysez-les

3 • Réagissez-y

CHAPTER 1.5

Prévenir les agressions et y réagir

Objectifs:

Évaluer la probabilité que différents types d'agression surviennent.

Empêcher de possibles agressions directes contre les défenseurs.

Effectuer une contre-surveillance.

Agressions contre des défenseurs des droits humains

La violence est autant un processus qu'un acte. Une agression violente contre un défenseur des droits humains n'a jamais lieu par hasard. L'analyse détaillée des agressions violentes montre qu'elles sont souvent le point culminant de conflits, de différends, de menaces, d'incidents de sécurité et d'erreurs accumulés qui se sont aiguisés avec le temps et dont les origines peuvent être identifiées.

Les agressions contre les défenseurs des droits humains sont le fruit d'au moins trois facteurs interactifs concernant:

1 • **La partie qui recourt à la violence et des moyens.** Souvent, les agressions à l'encontre des défenseurs naissent de raisonnements et de comportements que nous sommes à même de comprendre et qui apportent un éclairage nouveau, même si elles sont illégales L'agresseur devra investir des moyens ne fût-ce que pour recueillir des informations (incidents de sécurité) sur le DDH cible.

2 • **Les circonstances et déclencheurs qui amènent l'agresseur à envisager la violence comme option.** Aux yeux de la majorité des agresseurs, l'agression est un moyen "efficace" d'atteindre un but ou de "résoudre un problème". L'impunité et/ou la disponibilité à payer le coût politique car " il en vaut la peine ".

3 • **Le cadre,** qui favorise la violence, la permet ou ne l'empêche pas. Un accès (et une issue) rapide au défenseur.

Qui représente alors un danger pour les défenseurs des droits humains?

En général, quiconque pense qu'une agression d'un défenseur est un moyen possible, souhaitable, admissible et potentiellement efficace d'atteindre un objectif peut être défini comme un agresseur potentiel. La menace s'alourdit d'autant plus que la personne dispose, ou peut disposer, de la capacité d'agresser un défenseur.

La menace d'une agression peut décroître quand la capacité des agresseurs potentiels à organiser une agression est modifiée, que leur conception de l'acceptabilité d'une agression change, et quand la probabilité d'être arrêtés et condamnés augmente.

Certaines agressions sont précédées de menaces, d'autres non. Cependant, le comportement des individus qui prévoient une agression ciblée est souvent un indicateur subtil, puisqu'ils doivent obtenir les détails quant au meilleur moment d'agresser, organiser la manière d'atteindre leur cible et leur fuite.

Il est donc fondamental de détecter et d'analyser tout indice d'une agression éventuelle. Ceci suppose:

- de déterminer la probabilité qu'une menace soit mise à exécution (voir chapitre 1.3).
- d'identifier et analyser les incidents de sécurité.

Les incidents de sécurité au cours desquels des défenseurs ou leurs lieux de travail ont été surveillés servent à obtenir des informations. Elles peuvent ne pas intervenir dans l'agression, mais dans la mesure du possible, il est important de vérifier ce fait (voir chapitre 1.4).

La surveillance peut poursuivre différents objectifs:

- déterminer quelles activités sont menées, quand, par qui ou avec qui.
- utiliser ces informations ultérieurement pour agresser des personnes ou une organisation.
- réunir les informations nécessaires pour mener une agression.
- réunir des informations dans le but d'engager des poursuites judiciaires ou d'autres formes de harcèlement (sans recours à la violence).
- vous intimider, vos alliés ou d'autres personnes travaillant avec vous.

Il faut retenir que la surveillance est généralement indispensable à l'agression, mais qu'elle ne constitue pas en elle-même une agression. De plus, toute surveillance n'est pas forcément suivie d'une agression. La violence ciblée peut aussi surgir lorsque l'agresseur voit soudain une occasion de frapper; mais même dans ces cas, l'agression a été préparée.

Souvent, les informations qui pourraient permettre de détecter la préparation d'une agression sont rares. Peu d'études existent sur le sujet. La disparité entre la quantité infime d'études existantes et le vaste nombre d'agressions contre les défenseurs des droits humains est d'ailleurs frappante. Néanmoins, les recher-

ches qui existent sont intéressantes à plusieurs égards. Il en résulte notamment les éléments suivants:[11]

- **Agresser un défenseur n'est pas facile et requiert des ressources.** La surveillance est nécessaire pour connaître les faits et gestes d'un individu et le meilleur endroit pour l'agresser. Accéder à la cible et réussir une fuite rapide est également fondamental. (Cependant, si les circonstances sont extrêmement favorables à l'agresseur, les agressions sont plus faciles à réaliser).

- **Ceux qui agressent les défenseurs font normalement preuve d'une certaine cohérence.** La majorité des agressions visent des défenseurs des droits humains qui s'occupent de très près de questions qui affectent les agresseurs. En d'autres termes, les agressions ne sont habituellement ni aléatoires, ni gratuites, mais correspondent aux intérêts immédiats des agresseurs.

- **Des facteurs géographiques entrent en ligne de compte.** Les agressions contre les défenseurs dans des zones rurales, par exemple, sont moins médiatisées et ne suscitent donc pas la même réaction de la part des forces de l'ordre et de la sphère politique que les agressions dans les villes. Les attaques contre des sièges d'ONG ou d'organisations très connues dans les villes provoquent davantage de réactions.

- **Les choix et les décisions sont arrêtés avant une agression.** Ceux qui envisagent une agression contre une organisation de défenseurs doivent décider s'ils vont s'attaquer aux directeurs et responsables ou aux simples membres, et choisir entre une agression unique (contre un haut responsable, éventuellement célèbre, d'où un coût politique élevé pour l'agresseur) et une série d'agressions (visant les membres de l'organisation). Les rares études sur les agressions contre les défenseurs constatent que les deux stratégies sont régulièrement utilisées.

Déterminer si une agression est réalisable

Déterminer la probabilité qu'une agression ait lieu nécessite une analyse des facteurs qui entrent en ligne de compte. Pour les définir, il faut distinguer les différents types d'agression, à savoir les délits et crimes de droit commun, les agressions inhérentes à la situation de conflit ("se trouver au mauvais endroit au mauvais moment") et agressions directes (ciblage), à l'aide des trois tableaux suivants:[12]

11 Claudia Samayoa et Jose Cruz (au Guatemala) et Jaime Prieto (en Colombie) ont fourni des études intéressantes sur les agressions à l'encontre des défenseurs des droits humains (www.protectionline.org, Bibliothèque). Mahony et Eguren (1997, Unarmed Bodyguards) ont analysé de telles attaques.

12 La classification des agressions est identique à celle des menaces: pour de plus amples explications, veuillez consulter le chapitre 1.3 sur les menaces.

Tableau 1: définir la probabilité d'une agression directe (ciblage)

(**AP** signifie agresseur potentiel)

Probabilité d'agressions directes (ciblage)			
Facteurs	Probabilité faible	Probabilité moyenne	Probabilité élevée
Capacité d'agresser	Les AP ont une marge de manœuvre limitée dans vos domaines de travail	Les AP ont une capacité opérationnelle près de vos lieux de travail	Les zones où vous travaillez sont sous contrôle étroit de l'AP
Mobile financier	Les AP n'ont pas besoin de votre équipement ou de liquidités pour leurs activités	Votre matériel, vos liquidités ou autres sources de profit financier (p.ex. la prise d'otages) peuvent intéresser les AP	Les AP ont un besoin clair de matériel ou de liquidités
Mobile politique et militaire	Aucun, votre travail n'est pas lié aux objectifs des AP	Intérêt partiel, votre travail réduit les objectifs politiques et militaires des AP	Votre travail entrave les intérêts des AP, favorise leurs opposants, etc.
Agressions préalables connues	Aucune ou isolée	Quelques cas épisodiques	Beaucoup d'agressions préalables
Positions ou intentions	Sympathie ou indifférence	Indifférence Menaces épisodiques Mises en garde fréquentes	Agressivité avec des menaces réelles et claires
Capacité des forces de sécurité à dissuader les agressions	Existante	Faible	Inexistante, ou collaboration des forces de sécurité avec l'AP
Influence politique de l'organisation et membres mobilisables contre l'AP	Bonne	Moyenne ou faible	Réduite (en fonction du contexte) ou inexistante

Exemple

de probabilité d'agressions directes (ciblage):

Les agresseurs potentiels contrôlent les zones où vous travaillez mais n'ont pas d'intérêt financier à vous agresser. Votre travail ne limite que partiellement leurs objectifs politiques et militaires, et il n'y a aucun exemple d'une agression similaire dans la ville. Ils sont indifférents et ne souhaitent visiblement pas faire l'objet de l'attention nationale ou de pressions en vous attaquant.

La probabilité d'une agression directe dans ce cas est donc faible à moyenne.

Tableau 2: établir la probabilité d'une agression criminelle

(**DC** signifie délinquants et criminels)

Probabilité des agressions criminelles			
Facteurs	Probabilité faible	Probabilité moyenne	Probabilité élevée
Mobilité et situation du criminel	Les DC restent habituellement dans leurs zones, évitent vos zones de travail	Les DC font des incursions dans d'autres zones (ou à proximité de vos zones de travail) la nuit	Les DC agissent partout, jour et nuit
Agressivité des DC	Les DC évitent la confrontation (commettent les infractions principalement dans des zones que vous ne fréquentez pas habituellement)	Les DC se livrent à des délits ou crimes dans la rue (mais pas dans les bureaux du personnel)	Les DC commettent des attaques armées et entrent dans les locaux pour commettre un délit
Accès aux armes et utilisation d'armes	Les DC sont non armés ou utilisent des armes non meurtrières	Les DC utilisent des armes de choc, y compris des machettes	Les DC utilisent des armes à feu, parfois puissantes
Taille et organisation	Les DC agissent seuls ou à deux	Les DC agissent en groupe de deux à quatre	Les DC agissent en groupe
Réponse des forces de l'ordre (police) et dissuasion	Réponse rapide, capacité de dissuasion	Réponse lente, peu d'interventions sur le fait	Réactions de la police sans la moindre efficacité
Formation et professionnalisme des forces de l'ordre	Bien formées et professionnelles (mais un manque de ressources est possible)	Régulièrement formées, mais soldes maigres, ressources limitées	Inexistants ou police corrompue (collabore avec les DC)
Situation générale de sécurité	Absence d'Etat de droit mais sécurité relative	Sécurité défaillante	Les droits ne sont pas respectés, impunité totale

Exemple

de probabilité d'agressions criminelles:

Dans cette ville, les délinquants agissent dans différentes zones, à deux ou en petits groupes, parfois de jour. Ils sont souvent agressifs et munis d'armes à feu. La police réagit mais lentement et de manière inefficace; les forces de l'ordre (police, gendarmerie) ne sont pas professionnelles et manquent de ressources. Cependant, la direction de la police est bien disciplinée. La sécurité est manifestement faible, et si l'on tient compte des quartiers périphériques de la ville, la menace de criminalité est à son comble puisque tous les indicateurs sont élevés.

La probabilité d'une agression criminelle dans le centre de cette ville est moyenne à élevée.

Tableau 3: établir la probabilité d'agressions inhérentes à la situation de conflit

(**AP** signifie agresseur potentiel)

Probabilité d'agressions accidentelles			
Facteurs	Probabilité faible	Probabilité moyenne	Probabilité élevée
Votre connaissance des zones de conflit	Bonne	Approximative	Vous avez très peu d'informations quant à l'endroit des zones de combat
Distance qui vous sépare des zones de conflit	Vous travaillez loin de ces zones	Votre travail a lieu à proximité de ces zones et vous les traversez périodiquement	Vous travaillez en zone de conflit
Déplacement géographique des zones de conflit	Zones de conflit géographiquement stables, déplacement faible et répertorié	Déplacement relativement fréquent de ces zones	Déplacement géographique continu, les zones de conflit sont imprévisibles
Votre connaissance des régions minées (mines terrestres)	Bonne connaissance ou absence de zones minées	Connaissance approximative	Connaissance nulle
Distance entre votre lieu de travail et les zones minées	Vous travaillez loin des zones minées	Vous travaillez à proximité des zones minées et vous y entrez occasionnellement	Vous travaillez dans les zones minées
Tactiques de combat et armes des AP	Connues et répertoriées	Connues et répertoriées avec emploi périodique d'artillerie, d'embuscades et de francs-tireurs	Toutes, sans discrimination: bombardement, artillerie lourde, attentats terroristes ou attaques à la bombe

Exemple

d'évaluation de la probabilité d'agressions inhérentes à la situation de conflit:

Dans cette région, vous connaissez bien les zones de combat qui évoluent lentement et de manière vérifiable. Vous travaillez près des zones de combat et vous y effectuez des visites et séjours périodiques. Vous n'êtes pas à proximité de zones minées. Les tactiques de combat sont ciblées et touchent rarement les populations civiles.

Le degré de risque d'agressions inhérentes à la situation de conflit lié au travail dans cette zone est faible.

La prévention d'une possible agression directe / indirecte

Bien que le défenseur soit la cible dans les deux cas, faisons la distinction entre:

- une agression directe: à l'encontre du défenseur
- une agression indirecte à l'encontre du défenseur: quand celle-ci concerne une personne proche du défenseur

Dans les deux cas la prévention nécessitera la même logique sous-jacente.

Vous savez désormais que la menace peut diminuer si la capacité des agresseurs potentiels à organiser une agression est modifiée, si la tolérance à l'égard de l'acte d'agression change et si la probabilité qu'ils soient pris et condamnés augmente.

Pour prévenir une agression, il est donc nécessaire de:

- Persuader l'agresseur potentiel ou celui qui vous menace qu'une agression représenterait, pour lui, un coût politique et des conséquences inacceptables.

- Rendre ces agressions moins réalisables.

Ce genre de prévention d'agressions est semblable à l'analyse effectuée au chapitre 1.2 où nous expliquons que le risque est déterminé par les vulnérabilités et les capacités des défenseurs des droits humains. Nous mentionnons de même que pour vous protéger et réduire le risque, vous devez agir contre les menaces, limiter votre vulnérabilité et renforcer vos capacités.

Lorsqu'il y a une menace et que vous voulez réduire son risque inhérent, il est important d'agir non seulement contre la menace elle-même, mais aussi sur les vulnérabilités **et les capacités les plus étroitement liées à la menace**. En période de fortes pressions, quand vous souhaitez agir le plus rapidement possible, vous commencez souvent par agir sur les vulnérabilités les plus simples à modifier ou qui vous touchent directement plutôt que par privilégier celles qui sont inhérentes à la menace.

Mais attention: si le risque d'agression est élevé (c'est-à-dire si la menace est grave et réelle, et que vos vulnérabilités dépassent vos capacités), vouloir aborder le risque par les vulnérabilités et les capacités ne sera pas efficace puisque leur modification et mise en œuvre prend du temps. Si le risque est extrêmement élevé (une agression directe et sévère imminente), vous n'avez que trois possibilités pour l'empêcher:

a L'action immédiate et efficace pour contrer la menace, si toutefois vous êtes certains d'obtenir un résultat immédiat et spécifique qui permettra d'empêcher l'agression (en règle générale, il n'y a aucune garantie de résultat immédiat et efficace: les réactions prennent du temps et ce dernier est précieux à ces moments-là).

b b. La réduction de votre exposition au maximum en vous cachant ou en quittant la zone.[13]

[13] Il y aura des cas où voyager/se déplacer exposera le défenseur à davantage de risque que de rester sur place.

c ◆ La recherche d'une protection efficace: voir les deux exemples de protection efficace (dépendant du contexte):

- la protection de la communauté: si vous vous cachez ou trouvez refuge au sein de la communauté, la présence de témoins peut dissuader l'agresseur potentiel.

- la protection armée peut être utile dans certains cas, mais à condition qu'elle soit rapidement disponible (immédiate), qu'elle puisse effectivement dissuader l'agresseur potentiel et n'expose pas le défenseur à un danger accru à moyen et à long terme. L'expérience montre qu'une protection armée correspondant à ces exigences est extrêmement difficile à trouver. Parfois, un gouvernement offre une escorte armée au défenseur à la suite de pressions nationales ou internationales. Dans ce cas, consentir à l'escorte ou la refuser pourrait rappeler l'Etat à ses responsabilités de protection en matière de sécurité des défenseurs, mais en aucun cas un gouvernement ne pourra s'estimer délesté de ses responsabilités si le défenseur refuse l'escorte armée. Les entreprises de sécurité privée peuvent aggraver le risque si elles ont des liens avec les agresseurs.[14] Quant au port d'arme par les défenseurs des droits humains, nous devons admettre son inefficacité dans la majorité des cas en situation d'agression organisée. De plus, il rend les défenseurs vulnérables car un gouvernement peut les attaquer sous prétexte de la lutte contre le terrorisme ou de la répression d'une insurrection. Qui plus est, le port d'arme pourrait être retourné contre les défenseurs comme étant en contradiction avec la déclaration des Nations unies sur les DDH.

Les menaces qui peuvent conduire à une agression sont plus faciles à gérer dès lors que d'autres acteurs importants en matière de protection ou parties prenantes sont impliqués et coopèrent. Prenons par exemple l'efficacité du système judiciaire, l'existence de réseaux de soutien (nationaux et internationaux) capables d'exercer une pression politique sur les détenteurs des obligations concernés et de réseaux sociaux (au sein des organisations), les réseaux personnels et familiaux, les forces de maintien de la paix de l'ONU ou internationales, etc.

Surveillance et contre-surveillance

La contre - surveillance permet de savoir si vous êtes surveillé. Comme il est difficile de vérifier si vos communications téléphoniques sont placées sur écoute et si vos communications par internet sont surveillées, il vaut toujours mieux le supposer.[15] Cependant, vous pouvez découvrir si vos faits et gestes ainsi que vos bureaux sont placés sous surveillance.

Qui est susceptible de vous surveiller?

Les personnes que vous rencontrez régulièrement dans votre quartier, comme les concierges ou les portiers des immeubles, les marchands ambulants qui s'in-

[14] Pour plus d'informations sur les mesures de sécurité, voir chapitre 1.8 "Améliorer la sécurité au travail et au domicile".

[15] Voir chapitre 1.11 "Sécurité, la communication et les technologies de l'information."

stallent à proximité de l'entrée de vos locaux, des individus dans les voitures garées à proximité, les visiteurs, etc. sont tous susceptibles de vous surveiller. La surveillance est un moyen de gagner sa vie; elle peut aussi être imposée sous la menace; elle est parfois l'expression de convictions politiques; elle peut être une combinaison de tout cela. Ceux qui déclenchent la surveillance peuvent aussi placer leurs collaborateurs ou des membres de leur organisation dans votre quartier.

Des personnes peuvent également vous surveiller à distance. Dans ce cas-là, ils appartiennent quasi tous à une organisation et vous surveillent à votre insu. Cette tactique comprend probablement: vous suivre de loin, se relayer fréquemment, changer de poste d'observation, de véhicules, etc.

Vérifier si vous êtes surveillé(s)

Vous pouvez déterminer si vous êtes sous surveillance en observant à votre tour ceux qui pourraient vous surveiller et en adoptant les règles suivantes (sans pour autant céder au délire de persécution):

- Si vos suspicions d'être surveillé sont fondées, vous devriez observer les mouvements des individus dans votre quartier ainsi que leurs changements de comportement, comme lorsqu'ils commencent à se renseigner sur vos activités. Rappelez-vous que la surveillance peut être effectuée indifféremment par des femmes et des hommes, des personnes âgées ou très jeunes.

- Si vous soupçonnez quelqu'un de vous suivre, vous pouvez recourir à une tierce personne de confiance, inconnue de vos espions suspectés, et la charger de les espionner à son tour. Cela s'appelle une mesure de contre - surveillance. La tierce personne peut observer leurs mouvements de loin lors de votre arrivée, de votre départ ou de vos déplacements. Celui ou celle qui vous surveille vous observera en toute probabilité depuis un poste qui permet de vous garder à l'œil aisément, qu'il s'agisse de votre domicile, des bureaux ou d'autres lieux de travail.

Exemple:

Avant de rentrer à votre domicile, demandez à un parent ou à un voisin digne de confiance de se placer dans les environs (p.ex. en affectant de changer la roue d'un véhicule) pour vérifier si quelqu'un attend votre arrivée. Faites de même pour le moment où vous quittez le bureau à pied. Si vous utilisez une voiture particulière, il faudra qu'une deuxième voiture attende que l'observateur potentiel vous ait pris en filature avant de la suivre à son tour.

L'avantage de la contre - surveillance est, au moins initialement, que la personne qui vous observe ignore que vous avez remarqué sa surveillance. Par conséquent, toutes les personnes impliquées dans la contre-surveillance doivent être conscientes que mieux vaut ne pas entrer en conflit ou en contact avec votre observateur potentiel. Ils / elles se rendront alors compte que vous êtes au fait de leurs activités, ce qui pourrait provoquer une réaction violente. Il est important de prendre les plus grandes précautions et de garder vos distances si vous êtes conscients d'être surveillé(s). Une fois la surveillance confirmée, vous pouvez agir en conséquence en appliquant nos recommandations.[16]

[16] Voir chapitre 1.11 "Sécurité, la communication et les technologies de l'information."

Notre analyse de la contre-surveillance s'applique presque exclusivement aux zones urbaines ou semi-urbaines. Dans les campagnes, la situation est très différente, les défenseurs et les communautés locales remarquant beaucoup plus rapidement la présence de tout étranger. Quelqu'un qui organise votre surveillance trouvera la prise de contact avec les habitants ruraux plus compliquée, sauf en cas d'hostilité explicite de la population à l'égard de votre travail.

Une remarque: créer des liens avec les forces de sécurité qui vous surveillent peut s'avérer utile dans les cas où la surveillance ne se fera pas de manière aussi couverte puisqu'elle est censée être remarquée et intimider. Parfois, les défenseurs soignent leurs liens avec des éléments individuels des forces de sécurité afin qu'ils les préviennent lorsqu'ils sont surveillés ou qu'une agression potentielle est préparée à leur intention.

Quand devez-vous vérifier si vous êtes surveillé(s).

La raison nous commande de procéder systématiquement à cette vérification au moindre indice fondé, notamment lorsque des incidents de sécurité pourraient indiquer que l'on vous a observé. Si votre activité de défenseur de droits humains vous expose à un certain risque, il peut être utile de mener un exercice simple de contre-surveillance de temps en temps, par souci de sécurité.

Vous devez aussi penser au risque auquel vous exposez autrui si vous vous trouvez sous surveillance, le risque pouvant être plus élevé pour un témoin ou un membre d'une famille que vous allez rencontrer que pour vous-même. Vous devrez éventuellement les avertir que vos faits et gestes sont potentiellement surveillés.

Réagir aux agressions

Il n'y a pas une seule règle applicable à toutes les agressions contre les défenseurs. Qui dit agression dit aussi incident de sécurité, et nous traitons les réactions appropriées à ceux-ci au chapitre 1.4.

Quelle que soit la nature de l'agression, retenez ces deux choses essentielles:

- Soyez toujours conscients de la sécurité, que ce soit **pendant** ou **après** l'agression (si on vous agresse et que vous êtes forcé(e) de choisir entre deux réactions possibles, prenez toujours la plus sûre !).

- Après une agression, il faudra récupérer ses forces physiques et psychiques, trouver une solution à la situation et rétablir un cadre de travail sûr pour vous et votre organisation. Il est crucial de rassembler tous les éléments d'information disponibles sur l'agression: les faits, l'identité et le nombre d'agresseurs, les plaques d'immatriculation des véhicules, des descriptions, etc. Ceci peut permettre de constituer un dossier sur l'affaire qui devra être complété aussi vite que possible. Gardez des copies de toutes les pièces remises aux autorités pour conserver une copie du dossier complet.

En résumé

L'agression est le point culminant d'un processus qui a certainement inclus des incidents de sécurité et souvent des menaces.

Ainsi, une agression n'est pas un événement "inattendu".

L'agression peut être fortuite ou ciblée.

Il n'est pas aisé d'agresser des défenseurs des droits humains dans la mesure où il s'agit de figures publiques jouissant d'une certaine forme de soutien.

L'agression est le produit de trois facteurs interagissant les uns avec les autres:

- la partie à l'origine de l'action violente et des moyens
- le contexte et les déclencheurs conduisant l'agresseur à voir la violence comme une possibilité
- un environnement favorable

Une agression requiert des ressources et capacités adéquates, l'accès aux personnes, une possibilité de fuite rapide et un certain niveau d'impunité ou la décision de l'agresseur que le coût politique vaut la peine d'être payé.

Par conséquent, la prévention d'une attaque requiert des mesures pour que le coût politique reste aussi élevé que possible (réduire le niveau d'impunité) et pour ramener l'exposition physique au risque à un niveau aussi proche de zéro que possible.

CHAPITRE 1.6

Élaborer une stratégie de sécurité globale

Objectifs:

Reconnaître les stratégies et tactiques existantes

Analyser les stratégies et tactiques existantes

Définir la stratégie globale pour occuper l'espace de travail

Stratégies et tactiques de dissuasion ad hoc

Les défenseurs et les groupes menacés utilisent différentes stratégies de dissuasion ad hoc pour faire face aux risques perçus. Ces stratégies varient selon l'environnement (rural, urbain), le type de menace, les ressources sociales, financières et juridiques à disposition, etc.

La plupart des stratégies ad hoc peuvent être mises en place immédiatement en vue d'objectifs à court terme. C'est pourquoi elles peuvent être considérées comme des tactiques plutôt que comme des stratégies globales. La plupart des stratégies est liée à la perception individuelle et subjective du risque par les personnes concernées et peuvent occasionnellement causer des dommages au groupe, surtout si les stratégies utilisées ne peuvent pas être évalues et revues.

Les stratégies ad hoc sont étroitement liées au type et à la gravité de la menace ainsi qu'aux capacités et à la vulnérabilité du groupe.

Lors de la réflexion sur la sécurité et la protection, vous devez prendre en compte vos stratégies ad hoc et celles des autres personnes. Renforcez celles qui sont efficaces, limitez celles qui sont préjudiciables et essayez de respecter celles des autres (en particulier des stratégies ad hoc liées à des croyances religieuses ou culturelles).

Exemples de stratégies ad hoc adoptées par les défenseurs:

- Renforcer les barrières protectrices, cacher les objets de valeur.
- Éviter un comportement qui pourrait être mis en question par un autre acteur, surtout si le contrôle du territoire dans lequel vous travaillez fait l'objet de disputes militaires.

- Se cacher pendant les situations à haut risque, y compris dans des endroits difficiles d'accès comme la montagne ou la jungle, ou en changeant de maisons etc. Parfois les familles entières se cachent, parfois uniquement les défenseurs. Se cacher peut être fait pendant une nuit ou plusieurs semaines et peut inclure l'absence de contacts extérieurs.

- Rechercher la protection armée ou politique de l'un des acteurs en jeu.

- L'arrêt des activités, la fermeture des bureaux, l'évacuation. La migration forcée (déplacement interne ou bien en tant que réfugié) ou bien l'exil.

- S'en remettre à la "chance" ou bien faire appel à des croyances religieuses ou "magiques".

- Devenir plus secret, y compris avec ses collègues: choisir le déni en refusant de parler des menaces; la consommation excessive d'alcool, le surmenage, le comportement erratique.

Les défenseurs mettent également en œuvre des stratégies de réaction. Celles-ci peuvent consister en la publication de rapports pour rendre un sujet particulier public, faire des déclarations, organiser des manifestations etc. Dans de nombreux cas, ces stratégies ne sont pas équivalentes à des stratégies à long terme, mais parent uniquement au plus pressé. Dans certains cas, les stratégies adoptées peuvent engendrer des problèmes pour la sécurité bien plus grands que ceux auxquels ils étaient censés répondre.

Analyser les stratégies de dissuasion

Qu'il s'agisse de stratégies de dissuasion ad hoc ou globales, tenez compte des aspects suivants:

- **Réactivité:** vos stratégies peuvent-elles répondre rapidement aux besoins de la sécurité d'un individu ou d'un groupe?

- **Adaptabilité:** vos stratégies peuvent-elles être rapidement adaptées aux nouvelles circonstances une fois le risque d'une attaque passé? Un défenseur peut avoir différents choix à sa disposition, comme par exemple se cacher ou bien habiter dans la maison d'autres personnes. De telles stratégies peuvent paraître faibles ou manquant de stabilité, mais elles sont souvent d'une grande efficacité.

- **Durabilité:** vos stratégies résistent-elles à l'épreuve du temps en dépit des menaces ou des attaques non mortelles?

- **Efficacité:** vos stratégies protègent-elles de manière adéquate les personnes ou groupes concernés?

- **Réversibilité:** si vos stratégies ne fonctionnent pas ou si la situation change, sont-elles réversibles et/ou peuvent-elles être modifiées?

Gérer le risque après une évaluation du risque

Une fois l'évaluation du risque faite, il est impératif d'examiner les résultats. Comme il est impossible de mesurer la "quantité" de risque auquel vous êtes exposé, vous devez développer une bonne compréhension du **niveau** de risque.

Selon les défenseurs ou les organisations, les niveaux de risque peuvent être perçus différemment. Ce qui est inacceptable pour certains défenseurs peut être acceptable pour d'autres, même à l'intérieur de la même organisation. Plutôt que de discuter ce qui "doit" être fait ou de déterminer si vous êtes en mesure de continuer le travail malgré le risque, les seuils de risque, qui varient en fonction des personnes, doivent être pris en compte: il est impératif de trouver un seuil de risque acceptable pour tous les membres du groupe.

Cela dit, il existe différentes manières de gérer le risque:

- Vous pouvez **accepter** le risque tel qu'il est, parce que vous vous sentez en mesure de le supporter.
- Vous pouvez **réduire** le risque en agissant sur les menaces, les vulnérabilités et les capacités
- Vous pouvez **partager** le risque par des actions concertées avec d'autres défenseurs pour rendre des menaces potentielles concernant un défenseur ou une organisation moins effectives.
- Vous pouvez **différer** un risque en modifiant vos activités ou bien en modifiant votre approche pour réduire les menaces potentielles.
- Vous pouvez **échapper** au risque en réduisant ou cessant vos activités (dans certains cas cela peut impliquer l'exil).
- Vous pouvez **ignorer** le risque en refusant d'en tenir compte. Il est inutile d'ajouter que ce n'est pas la meilleure solution.

Tenez compte du fait que le niveau de risque diffère selon chaque organisation et chaque individu impliqué dans un cas de droits humains et que les attaquants ont généralement tendance à frapper le maillon le plus faible.

Exemple:

Prenons le cas d'un paysan tué par la milice privée d'un propriétaire foncier. Il est possible que plusieurs organisations ou personnes soient impliquées, comme par exemple un groupe d'avocats de la principale ville voisine, un syndicat local de paysans et trois témoins (des paysans vivant dans un village proche). Il est crucial d'évaluer les différents niveaux de risque liés à chacune des ces parties prenantes en vue de planifier avec justesse la sécurité de tous.

En résumé

En matière de sécurité, les défenseurs ne partent pas de zéro. Ils ont tous développé des façons de gérer les risques et les menaces. Le contraire impliquerait qu'ils ne soient plus présents ou qu'ils aient cessé leur travail.

Les défenseurs ont développé des stratégies et des tactiques de dissuasion ad hoc. Certains auront peut être développé une stratégie de dissuasion globale.

Quelles que soient les stratégies, elles devront tenir compte au moins des critères suivants: réactivité, adaptabilité, durabilité, efficacité et réversibilité.

Une évaluation du risque doit être réalisée en vue de déterminer s'il est "acceptable". De plus, le défenseur devra agir pour réduire, partager, différer le risque ou échapper au risque.

Les défenseurs des droits humains et les environnements hostiles

Trop souvent les défenseurs des droits humains travaillent dans des environnements hostiles. Les raisons en sont multiples. Beaucoup d'entre elles sont liées au fait que leur travail peut les amener à s'affronter à de puissants acteurs qui violent les lois internationales sur les droits humains, que ce soit des gouvernements ou autorités de l'État, des forces de sécurité, des groupes armés de l'opposition ou des milices armées privées. Ces acteurs peuvent riposter en essayant de mettre fin au travail des défenseurs, par des moyens qui vont de la répression voilée de tentatives de libre expression à des menaces déclarées et des offensives directes. Le degré de tolérance par les acteurs dépendra du travail des défenseurs. Les acteurs jugeront qu'ils peuvent accepter certaines activités, mais en condamneront d'autres. En règle générale, leur décision au cas par cas est voulue.

Deux observations doivent être faites à ce propos: dans de nombreux cas, seuls certains éléments **à l'intérieur** d'un groupe d'acteurs complexe (comme ceux mentionnés ci-dessus) sont hostiles aux défenseurs. Par exemple, certains membres d'un gouvernement attacheront de l'importance à la protection des défenseurs, alors que d'autres voudront leur porter atteinte. Les défenseurs peuvent rencontrer une hostilité lors de bouleversements politiques par exemple, dans le cas d'élections ou d'événements politiques marquants.

L'espace de travail sociopolitique des défenseurs des droits humains

Ce manuel examine la protection et la sécurité des défenseurs des droits humains qui travaillent dans des environnements hostiles et les mesures propres à renforcer leur sécurité. Il existe bien sûr des actions sociopolitiques: les campagnes et initiatives des défenseurs des droits humains visent à consolider la reconnaissance effective des droits humains par la société ou à exiger des acteurs politiques qu'ils prennent des mesures plus efficaces. Souvent, il nous arrive de ne pas considérer ces activités comme relevant de la sécurité sauf lorsque nous remarquons qu'elles ont eu une incidence positive sur la protection de **l'espace de travail sociopolitique** des défenseurs des droits humains.

Cet espace d'activité sociopolitique est défini par **toute activité que le défenseur peut mener sans dépasser son seuil personnel de tolérance au risque**. En d'autres termes, le défenseur perçoit un "large éventail d'activités politiques possibles et associe à chacune d'entre elles un certain coût ou un ensemble de conséquences." En définissant certaines conséquences comme "tolérables, et d'autres comme intolérables, le défenseur circonscrit un espace politique défini."[17]

Par exemple:

> *un groupe de défenseurs peut s'occuper d'un cas de violation des droits humains jusqu'à ce que l'un des membres du groupe reçoive une menace de mort. S'ils considèrent qu'ils ont un espace sociopolitique suffisant, ils peuvent décider d'informer le public de cette menace, et éventuellement de poursuivre leur travail. En revanche, si leur espace sociopolitique leur paraît réduit, ils peuvent juger que dénoncer la menace entraînera un prix inacceptable. Ils pourraient même stopper de travailler sur ce dossier provisoirement et améliorer leurs capacités de sécurité dans l'intervalle.*

Le concept de risque "tolérable" peut varier au fil du temps et différer énormément d'un individu à un autre ou d'une organisation à une autre. Pour certains, la torture ou la mort d'un membre de la famille constituent les risques les plus insupportables. D'autres défenseurs estiment que l'emprisonnement est un risque tolérable tant qu'il leur permet d'atteindre leurs objectifs. Pour d'autres encore, le seuil peut être atteint dès la première menace.

Cet espace politique d'activité, en plus d'être défini subjectivement par ceux qui y évoluent, est très sensible au moindre changement de l'environnement politique national. Il faut considérer qu'il s'agit d'un espace fluctuant et relatif.

La sécurité et l'espace de travail des défenseurs des droits humains

Toutes les stratégies de sécurité peuvent être résumées en quelques mots: vous voulez étendre et protéger votre espace de travail. En termes rigoureusement sécuritaires, l'espace de travail des défenseurs exige au moins un niveau de tolérance minimale des principaux acteurs de la région, essentiellement des

[17] Cette définition et les autres éléments-clés de ce concept ont été empruntés à Mahony et Eguren (1997), p. 93. (Unarmed Bodyguards). Ils ont aussi développé un modèle d'analyse d'espace politique qui intègre l'espace de travail des défenseurs à l'accompagnement de protection des défenseurs.

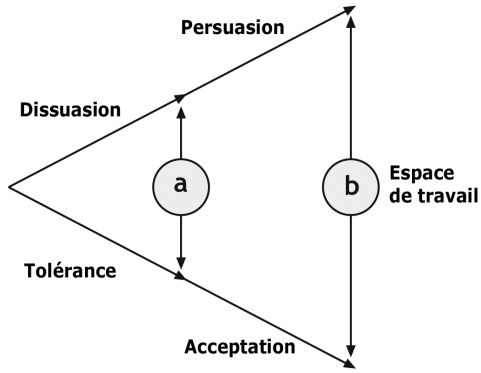
autorités politiques et militaires ainsi que des groupes armés, susceptibles d'être touchés par le travail des défenseurs et donc d'agir à leur encontre.

Il peut s'agir d'une tolérance **explicite**, comme l'autorisation officielle des autorités, ou **implicite**, comme dans le cas de groupes armés. La tolérance sera d'autant plus solide que l'acteur compte pouvoir retirer des avantages du travail des défenseurs. Il sera plus faible si l'acteur entrevoit des coûts connexes. Dans ce cas, son degré de tolérance dépendra du coût politique d'une offensive contre des défenseurs. Ces questions sont particulièrement importantes dans les conflits armés où les défenseurs ont affaire à plusieurs parties armées. L'un de ces acteurs armés peut juger que le travail des défenseurs avantage son adversaire. La reconnaissance ouverte de ce travail par une partie tierce peut aussi causer la malveillance de son adversaire.

L'espace de travail des défenseurs des droits humains peut être représenté par deux axes:

- Le premier représente le degré de tolérance ou d'acceptation de votre travail par un acteur par rapport à l'impact de votre travail sur ses objectifs ou ses intérêts stratégiques (le binôme tolérance - acceptation).

- Le deuxième montre votre capacité à dissuader des agressions en raison de coûts politiques élevés, puis votre capacité à dissuader l'acteur en invoquant des raisons rationnelles ou morales, voire votre capacité à le persuader des avantages politiques s'il renonce à vous agresser ou à violer les droits humains (le binôme dissuasion - persuasion).



Il est possible d'élargir votre espace de travail au fil du temps. Faire accepter le travail des défenseurs par une stratégie de persuasion devrait prendre en compte les besoins des citoyens, votre image, les procédures, l'intégration, etc. que représente l'intersection "b". Inversement, dans les régions de conflit, l'espace se limite généralement à ce que la tolérance des acteurs armés autorise, et découle partiellement du coût politique que représentent les agressions à l'encontre des défenseurs (dissuasion), l'espace étant alors réduit à l'intersection "a".

De manière générale, l'espace "b" sera plus probablement occupé par des défenseurs non revendicatifs que par des défenseurs dénonçant publiquement des abus, à moins que l'agresseur potentiel effectue une conversion morale et soit persuadé du bien-fondé du travail du défenseur au point de l'accepter.

- Étendez votre espace de travail en augmentant la tolérance et l'acceptation.
- Étendez votre espace de travail en augmentant la dissuasion et la persuasion.

Déterminer et mettre en oeuvre une stratégie de sécurité globale contribuera à augmenter le coût politique des actions contre les défenseurs en réduisant le niveau d'impunité des agresseurs potentiels et en étendant l'espace de travail des défenseurs. C'est pourquoi la stratégie de sécurité globale dépend en grande partie des capacités de communication.

Elargir l'espace de travail en augmentant la tolérance et l'acceptation

Votre travail peut affecter les objectifs et les intérêts stratégiques d'une personne ou d'un groupe qui se moque des droits humains, ce qui peut entraîner un climat hostile pour les défenseurs. Afin d'obtenir l'acceptation, ou au moins une tolérance vis à vis de vos activités, il est important de limiter l'affrontement à un strict minimum. Ci-dessous quelques suggestions pour y parvenir:

- **Offrez des informations et des formations à propos de la nature et de la légitimité du travail des défenseurs.** Les fonctionnaires du gouvernement et autres acteurs seront plus enclins à coopérer s'ils connaissent et comprennent votre travail et vos motivations. Il ne suffit pas d'informer les hauts fonctionnaires car le travail quotidien des défenseurs les amène à côtoyer tous les échelons d'une hiérarchie dans tous les organismes d'Etat. Vous devez consentir un effort soutenu pour informer et former le maximum de fonctionnaires à tous les échelons.

- **Clarifiez les objectifs du travail des défenseurs.** Dans tout conflit, il est utile de clarifier et de définir les limites de votre travail. Cela permettra de dissiper certains malentendus et de limiter les confrontations inutiles qui peuvent empêcher les défenseurs à mener leurs activités à bien.

- **Limitez vos objectifs pour qu'ils correspondent à votre espace sociopolitique d'activité.** Lorsque le travail des défenseurs touche les intérêts stratégiques d'un acteur armé, celui-ci peut réagir de manière violente et attacher moins d'importance à son image. Certaines activités rendent les défenseurs plus vulnérables que d'autres, donc veillez à ce que vos objectifs correspondent autant que possible au risque que vous pouvez assumez et à vos capacités de protection.

- **Dans vos stratégies, prévoyez des voies de sorties permettant à l'acteur de "sauver la face".** Si vous devez vous affronter à un acteur à propos de violations de droits humains, donnez-lui la possibilité de s'attribuer le mérite d'avoir pris les mesures réclamées par la situation.

- **Concluez des alliances** différentes dans autant de secteurs sociaux que possible.

- **Trouvez le juste moyen** entre la transparence de votre travail qui démontre que les défenseurs légitimes n'ont rien à cacher, et la protection nécessaire de toute information susceptible de compromettre votre travail et votre sécurité.

- **Finalement,** retenez que la légitimité et la qualité de votre travail sont des conditions nécessaires pour protéger votre espace de travail, mais elles ne suffiront parfois pas. Il vous faudra également acquérir des capacités de dissuasion des agresseurs potentiels (voir ci-dessous).

Élargir votre espace de travail en augmentant la dissuasion et la persuasion

Les défenseurs qui oeuvrent dans des milieux hostiles devraient être en capacité d'invoquer le risque de coûts politiques suffisamment lourds pour que l'agresseur renonce par peur: c'est ce qu'on appelle **dissuasion**.

Il est utile de distinguer entre dissuasion "générale" et dissuasion "immédiate". **La dissuasion générale** est le résultat combiné des efforts nationaux et internationaux de protection des défenseurs, à savoir tout ce qui fait comprendre les conséquences négatives des agressions contre les défenseurs. Ceci comprend les campagnes thématiques générales, des formations ou des informations sur la protection des défenseurs. D'un autre côté, la dissuasion immédiate envoie le message précis à un agresseur donné de ne pas s'en prendre à une cible concrète. La dissuasion **immédiate** s'impose lorsque la dissuasion générale a échoué ou est jugée inefficace, et lorsque les efforts de protection se concentrent sur des cas particuliers.

La **persuasion** est un concept plus complet. Elle se définit comme le résultat de tout effort pour convaincre son adversaire de renoncer à exécuter l'action hostile envisagée. L'argumentation rationnelle, l'appel à la morale, une coopération renforcée, l'appel à des sentiments d'humanité, le détournement d'attention, des politiques non agressives et la prévention peuvent tous être utilisés comme moyens de persuasion. Chacune de ces tactiques est utilisée à différents moments par les défenseurs sur le plan national et international. Les défenseurs ne peuvent pas recourir trop fréquemment aux "menaces" directes: la stratégie vise davantage à rappeler aux acteurs les **conséquences possibles** de leurs décisions.

La dissuasion à l'oeuvre

Afin de vérifier si votre dissuasion est efficace, une série de conditions doivent être remplies:

1 ◆ **Les défenseurs doivent spécifier et communiquer clairement à l'agresseur quels types d'actions sont intolérables.** La dissuasion ne fonctionnera pas si l'agresseur ignore quels actes provoqueront une réaction.

2 ◆ **L'organisation des défenseurs doit exprimer sa résolution à dissuader de l'agression de façon à ce que l'agresseur en soit conscient.** L'organisation doit également disposer d'une stratégie de dissuasion en vigueur.

3 ◆ **L'organisation des défenseurs doit avoir les moyens de dissuader et en convaincre l'agresseur.** Si la menace de mobiliser une réaction nationale ou internationale n'est pas crédible, il n'y a pas lieu de s'attendre à un effet de protection.

4 ◆ **Les défenseurs doivent savoir qui est l'agresseur.** Les commandos de tueurs agissent souvent en pleine nuit et revendiquent rarement leurs actions. Ceci revient donc souvent à analyser qui peut avoir un intérêt direct à agresser. Afin que les réactions nationales ou internationales soient plus efficaces, la supposition d'une "implication du gouvernement", même avérée, exige des informations plus spécifiques concernant les factions de l'appareil d'Etat à l'origine de l'attaque.

5 ◆ **L'agresseur doit avoir eu l'intention réelle de passer à l'acte puis s'être rétracté** parce que le coût politique - grâce à la résolution des défenseurs - paraissait plus lourd que les avantages.

Il est difficile pour les défenseurs de dissuader un agresseur que leur "détermination à la dissuasion" laisse indifférent. Ceci est le cas quand les gouvernements peuvent faire l'objet de sanctions de la communauté internationale mais qu'ils ne peuvent à leur tour punir l'auteur réel des violations des droits humains. Par exemple, les milices privées peuvent être hors de la portée des gouvernements ou ne pas partager ses intérêts. Dans ces cas, l'agresseur pourra même tirer parti des agressions contre les défenseurs, parce que des agressions placeront le gouvernement dans une situation délicate et nuiront à son image.

Les défenseurs ne seront jamais certains que leur "détermination à dissuader" suffira à dissuader une agression potentielle. L'agresseur peut espérer des avantages dont les défenseurs ne sont pas conscients. Analyser la situation aussi précisément que possible relève du défi permanent et peut s'avérer impossible par manque d'information cruciale. Les organisations des défenseurs doivent donc mettre au point des solutions de repli extrêmement flexibles et une capacité de réaction rapide à des événements inattendus.

Tableau: prévention d'une agression directe - les différents résultats de la protection

PRÉVENTION D'UNE AGRESSION DIRECTE: LES DIFFÉRENTS RÉSULTATS DE LA PROTECTION	
1 **Changements dans le comportement de l'agresseur:** suite à lsuasion des agresseurs par l'augmentation du coût politique d'une agression. 2 **Changements d'attitude, de la part des acteurs responsables de la protection, quant au respect de la déclaration des NU sur les DDH:** dissuader les agresseurs en augmentant la probabilité que les autorités prennent la défense des défenseurs ou punissent les auteurs d'une agression.[18]	→ **Confrontation** et **réduction des menaces** (en agissant soit directement sur la source, soit contre les actions entreprises par la source)
3 **Réduction de la faisabilité d'une agression:** suite à la réduction de l'exposition des défenseurs par l'amélioration de leur environnement de travail, la gestion correcte de la peur et du stress, le développement de plans de sécurité, etc.	→ Réduction des **vulnérabilités**, augmentation des **capacités**

[18] Voir le chapitre 1.1. Par exemple, après qu'un défenseur ait dénoncé des menaces, le procureur, la police ou tout autre instance enquête sur les événements ayant eu lieu, et cette investigation a pour résultat une action contre ceux qui menacent le défenseur. Cela devrait du moins être l'objectif d'une réaction pour prévenir une agression.

CHAPITRE 1.7

Préparer un plan de sécurité

Objectif:

Apprendre à élaborer un plan de sécurité

Elaborer le plan de sécurité

Maintenant que vous avez dressé le tableau des parties prenantes de la protection, déterminé les forces en présence, évalué votre risque, identifié les stratégies existantes et mis au point votre stratégie globale, il ne devrait pas être difficile d'élaborer un plan de sécurité.

La sécurité est complexe et résulte de la combinaison de plusieurs facteurs. Certains doivent toujours être présents. D'autres peuvent être ajoutés lorsque c'est nécessaire. Ensemble, ils constituent le plan de sécurité.

Ils doivent être mis en oeuvre au niveau des personnes, de l'organisation et entre organisations.

Comment faire? Voici comment procéder en quelques étapes:

1 ◆ **Les éléments du plan.** Un plan de sécurité vise à réduire le risque. Il comportera donc au moins trois objectifs, en fonction de votre évaluation du risque:

- Réduire le degré de risque auquel vous êtes exposé.
- Réduire vos vulnérabilités.
- Renforcer vos capacités.

Un plan de sécurité devrait inclure des politiques de routine ainsi que des mesures et protocoles pour gérer des situations spécifiques:

Des politiques quotidiennes et des mesures pour le travail de routine:

- Une communication permanente, du "réseautage", un code éthique, une culture de la sécurité, une gestion de la sécurité, etc.
- Des mesures permanentes pour s'assurer que le travail de routine est effectué en conformité avec les normes de sécurité.

Des protocoles pour des situations spécifiques:

- Des protocoles préventifs: par exemple, comment préparer une conférence de presse ou bien une visite dans un lieu éloigné.
- Des protocoles d'urgence pour réagir à des problèmes spécifiques comme la détention ou la disparition.

Plus nombreuses seront les politiques de gestion quotidiennes et ces mesures appliquées, plus les protocoles destinés aux situations spécifiques fonctionneront.

Quelques exemples:

- si un ensemble permanent de politiques et de mesures concernant la gestion de l'information est mis en oeuvre, la perquisition d'un bureau (urgence) aura moins d'impact.

- si un ensemble permanent de politiques de gestion et de mesures concernant les relations publiques est mis en oeuvre, une mise en garde déclenchée par une attaque contre un défenseur des droits humains aura plus de probabilités de conduire à une réaction des parties prenantes-clé, atteignant ainsi l'objectif déterminé par le défenseur en cas d'attaque.

  Pour atteindre cet objectif, le plan de sécurité devra comprendre une communication permanente avec les détenteurs d'obligations et les parties prenantes-clé. Une politique de comportement éthique sera exigée et mise en application dans tous les aspects du travail de l'organisation, ainsi qu'à tous les niveaux concernant les individus/l'organisation/les organisations entre elles.

- dans le cas d'une détention, si le plan permanent en place comprend une politique de comportement éthique des individus, les infractions personnelles de droit commun peuvent alors être raisonnablement exclues comme cause de la détention et le protocole d'urgence peut donc être mis en oeuvre. Bien sûr, une infraction de droit commun pourrait servir de prétexte; mais l'avocat ou le juriste de l'organisation saura alors quoi faire. De plus, grâce au plan, le défenseur détenu saura quelles mesures sont prises, pourra les imaginer ou les réciter, presque en concordance avec le timing prévu, et parviendra à "décompresser" (impact psychologique), sachant que les mesures nécessaires auront étés prises à l'extérieur. Il vaut mieux éviter de défier les autorités et de s'exposer à davantage de risque que celui déjà encouru.

- dans le cas de missions sur le terrain dans des zones dangereuses, les parties prenantes importantes auront été informées au préalable et se tiendront prêtes à réagir en cas de besoin jusqu'à ce que l'équipe revienne saine et sauve.

2 ◆ **Les responsabilités et ressources pour mettre en oeuvre le plan.** Pour s'assurer que le plan est appliqué, des habitudes de sécurité doivent être intégrées aux activités quotidiennes:

- Incluez régulièrement l'évaluation de la situation et la sécurité à vos ordres du jour.
- Consignez et analysez tous les incidents de sécurité.

- Attribuez des responsabilités.
- Affectez des ressources (du temps et un budget) à la sécurité.

3 ◆ **Élaborer le plan - par où commencer?** Si vous avez évalué les risques pour un défenseur ou une organisation, vous pourriez avoir une longue liste de vulnérabilités, de plusieurs types de menaces et d'un certain nombre de capacités. Il n'est pas réaliste de tout couvrir à la fois. Par où commencer? C'est très facile:

- **Sélectionnez quelques menaces.** Déterminez la priorité des menaces énumérées, qu'elles soient réelles ou potentielles, à l'aide d'un des critères suivants: la menace la plus grave, à savoir par exemple des menaces de mort explicites; **OU** la menace la plus probable et grave, à savoir si des organisations similaires à la vôtre ont été attaquées, si vous êtes clairement potentiellement menacé; **OU** le type de menace auquel vous êtes le plus vulnérable parce que vous le risquez davantage.
- **Enumérez vos vulnérabilités pertinentes.** Il faut aborder ces vulnérabilités en premier lieu, mais souvenez-vous que toutes les vulnérabilités ne correspondent pas à toutes les menaces (voir l'exemple ci-dessous).
- **Enumérez vos capacités pertinentes.**

Exemple

d'un processus de sélection aboutissant à l'élaboration d'un plan de sécurité:

Le directeur d'une organisation de défenseurs (située en milieu rural ou urbain) a été l'objet de menaces de mort sérieuses. L'organisation évalue le risque que représentent les menaces et énumère ses capacités et ses vulnérabilités.

En conclusion, l'organisation décide de mettre en oeuvre les mesures de sécurité suivantes: pourvoir tous les placards de verrous, munir les fenêtres du bureau de barreaux en fer, acheter de nouveaux téléphones portables pour les membres encourant le plus grand risque et rendre publiques les menaces faites à l'encontre du défenseur.

En général, l'objectif est de définir et de démontrer la façon dont chaque mesure contribuera à réduire le risque spécifique (en d'autres termes, comment est-ce que cette mesure augmentera la sécurité concernant le risque spécifique)?

Par conséquent: comment est-ce que toutes ces mesures vont réellement réduire la menace de mort spécifique contre le directeur? (Bien sûr, elles pourraient contribuer à améliorer la sécurité globale de l'organisation, mais ce n'est pas le moment de le faire).

Demandez-vous: quelle est la probabilité que la menace de mort soit mise à exécution dans le bureau sachant que des personnes seront présentes? Le chef doit-il se trouver dans le bureau pour être tué? Le chef menacé ne sera pas toujours au bureau; il existe donc de nombreuses autres vulnérabilités telles que quitter le bureau seul et tard la nuit, voyager dans des régions isolées, ignorer des mesures de sécurité alors qu'on se trouve chez soi...

Bien que munir les placards de serrures soit important, cela ne réduira bien sûr pas les menaces à l'encontre du directeur de l'organisation et ses vulnérabilités. La même chose est valable pour les barreaux de fer des fenêtres. En effet, quelle utilité pourraient-ils avoir contre un tireur d'élite ou une grenade?

Comment est-ce qu'un téléphone portable peut réduire un risque? (Que peut-on réellement faire avec un téléphone portable pour empêcher quelqu'un de tuer le directeur?).

Il pourrait être plus utile de réduire l'exposition du directeur lors de ses trajets de son domicile à son lieu de travail ou pendant les week-ends. Voilà les vulnérabilités qui doivent être prises en considération d'abord. Elles sont bien plus importantes dans le contexte de menaces de cet ordre.

Si le processus de sélection est fait correctement, vous pouvez maintenant aborder les menaces choisies, les vulnérabilités et les capacités dans votre plan de sécurité et vous pouvez être relativement sûr de pouvoir réduire le risque dès le départ.

Veuillez noter que c'est une façon ad hoc d'élaborer un plan de sécurité. Il existe des façons plus "formelles", mais cette méthode est la plus directe. Elle garantit de traiter les questions de sécurité les plus urgentes, à condition que vous ayez correctement évalué le risque, et permet d'obtenir un plan "vivant" et "réaliste", et c'est cela qui compte en matière de sécurité. (Veuillez vous reporter à la liste détaillée des composants possibles des plans de sécurité en fin de chapitre, que vous pouvez également utiliser pour évaluer les risques).

Éléments possibles à inclure au plan de sécurité

Ce "menu" énumère des suggestions détaillées d'éléments qui peuvent être intégrés au plan de sécurité. Après avoir évalué les risques, vous pourrez choisir et combiner ces idées pour compléter votre plan de sécurité.

Un plan de sécurité comprend des éléments qui deviennent des processus politiques (comme par exemple rencontrer les autorités et les institutions internationales, réclamer la protection que l'État doit fournir) et des processus opérationnels (comme des préparations de routine pour les missions sur le terrain).

Éléments de politiques permanentes à prendre en compte et mesures à prendre pour le travail ordinaire:

- Le mandat de l'organisation, sa mission et ses objectifs généraux (les connaître et les respecter).

- Une déclaration de politique de sécurité de l'organisation (la connaître et la respecter).

- La sécurité devant être un élément transversal de tous les aspects de votre travail quotidien, prévoir des évaluations du contexte et des risques, analyse des incidents, tout comme l'évaluation de la sécurité.

- Prévoir comment garantir que l'ensemble des membres reçoive une formation correcte et suffisante en matière de sécurité et que les responsabilités de sécurité soient transmises lorsque les personnes concernées quittent l'organisation?

- Organiser la répartition des responsabilités: qui doit faire quoi, et dans quels cas?

- Pour la gestion d'une crise de sécurité, créer une cellule de crise ou un groupe de travail, déléguer la responsabilité des relations avec la presse, de l'information de la famille, etc.

- Prévoir les responsabilités de sécurité incombant à l'organisation: planification, suivi, contrats d'assurance, responsabilité civile, etc.

- Concernant les responsabilités individuelles de sécurité: prévoir des mesures pour la réduction permanente du risque, la gestion des périodes de temps libre et des activités de loisir, faire des rapports et consigner les incidents de sécurité, prévoir des sanctions (certains de ces éléments peuvent faire l'objet de clauses du contrat de travail, s'ils sont pertinents).

- Définir les politiques de l'organisation en matière de:
  - repos, temps libre et gestion du stress
  - sécurité des victimes et témoins
  - santé et prévention des accidents
  - liens avec les autorités, forces de sécurité et groupes armés
  - gestion et stockage de l'information, traitement des documents confidentiels et de l'information
  - votre propre image par rapport aux valeurs religieuses, sociales et culturelles
  - gestion de la sécurité dans les bureaux et les domiciles (y compris pour les visiteurs)
  - maniement d'argent liquide ou d'objets de valeur
  - moyens de communication et protocoles
  - l'entretien des véhicules
  - sécurité des femmes défenseurs
  - sécurité des défenseurs LGBTI
  - …

Eléments à prendre en compte pour l'adoption de mesures propres à une activité particulière et à des situations extraordinaires:

- prévoir des protocoles de prévention et de réaction concernant:
  - la préparation des missions sur le terrain
  - les mines terrestres
  - la réduction du risque d'être la cible de délits et crimes de droit commun, d'incidents armés ou d'agressions sexuelles

- la réduction du risque d'accidents pendant les déplacements ou dans des zones dangereuses
- des protocoles de réaction concernant: les urgences médicales et psychologiques (y compris sur le terrain)
- les blessures physiques, les agressions, y compris les agressions sexuelles
- les vols
- les réactions appropriées lorsqu'une personne attendue ne se présente pas alors qu'elle le devrait
- l'arrestation et la détention
- l'enlèvement ou la disparition
- les incendies et autres accidents
- l'évacuation
- les catastrophes naturelles
- les fouilles légales ou illégales ou les effractions dans les bureaux ou les domiciles
- si une personne est la cible de tirs
- si une personne est assassinée
- les situations de coup d'Etat
- ...

Mettre en œuvre un plan de sécurité

Les plans de sécurité sont importants, mais difficiles à mettre en oeuvre. La mise en œuvre est bien plus qu'un simple processus technique, c'est un processus qui implique l'organisation dans son ensemble. Ceci signifie découvrir les angles d'attaque et les circonstances favorables à sa mise en place, ainsi que les obstacles et les difficultés.

Un plan de sécurité doit impérativement être mis en œuvre à au moins trois niveaux:

1 ◆ au niveau **individuel**. Chaque personne doit respecter le plan afin que ce dernier fonctionne.

2 ◆ au niveau de l'**organisation**. L'organisation entière doit respecter le plan.

3 ◆ au niveau **inter-organisationnel**. Une certaine coopération entre les organisations intervient normalement dans le maintien de la sécurité.

Exemples de "portes d'entré" et d'opportunités

pour lancer la mise en oeuvre d'un plan de sécurité

- Plusieurs incidents de sécurité mineurs sont survenus dans votre organisation ou dans une autre et cela inquiète un certain nombre de membres.
- La situation sécuritaire du pays est préoccupante.
- De nouveaux membres arrivent et doivent être formés pour appliquer de bonnes pratiques de sécurité dès le départ.
- Une autre organisation vous propose une formation sur la sécurité.

Exemples de **difficultés** et **d'obstacles** lors de la mise en place d'un plan de sécurité:

- Certains pensent que plus de mesures de sécurité signifieront une charge de travail encore plus lourde.
- D'autres pensent que la sécurité de l'organisation est déjà satisfaisante.
- "Nous n'avons pas le temps pour des choses comme ça!"
- "D'accord. Prenons le temps nécessaire d'en discuter samedi matin, mais cela s'arrêtera là."
- "Nous devons mieux prendre soin de ceux que nous voulons aider, pas de nous-mêmes."

Moyens pour améliorer la mise en oeuvre d'un plan de sécurité

- **Tirez parti des circonstances et des "portes d'entrée"** pour faire face aux problèmes et vaincre la résistance.
- **Avancez étape par étape.** Il est inutile de croire que tout peut être fait en même temps.
- **Insistez sur l'importance de la sécurité pour votre mission principale au nom des victimes.** Soulignez que la sécurité des témoins et des membres d'une famille est décisive pour l'efficacité de votre mission principale et que la meilleure gestion passe par l'intégration de bonnes pratiques de sécurité à tous les domaines du travail. Dans les formations ou dans les discussions, prenez des exemples qui démontrent l'impact négatif probable d'une sécurité négligée pour les témoins et les victimes.
- Un plan établi par deux "experts" et imposé à toute l'organisation est probablement voué à l'échec. **La participation est la clé** en matière de sécurité.
- **Un plan doit être réaliste et faisable.** Une longue liste de choses à faire avant chaque mission sur le terrain ne fonctionnera pas. Limitez-vous au strict minimum nécessaire pour garantir la sécurité. C'est une raison de plus pour impliquer ceux qui réellement effectuent le travail, par exemple les membres qui font des missions régulières.
- **Le plan n'est pas un document ponctuel.** Il doit être révisé et mis à jour constamment.
- **Il ne faut pas voir le plan comme générant "encore plus de travail" mais comme "une meilleure façon de travailler".** Persuadez les membres et collègues de ses avantages, comme par exemple, celui d'éviter les rapports répétés sur un même problème. Veillez à ce que les rapports sur les missions comportent une section consacrée à la sécurité, discutez systématiquement de la sécurité en réunions d'équipe, intégrez les aspects de sécurité à d'autres formations, etc.

- **Insistez sur le fait que la sécurité n'est pas une affaire de choix personnel**. Des décisions individuelles, certaines positions et un certain comportement qui affectent la sécurité peuvent avoir des conséquences pour la sécurité des victimes, témoins, des membres de la famille des victimes et des collègues. Il faut s'engager collectivement à mettre en œuvre de bonnes pratiques de sécurité.

- **Du temps et des ressources doivent être affectés** à la mise en œuvre du plan puisqu'on ne devra pas travailler à l'amélioration de la sécurité pendant le temps libre des personnes. En effet, pour qu'elles soient perçues comme "importantes", les activités de sécurité doivent figurer parmi les activités "importantes".

- **Tous doivent adhérer de manière visible au plan,** en particulier les directeurs et les personnes responsables du travail collectif. Le fait que certaines personnes refusent obstinément d'adhérer au plan ne doit pas rester sans conséquences.

En résumé

Un plan de sécurité doit diminuer les vulnérabilités et augmenter les capacités pour que les menaces soient réduites ou bien que leur réalisation soit rendue moins réalisable, ce qui a pour conséquence de réduire le risque.

Un plan de sécurité doit correspondre à vos besoins actuels et à votre espace de travail.

L'objectif n'est pas de couvrir un domaine sociopolitique étendu, mais plutôt de se situer dans l'espace adéquat, c'est à dire occuper l'espace que l'on peut se permettre du point de vue de la sécurité, et couvrir l'environnement de travail, autant que possible, par le biais du "réseautage" en accord avec d'autres organisations. Il s'agit de la mise en place de procédures de sécurité qui doivent transcender les différences politiques.

La sécurité est l'affaire de tous et elle est individuelle, organisationnelle et inter-organisationnelle.

La sécurité est complexe et résulte de la combinaison de plusieurs facteurs. Certaines mesures doivent toujours être présentes; d'autres peuvent être ajoutées à des moments spécifiques. Ensemble, ils constituent le plan de sécurité.

Votre plan de sécurité devrait comprendre des politiques de routine, des mesures et des protocoles spécifiques à des situations.

Les deux comprennent des procédures politiques et opérationnelles.

CHAPITRE 1.8

Améliorer la sécurité au travail et au domicile

Objectifs:

Évaluer la sécurité au travail et au domicile.

Planifier, améliorer et vérifier la sécurité au bureau et au domicile.

La sécurité au travail et au domicile

La sécurité du siège de l'organisation ou de ses bureaux, et des domiciles des défenseurs est d'une importance fondamentale pour leur travail. Nous prendrons le temps d'étudier en profondeur la manière d'analyser et d'améliorer la sécurité d'un bureau ou d'un domicile. (Par simplicité, nous parlerons désormais uniquement de "bureaux" bien que l'information qui suit s'applique de la même façon à la sécurité au domicile.)

Aspects généraux de la sécurité au bureau

Notre objectif pour l'amélioration de la sécurité se résume en quelques mots: **empêcher tout accès non autorisé**. Ceci est valable que votre bureau se trouve en zone urbaine ou rurale. Dans de rares cas il pourra être également nécessaire de protéger un bureau contre une attaque éventuelle (ex. contre un bombardement).

Ceci nous amène à la première considération: les vulnérabilités d'un bureau. Elles peuvent augmenter les risques, en fonction du degré de menace auquel vous êtes confronté. Par exemple, s'il existe un risque que l'on vous vole du matériel ou des informations, vous devrez vous attaquer aux vulnérabilités. Une alarme de nuit (électrique, si vous avez accès à l'électricité, un gardien de nuit ou alors un chien) ne servira pas à grand-chose si on ne prévoit personne pour se déplacer et vérifier ce qui se passe. Par ailleurs, s'il y a effraction violente en plein jour, une grille renforcée sur les portes ou des alarmes ne seront pas très utiles. En bref, agissez en fonction des menaces auxquelles vous êtes confronté et du contexte dans lequel vous travaillez.

Les vulnérabilités d'un bureau doivent être évaluées à la lumière des menaces rencontrées.

Il est cependant important de trouver un moyen terme entre l'adoption de mesures de sécurité appropriées et le fait de donner l'impression aux personnes de l'extérieur que vous "cachez" ou "protégez" quelque chose, car cela suffit à vous exposer au risque. En matière de sécurité d'un bureau, il vous faudra souvent choisir entre un profil bas ou des mesures plus visibles lorsqu'elles s'imposeront. D'un autre côté, un agresseur potentiel sera conscient du fait que votre bureau contient des objets de valeur ou des informations sensibles et que vous avez "besoin" de le protéger.

La sécurité d'un bureau n'est équivalente qu'à la sécurité de son élément le plus faible.

Si des personnes veulent entrer dans votre bureau à votre insu, ils ne choisiront pas le point d'accès le plus difficile pour le faire. D'ailleurs, le moyen le plus facile d'entrer dans un bureau pour observer ce qui se passe à l'intérieur des locaux revient parfois à frapper tout simplement à la porte et à entrer.

Emplacement du bureau

Que le bureau soit situé dans une zone rurale ou urbaine, les facteurs à considérer en créant un bureau sont: le voisinage, si l'immeuble est associé à des personnes particulières ou à des activités passées, l'accessibilité pour le public et aux moyens de transport, le risque d'accidents, la facilité de mettre en place des mesures de sécurité dans l'immeuble en question, etc. (Voir également évaluation du risque de l'emplacement ci-dessous).

Il est utile d'étudier quelles mesures de sécurité ont été prises par d'autres dans le même quartier. Si les mesures sont nombreuses, cela peut indiquer qu'il y a de l'insécurité liée à la criminalité de droit commun. Il est aussi important de parler de la sécurité locale avec les habitants des environs. Dans tous les cas, veillez à ce que les mesures de sécurité puissent être prises sans attirer une attention excessive. Il est également utile de faire connaissance avec les habitants puisqu'ils pourront vous informer de la moindre chose suspecte dans le voisinage.

Lors du choix d'un bureau, il convient de prendre en compte quel public il recevra. Un bureau qui dispensera des conseils juridiques aux victimes devra répondre à d'autres exigences qu'un bureau servant avant tout de lieu de travail administratif. Il est important de prendre en considération la question de l'accès à ce bureau par les transports publics. Les trajets entre les domiciles des membres et le lieu où se déroulent la majeure partie des activités, etc. seront-ils dangereux? Les environs doivent être analysés, particulièrement si l'on veut éviter de devoir traverser des zones dangereuses.

Dans certains cas, le bureau pourra tout simplement être la maison du défenseur (voir zones rurales ci-dessous). Cependant, il faut considérer les éléments énumérés plus haut.

Une fois que l'emplacement a été choisi, il est important d'évaluer ponctuellement la donne, qui peut évoluer, comme par exemple quand un "élément indésirable" s'installe dans le quartier.

Liste de contrôle pour choisir le bon emplacement d'un bureau dans des zones desservies:	
Environs immédiats:	Statistiques sur les délits et les crimes; proximité de cibles potentielles d'attaques armées telles que les installations militaires ou gouvernementales; locaux sûrs pouvant servir de refuge; proximité d'autres organisations nationales ou internationales avec qui vous êtes en relation.
Relations:	Type de voisins; propriétaire, anciens locataires, utilisations précédentes des locaux.
Facilité d'accès:	Une ou plusieurs routes d'accès en bon état (plus il y en a, mieux c'est. Mais gardez à l'esprit que l'agresseur potentiel aura également un plus large choix); accès par les transports publics et privés.
Services publics:	Eau, électricité et ligne téléphonique.
Éclairage public:	Dans les environs.
Prédisposition aux accidents et risques naturels	Risques d'incendies, d'inondations graves, de glissements de terrain, de déversement de substances toxiques, proximité avec usines de produits toxiques.
Structure physique du bâtiment:	Solidité du bâtiment, aménagement pour l'installation d'un équipement de sécurité, portes et fenêtres, périmètre et barrières de protection, différents accès (voir ci-dessous).
Pour les véhicules:	Un garage, ou au moins une cour intérieure ou un espace fermé, avec barrière de parking.

Dans le cas où le bureau est situé dans une zone isolée, éloignée et mal desservie, la liste de contrôle peut indiquer des éléments n'existant pas dans la zone. Des capacités devront alors être développées pour compenser les vulnérabilités spécifiques. Par exemple, s'il n'y a pas d'autres organisations dans les environs, vous pouvez envisager de faire appel à la communauté locale. Ou bien, au cas où il n'y aurait pas d'eau courante ou d'extincteur, assurez-vous d'avoir un récipient d'eau suffisamment grand et toujours rempli.

Accès de tiers au bureau: barrières matérielles et procédures pour les visiteurs

Vous savez maintenant que le but principal de la sécurité du bureau est de refuser l'accès aux personnes non autorisées. Une ou plusieurs personnes pourraient faire effraction pour voler, obtenir des informations, cacher quelque chose qui puisse vous compromettre ultérieurement, comme de la drogue ou des armes, vous menacer, etc. Chaque cas est unique, mais l'objectif reste identique: l'empêcher.

L'accès à un édifice est contrôlé par des **barrières matérielles** (grillages, portes, portails), par des **moyens techniques** (comme les alarmes avec lumière) et par des **procédures d'accès** aux visiteurs. Chaque barrière et chaque procédure sont autant de **filtres** par lesquels celui / celle qui voudra entrer dans le bureau devront obligatoirement passer. Idéalement, il faudrait une combinaison particulière de plusieurs de ces filtres afin de former plusieurs couches de protection en mesure de dissuader différentes tentatives d'entrée non autorisée.

Les barrières matérielles

Les barrières servent à bloquer physiquement l'entrée aux personnes non autorisées. Le niveau d'utilité des barrières physiques dépend de leur **solidité** et de la capacité à boucher **toutes les brèches vulnérables** des murs.

Le bureau peut avoir des barrières matérielles dans trois zones:

1 ◆ La **zone extérieure**: les clôtures, les murs ou autres, au-delà d'un jardin ou d'une cour. En l'absence de périmètre externe physique, vous pourriez définir l'extension du périmètre extérieur que vous allez effectivement surveiller.

2 ◆ Le **périmètre** du **bâtiment**.

3 ◆ La **zone intérieure**: les barrières qui peuvent être créées à l'intérieur d'un bureau pour protéger une ou plusieurs pièces. Ceci est très utile dans les bureaux avec beaucoup de passage, puisque cela permet de délimiter une zone accessible au public et une zone plus restreinte qui peut être protégée par des barrières supplémentaires.

La zone extérieure

Le bureau devrait être délimité de manière visible à l'extérieur par des clôtures hautes ou basses, de préférence solides et hautes pour rendre l'accès plus difficile. Une grille ou du treillis métallique exposeront davantage le travail de l'organisation, et il est donc souhaitable de faire construire un mur en brique ou d'un matériau solide similaire.

En l'absence de périmètres extérieurs clairement délimités, vous pouvez décider de la surface de la zone extérieure à contrôler visuellement pour déceler les éléments indésirables s'approchant de votre bureau. Vous pouvez envisager d'utiliser des miroirs convexes.

Le périmètre du bâtiment

Ceci comprend les murs, les portes, les fenêtres et le plafond et le toit. Les portes et les fenêtres doivent avoir des verrous de qualité et être renforcés par des grilles, de préférence avec des barreaux verticaux et horizontaux qui soient fermement scellés dans la paroi. Le toit devrait offrir une bonne protection, et ne pas être simplement une tôle de zinc ou une couche de tuiles. Si le toit ne peut pas être renforcé, il faut bloquer tous les accès possibles au toit depuis la rue ou les bâtiments alentour.

Si la fenêtre de votre bureau donne sur la rue ou sur un espace public, placez votre bureau de telle façon qu'on ne puisse pas vous voir. Si elle donne sur de la végétation, assurez-vous que personne ne peut s'y cacher sans être vu.

Certains bureaux peuvent avoir plusieurs portes et par conséquent, l'une d'entre elles pourra servir de "sortie de secours". Rappelez-vous qu'une sortie de secours peut également être utilisée comme point d'accès par des éléments indésirables.

Dans un endroit où il existe un risque d'attaques armées, il faut établir des zones protégées à l'intérieur même du bureau (voir dans ce manuel le chapitre sur la sécurité dans des zones de conflit armé).

La zone interne

Il en va de même que pour les bâtiments et les locaux. Il est très utile d'avoir un espace à sécurité maximale dans les locaux et généralement, il est assez facile à créer. Même un coffre-fort peut compter comme zone intérieure de sécurité.

Si votre bureau est constitué d'une pièce seulement, vous pouvez envisager d'utiliser des cloisons mobiles pour fermer les espaces privés à la vue des visiteurs.

En ce qui concerne les clés

- Aucune clé ne devrait être visible ou accessible aux visiteurs. Gardez toutes les clés dans un placard ou un tiroir fermé par une serrure à combinaison, la combinaison ne devant être communiquée qu'à quelques membres du groupe. Veillez à la changer régulièrement pour une meilleure sécurité.

- Si les clés portent des étiquettes individuelles, n'indiquez en aucun cas les pièces, placards ou tiroirs auxquels elles correspondent car cela faciliterait un cambriolage. Utilisez un numéro, une lettre ou un code couleur à la place.

Les mesures techniques: l'éclairage et les alarmes

(au cas où votre bureau ait accès à l'électricité ou soit équipé d'un générateur électrique).

Les mesures techniques renforcent les barrières matérielles ou les procédures d'admission des visiteurs, comme par exemple les judas, les interphones, les caméras vidéo (voir ci-dessous). **Les mesures techniques ne sont utiles que si elles visent à la dissuasion des cambrioleurs.** Elles doivent provoquer un **effet automatique déterminé**, par exemple attirer l'attention des voisins, de la police ou d'une entreprise de sécurité privée. Si ce n'est pas le cas, et que l'intrus sait qu'il n'en sera rien, de telles mesures ne servent à rien et se limiteront à empêcher des délits de vol insignifiants ou à garder une trace des personnes qui sont rentrées.

- **L'éclairage** autour du bâtiment (des cours intérieures, des jardins, du trottoir) et sur le palier est essentiel.

- **Les alarmes** ont des buts multiples, y compris celui de détecter les intrus et de dissuader d'éventuels intrus d'entrer ou de continuer d'essayer d'entrer.

Une alarme peut déclencher un signal sonore d'avertissement à l'intérieur d'un bureau, une lampe de sécurité, un son, un bruit ou une sonnette très sonores, ou un signal dans un centre de sécurité indépendant. Une alarme audio est utile pour attirer l'attention mais peut être contre-productive dans les situations de conflit ou si vous ne vous attendez pas à ce que les voisins réagissent. Il faut faire un choix judicieux entre une alarme sonore et une alarme lumineuse (soit une lumière fixe et puissante, soit une lumière rouge intermittente). Cette dernière peut suffire à dissuader un intrus parce qu'elle annonce d'autres mesures une fois l'intrus détecté.

Les alarmes devraient être posées aux points d'accès (les cours intérieures, les portes et les fenêtres, et les espaces vulnérables tels que les pièces où sont conservées des informations sensibles). Les alarmes les plus simples sont les détecteurs de **mouvement**, qui activent une lumière, émettent un signal sonore ou déclenchent une caméra lorsqu'un mouvement est détecté.

- Les alarmes devraient:
  - Avoir une **batterie** pour continuer à fonctionner lors des coupures de courant.
  - Comporter un mécanisme à **retardement** pour les désactiver si un membre les avait déclenchées par mégarde.
  - Pouvoir être activées **manuellement** au cas où le personnel aurait besoin de les activer.
  - Être faciles **d'installation** et **d'entretien**.
  - Se distinguer visiblement de l'alarme contre les incendies.

Les caméras de vidéo surveillance

Les caméras vidéo peuvent être un facteur d'amélioration des procédures d'admission (voir ci-dessous) ou d'enregistrement des personnes qui entrent dans le bureau. Cependant, l'enregistrement doit se faire depuis un point hors d'accès de l'intrus qui pourrait ouvrir la caméra et détruire la cassette.

Vous devrez cependant vérifier que les caméras ne dissuadent pas votre public cible, à savoir les victimes et les témoins, et qu'elles ne soient pas prises pour un butin facile qui attire les cambrioleurs. Il est bon de signaler aux visiteurs qu'ils seront filmés par une affiche d'information (le droit au respect de la vie privée est également un droit humain).

Éclairage et alarmes si votre bureau n'a pas d'électricité ou n'est pas équipé d'un générateur d'électricité

Évitez simplement de rester dans votre bureau une fois la nuit tombée.

L'alarme électrique peut être remplacée par un autre système d'alarme: prenez un gardien de nuit, des chiens; faites appel aux voisins, à la famille, à la communauté: persuadez-les d'agir comme "votre système d'alarme".

Les entreprises privées de sécurité

Ce domaine est sensible. Dans beaucoup de pays, les entreprises de sécurité privées sont constituées d'anciens membres des forces de sécurité. Il existe des cas documentés sur des personnes impliquées dans la surveillance des défenseurs des droits humains et dans les attaques à leur encontre. Il relève donc du bon sens de se méfier des entreprises de sécurité si vous craignez une surveillance ou des attaques par les forces de sécurité. De plus, si une entreprise a accès à vos bureaux, elle pourrait cacher des micros ou laisser entrer d'autres personnes.

Si vous estimez avoir besoin de recourir à une entreprise de sécurité, vous devriez vous prémunir par un contrat clair établissant ce que vous autorisez son personnel à faire en votre nom, ce que vous n'autorisez pas et à quelles parties du bâtiment vous lui donnez libre accès. Evidemment, il vous appartient de veiller à ce que le contrat soit respecté.

Par exemple:

> *Si vous avez engagé un service de sécurité qui envoie un garde inspecter en cas de déclenchement de l'alarme, ce garde pourra éventuellement avoir accès aux zones sensibles de votre bureau et poser des puces dans votre salle de réunion.*

Il est préférable que vous ayez le droit de donner votre accord sur les personnes spécifiques qui travailleront pour vous (et que vous les sélectionniez), mais c'est rarement le cas.

Si les gardes de sécurité sont armés, l'organisation des droits humains se doit de connaître exactement les règles d'utilisation des armes. Mais il est encore plus essentiel de comparer les avantages de l'utilisation de ces armes aux inconvénients. Les armes de petit calibre ne constituent aucune dissuasion à l'encontre d'assaillants munis d'armes à plus gros calibre (ce qui est en général le cas); par contre, si les agresseurs sont prévenus de la présence dans vos locaux d'armes à petit calibre, ils décideront peut-être d'entrer par effraction prêts à ouvrir le feu pour se protéger lors de l'attaque. En d'autres termes, votre capacité armée (petites armes à feu) incitera probablement les assaillants à utiliser leurs armes de gros calibre. À ce stade, si vous estimez avoir besoin de gardes armés de mitrailleuses, posez vous la question de savoir si vous disposez vraiment de l'espace sociopolitique nécessaire pour faire votre travail?

Filtres de procédures d'admission

Les barrières matérielles doivent être complétées par le "filtre" de **procédures d'admission.** De telles procédures déterminent quand, comment et qui peut avoir accès au bureau. L'accès aux zones sensibles, à savoir aux clés, aux informations et à l'argent, doit être restreint.

Le moyen le plus facile pour entrer dans un bureau où travaillent des défenseurs des droits humains est de frapper à la porte et d'entrer. Beaucoup de personnes le font tous les jours. Afin de concilier le principe d'accueil d'un bureau des droits humains et le besoin de maîtriser qui veut entrer et pourquoi, il vous faut des procédures d'admission appropriées.

En général, les personnes ont une raison particulière de vouloir entrer ou de frapper à votre porte. Elles veulent en général poser des questions ou effectuer une livraison, et elles ne demanderont pas nécessairement l'autorisation au préalable. Examinons ceci cas par cas:

Quelqu'un se présente et souhaite entrer pour une raison donnée

Vous devrez alors suivre trois étapes simples:

1 ◆ **Demander à la personne de décliner son identité et pourquoi elle souhaite entrer.** Si lui/elle demande à voir un membre particulier, consultez la personne concernée. Si cette personne est absente, demandez au visiteur de revenir plus tard ou un autre jour ou alors d'attendre en dehors de la zone restreinte. Il est important d'utiliser des judas, des caméras ou un interphone (ces deux derniers, pour ne pas devoir vous rapprocher de la porte) afin d'éviter de devoir ouvrir pouvoir refuser l'entrée le cas échéant ou en cas d'assaut violent ou forcé. Il est également bon de définir une salle d'attente pour les visiteurs qui soit physiquement séparée de l'entrée interne du bureau. Si vous devez avoir une zone publique facile d'accès, veillez à équiper le bureau de barrières physiques qui empêchent l'accès aux zones restreintes.

Une personne peut vouloir entrer pour prétendument vérifier ou réparer la plomberie ou l'installation électrique ou effectuer d'autres travaux de maintenance. Elle peut aussi prétendre être un représentant des médias, ou un fonctionnaire public, etc. Faites-vous toujours confirmer leur identité par l'entreprise ou l'organisation à laquelle ils disent appartenir avant de les laisser entrer. Souvenez-vous que ni un uniforme ni une carte d'identité ne constituent la garantie d'authenticité d'une identité, tout particulièrement dans une situation à risque moyen ou élevé.

2 ◆ **Décidez d'autoriser ou de refuser l'accès.** Une fois que vous connaissez la raison d'entrer de votre visiteur et son identité, vous devez décider si vous autorisez l'accès ou non. Il ne suffit pas que quelqu'un vous donne une raison d'être venu pour le laisser entrer. Si vous avez un doute sur le but de sa visite, ne le laissez pas entrer.

3 ◆ **Surveillez les visiteurs jusqu'à leur départ.** Une fois que le visiteur est entré dans le bureau, faites en sorte qu'il soit surveillé pendant la durée entière de sa visite. Il est utile d'avoir une salle séparée où rencontrer les visiteurs, éloignée des zones à l'accès restreint.

Notez précisément les détails de chaque visite en indiquant le nom du visiteur, son organisation, le but de sa visite, quels collaborateurs il a rencontrés, l'heure de son arrivée et de son départ. Ceci peut s'avérer particulièrement précieux après un incident de sécurité au moment d'analyser ce qui n'a pas fonctionné.

Quelqu'un se présente, téléphone ou sonne pour poser des questions

Quelles que soient les affirmations de la personne, vous ne devez en aucun cas l'informer de l'endroit où se trouve le collègue ou les personnes demandées, ni donner d'informations personnelles. Si la personne insiste, demandez-lui de

laisser un message, de rappeler ou de revenir à un autre moment, ou encore proposez de prendre un rendez-vous avec la personne qu'elle désire rencontrer.

Il arrive souvent que des personnes se présentent aussi par erreur, demandant si untel habite-là ou si vous avez des objets à vendre. Certains veulent vous vendre quelque chose, les mendiants peuvent vouloir de l'aide. Si vous leur refusez le droit d'entrée et ne donnez pas de renseignements, vous éviterez tout risque de sécurité.

Quelqu'un veut livrer un objet ou un paquet

Le risque peut provenir du fait que le contenu de l'objet ou du paquet pourrait vous compromettre ou vous blesser, surtout s'il s'agit d'une lettre ou d'une lettre piégée. Quelque soit son aspect, ne touchez ni ne manipulez le paquet avant d'avoir pris ces trois mesures simples:

1 ◆ **Vérifiez si le destinataire annoncé attend le paquet.** Il ne suffit pas que le destinataire connaisse l'expéditeur car on a pu emprunter son nom. Si le destinataire n'attend pas de paquet, il/elle doit vérifier auprès de l'expéditeur annoncé qu'il a effectivement fait un envoi. Si le paquet a été simplement envoyé à l'adresse du bureau, vérifiez l'expéditeur. Attendez et réfléchissez ensemble à la question avant de prendre une décision finale.

2 ◆ **Décidez d'accepter ou non le paquet ou la lettre**. Si l'identité de l'expéditeur ne peut être vérifiée, ou que cela doit prendre du temps, la meilleure solution est de le refuser, surtout dans un environnement à risque moyen ou élevé. Vous pouvez toujours demander qu'il soit relivré ultérieurement ou dire que vous irez le retirer vous-même à la poste.

3 ◆ **N'égarez pas le paquet au bureau.** Jusqu'à ce que le destinataire l'accepte, assurez-vous de savoir où se trouve le paquet au bureau à tout moment.

Dans certains pays, les paquets sont annoncés par téléphone et c'est le défenseur qui doit aller les chercher. Il pourrait s'agir d'un piège pour attirer le défenseur et l'exposer à une agression. Comme le téléphone peut ne pas être enregistré, il est impossible de connaître la personne appelant. Une fois que le défenseur s'est informé sur l'origine du paquet, il peut vérifier l'information avec l'expéditeur supposé et lui demander l'itinéraire du paquet. Ensuite le défenseur décidera si oui ou non il peut aller chercher le paquet sans danger. Il peut également demander à la personne qui appelle de déposer le paquet au bureau en suivant la procédure décrite plus haut. S'il s'agit d'un piège, il est probable que la personne qui appelle évite de se présenter au bureau.

Durant les réceptions ou les soirées

Dans ces cas-là, la règle est simple: ne laissez entrer personne que vous ne connaissez pas en personne. Seules les personnes connues de vos collègues dignes de confiance devraient avoir le droit d'entrer, et ceci seulement lorsque ce col-

lègue est présent et qu'il peut identifier le visiteur. Si une personne se présente et dit connaître une personne du bureau qui est absente, ne la laissez pas entrer.

Les défenseurs peuvent hésiter et trouver difficile de se renseigner sur un visiteur et de lui demander de partir. Cependant, ils ne sont pas obligés d'agir en leur nom; ils peuvent simplement dire qu'ils ne sont pas autorisés à laisser entrer la personne.

Pour toutes les procédures d'admission, rappelez-vous que si le visiteur est fiable, il appréciera les précautions prises par l'organisation en matière de sécurité et que si le visiteur ne l'est pas, il sera conscient que des mesures de sécurité sont appliquées. Dans tous les cas, les défenseurs peuvent se donner simplement le droit de refuser l'accès au visiteur inconnu. Si cela peut être utile, ils peuvent se servir d'un "non et...": "je ne suis pas autorisé à laisser entrer des visiteurs inconnus, cependant, si vous désirez laisser votre carte de visite, je serais heureux de vous tenir informé des événements publics à venir".

Prenez note des appels téléphoniques et des visiteurs

Il peut également être utile de prendre note des appels téléphoniques et des numéros de téléphone ainsi que de noter toutes les personnes qui visitent l'organisation (dans certaines organisations les nouveaux visiteurs doivent présenter un document les identifiant et l'organisation enregistre le numéro du document).

Faire des heures supplémentaires au bureau

Il faudra mettre en place des procédures pour les membres du personnel qui font des heures supplémentaires. Les membres d'une organisation qui font des heures supplémentaires tard le soir devraient faire rapport à des heures précises à d'autres membres prédéterminés, faire particulièrement attention lorsqu'ils quittent les locaux, etc.

Chaque membre de l'organisation a la responsabilité de prendre des mesures à l'encontre de toute personne qui n'observerait pas pleinement les procédures d'admission. Il/elle devrait également consigner tout mouvement de personnes ou de véhicules suspects dans le cahier des incidents de sécurité. Le même principe est valable pour tout objet placé à proximité du bâtiment, afin d'écarter tout risque potentiel de bombe. Si vous suspectez qu'il s'agit d'une bombe, ne l'ignorez pas, **n'y touchez pas**, et contactez la police.

Lors d'un éventuel déménagement de bureau ou quand des clés ont été perdues ou volées, il est primordial de faire changer toutes les serrures de la zone d'entrée des bureaux.

Liste de contrôle: identifier les points faibles des procédures d'admission:
◆ **Qui** accède régulièrement à **quelles** zones et **pourquoi?** Limitez l'accès aux visiteurs absolument nécessaires.
◆ Distinguer les différents **types** de visiteurs (messagers, ouvriers de maintenance, techniciens informatiques, membres d'ONG lors de réunions, personnalités publiques, invités, etc.) **et établir des procédures d'admission adaptées à chaque type.** Chaque membre devrait connaître les procédures pour chaque type de visiteur et assumer la responsabilité de les appliquer.
◆ Une fois le visiteur à l'intérieur du bureau, peut-il avoir accès à des points faibles? Établissez des stratégies pour l'éviter.
Liste de contrôle: l'accès aux clés
◆ **Qui** a accès à **quelles** clés et **quand?**
◆ Où et comment les **clés** et leurs doubles sont-ils gardés?
◆ Existe-il un **contrôle des doubles** des **clés** en circulation?
◆ Est-il possible que quelqu'un puisse faire des **doubles des clés sans autorisation?**
◆ **Qu'arrive-t-il si quelqu'un perd une clé?** La serrure correspondante doit être changée, à moins qu'il soit certain que la clé ait été égarée par mégarde et que personne ne puisse identifier le propriétaire de la clé et son adresse. Souvenez-vous qu'une clé peut être volée, par exemple, lors d'un cambriolage fictif, dans le but de s'assurer l'accès au bureau.

Liste de contrôle: les procédures générales de sécurité du bureau

- Equipez les locaux en extincteurs et en lampes électriques (fonctionnant sur piles que vous pouvez remplacer). Assurez-vous que tous les membres du bureau savent s'en servir.
- Installez un générateur d'électricité si des coupures de courant vous paraissent vraisemblables. Les coupures de courant peuvent compromettre la sécurité (lampes, alarmes, téléphones, etc.), surtout dans les zones rurales.
- Ayez à portée de main une liste de numéros de téléphone d'urgence locaux, tels que la police, les pompiers, les ambulances, les hôpitaux les plus proches, etc.
- En cas de risque de conflit à proximité, prévoyez des provisions d'aliments et d'eau.
- Localisez les endroits sûrs à l'extérieur du bureau en cas d'urgence (par exemple, les bureaux d'autres organisations).

- Aucune personne étrangère à l'organisation ne devrait être laissée **seule** dans une zone vulnérable avec accès aux clés, aux informations ou objets de valeur.

- **Les clés:** ne laissez jamais des clés à un endroit auquel les visiteurs pourraient avoir accès. Ne "cachez" jamais des clés hors de l'entrée du bureau puisque cela les rendrait accessibles (et pas cachées).

- **Les procédures d'admission:** si un intrus potentiel est autorisé à entrer dans le bureau, les barrières de sécurité n'offrent bien évidemment plus aucune protection. Les points principaux à retenir sont:
  - Chaque membre est responsable du contrôle des visites et de l'admission.
  - Tout visiteur doit être accompagné pendant la durée entière de sa présence dans le bureau.

- Si un visiteur sans autorisation est découvert dans le bureau:
  - N'affrontez en aucun cas quelqu'un qui vous semble pouvoir être violent pour parvenir à ses fins (au cas où par exemple la personne serait armée). Dans ce cas, alertez vos collègues, trouvez un endroit sûr pour vous cacher et tentez d'obtenir l'aide de la police.
  - Essayez avec la plus grande prudence d'entrer en contact avec la personne ou demandez de l'aide aux autres personnes présentes dans le bureau ou à la police.

- Dans des situations à haut risque, gardez toujours le contrôle sur les objets sensibles, comme les informations stockées sur le disque dur, afin de les rendre inaccessibles et emportez-les en cas d'évacuation d'urgence.

- Sachez qu'en cas de confrontation avec un intrus potentiel, les personnes qui travaillent dans le bureau sont en première ligne. Veillez à ce qu'elles aient reçu la formation et le soutien nécessaires pour être en mesure de réagir à tout moment à toute situation possible, et cela sans se mettre en danger.

Inspections régulières de la sécurité du bureau

Contrôler ou inspecter régulièrement la sécurité du bureau est fondamental car les conditions de sécurité et les procédures varieront probablement au fil du temps, comme lorsque l'équipement se détériore ou que les membres se renouvellent fréquemment et lorsque les activités changent. Il est également important que les membres fassent leurs les règles de sécurité.

La personne responsable de la sécurité doit procéder au minimum à une révision de la sécurité du bureau **tous les six mois**. A l'aide de la liste ci-dessous, cela ne devrait pas prendre plus d'une ou deux heures. La/le responsable de la sécurité doit s'assurer que tous les membres se sont exprimés avant la rédaction du rapport final sur la sécurité et le soumettre ensuite à l'organisation qui prendra les décisions qui s'imposent et les mettra à exécution. Le rapport devrait alors être classé jusqu'à la révision de sécurité suivante.

LISTE DE CONTRÔLE: RÉVISION DE LA SÉCURITÉ DU BUREAU

OBJET DE LA RÉVISION:
EFFECTUÉE PAR:
DATE:

1 ◆ **CONTACTS EN CAS D'URGENCE:**

◆ Y a-t-il une liste à jour et à portée de main des numéros de téléphone et adresses des autres ONG locales, des hôpitaux d'urgence, de la police, des pompiers et des ambulances, ambassades et réseaux internationaux?

2 ◆ **BARRIÈRES TECHNIQUES ET MATÉRIELLES (EXTÉRIEURES, INTERNES ET À L'INTÉRIEUR):**

◆ Vérifiez l'état et le fonctionnement des portails/clôtures externes, des portes d'entrée du bâtiment, des fenêtres, des murs et du toit.

◆ Vérifiez l'état et le bon fonctionnement de l'éclairage à l'extérieur, des alarmes, des caméras ou des interphones vidéo.

◆ Vérifiez les procédures relatives aux clés; vérifiez que les clés soient bien gardées et étiquetées selon un code garantissant leur sécurité; vérifiez l'attribution des responsabilités du contrôle des clés et de leurs doubles; vérifiez que les clés et les doubles fonctionnent. Veillez à ce que les serrures soient changées en cas de perte ou de vol des clés, et qu'on ait fait un rapport sur la perte ou le vol.

3 ◆ **LES PROCÉDURES D'ADMISSION ET LE "FILTRAGE" DES VISITEURS:**

◆ Existe-il des procédures d'admission en vigueur pour chaque type de visiteur? Est-ce que les membres les connaissent et les appliquent?

◆ Faites le bilan de tous les incidents de sécurité enregistrés liés aux procédures d'admission ou "filtres".

◆ Demandez aux membres du personnel responsables des procédures d'admission si celles-ci fonctionnent correctement et dans le cas contraire, quelles améliorations sont nécessaires.

4 ◆ **LA SÉCURITÉ EN CAS D'ACCIDENT:**

◆ Vérifiez l'état des extincteurs, des valves/tuyaux à gaz et des robinets d'eau, des prises électriques et des câbles, des générateurs d'électricité (s'ils existent) ajouter "et des véhicules".

5 ◆ **LES RESPONSABILITÉS ET LA FORMATION::**

◆ A-t-on désigné un(e) responsable de la sécurité? Est-ce efficace?

◆ Existe-il une formation sur la sécurité du bureau? Est-ce qu'elle aborde tous les éléments de cette révision? A-t-on veillé à former les nouveaux membres aux questions de sécurité? La formation est-elle efficace?

Dans les zones rurales:

Les défenseurs peuvent aussi travailler dans des zones rurales, soit dans un village, soit dans une zone éloignée et isolée. Ils peuvent ne pas avoir le choix de l'emplacement de leur bureau. Ils doivent cependant protéger leur espace de travail des visiteurs et objets indésirables.

Concernant un village: s'il est comparable à une micro-zone urbaine, la plupart des considérations citées plus haut sont valables et elles peuvent être complétées avec les observations suivantes.

Concernant un emplacement éloigné et isolé: assurez-vous que la communauté environnante, votre famille et vos amis peuvent contribuer à votre système d'alarme. Essayez cette possibilité et demandez-leur de vous rendre régulièrement visite à vous et à votre bureau (qu'il s'agisse de votre domicile ou non). Vous pourriez envisager d'avoir un chien dressé pour aboyer en cas de visites. Assurez-vous qu'il n'attaque pas les gens et qu'il ne puisse pas être approché facilement et empoisonné.

Prenez des chemins sûrs pour accéder à la zone et évitez de rester dehors la nuit. Vous pouvez envisager de mettre en place des relais de communication par le biais de personnes de confiance pour obtenir le plus rapidement possible une réaction de soutien au cas où vous en auriez besoin.

En résumé

L'objectif des mesures de sécurité pour le bureau et le domicile est de réduire le risque d'accès indésirables.

La sécurité d'un bureau / domicile n'est jamais plus élevée que son élément le plus faible.

Que votre bureau/domicile soit situé dans une zone urbaine ou rurale, vous pouvez utiliser l'équation[19] sur le risque en vue de réduire le risque d'accès indésirables.

Les menaces peuvent être assimilées à des conséquences du risque.

Faites la liste de toutes vos menaces/conséquences concernant le risque d'accès indésirables. Ensuite, par menace/conséquence, faites la liste des vulnérabilités et capacités correspondantes et améliorez-les.

[19] Voir le chapitre 1.2 sur l'évaluation du risque: menaces, vulnérabilités et capacités

CHAPITRE 1.9

La Sécurité pour les défenseurs des droits humains femmes

Objectifs:

Examiner la sécurité du point de vue des défenseurs des droits humains femmes.

Fournir aux défenseurs des droits humains femmes et hommes des connaissances et outils supplémentaires en matière de sécurité.

Introduction

Bien que la sécurité des défenseurs des droits humains femmes soit liée à la sécurité de tous les défenseurs des droits humains, nous avons décidé de dédier un chapitre spécifique à la sécurité de celles-ci parce que l'expérience dans ce domaine montre qu'elle n'est pas prise en compte dans sa spécificité de manière systématique. Il y a de multiples raisons à cela, liées au contexte social, culturel et religieux.[20] C'est pourquoi nous avons choisi d'introduire ce sujet par une brève compilation de commentaires puisés directement de l'expérience en ce domaine, laquelle souligne la convergence des intérêts et la collaboration nécessaire entre les défenseurs des droits humains hommes et femmes.

Les femmes en tant que défenseurs des droits humains

Les femmes ont toujours été des protagonistes importants de la défense et de la protection des droits humains. Pourtant, leur rôle n'a pas toujours été reconnu positivement. Les femmes travaillent seules et /ou collaborent avec des hommes pour défendre les droits humains.

Trop souvent malheureusement:

- elles doivent faire face non seulement à la violence liée à leur condition de femme en dehors de leur organisation, mais aussi aux préjugés et à la discrimination à l'intérieur des organisations de défense des droits humains.

[20] Ethique des soins: Dans son livre *In a Different Voice* (1982), Carol Gilligan (psychologue de Harvard) soutient que, contrairement à la morale des hommes basée sur la justice et les droits, celle des femmes se base sur les soins reconnaissant l'importance des relations humaines et de l'attention accordée aux besoins des autres. A partir de là, il est légitime de penser que si les hommes adhéraient à l'éthique des soins, il y aurait moins de violence.

- Il est souvent invoqué des excuses pour "reporter" la question du droit des femmes et pour ne pas en faire une priorité ou bien pour en faire un sujet "extraordinaire", comme s'il était question de priorités alors qu'il s'agit d'interdépendance avec les droits humains. Ceci se produit dans des organisations de défense de droits humains mixtes.

- les défenseurs des droits humains femmes sont très souvent considérés comme des auxiliaires par leurs collègues masculins. Les collaborateurs masculins refusent souvent des tâches considérées comme moins fondamentales, comme si leur virilité en dépendait.

Le sexisme, les préjugés de classe, le racisme, l'"esprit de caste", la xénophobie et l'homophobie sont plus ou moins les facettes d'une même logique sous-jacente qui est à l'origine des violations des droits humains contre les hommes, les femmes, les personnes d'une orientation sexuelle différente, les enfants, les personnes âgées, les groupes ethniques, les personnes pauvres... Elles ont toutes un impact sur la sécurité: par exemple, dans certains endroits, les parias ne sont pas du tout pris en compte pour l'élaboration d'un plan de sécurité: ni positivement (par exemple, en tant que personnes éventuellement conscientes de leur environnement) ni négativement (en tant qu'informateurs possibles de l'agresseur potentiel).

Le concept de violence contre les femmes subit souvent une entorse:

- on parle de lutter contre la violence "envers les femmes" plutôt que de lutter contre la violence "masculine" (on évite de préciser l'origine).

- on emploie l'euphémisme "violence conjugale" pour "violence masculine".

Or, en oeuvrant pour mettre fin à la violence masculine, la cessation de la violence conjugale devrait être l'un des résultats. Ce ne sont pas des sujets distincts.

Les femmes sont souvent considérées comme des êtres humains de moindre valeur, bien que la science moderne ait établi que les différences de genre n'entraînent aucune hiérarchie de capacités. Malgré ce, on continue socialement à les considérer comme inférieures sur ce plan, et par voie de conséquence à les considérer comme des êtres de moindre valeur. Cela paraît évident, mais l'expérience du terrain dans ce domaine et les ateliers de travail avec les défenseurs montrent que cette idée n'a pas été nécessairement intégrée. Ceci explique notre insistance.

Depuis que les femmes ont accès à l'école et à l'éducation, elles ont démontré qu'elles étaient aussi intelligentes que les hommes (pour ne citer que l'intelligence scolaire).

Il existe souvent une confusion entre intelligence et connaissances, ces dernières étant conditionnées par l'accès. La même chose est valable pour des minorités ethniques et tout autre groupe subissant des discriminations: ce n'est pas une question anthropologique, mais bien plutôt une question sociale. Une personne ou un groupe éduqué peut argumenter d'égal à égal et remettre en question l'ordre établi. Ceci peut expliquer pourquoi trop de filles et de femmes n'ont toujours pas accès à l'éducation.

Les femmes remarquent particulièrement la contradiction entre la défense des droits humains et la discrimination qu'elles subissent. Inévitablement, quelques fois, les femmes aimeraient dire à leurs collègues masculins de "retourner à la case départ" et de revenir une fois qu'ils en auront pris conscience et seront disposés à changer de comportement. Malgré ce, les femmes restent et poursuivent leur travail aux côtés de leurs collègues masculins. Il est d'ailleurs plus fréquent que des femmes rejoignent des activités de droits humains organisés par des hommes que l'inverse.

Quand des femmes sont victimes de violence, même quand il s'agit d'une seule femme (ou tout autre groupe ou individu), ce n'est pas une question de culture ou de religion mais de pouvoir.

Dans le cas de Nelson Mandela et de Desmond Tutu par exemple, l'apartheid n'a pas cessé parce que la dignité des noirs a soudain été reconnue, mais parce que quelques blancs ont tout à coup réalisé avoir perdu la leur. La même chose est valable pour une discrimination basée sur le genre et pour toute autre forme de discrimination.

Tant que des défenseurs de droits humains masculins ne comprendront pas que la discrimination basée sur le genre puise son origine dans la même logique perverse légitimant tous les autres types de discrimination, les mouvements de défenseurs des droits humains n'auront que la moitié de la force qu'ils pourraient potentiellement avoir. Et cela continuera à servir les fins des violateurs des droits humains: diviser pour régner.

Les droits des femmes
ne sont donc pas uniquement les droits des femmes

Ce chapitre n'est pas une tentative de changer les mentalités et les valeurs, mais il essaie de déterminer quel impact la discrimination basée sur le genre et toutes les autres formes de discriminations ont sur la sécurité et la protection des femmes d'abord, mais également sur celle des défenseurs masculins. Si un changement des mentalités peut être un but trop ambitieux, la dissuasion de discriminer ne l'est pas et implique un changement des comportements. Dans ce cas, la solidarité masculine sur les questions de sécurité concernant les femmes contribue à la sécurité de tous les défenseurs des droits humains.

Dans le contexte de la consultation internationale sur les défenseurs des droits humains femmes de Colombo, Sri Lanka, en 2005,[21] plus de documents ont été rédigés à ce sujet.

http://defendingwomen-defendingrights.org/pdf/WHRD-Proceedings.pdf

Agressions à l'encontre des femmes défenseurs des droits humains

Dans son **rapport annuel à la commission sur les droits humains de 2002**, Hina Jilani, l'ancienne représentante spéciale du Secrétaire général des Nations unies sur les défenseurs des droits humains, déclare que:

[21] Un guide très utile sur les defenseurs desdroits humains femmes de UNHCHR: http://www.unhchr.ch/defenders.tiwomen.htm. Voir aussi Rapport: Consultation sur les femmes DDH avec la Représentante spéciale du Secrétaire général sur les défenseurs des droits humains, avril 3-4 2003, publié par Asia Pacific Forum on Women, Law and Development. Essential actors of our time. Human rights defenders in the Americas, par Amnesty International.

Les femmes défenseurs des droits humains sont sur un pied d'égalité avec leurs collègues hommes lorsqu'elles se mettent en première ligne pour la défense et la protection des droits humains. Mais en tant que femmes cela les expose à un risque propre à leur genre qui vient s'ajouter au risque vécu par les hommes.

En premier lieu, en tant que femmes, elles sont plus repérées. En effet, les femmes défenseurs peuvent provoquer plus d'hostilité que leurs collègues masculins car en tant que femmes défenseurs des droits humains elles bravent parfois certaines valeurs culturelles, religieuses et sociales de la féminité et du rôle de la femme dans un pays ou une société donnés. Dans ce contexte, elles peuvent subir des violations des droits humains en raison de leur activité de défense des droits humains, et ceci d'autant plus qu'elles appartiennent au genre féminin et que leur travail peut aller à l'encontre de stéréotypes de la société comme celuide la nature soumise des femmes, ou encore contester les notions sociétales sur le statut des femmes.

En second lieu, il n'est pas improbable que l'hostilité, le harcèlement et la répression subis par les défenseurs femmes ciblent précisément des femmes, depuis la violence verbale explicitement liée au genre jusqu'au harcèlement sexuel et au viol.

A cet égard, l'intégrité professionnelle des femmes et leur position dans la société peuvent être menacées et discréditées de façon spécifique, comme lorsque leur probité est rituellement mise en doute quand elles revendiquent leur droit à la santé sexuelle et à la procréation, ou à l'égalité face aux hommes, y compris leur droit à une vie sans discrimination et violence. Ainsi, des femmes défenseurs des droits humains ont été jugées au nom de lois condamnant la jouissance et l'exercice de droits garantis par le droit international, inculpées sans fondement à cause de leurs convictions et de leur défense des droits des femmes.

En troisième lieu, les violations des droits humains perpétrées à l'encontre des femmes défenseurs des droits humains peuvent, à leur tour, avoir des répercussions spécifiques au genre. Par exemple, les violences sexuelles et le viol d'une femme défenseur des droits humains en détention provisoire peut entraîner une grossesse et la contagion par des maladies sexuellement transmissibles (les MST), notamment le VIH.

Certains droits spécifiques aux femmes sont presque exclusivement défendus et protégés par des femmes défenseurs des droits humains. La défense et la protection des droits des femmes peut être un facteur de risque supplémentaire, puisque la revendication de certains de ces droits est perçue comme un défi au patriarcat et un facteur de perturbation des mœurs culturelles, religieuses et sociales. Défendre le droit des femmes à la vie et à la liberté a valu aux défenseurs femmes une atteinte à leur propre vie et liberté dans certains pays. De même, une personnalité connue pour la défense des droits des femmes a été poursuivie pour apostasie pour avoir dénoncé des pratiques de discrimination.

Les facteurs comme l'âge, l'origine ethnique, l'éducation, l'orientation sexuelle et l'état civil doivent également être pris en compte puisque chaque groupe de défenseurs femmes connaît des défis différents avec des besoins de protection et de sécurité spécifiques.

L'évaluation des besoins de protection des femmes défenseurs permettra de révéler plus précisément la spécificité et la variété de leurs besoins, leurs vulnérabilités et leurs stratégies pour y faire face. De cette façon, leurs problèmes peuvent trouver des réponses plus appropriées dans les cas d'urgence ou face aux difficultés au quotidien.

LA DÉCLARATION SUR L'ÉLIMINATION DE LA VIOLENCE À L'ÉGARD DES FEMMES (1993) DÉFINIT LA VIOLENCE CONTRE LES FEMMES COMME:

"Tout acte de violence de genre causant ou pouvant causer aux femmes un préjudice ou des souffrances physiques, sexuelles ou psychologiques, y compris la menace de tels actes, la contrainte ou la privation arbitraire de liberté, que ce soit dans la vie publique ou dans la vie privée". (Article 1)

La violence à l'égard des femmes s'entend comme englobant, sans y être limitée, les formes de violence énumérées ci-après:

a) ◆ La violence physique, sexuelle et psychologique exercée au sein de la famille, y compris les coups, les sévices sexuels infligés aux enfants de sexe féminin au foyer, les violences liées à la dot, le viol conjugal, les mutilations génitales et autres pratiques traditionnelles préjudiciables à la femme, la violence non conjugale, et la violence liée à l'exploitation.

b) ◆ La violence physique, sexuelle et psychologique exercée au sein de la collectivité, y compris le viol, les sévices sexuels, le harcèlement sexuel et l'intimidation au travail, dans les établissements d'enseignement et illeurs, le proxénétisme et la prostitution forcée.

c) ◆ La violence physique, sexuelle et psychologique perpétrée ou tolérée par l'Etat, où qu'elle s'exerce. (Article 2)

Sécurité pour les femmes défenseurs des droits humains

Les femmes défenseurs des droits humains payent un lourd tribut pour leur travail de défense et de promotion des droits humains. Les femmes défenseurs doivent faire face à des risques inhérents à leur genre et leur sécurité nécessite par conséquent une démarche spécifique.

Les causes devront être prises en considération dans les politiques et protocoles de sécurité de l'organisation.Voici une liste non-exhaustive des causes évoquées dans le rapport de 2002 d'Hina Jilani cité plus haut.

- Les femmes peuvent susciter de l'attention malveillante.
- Les femmes défenseurs devront peut-être enfreindre certaines lois patriarcales et certains tabous sociaux.
- Il existe des types d'agressions spécifiques contre les femmes défenseurs.
- Les femmes défenseurs se verront obligées de "défendre" leur intégrité.
- Leurs collègues masculins pourront ne pas comprendre, ou même rejeter le travail des femmes défenseurs.
- Les femmes défenseurs peuvent être victimes de violence conjugale.
- Elles ont des obligations familiales supplémentaires.
- Toutes ces pressions constituent une charge de travail et de stress supplémentaires pour les défenseurs femmes.

Vers une meilleure sécurité et protection des femmes défenseurs des droits humains: Politiques et mesures globales et permanentes de sécurité

Garantir l'intégration transversale de la participation des femmes

Il est nécessaire de garantir l'intégration de leur participation, ce qui signifie en substance de garantir la participation à part entière des femmes aux prises de décision aux côtés des hommes, pour aborder les questions de sécurité des femmes et placer les femmes sur un pied d'égalité avec les hommes lorsqu'on définit les mesures préventives de sécurité. Il est important de prendre en compte les expériences des femmes et leurs points de vue et de garantir qu'elles définissent effectivement les règles et procédures de sécurité, les vérifient et les évaluent.

Garantir le traitement des besoins de sécurité et de protection propres au genre

Comme pour les autres besoins de sécurité, il est essentiel de répartir les responsabilités en matière de violence contre les femmes et de risques de sécurité des défenseurs femmes au sein d'une organisation ou d'un groupe de défenseurs. Idéalement, les responsables de la sécurité doivent bien connaître

les besoins spécifiques des défenseurs femmes. Parfois, il faudra nommer quelqu'un qui puisse apporter une connaissance et une compréhension précises à la question. Une personne peut être chargée de la sécurité, et l'organisation peut ensuite charger une autre personne formée et compétente sur la question de la violence fondée sur le genre. Dans ces cas, les deux personnes devront veiller par une collaboration étroite à ce que les procédures de sécurité fonctionnent toutes sans heurt et répondent aux besoins spécifiques de chacun.

La formation

La formation de tous ceux qui travaillent ensemble au sein d'une organisation des droits humains est la clé pour améliorer la sécurité et la protection. Elle devrait aussi sensibiliser aux besoins spécifiques des femmes défenseurs.

Il convient de sensibiliser sur les points suivants:

- toutes les confusions entre valeurs sociales, culturelles, religieuses et droits des femmes, droits humains.
- la violence domestique envers les femmes comprenant tout préjudice physique, sexuel et psychologique ayant lieu dans la famille, comprenant les sévices, le viol conjugal, la mutilation des parties génitales féminines et d'autres pratiques traditionnelles portant atteinte aux femmes et mettant leur vie en danger.
- le besoin au sein des familles des défenseurs des droits humains femmes de prendre les mêmes mesures qu'elles appliquent contre la même violence à l'extérieur dans la sphère privée. D'un point de vue de la sécurité, cela implique un possible discrédit de l'organisation entière avec une possible diminution du soutien par des parties prenantes-clé.
- le fait que de nombreuses femmes sont influencées en ce qui concerne la sécurité parce qu'elles s'occupent d'enfants et d'autres membres de la famille en plus de leur travail habituel; le fait que les hommes pourraient promouvoir le partage des tâches domestiques sans nuire à leur virilité, et de quelle manière.
- le fait que l'on reproche aux défenseurs des droits humains hommes et femmes de s'occuper d'autres personnes plutôt que de leurs familles.

En résumé

Les différents besoins de sécurité des femmes sont liés à différents types de menaces, à leurs rôles différents et aux différences entre des situations spécifiques (comme la détention, le travail sur le terrain, etc.). L'objectif est de mettre au point des réponses à la violence contre les femmes et autres défenseurs tenant compte du genre.

Commentaire supplémentaire

Les violences basées sur le genre sont toujours **insuffisamment signalées** et documentées. Une conscience plus élevée concernant les violences liées au genre au sein de l'organisation ou du groupe peut rendre la discussion sur les menaces ou les incidents liées au genre plus facile. Des membres du personnel ayant un sens de l'écoute, peuvent également servir d'interlocuteurs, de personnes relais, pour les défenseurs femmes et hommes voulant trouver des solutions aux menaces et violences basées sur le genre, que celles-ci soient dirigées contre eux ou d'autres membres de l'organisation ou de la communauté.

Les agressions sexuelles et la sécurité personnelle

En termes de statistiques, le viol affecte plus souvent les femmes que les hommes. Quelques défenseurs des droits humains hommes qui en ont été victimes en parlent comme d'une torture sexuelle et sont conscients de ce que les femmes vivent en pareils cas. Le viol est une torture à part entière étant donné l'objectif de porter atteinte à l'intégrité physique et psychologique d'une personne.

Comme les crimes de droit commun cachent en réalité souvent des agressions ciblées quand il s'agit de défenseurs des droits humains, il faudrait par souci de différentiation parler de viol en cas de véritable délit de droit commun et parler de torture sexuelle[22] en cas de crime politique (répression du travail des défenseurs, pendant laquelle les victimes sont présélectionnées ou constituent des cibles opportunes).

Il s'agit d'un crime de pouvoir et violence. La torture sexuelle est un moyen pour l'agresseur de prouver son pouvoir sur la victime.

Il faut garder à l'esprit que dans de nombreux cas, les femmes emmenées vers un autre endroit par un agresseur potentiel sont violées, battues voire même tuées. Les femmes devraient donc toujours prendre la décision ferme et définitive d'essayer de ne pas suivre un agresseur potentiel (à moins qu'un tel refus mette leur vie en danger ou bien celle d'autrui).

Tous les défenseurs des droits humains femmes courent le risque de tortures sexuelles, mais tous les défenseurs femmes ne sont pas égaux devant celles-ci. Une partie des conséquences dépend en effet du contexte politique, social, culturel et religieux. Certaines femmes devront faire face aux conséquences physiques et psychologiques; d'autres aux conséquences physiques, psychologiques plus sociales et culturelles. Toutes subissent le calvaire du dépôt de plainte et d'être questionnées à ce sujet pendant l'instruction.

L'agression sexuelle devrait être examinée de tous les points de vue, en tenant compte de toutes les circonstances, y compris la dimension psychosociale. Comme lors de toute autre forme de torture, la personne torturée sexuellement

[22] Au sens de la déclaration des NU contre la torture: "(…) tout acte par lequel une douleur ou des souffrances aiguës, physiques ou mentales, sont intentionnellement infligées à une personne aux fins notamment d'obtenir d'elle ou d'une tierce personne des renseignements ou des aveux, de la punir d'un acte qu'elle ou une tierce personne a commis ou est soupçonnée d'avoir commis (….)"

peut éprouver le sentiment de culpabilité, d'une "dignité perdue", de méfiance, et dans des cas de viol, le sentiment de se sentir salie ... Les organisations peuvent donc considérer la possibilité d'analyser le concept de dignité: qu'est-ce que la dignité? Qui décide de la dignité d'une autre personne? Qui a réellement perdu sa dignité: la personne tombant si bas au point de torturer ou la personne torturée?

Une politique d'organisation permanente devrait toujours prendre en compte:

- les besoins spécifiques des défenseurs des droits humains femmes.
- la lutte contre les discriminations fondées sur le genre au sein de l'organisation.
- la dimension culturelle pour les victimes d'abus sexuels et de torture.
- ...

Des protocoles spécifiques doivent être définis concernant:

- les défenseurs femmes en mission sur le terrain.
- les relations publiques avec les parties prenantes-clé en matière de protection.
- la gestion des conséquences d'abus sexuels/torture sexuelle, comme des grossesses indésirées et les maladies et infections sexuellement transmissibles (MST et IST) comme par exemple le VIH/SIDA.

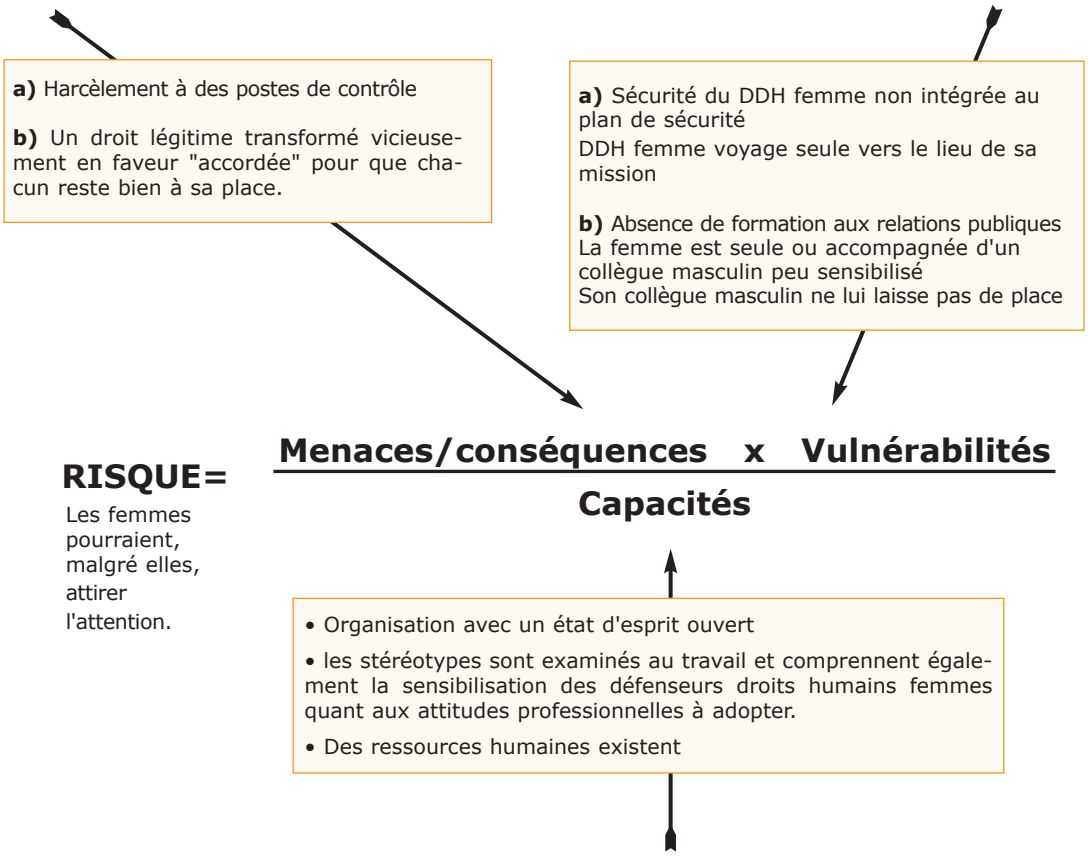
En définissant ces protocoles, il faut garder à l'esprit:

- que certaines femmes défenseurs des droits humains n'osent pas signaler à leurs collègues masculins qu'elles ont subi des abus sexuels ou des tortures par peur d'être stigmatisées ou déconsidérées (rappelons que les victimes ressentent souvent un sentiment de culpabilité bien que totalement infondé).
- que dans certains pays les organisation mixtes ne mentionnent quasiment pas ces sujets.
- que certains défenseurs des droits humains hommes ont des vues très arrêtées sur l'avortement. D'un autre côté, ils ne sont pas toujours prêts à prendre en charge l'enfant non désiré. Dans de nombreux pays où l'avortement est interdit par la loi, la culture ou la religion, l'infanticide est devenu une réelle alternative à l'abandon de l'enfant. L'abandon accentue le phénomène des enfants sorciers et l'augmentation du nombre d'enfants soldats, sans parler des autres plaies sociales. Ainsi, les femmes pourraient considérer la pilule du lendemain (une pilule qui provoque les règles qu'on soit ou non enceinte).
- qu'il n'y a pas de choix bon ou mauvais, mais seulement des conséquences qui doivent être évaluées au sein de l'organisation.
- **qu'il est important d'utiliser l'outil d'évaluation du risque.**

Example:

Des femmes peuvent attirer une attention malveillante.

Faites la liste de toutes les menaces et conséquences possibles concernant le risque décrit plus haut. Ensuite, pour chaque "menace/conséquence", corrélez les vulnérabilités et capacités correspondantes. Déterminez enfin les capacités nécessitées pour réduire les vulnérabilités et attaquez-vous à elles. En d'autres termes, il convient d'éliminer une à une les "couches" du risque, comme on ôte les couches successives d'un oignon. Pour chaque couche (menace/conséquence), déterminez les vulnérabilités et capacités correspondantes.



(Indiquez, parmi l'inventaire général des capacités générales plus haut, lesquelles pourraient être liées spécifiquement à vos vulnérabilités "a" et "b". Ensuite, déterminez quelles capacités supplémentaires vous devrez développer).

Réagir à une agression sexuelle[23]

Il y a très peu de choix pour réagir à une agression sexuelle et la décision appartient strictement à la victime. Il n'y a pas de bonne ou mauvaise façon de réagir. Les choix de la victime d'une agression sexuelle peuvent inclure:

[23] La plupart de ces informations sont tirées d'un livre de Koen Van Brabant, Operational Security in Violent Environments, et des manuels de sécurité de World Vision et du Conseil Œcuménique des Églises.

1 ◆ **La soumission.** Si la victime craint pour sa vie ou celle d'autrui, elle peut décider de se soumettre à son agresseur.

2 ◆ **La résistance passive.** Elle consiste dans le fait de faire ou de dire quelque chose de désagréable, dégoûtant ou d'attirer l'attention sur un danger pour la santé qui coupe l'appétit sexuel de l'agresseur. On peut par exemple dire qu'on a le SIDA (bien que la réaction de l'agresseur puisse être: "et alors? Moi aussi" ou qu'il devienne plus violent). On peut également dire qu'on a ses règles, ce qui est souvent considéré comme étant une impureté.

3 ◆ **La résistance active.** Elle consiste à mobiliser sa force physique comme on peut pour repousser l'agresseur, que ce soit en frappant, donnant des coups de pied, mordant, griffant, criant ou en s'enfuyant en courant.

Dans tous les cas:

- dans la mesure du possible, essayez de suggérer l'usage d'un préservatif. Dans certaines cultures et religions, leur usage est certes injustement perçu comme un "consentement", mais finalement ce n'est pas votre problème. Vos problèmes pourraient s'avérer beaucoup plus graves: vous tomberez peut-être enceinte, votre santé pourrait être affectée et, parmi toutes les pensées récurrentes, le doute persistera: "Et si…?" Tout cela implique que les défenseurs des droits humains femmes considèrent la question de se munir utilement de préservatifs ou bien de des préservatifs féminins pendant des missions sur le terrain en zones dangereuses. Ceci requiert une discussion sur le sujet au sein de l'organisation et son inclusion dans le budget. La même chose est valable pour la pilule du lendemain et pour tous les traitements hospitaliers (voir plus loin: les traitements prophylactiques post-exposition (PEP).

- essayez de mémoriser autant d'informations que possible sur le ou les agresseur(s). Il peut être utile, sur le moment, de se concentrer sur certains éléments qui pourront être utiles pour compléter le dossier en vue de poursuites judiciaires et qui réduiront la probabilité de l'impunité.

- si possible, tentez de séparer mentalement l'esprit du corps.

Dans tous les cas, faites ce que vous devez pour survivre. Suivez votre instinct. Personne ne sait comment il réagirait dans un cas pareil (ou dans tout autre type de torture) et votre réaction sera la bonne pour vous au vu de la situation.

Dans de nombreux endroits, la torture sexuelle prend des proportions dépassant l'imaginable

Alors que la logique fondamentale de sécurité imposerait d'éviter une mission sur le terrain pendant laquelle le risque d'être torturée sexuellement par les forces en conflit est extrêmement élevé, et ce avant d'avoir mis en place une dissuasion suffisante, certaines organisations de défense des droits humains et des défenseurs des droits humains femmes isolées décident de jouer leur propre sécurité en ne pensant qu'aux nombreuses autres victimes. Bien que la différence entre un risque acceptable et inacceptable relève de considérations subjectives et organisationnelles, nous ne pouvons qu'insister sur les règles fondamentales de sécurité. Pendant la formation, le brainstorming doit aller jusqu'à

analyser les options suivantes en cas d'agression sexuelle lors d'une mission sur le terrain: le défenseur des droits humains femme pourrait invoquer le SIDA (qu'il s'agisse d'une torture sexuelle collective ou non) et instiller le doute que tous pourraient être contaminés étant donné que nul ne sait qui pourrait avoir le SIDA. Le défenseur femme pourrait également dire à l'agresseur qu'elle a ses règles, ce qui signifie qu'en guise de prévention elle pourrait envisager le port de serviettes hygiéniques maculées pendant toute la durée de la mission sur le terrain. Elle pourrait aussi porter davantage de couches de vêtements en espérant que des secours viennent à temps.

Le SIDA est un fléau pour la société et attaque hommes et femmes indifféremment

Dans certains pays où la torture sexuelle de femmes est devenue une arme de guerre, de nombreuses femmes envisagent de rencontrer les agresseurs pour leur "expliquer" l'impact de ces actes pour tous, la question n'étant plus la torture sexuelle des femmes en guise de répression mais plutôt le fait qu'elle conduise à la mort collective et que c'est devenu une question de vie ou de mort pour tous, y compris pour les agresseurs. C'est une bombe à retardement pour tous, en plus du génocide culturel.

De nombreux défenseurs des droits humains hommes travaillent sur la torture sexuelle des femmes et le rejet culturel qui s'ensuit dans le but de promouvoir le changement d'attitude des familles à l'égard des victimes. Malgré cela, certains d'entre eux affirment qu'ils répudieraient leur femme si cela devait leur arriver.

Alorsqu'un de ces mêmes défenseurs soutenait un jour que la torture sexuelle équivalait à l'adultère, un de ses collègues lui répondit simplement: "Cela dépend de ce que votre femme représente pour vous".

Voilà la question sous-jacente. Bien trop souvent, la femme est principalement considérée comme un objet ou une possession sexuelle: une fois "cassé", il doit être abandonné et remplacé.

Une femme est souvent considérée comme la mère, la fille, la sœur ou la femme d'un homme, rarement comme un être, femme, à part entière ayant sa propre identité. Heureusement, beaucoup de femmes peuvent compter sur des collègues masculins qui offrent un soutien authentique à leurs collègues femmes.

Toutes les organisations et les groupes de défenseurs des droits humains devraient disposer de plans de prévention et de réaction pour les cas d'agressions sexuelles

Là où c'est possible, et en fonction du contexte local et de l'accès aux laboratoires médicaux, les choses suivantes devraient être disponibles:

- une visite médicale ou des soins médicaux avant de se laver - (pour prendre un échantillon de la semence ou de tout autre échantillon pour une analyse de l'ADN lorsque cette technique existe).
- des photos de l'état de la victime
- un soutien psychologique
- signaler l'événement aux autorités compétentes et porter plainte

Quoiqu'il en soit, le plan de réaction devrait comprendre au moins **des soins médicaux efficaces pour la victime, y compris un soutien psychologique et un suivi juridique** (rappelez vous qu'une femme pourrait préférer l'assistance d'une autre femme à celle d'un homme).

Pour prévenir une grossesse, la victime devrait avoir accès à la pilule du lendemain (sous 24 heures): il s'agit d'une contraception d'urgence (et non d'une pilule d'avortement).

Le traitement prophylactique post-exposition ("PEP") doit aussi être envisagé bien qu'il ne soit pas totalement fiable en raison des nombreux paramètres pour son application. Un kit post-viol est disponible dans certains hôpitaux contenant un traitement arrêtant la progression de plusieurs maladies, pour les victimes ayant pu recevoir des soins sous 72 heures après avoir été violées. Dans tous les cas, faites une visite médicale immédiatement, et par la suite régulièrement, s'il y a un risque de maladies sexuellement transmissibles-MST.[24]

Il faut trouver un juste milieu entre fournir à la victime un accès au soutien de spécialistes et veiller à ce que l'organisation réagisse en apportant le soutien approprié à la victime.

Veuillez vous rapporter également au chapitre 1.5, "Prévenir les agressions et y réagir.

[24] Plus d'information: International Committee of the Red Cross-ICRC: http://icrc.org/web/eng/siteeng0.nsf/html/congo-kinshasa-feature-201207 A

En résumé

Les femmes sont victimes d'abus, de harcèlement et de tortures engendrés par la structure patriarcale. Les organisations mixtes de défense des droits humains la reproduisent trop souvent à leur micro-échelon.

La sécurité des défenseurs des droits humains femmes est la sécurité de tous les défenseurs des droits humains.

Les politiques et protocoles de sécurité des organisations doivent intégrer transversalement la sécurité des défenseurs des droits humains femmes.

Une évaluation rigoureuse des risques n'est pas suffisante.

Il faut également:

- remettre en question les rôles et les comportements.
- démythifier les croyances erronées et modifier les comportements liés au genre.
- appliquer une discrimination positive pour favori-ser les changements.
- inclure dans le budget de sécurité l'achat de préservatifs, pilules du lendemain, trithérapie, ...

Une fois de plus, il n'y a aucune garantie en ce qui concerne les résultats. La torture sexuelle succède à l'agression physique. En réduisant l'exposition à cette dernière, la probabilité de torture sexuelle diminuera également.

CHAPITRE 1.10

La Sécurité dans les zones de conflit armé

Objectif:

Réduire les risques inhérents aux zones de conflit armé.

Le risque dans les situations de conflit

Travailler dans des zones de conflit expose les défenseurs des droits humains à des risques précis, particulièrement dans des situations de conflit armé: un nombre élevé de civils tués sont victimes de pratiques guerrières ou attaques indiscriminées et beaucoup d'autres meurent parce qu'on les prend pour cible, un fait qu'il faut reconnaître. L'action politique est toujours nécessaire pour le souligner et tenter d'y mettre fin.

Bien qu'il soit impossible de maîtriser les hostilités en cours, vous pouvez modifier votre comportement pour éviter d'être touché par le conflit ou pour réagir de manière adéquate si quelque chose se produit.

Si vous êtes établi dans une zone où l'action armée est fréquente, vous aurez probablement déjà pris les contacts nécessaires à votre protection ainsi qu'à celle de votre famille et de vos collègues, tout en essayant de poursuivre vos activités.

Cependant, si vous travaillez dans une zone de conflit armé où vous n'êtes pas basé, vous **devez dès le départ avoir trois choses à l'esprit:**

a ◆ Quel degré de risque êtes-vous prêt à tolérer? Ceci s'applique aussi aux individus ou aux organisations avec qui vous coopérez.

b ◆ Est-ce que les avantages de votre présence dans cette zone l'emportent sur les risques encourus? Les activités de défense des droits humains ne peuvent être poursuivies durablement au prix d'une exposition accrue à risque élevé.

c ◆ Estimer simplement que vous "connaissez la zone" et "en savez beaucoup sur les armes" ne vous protègera pas si l'on tire sur vous ou si vous subissez une attaque au mortier ou d'un franc-tireur.

Les types de tirs

Vous pouvez être exposé aux tirs de fusils d'assaut, de pistolets - mitrailleurs, d'obusiers, de lance-roquettes multiples, de bombes et de missiles sol-sol (balistiques), air-sol, mer-sol selon les cas. Les tirs vont des tirs d'un franc-tireur ou de l'assaut par hélicoptère de combat en cas de bonne visibilité aux assauts d'obusiers dirigés ou aux barrages d'artillerie. Les tirs peuvent vous viser plus ou moins directement. Il peut s'agir également de tirs de saturation qui visent à "pulvériser" une zone entière.

Plus le tir vise un but précis, plus le risque est faible tant que vous n'êtes pas la cible des tirs, ni la zone où vous vous trouvez ou les zones limitrophes. Dans de telles circonstances, le risque diminue si vous parvenez à quitter la région. **Dans tous les cas, souvenez-vous que si vous êtes sous le feu, il sera difficile de déterminer si vous êtes la cible ou non. Déterminer ceci n'est pas prioritaire**, comme nous verrons plus loin.

Prendre des précautions: réduire votre vulnérabilité aux tirs

1 ◆ Évitez les zones dangereuses

Dans les zones de combat ou de terrorisme, évitez d'installer votre base, d'avoir un bureau ou de séjourner de manière prolongée à proximité d'une cible d'attaque éventuelle, telle qu'une garnison ou une installation de télécommunications. Il en va de même avec les zones stratégiques comme les routes d'accès aux zones urbaines et les sorties, les aéroports et les points de vue contrôlant les environs.

2 ◆ Trouvez une protection adéquate contre les attaques

Les éclats de verre de fenêtres voisines sont l'une des causes principales de blessure. Obturer une fenêtre avec des planches ou les recouvrir de ruban adhésif peut réduire le risque de blessures. En cas d'attaque, éloignez-vous des fenêtres et couchez-vous immédiatement par terre, sous une table ou de préférence dans une pièce centrale aux murs épais, ou encore mieux, dans un sous-sol.

Les sacs de sable peuvent parfois être utiles. Il est cependant préférable de les utiliser seulement si les bâtiments voisins en sont également équipés, sinon vous risquez d'attirer une attention indésirable.

Si l'on n'a rien d'autre sous la main, se mettre au sol ou dans un renfoncement du sol peut protéger partiellement.

Un simple mur de briques ou la portière d'une voiture ne vous protègeront pas de tirs de fusil ou d'armes lourdes. Le pilonnage d'artillerie et les roquettes peuvent tuer à une portée de plusieurs kilomètres; on peut donc être touché même si l'on ne se trouve pas à proximité immédiate.

Les explosions de bombes ou d'obus peuvent endommager vos tympans. Couvrez-vous les oreilles des deux mains ou avec tout objet utile et ouvrez la bouche légèrement.

Une identification visible de vos bureaux, de votre emplacement ou de vos véhicules ne sera utile que **dans les régions où les attaquants respectent habituellement votre type de travail.** Si ce n'est pas le cas, vous courez un risque inutile. Si vous désirez signaler votre présence, faites-le avec un drapeau, des couleurs ou des signes sur les murs ou les toits (s'il y a un risque d'attaque aérienne).

3 ◆ Voyager à bord de véhicules

Si vous êtes à bord d'un véhicule sur lequel on tire, vous aurez peu de temps pour essayer d'évaluer la situation, et une évaluation correcte est très difficile à faire. En général, il est **préférable de supposer que le véhicule est la cible et il convient alors de quitter le véhicule et de vous mettre à l'abri immédiatement.** Un véhicule est une cible claire. Il est vulnérable et des éclats de verre des fenêtres ou l'explosion des réservoirs de pétrole peuvent vous blesser, en plus des tirs directs. Si les tirs ne sont pas trop proches, essayez plutôt de poursuivre votre route jusqu'à un abri à proximité.

Mines terrestres et artillerie non-explosée (UXO)[25]

Les mines terrestres et l'artillerie non-explosée sont une menace grave pour les civils dans les zones de conflit armé. Elles existent sous différentes formes:

- **Les mines:**
  - ◆ Les mines anti-char sont déposées sur les routes et les sentiers et sont capables de détruire un char mais peuvent aussi se déclencher au passage d'un véhicule normal.
  - ◆ Les mines anti-personnelles sont plus petites et sont susceptibles d'être posées partout où des personnes peuvent circuler. La plupart des mines anti-personnelles sont enfouies dans la terre. N'oubliez pas que les personnes qui plantent ces mines sur la route peuvent aussi les planter dans les champs d'à côté et sur des chemins plus petits des environs.
- **Les objets piégés (booby traps):**
  - ◆ Les objets piégés ou booby traps sont de petits explosifs cachés dans un objet paraissant inoffensif ou attrayant (il peut être colorié), qui explosent au moindre contact. Le terme est aussi utilisé pour les mines reliées à un objet qui peut être déplacé ou activé à distance (d'un cadavre à une voiture abandonnée).
- **L'artillerie non - explosée:**
  - ◆ Elle comprend toute munition qui a été tirée mais qui n'a pas explosé.

25 La plupart des informations de cette section ont été adaptées de l'excellent manuel de Koenraad van Brabant, Operational Security Management in Conflict Areas (voir bibliographie).

On fait face à la recrudescence de bombes à sous-munitions non explosées qui sont presque plus fréquentes actuellement que les mines anti-personnelles. Les sous-munitions sont les reliquats non explosés de bombes en grappes,[26] lesquelles sont composées chacune de plusieurs centaines de sous-munitions, éjectées dans toutes les directions. Elles sont conçues pour saturer une grande zone et exploser à l'impact, mais elles n'explosent cependant pas toutes en raison d'un fort taux de défaillance.[27] Elles sont plus instables que les mines, de sorte qu'elles peuvent ensuite exploser à tout moment. Certaines sont de couleur, et donc attractives pour les enfants.

La prévention contre les mines et l'artillerie non explosée

Le seul moyen d'éviter les zones minées ou qui comportent des sous-munitions non explosées est de connaître leur emplacement. Si vous n'êtes pas basé dans la région ou que vous n'y vivez pas, vous pourrez uniquement localiser celles-ci en demandant continuellement et activement à la population locale ou à des experts[28] si des explosions ou des combats ont eu lieu dans la région. Il vaut mieux emprunter des routes principales goudronnées, des routes praticables utilisées régulièrement et suivre les traces d'autres véhicules. **Ne quittez pas les routes principales avec ou sans votre véhicule et ne roulez pas sur le trottoir ou le bas côté / la bande d'arrêt d'urgence.** Les mines ou autres pièces d'artillerie non explosées peuvent rester cachées et sont actives pendant des années.

Les munitions non explosées sont présentes dans les endroits où des combats et des tirs ont eu lieu et sont parfois visibles. Dans ce cas, la règle d'or est de **ne pas vous en approcher ni de les toucher, de signaler si possible leur emplacement et d'informer autrui immédiatement, y compris -s'ils sont présents dans la zone- les ONG spécialisées dans le déminage et les services de déminage des Forces de maintien de la paix onusiennes**.

Les objets piégés se trouvent en général dans les zones abandonnées par les combattants. Dans ces endroits, il est impératif de ne toucher ni de bouger quoi que ce soit et de ne pas vous approcher de bâtiments à l'abandon.

26 Voir l'ouvrage *Principes de droit des conflits armés*, Eric David (ULB, Bruylant, 2002). Voir les campagnes récentes de Handicap International, Amnesty International etc; sites www.sousmunitions.org, www.controlarms.org

27 Les estimations du taux de défaillance sont de 5 à 80 % selon les types de bombes à sous-munition et la nature dure ou molle du terrain. Elles deviennent donc de fait de quasi mines anti-personnelles…

28 Tels que les ONG spécialisées dans le déminage ou les services de déminage des Forces de Maintien de la Paix des Nations Unies. Les autres ONG internationales disposent aussi parfois de cartes concernant les zones minées et déminées

Si une mine ou une sous-munition explose sous un véhicule ou sous les pieds d'une personne à proximité[29]

Il y a deux règles d'or:

- Une mine ou une sous-munition en annoncent toujours d'autres.
- N'agissez jamais de manière impulsive même s'il y a des personnes blessées.

Si vous devez quitter l'endroit où vous vous trouvez, rebroussez chemin sur les traces de vos pas si elles sont visibles. Si vous êtes à bord d'un véhicule et que vous suspectez la présence de mines anti-char, abandonnez le véhicule et rebroussez chemin en suivant les traces du véhicule.

Si vous vous approchez d'une victime ou que vous souhaitez vous éloigner du périmètre miné, il convient de vous mettre à genoux ou de vous allonger puis de commencer à donner de petits coups très légers avec la pointe d'une brindille de bois ou d'une tige en métal que vous enfoncez prudemment dans le sol à un angle de 30 degrés pour tenter de détecter un objet solide. Si vous trouvez un objet solide, ne le touchez pas, dégagez-en très doucement le pourtour jusqu'à ce que vous puissiez l'identifier clairement. Les mines peuvent être déclenchées par le contact, les vibrations mais aussi par des fils de détente. Ne coupez pas de fils si vous en trouvez

Tout ceci peut, bien entendu, prendre un temps considérable.

[29] Vous pouvez trouver des manuels et des documents sur la sensibilisation et la formation à la question des mines sur le site Internet de la campagne *International Campaign to Ban Landmines*: www.icbl.org (campagne internationale pour l'interdiction des mines terrestres).

CHAPITRE 1.11

La Sécurité, la communication et les technologies de l'information

(Avec la collaboration de Privaterra –www.privaterra.org)

Objectif:

Les énormes disparités en matière de technologie de l'information à travers le monde affectent également les défenseurs des droits humains. Ce chapitre se concentre principalement sur la technologie de l'information, c'est-à-dire les ordinateurs et Internet.[30] Les défenseurs qui n'ont pas d'accès aux ordinateurs ou à Internet considéreront peut-être que ces informations sont peu utiles dans l'immédiat. Cependant, ils ont d'urgence besoin des moyens et de la formation nécessaires qui leur permettront d'utiliser la technologie de l'information au service de la défense des droits humains.

Un guide des problèmes de sécurité dans les communications et les moyens de les éviter

Le savoir est un pouvoir, et connaître les problèmes de sécurité susceptibles de toucher vos communications renforcera la sécurité au travail. La liste ci-après décrit les manières différentes d'accéder illégalement à vos informations et communications comme de les manipuler et propose des solutions pour éviter ces problèmes de sécurité.

Parler

Le risque d'accès illégal à vos informations n'existe pas que sur Internet. Quand vous parlez de sujets sensibles, réfléchissez aux questions suivantes:

1 ◆ Avez-vous confiance en vos interlocuteurs?

2 ◆ Doivent-ils connaître les informations que vous leur donnez?

[30] Ce chapitre est basé sur le travail de Robert Guerra, Katitza Rodriguez et Caryn Mladen de Privaterra, une ONG qui travaille dans le monde entier sur la sécurité et les technologies de l'information pour les défenseurs des droits humains par des cours et des activités de conseil. (Certaines parties de ce texte ont été légèrement adaptées par Marie Caraj et Enrique Eguren).

3 ◆ Vous trouvez-vous dans un cadre sûr? Des micros cachés et des dispositifs d'écoute sont souvent posés délibérément aux endroits où les personnes croient être en sécurité comme les bureaux privés, les rues animées, les chambres à coucher et les voitures.

Il sera peut-être difficile de répondre à la troisième question car des micros cachés peuvent être posés dans une pièce pour enregistrer ou transmettre tout ce qui y est dit. Des micros laser peuvent aussi être réglés de très loin sur une fenêtre pour écouter ce qui est dit à l'intérieur d'un bâtiment. D'épais rideaux peuvent apporter une certaine protection contre les micros laser, tout comme l'installation du double vitrage. Dans certains bâtiments sûrs, il y a deux fenêtres dans les bureaux pour réduire le risque de dispositifs d'écoute laser.

Que pouvez-vous faire?

□ **Supposez toujours que vous êtes sur écoute.** En adoptant une "saine paranoïa", vous serez probablement plus prudent quand il s'agit de sujets confidentiels.

□ **Des détecteurs de micros (balayeurs ou renifleurs) peuvent détecter ces appareils d'écoute**, mais sont onéreux et difficiles à se procurer. En plus, les personnes chargées du balayage sont quelquefois responsables de la mise sur écoute initiale. Lors d'un dépistage, ils trouvent quelques "micros jetables" (des micros économiques prévus pour être dénichés) ou ne trouvent rien comme par miracle et déclarent vos bureaux "sains".

□ **Tous les agents de nettoyage peuvent menacer sérieusement votre sécurité.** Ils entrent au bureau après l'heure de fermeture et emportent vos déchets chaque soir. Ils devraient être soumis à des contrôles de sécurité réguliers car ils pourraient vous compromettre après avoir commencé à travailler pour vous.

□ **Changez de salle de réunion aussi souvent que possible.** Plus vous changez de salles ou d'endroits, plus il faudra d'équipement et de techniciens pour vous écouter.

□ **Méfiez-vous de cadeaux destinés à vous accompagner en permanence,** tels que des stylos de luxe, épingles à cravate, broches ou objets de bureau comme un très beau presse- papier ou une illustration de grand format. On a pu écouter des conversations avec ce genre d'objets.

□ **Attendez-vous à ce que certaines informations filtrent en permanence**. Vous devriez changer fréquemment vos plans et codes en ne divulguant que quelques fragments de la vérité à vos auditeurs. Vous pouvez aussi diffuser de fausses informations pour vérifier si quelqu'un les utilise ou y réagit.

□ Pour entraver l'efficacité des micros laser, **abordez les sujets délicats dans un sous-sol ou dans une pièce sans fenêtre.** Certains dispositifs d'écoute laser peuvent être moins efficaces pendant une pluie torrentielle ou d'autres perturbations atmosphériques.

□ **Passez un enregistrement audio de bruit blanc (exemple, le son produit lors de l'effet de "neige" sur un téléviseur non réglé) ou d'une chan-**

son populaire pour brouiller la détection et la captation de sons. En effet, il existe des appareils d'écoute externe capables de capter une conversation jusqu'à une distance d'environ 50 mètres. En d'autres termes, votre lieu de réunion n'a pas besoin d'avoir été "équipé" de microphones physiquement. Seule une technologie onéreuse permet de filtrer le bruit et d'entendre une conversation.

- **Les grands espaces en plein air sont à la fois favorables et dangereux.** Un rendez-vous à l'écart permet de voir si on vous suit ou vous observe, mais il sera plus difficile de vous fondre dans la masse pour leur échapper. Les foules permettent de se fondre dans la masse mais vous serez plus rapidement repéré et entendu.

- **Si votre bureau ou lieu de réunion devait se trouver dans une zone rurale,** zone silencieuse ou dans un bâtiment sans isolation phonique ou sans vitres / portes, demandez à un collègue de rester à l'extérieur et de vous faire savoir si on peut entendre votre conversation et demandez-lui d'observer les éventuels éléments indésirables pendant la durée de votre réunion.

Les téléphones portables

Tous les appels téléphoniques peuvent être écoutés si celui qui écoute dispose des capacités technologiques nécessaires. Attendez-vous à ce qu'aucune communication téléphonique ne soit sûre. Les téléphones portables analogiques sont beaucoup moins sûrs que les téléphones portables numériques et ces derniers sont beaucoup moins sûrs que les lignes fixes.

Vos emplacements et conversations peuvent être décelés par surveillance cellulaire. Nul besoin de parler pour que votre emplacement soit repéré, cela peut se faire à chaque fois que vous allumez votre téléphone portable.

N'enregistrez aucun nom, numéro ou informations sensibles dans la mémoire de votre téléphone. Si on vous volait votre téléphone, l'information permettrait de localiser et d'impliquer des personnes que vous souhaitez protéger.

En cas d'urgence, vous pouvez envisager d'utiliser deux numéros de téléphone non identifiables (des cartes prépayées et "go phone"). Ils doivent uniquement être utilisés pour **s'appeler entre eux** et jamais pour appeler ou être appelé par un numéro "connu" (dans la mesure où le numéro connu peut être sur une liste noire et pourrait alors trahir le nouveau numéro). Ne les utilisez pas depuis des endroits qui peuvent facilement être liés à vous. Rappelez-vous qu'il ne faut pas les laisser sur votre téléphone quand vous ne vous en servez pas car ils peuvent être tracés. Changez-les tous les deux régulièrement. Utilisez la même discrétion qu'avec votre numéro habituel.

La sécurité matérielle des informations dans un bureau

Il faut que le bureau soit fermé à clé à tout moment de la journée et de la nuit, y compris les portes et les fenêtres. Choisissez des clés qu'on ne peut reproduire qu'avec une autorisation spécifique et sachez précisément où se trouvent les doubles. NE confiez PAS de clés à des tiers, même s'il s'agit du personnel d'entretien et de nettoyage, et veillez à ce que quelqu'un, vous-même ou un collègue fiable, soit toujours présent lorsque des tiers sont dans le bureau. Si c'est impos-

sible, assurez-vous de pouvoir conserver les dossiers sensibles dans une pièce à accès restreint. Vous devez fermer toutes les portes de votre bureau à clé et déposer les déchets non sensibles dans le couloir ou l'entrée du bâtiment la nuit.

Utilisez un destructeur de documents **à coupe croisée** pour tout document confidentiel. Les destructeurs à coupe fibres ou lanières sont généralement totalement inutiles. Pour jeter des documents particulièrement confidentiels, il faudrait brûler les fibres, pulvériser la cendre et les jeter dans les sanitaires.

Sécurité de base des ordinateurs et des fichiers[31]

Mettez si possible les ordinateurs sous clé lorsque vous quittez le bureau. Positionnez les écrans d'ordinateurs dos aux fenêtres.

Utilisez des onduleurs sur toutes les prises électriques pour protéger l'alimentation de votre ordinateur contre les surtensions et les variations de courant.

Gardez les données sauvegardées dans un endroit sûr et indépendant du bureau, y compris les dossiers sur papier. Protégez les sauvegardes en les confiant à une organisation fiable de sauvegarde sécurisée qui les stockera sur son disque dur chiffré, ou protégez-les par des verrous sophistiqués.

Pour réduire le risque d'un accès à votre ordinateur, sécurisez l'accès par un mot de passe et éteignez-le systématiquement quand vous ne l'utilisez plus.

Chiffrez vos fichiers au cas où quelqu'un entre dans votre ordinateur et parvienne à "craquer" ou à "casser" votre mot de passe.

Si votre ordinateur est volé ou détruit, vous pourrez encore récupérer vos fichiers si vous en avez fait des sauvegardes sécurisées tous les jours. Veillez à conserver les sauvegardes chiffrées dans un endroit sûr, indépendant de votre bureau.

Vous pouvez également utiliser un serveur externe sécurisé pour sauvegarder votre information sur Internet. Ceci vous permettra de récupérer tous vos fichiers sauvegardés même si votre ordinateur est volé ou détruit.

Il n'est pas possible de reconstituer les fichiers nettoyés à l'aide d'un logiciel de nettoyage à réécriture aléatoire du type PGP Wipes ou autre, contrairement aux fichiers supprimés que vous avez envoyés simplement à la corbeille de votre système d'exploitation ou à la corbeille de recyclage d'un logiciel externe.

On peut programmer votre ordinateur pour l'envoi automatique et illégal de vos fichiers à un autre ordinateur ou vous rendre vulnérable à votre insu par d'autres moyens. Pour l'éviter, achetez votre ordinateur chez un fournisseur fiable, reformatez le disque dur avant de l'utiliser pour la première fois et n'installez les logiciels souhaités qu'une fois le disque dur reformaté. N'autorisez l'entretien de votre ordinateur qu'aux techniciens informatiques fiables et surveillez-les à tout moment.

[31] Plus de conseils détaillés sur la sécurité informatique sont disponibles auprès de Front Line en contactant: info@frontlinedefenders.org ou auprès de Privaterra sur info@privaterra.org.

Débranchez les connexions téléphoniques et modems de votre ordinateur, ou coupez votre connexion à Internet lorsque l'ordinateur est sans surveillance. De cette manière, les programmes escrocs actifs pendant la nuit ne fonctionneront pas. Ne laissez jamais votre ordinateur allumé lorsque vous quittez le bureau pendant la journée. Pensez à installer une application pour bloquer l'accès à l'ordinateur au-delà d'une certaine durée d'inactivité. Ainsi, votre ordinateur ne sera pas vulnérable pendant que vous allez chercher un café ou que vous faites des photocopies.

Dans vos préférences Internet, activez **l'extension des fichiers** afin de savoir à quel type de fichier vous avez affaire avant de l'ouvrir. Sinon, vous risquez de lancer un virus en ouvrant un fichier exécutable que vous prendrez pour un fichier texte. Dans Internet Explorer, allez dans "Outils" et choisissez "Options des fichiers". Cliquez sur "Aperçu" et vérifiez que la case "Cacher l'extension pour les types de fichiers connus" n'est PAS cochée.

Sécurité Internet de base

Quand vous envoyez votre courrier électronique ou courriel, il ne va pas directement sur l'ordinateur de votre destinataire. Il transite par plusieurs nœuds en laissant des informations derrière lui. **Ce message peut être intercepté sur l'ensemble de cet itinéraire (et non seulement dans ou depuis votre pays!).**

Quelqu'un pourrait regarder par dessus votre épaule lorsque vous tapez votre mot de passe ou message. C'est particulièrement problématique dans les cybercafés ou cafés Internet. Par ailleurs, si vous êtes relié à un réseau (Intranet), toutes les personnes du bureau peuvent avoir accès à votre courriel. L'administrateur du système peut avoir des privilèges administratifs spéciaux qui lui permettent également d'accéder à tous vos courriels.

Votre fournisseur d'accès à Internet (FAI ou ISP en anglais) a accès à vos courriels, et toute personne ayant une influence sur votre fournisseur peut le forcer à lui transmettre des copies de tous vos courriels ou à empêcher que certains courriels n'atteignent leur destinataire.

En circulant sur Internet, vos courriels transitent par des centaines de serveurs non sécurisés. Les pirates informatiques peuvent avoir accès à vos courriels lors de leur passage. Le fournisseur d'accès à Internet de votre destinataire peut également être vulnérable, tout comme peuvent l'être son réseau interne (Intranet) et son bureau.

Sécurité Internet de base

Les virus et autres problèmes, comme les chevaux de Troie (trojan), peuvent provenir de n'importe quelle source. Même des amis peuvent diffuser ces virus sans le vouloir. Utilisez un bon logiciel anti-virus et utilisez la mise à jour automatique en ligne.

De nouveaux virus sont constamment créés et découverts, par conséquent, consultez *The Virus Information Library* (bibliothèque des informations sur les virus) sur www.vil.nai.com pour les dernières mises à jour de listes de signatures des virus connus.

Les virus se propagent pour la majorité grâce aux courriels, et vous devez par conséquent sécuriser vos courriels (voir ci-dessous). Les virus sont des logiciels uniques conçus pour se reproduire et ils peuvent être nocifs ou non. Les chevaux de Troie sont des logiciels créés pour permettre à un tiers (ou à n'importe qui d'autre !) d'accéder à votre ordinateur.

Un bon logiciel pare-feu (firewall) permet de rester inconnu des pirates informatiques et d'empêcher les intrusions non désirées dans votre système. Ceci permet de limiter la connexion à Internet depuis votre ordinateur aux applications que vous y autorisez et empêche des logiciels tels que les chevaux de Troie d'envoyer des données depuis votre ordinateur ou de donner accès à votre ordinateur à des pirates informatiques.

Un système de "key logger" (carnet de bord des touches du clavier) permet d'enregistrer chaque touche de clavier que vous actionnez. De tels logiciels peuvent être installés par quelqu'un sur votre ordinateur en votre absence, ou être déployé par un virus ou un cheval de Troie qui attaque votre système par Internet. Les key loggers enregistrent chaque touche actionnée et font des rapports sur vos activités, le plus souvent par Internet. On peut se protéger en protégeant ou sécurisant les mots de passe, en sécurisant son courrier électronique, en utilisant un logiciel anti-virus, et en tapant son mot de passe avec la souris (application souris) plutôt que sur le clavier. Les key loggers peuvent aussi être mis hors d'état de nuire en coupant la connexion à Internet de votre ordinateur, plus encore en débranchant votre connexion téléphonique à Internet lorsque vous ne vous servez pas de l'ordinateur.

Une adresse électronique peut être falsifiée ou usurpée par quelqu'un d'autre que le vrai titulaire du compte Internet ou de la messagerie. Ceci peut être réalisé en obtenant l'accès à l'ordinateur ou au mot de passe d'une autre personne, en piratant le FAI ou en utilisant une adresse électronique qui correspond à peu près à l'adresse particulière de la personne. Par exemple, en substituant le chiffre "1" à la minuscule "i", l'usurpateur crée une adresse similaire et la plupart des personnes destinataires des courriels ne se rendront pas compte de la différence. Afin d'éviter d'être berné par un faux, remplissez le champ "objet" par une phrase significative et posez de temps en temps des questions auxquelles seul votre interlocuteur authentique peut répondre. Vérifiez la nature suspecte de toute demande d'informations en prenant des informations sur l'identité de l'auteur par d'autres voies que l'informatique.

Protégez la confidentialité de votre activité de navigation en rejetant les cookies et en effaçant votre mémoire cache après chaque visite sur la toile. Dans Internet Explorer, cliquez sur *"Outils"* puis sur *"Options"*. Dans *Netscape Navigator*, cliquez sur *"Éditer"* puis *"Préférences"*. Lorsque vous êtes dans l'un de ces menus, éliminez tout l'historique, tous les cookies et videz votre mémoire cache. Pensez à éliminer aussi tous vos ajouts de signets. Les navigateurs enregistrent tous les sites que vous avez visités sous format de fichiers cache; il faudra donc déterminer quels fichiers vous devez supprimer de votre système.

Mettez à jour tous les navigateurs Internet pour les rendre compatibles avec le chiffrage à 128-bits. Ceci permettra de sécuriser toute l'information que vous voulez faire transiter par la toile, y compris les mots de passe et autres données sensibles dans les documents. Installez les corrections de sécurité (security

patches) les plus récentes de tous vos logiciels, particulièrement *Microsoft Office, Microsoft Internet Explorer et Netscape*.

Ne naviguez pas sur Internet pour votre distraction à partir d'un ordinateur rempli de données confidentielles. L'idéal est de dédier un ordinateur à internet qui ne contienne aucune donnée.

L'envoi et la réception de courriels sécurisés

Ce sont des modes d'échange de courrier électronique sécurisé que vous-même, tous vos collaborateurs et amis devriez appliquer. Informez-les que vous n'ouvrirez aucun de leurs courriels tant qu'ils ne pratiqueront pas le courrier électronique sécurisé.

1 ◆ N'ouvrez JAMAIS un courriel d'un(e) inconnu(e).

2 ◆ Ne faites JAMAIS suivre le courriel d'un(e) inconnu(e), ou qui a été envoyé initialement par un(e) inconnu(e). Tous les messages contenant des "chaînes du bonheur" peuvent contenir des virus. En les envoyant à vos amis ou collaborateurs, vous infecterez peut-être leurs ordinateurs. Si le message "chaîne du bonheur" vous plait, recopiez le contenu dans un nouveau message que vous enverrez de votre compte. Si vous estimez ne pas avoir le temps, c'est que le message en lui-même n'est probablement pas important.

3 ◆ Ne téléchargez JAMAIS une pièce jointe et ne l'ouvrez que si vous connaissez son contenu et que celui-ci est sécurisé. Désactivez les options de téléchargement automatique de vos programmes de courrier électronique. Beaucoup de virus et de chevaux de Troie se propagent sous forme de "bogues" et les bogues d'aujourd'hui vous donneront l'impression d'avoir été envoyés par quelqu'un que vous connaissez. Des bogues intelligents peuvent ainsi scanner votre carnet d'adresse, surtout si vous utilisez Microsoft Outlook ou Outlook Express, et se reproduire automatiquement en se faisant passer pour des pièces jointes authentiques envoyés par des contacts authentiques. Utilisez un logiciel comme PGP pour crypter vos courriels avec ou sans vos pièces jointes, et signez-les pour éviter une confusion sur la sécurité des pièces jointes que vous envoyez à vos collègues (PGP est un logiciel qui chiffre les données; voir ci-dessous "cryptographie").

4 ◆ N'utilisez JAMAIS les formats HTML, MIME ou du "texte riche" (rich text) dans vos courriels, seulement du "texte simple". Les courriels en "texte riche" contiennent des logiciels cachés qui pourraient permettre l'accès à votre système ou endommager vos fichiers.

5 ◆ Quand vous utilisez Outlook ou Outlook Express, décochez l'option d'écran de prévisualisation.

6 ◆ Encryptez (chiffrez) vos courriels autant que possible. Un courriel non chiffré ressemble à une carte postale pouvant être lue par toute personne qui la voit et qui en obtient l'accès. Un message crypté ressemble au contraire à une lettre dans une enveloppe à l'intérieur d'un coffre-fort.

7 ◆ Envoyez des champs "objets" éloquents pour que votre lecteur sache que vous aviez l'intention de lui envoyer le message. Dites à vos amis et collègues de toujours mentionner quelque chose de personnel dans le champ "objet" afin que vous sachiez qu'ils sont les auteurs réels du message. Autrement, quelqu'un peut usurper leur adresse électronique, ou alors un cheval de Troie pourrait avoir envoyé un programme infecté à leur liste de contacts toute entière, vous y compris. Cependant, abstenez-vous de dévoiler des données sensibles dans vos champs "objet" liés aux informations sensibles que vous transmettez dans votre courriel chiffré. Sachez qu'un champ "objet" n'est pas crypté et qu'il peut dévoiler le contenu de votre message crypté, ce qui pourrait susciter une attaque. Beaucoup de logiciels pirates scannent et copient automatiquement le contenu de courriels qui sont signalés dans le champ objet par la mention de "rapport", "confidentiel" ou "privé" par exemple, ou toute autre indication qui rende le message "intéressant".

8 ◆ N'envoyez JAMAIS un message à un groupe de diffusion important, avec des adresses multiples dans le champ "destinataires", et des copies du message à d'autres adresses multiples (champs "Envoyer à" et "CC" -copie-). Préférez envoyer le courriel à vous-même en tapant le nom de tous les destinataires dans le champ "CCI" (copie invisible). C'est faire preuve d'une courtoisie élémentaire et constitue une bonne pratique de protection de la confidentialité. Dans le cas contraire, vous pourriez être en train d'envoyer MON adresse électronique à des personnes que je ne connais pas, ce qui est impoli, choquant et pourrait s'avérer à la fois frustrant et dangereux.

9 ◆ Ne répondez JAMAIS aux messages spam, c'est-à-dire à l'envoi massif de courriels non désirés (ou encore "pourriels"), même si c'est pour indiquer que vous souhaitez être rayé de leurs listes. En effet, les serveurs de spam envoient des courriels à un nombre extrêmement important d'adresses électroniques sans savoir lequel des destinataires est vraiment "en direct", à savoir en train d'utiliser son compte de messagerie au moment de l'envoi. Si vous répondez, le serveur vous détecte comme compte actif et vous pourriez recevoir encore plus de courriels indésirables.

10 ◆ Si cela vous est possible, prévoyez un ordinateur qui ne soit pas relié en réseau à d'autres ordinateurs pour recevoir des courriels ordinaires et qui en outre ne contient aucun fichier de données.

11 ◆ Vous pouvez également utiliser deux adresses uniquement pour communiquer **entre elles** (comme avec l'exemple des deux numéros de téléphone d'urgence et avec les mêmes règles),ou alors une seule adresse à laquelle plusieurs personnes de confiance membres de votre organisation ont accès: les mails ne devront pas voyager plus d'une fois et peuvent être consultés par plusieurs personnes. Rappelez-vous que plus il y a des personnes qui sont au courant, moins l'adresse est sûre. Changez l'adresse de temps à autre.

Le cryptage (cryptographie): questions et réponses

Ce qui suit constitue une liste des questions les plus fréquemment posées et leurs réponses. Vous pouvez contacter pour toute question l'ONG Privaterra sur www.privaterra.org.

Q: Qu'est-ce que le cryptage?

R: Le cryptage signifie brouiller des données par un code secret que seul le destinataire peut déchiffrer. Avec du temps et les moyens informatiques suffisants, tout message crypté peut être lu, mais cela peut prendre longtemps et exiger beaucoup de ressources. Autrement dit, le cryptage est une façon de protéger vos fichiers et vos courriels d'éventuels logiciels-espions. Vos fichiers sont traduits en code, une série apparemment aléatoire de chiffres et de lettres qui est illisible par toute personne non initiée. Pour chiffrer un fichier, vous le "verrouillez" avec une clé représentée par un mot de passe. Pour chiffrer un courriel, vous le verrouillez avec deux clés en utilisant votre mot de passe. Il ne peut être ouvert que par le destinataire voulu qui utilisera son propre mot de passe.

Q: Pourquoi les défenseurs des droits humains devraient-ils utiliser le cryptage?

R: Tout le monde devrait utiliser le cryptage parce que les communications électroniques sont essentiellement non sécurisées. Cependant, les défenseurs des droits humains sont beaucoup plus menacés que la plupart des personnes et leurs fichiers et communications sont beaucoup plus sensibles. Il est impératif que les défenseurs des droits humains utilisent le cryptage pour se protéger ainsi que protéger toutes les personnes qu'ils essayent d'aider.

La technologie numérique constitue un atout pour les organisations de droits humains car elle leur permet des échanges plus faciles (rapides et moins onéreux), une plus grande efficacité et leur offre davantage de possibilités. Cependant, tout avantage comporte certains écueils. Ces écueils ne sont néanmoins pas systématiques. e n'est pas parce que vous avez mis votre ceinture de sécurité que vous allez nécessairement avoir un accident à chaque fois que vous prenez le volant. Mais quand vous roulez dans des circonstances plus dangereuses, comme dans une course automobile, vous serez plus enclins à mettre la ceinture de sécurité, simplement parce que vous serez plus conscients de votre sécurité.

Les défenseurs des droits humains sont des cibles de surveillance connues. Puisque les courriels non chiffrés sont accessibles à tout le monde, et que tout le monde peut les lire, il est presque inévitable que tôt ou tard l'on ait accès à vos courriels non cryptés. En ce moment précis, vos messages pourraient déjà faire l'objet d'une surveillance de la part de vos adversaires et vous pourrez parfaitement ne jamais vous en apercevoir. **Attention, les adversaires des personnes que vous aidez sont également les vôtres.**

Q: Est-ce illégal d'utiliser le cryptage?

R: Dans certains cas. Il est parfaitement légal d'utiliser le cryptage dans la plupart des pays. Il existe cependant des exceptions. En Chine, par exemple, les

organisations doivent obtenir une autorisation pour avoir le droit de chiffrer leurs données, et toute technologie de cryptage sur votre ordinateur portable doit être déclarée lorsque vous vous rendez dans le pays. À Singapour et en Malaisie, la loi exige que les personnes souhaitant utiliser le cryptage communiquent leurs clés privées. Des lois similaires sont actuellement envisagées en Inde. Il y a également d'autres exceptions.

Le Electronic Privacy Information Centre (EPIC, centre d'information sur la confidentialité électronique) réalise une "Enquête internationale des politiques en matière de cryptage" examinant la législation en vigueur dans la plupart des pays, qui est disponible sur l'URL http://www2.epic.org/reports/crypto2000/. Cette liste a été remise à jour pour la dernière fois en 2000. Si vous avez une question précise, vérifiez auprès de Privaterra avant d'utiliser le cryptage dans un pays donné.

Q: De quoi avons-nous besoin pour préserver la sécurité de nos systèmes de technologie de l'information?

R: Tout dépend du système et de vos activités, mais en règle générale n'importe qui devrait disposer de:

- Un logiciel pare-feu.
- La possibilité de chiffrer le contenu intégral du disque dur.
- Un logiciel de cryptage de courriels permettant également les signatures numériques, comme le logiciel PGP.
- Un logiciel de détection de virus.
- Un système de sauvegarde sécurisée: envoyez toutes les informations par courrier électronique à un site sécurisé et procédez à un enre-gistrement hebdomadaire de tous les fichiers sur disque compact enre-gistrable, un CD-RW. Ensuite, conservez-le dans un endroit indépendant et sûr.
- Utilisez des mots de passe que vous pouvez mémoriser mais qui ne peuvent pas être devinés ou déduits par un tiers.
- Restreignez l'accès aux données et aux fichiers en fonction de l'organigramme de votre organisation. Tous les membres de l'organisation n'ont pas besoin d'avoir accès à l'intégralité des informations
- Faites preuve de cohérence et d'assiduité car aucun de ces outils ne peut être efficace si vous ne l'utilisez pas de manière systématique!

Mais posséder le bon logiciel ne constitue pas la panacée. **Ce sont les utilisateurs qui représentent souvent le maillon le plus faible, et non la technologie.** Le cryptage ne fonctionne pas si les individus ne l'utilisent pas de manière systématique, s'ils communiquent leur mot de passe de manière indiscriminée ou s'ils le rendent visibles, par exemple en l'inscrivant sur une note adhésive (post - it) qu'ils collent à leur écran. Par ailleurs, les logiciels de sauvegarde ne vous mettront pas à l'abri d'un incendie ou d'une perquisition (ou cambriolage) si vous ne gardez pas la copie de sauvegarde dans un endroit indépendant et sûr. Les informations sensibles doivent être divulguées au compte-gouttes et uniquement au membre de l'organisation qui en a réellement besoin pour son activité, selon le principe de "qui doit savoir?" au lieu d'être communiquées indifféremment à tous les membres. Ceci implique d'élaborer une **hiérarchie et des protocoles d'accès.** En général, il est important d'être con-

scient de la confidentialité et de la sécurité dans vos activités quotidiennes. Nous appelons cela la "paranoïa saine".

Q: Comment faire pour savoir quel logiciel de cryptage utiliser?

R: Généralement, vous pouvez demander à vos amis et ensuite vérifier auprès de notre organisation. Vous devez pouvoir communiquer avec des personnes ou des groupes donnés et s'ils utilisent un système de cryptage précis vous devriez utiliser le même pour faciliter les communications. Cependant, vérifiez auprès de notre organisation d'abord. En effet, certains logiciels ne sont tout bonnement pas efficaces du tout, d'autres sont des "bonbons": les "bonbons" vous bercent dans l'illusion d'utiliser des logiciels gratuits et apparemment d'excellente qualité alors qu'ils ont été mis au point par ceux qui veulent vous espionner. Quelle meilleure façon de lire vos communications les plus sensibles que celle d'être officiellement chargé d'installer votre logiciel de cryptage? Quoi qu'il en soit, il existe beaucoup de fabricants reconnus de logiciels propriétaires et de "gratuiciels", alors souvenez-vous seulement que vous devez examiner tout logiciel avant de l'utiliser.[32]

Q: Est-ce que l'utilisation du cryptage va m'exposer à un risque plus élevé de répression?

R: Personne ne saura que vous utilisez le cryptage à moins que vos échanges de courriels ne soient dores et déjà surveillés. Si c'est le cas, vos informations confidentielles sont déjà lues. Cela signifie que vous faites déjà l'objet de répression (ou que vous risquez déjà de faire l'objet d'une répression) de la part de ceux qui vous surveillent. Il se peut que ceux qui vous surveillent se voient contraints d'avoir recours à d'autres moyens s'ils sont privés de la possibilité de lire vos courriels. Il est donc important de bien connaître vos collègues, de mettre en place des politiques de sauvegarde sécurisées et de gestion efficace des activités administratives en même temps que la première utilisation du cryptage.

Notez que nous n'avons pas été informés de cas où l'utilisation de logiciels de cryptage ait causé des difficultés à des défenseurs. Néanmoins, examinez cette possibilité avec prudence avant de vous mettre au cryptage, surtout si vous vous trouvez dans un pays en proie à des conflits armés, car les services d'intelligence de l'armée pourraient vous soupçonner de communiquer des informations d'intérêt stratégique. Soyez vigilants également si peu de défenseurs utilisent le cryptage, auquel cas cela pourrait vous valoir une attention indésirable.

Q: Pourquoi faut-il que nous cryptions systématiquement tous les courriels et documents?

R: Si vous n'utilisez le cryptage que pour des sujets sensibles, les personnes qui vous surveillent ou qui surveillent vos victimes peuvent deviner qu'une activité sensible a lieu et pourraient être incités à mener une descente chez vous ou chez les victimes. S'ils ne peuvent pas lire vos messages cryptés, ils observeront le nombre de messages chiffrés et de messages non chiffrés (ou clairs). Une soudaine augmentation des messages cryptés peut donc provoquer une perquisition (ou cambriolage), si bien que c'est une bonne idée de commencer à

[32] Par exemple, PGP - "Pretty Good Privacy"- est un logiciel bien connu et protégé. Vous pouvez le télécharger depuis www.pgpi.org.

crypter avant de lancer des projets spéciaux/sensibles. En fait, l'idéal est d'introduire le cryptage de manière maîtrisée pour éviter les pics de messages chiffrés. Envoyez des messages cryptés à intervalles réguliers même si vous n'avez pas de nouvelles données à communiquer. De cette façon, lorsque vous aurez à envoyer des informations délicates, elles seront moins manifestes.

Q: Si je dispose déjà d'un logiciel pare-feu, pourquoi ai-je besoin de crypter mes courriels?

R: Les pare-feux bloquent l'accès à votre disque dur et à votre réseau aux pirates de l'informatique; or, dès que vous envoyez votre message sur Internet, il est aux mains de tous. Vous devez le sécuriser avant de l'envoyer.

Q: Il n'y a pas d'effractions dans nos bureaux, pourquoi utiliser alors un logiciel de protection de la confidentialité?

R: Vous ne savez pas si quelqu'un est en passe de s'introduire dans votre système ou d'être à l'origine de fuites de données depuis votre ordinateur. Sans cryptage des communications, sans protection matérielle et protocoles de confidentialité, n'importe qui peut être en passe d'accéder à vos fichiers, de lire vos courriels et de manipuler vos documents à votre insu. Vos communications non sécurisées peuvent aussi mettre d'autres personnes en danger dans les endroits où des perquisitions (ou cambriolages) de nature politique sont plus probables. Tout comme vous fermez vos portes à clé, vous devriez crypter vos documents. C'est aussi simple que ça.

Q: Nous n'avons pas accès à Internet et sommes obligés d'utiliser des cafés Internet. Comment protéger les communications envoyées d'un ordinateur extérieur?

R: Vous avez toujours la possibilité de crypter vos courriels et vos fichiers. Avant d'aller dans un café Internet, chiffrez les fichiers que vous souhaitez envoyer et copiez le fichier chiffré sur une disquette ou un disque compact. Au café Internet, souscrivez à un service de cryptage comme par exemple www.hushmail.com ou utilisez un service respectant l'anonymat tel que www.anonymiser.com. Appliquez-les lors de l'envoi de vos courriels. Vérifiez que vos destinataires ont également souscrit à ces services.

Q: S'il est important de sécuriser nos dossiers et nos communications, pourquoi est-ce que tout le monde ne le fait pas?

R: Cette technologie est relativement récente, mais son usage se répand. Les banques, les multinationales, les agences de presse et les gouvernements utilisent tous le cryptage, et l'envisagent comme un investissement solide et un coût nécessaire à leur activité. Les ONG sont plus exposées que les entreprises, ce dont la majorité des gouvernements se réjouissent. Les ONG sont des cibles de surveillance plus probables et doivent donc s'efforcer de mettre en place activement cette technologie. Les défenseurs des droits humains se chargent de protéger des individus ou des groupes persécutés. Pour cela, ils conservent des dossiers qui peuvent permettre d'identifier et de localiser ces personnes. Si l'on donne l'accès à ces dossiers, ces individus peuvent être assassinés, torturés, enlevés ou "persuadés" de ne plus faire appel ou fréquenter les ONG. De même,

les membres ou correspondants des ONG peuvent être "persuadés" de ne plus aider la structure. Les informations contenues dans ces dossiers peuvent aussi être utilisées comme preuves contre les ONG et leurs "clients" lors de procès politiques.

Q: Un des nos principes est celui de la transparence. Nous militons en faveur d'une plus grande transparence des gouvernements. Comment pouvons-nous dans ce contexte utiliser la technologie de la confidentialité?

R: La confidentialité est compatible avec la transparence. Si le gouvernement souhaite obtenir vos dossiers ouvertement, il en a la possibilité par les voies légales et reconnues. La technologie de la confidentialité empêche toute personne d'accéder à vos informations de manière illégale.

Q: Nous suivons tous les protocoles de confidentialité et de sécurité et nos informations continuent à faire l'objet de fuites. Pourquoi?

R: Il y a peut-être un espion dans vos rangs ou quelqu'un simplement incapable de respecter la confidentialité des données. Réexaminez la hiérarchie de vos informations et restreignez l'accès aux informations délicates à encore moins de personnes et gardez un œil tout particulièrement vigilant sur ces personnes-là. De grandes entreprises et des organisations procèdent à titre de routine à des diffusions régulières d'éléments d'informations incorrectes à certaines personnes. Si ces informations incorrectes sont divulguées, on peut remonter la fuite jusqu'à la personne qui les a reçues au départ.

Les choses à faire et à ne pas faire en matière d'utilisation du cryptage

- **Veillez à utiliser** le cryptage de manière cohérente. Si vous n'utilisez le cryptage que pour les données sensibles, toute personne vous surveillant sera informée qu'une chose importante est sur le point d'arriver. Une augmentation abrupte de l'utilisation du cryptage peut provoquer une perquisition (ou cambriolage).

- **N'indiquez aucune** information sensible dans les champs "objet". Ils ne sont en général pas cryptés, même si le texte du message l'est.

- **Veillez à utiliser** un mot de passe contenant des lettres, des chiffres, des espaces et de la ponctuation dont vous seul pouvez vous souvenir. Certaines techniques de création de mots de passe sécurisés utilisent des symboles de votre clavier ou des combinaisons aléatoires de mots et de symboles. En général, plus le mot de passe est long, moins il est vulnérable.

- **N'utilisez pas** de mot ou de nom uniques, de proverbe ou d'adresse de votre répertoire d'adresses comme mot de passe. Ils peuvent être déchiffrés en quelques minutes.

- **Faites une copie de sauvegarde de votre clé privée** (c'est-à-dire le dossier qui contient votre clé privée pour le logiciel de cryptage) dans un seul endroit bien à l'abri, par exemple copiez-le sous forme cryptée sur une disquette ou sur une petite clé de mémoire USB détachable, "à porter en médaillon autour du cou".

- **N'envoyez pas** d'informations sensibles à un destinataire simplement parce qu'il vous a envoyé un courriel crypté à partir d'une adresse que vous connaissez. Tout un chacun peut usurper le nom de quelqu'un d'autre en rendant son adresse électronique quasi identique à celle d'une personne que vous connaissez. Vérifiez toujours l'identité de la personne avant d'estimer que la source est fiable, communiquez donc de vive voix, vérifiez par téléphone ou envoyez un courriel de réponse anodin pour être absolument sûr(e).

- **Enseignez** le cryptage aux autres. Plus il y aura de personnes qui s'en serviront, plus nous serons nombreux à être protégés.

- **N'oubliez pas** de signer électroniquement votre message en plus de le chiffrer. Votre but est que le destinataire du message sache s'il a été modifié en cours de route.

- **Cryptez** les fichiers que vous envoyez en pièces jointes. En général, ils ne sont pas chiffrés automatiquement lorsque vous envoyez un courriel crypté.

Un guide de la gestion plus sûre des bureaux et des informations

Une gestion des bureaux plus sûre

Créer de nouvelles habitudes peut entraîner une gestion administrative plus sûre. Les habitudes adoptées en matière de gestion administrative peuvent à la fois être bonnes et dangereuses. Pour développer de bonnes habitudes de gestion administrative, il faut comprendre le raisonnement qui les suscite. Nous avons établi une liste des habitudes qui peuvent améliorer la sécurité de votre gestion administrative, si et seulement si vous vous les appropriez et réfléchissez aux raisons de leur importance.

Qu'est-ce qui compte le plus pour la confidentialité et la sécurité de la gestion administrative?

- Soyez conscients de votre information et des personnes qui y ont accès.
- Encouragez les habitudes sûres et utilisez-les de façon cohérente.
- Utilisez les outils de façon adéquate.

L'administration

Beaucoup d'organisations ont un administrateur de système ou quelqu'un ayant des privilèges administratifs lui donnant accès aux courriels, aux réseaux informatiques et l'autorisant à surveiller l'installation de nouveaux logiciels. Si une personne quitte l'organisation ou si elle n'est pas disponible, l'administrateur a le droit d'accéder aux informations de cet individu sans que cela perturbe le cours des choses au sein de l'organisation. De plus, cela signifie qu'il y a une personne responsable de la sécurité informatique qui garantit que les logiciels du système ne présentent aucun virus et qu'ils proviennent d'une source fiable.

Le problème est que l'organisation assimile cette tâche à du simple entretien technique et permet à un contractant externe de détenir ces privilèges adminis-

tratifs. Cet administrateur a le contrôle effectif de toute l'information de l'organisation, et doit donc être absolument digne de confiance. Certaines organisations répartissent les responsabilités d'administrateur au directeur de l'organisation et à une deuxième personne digne de confiance.

Certaines organisations choisissent de noter toutes les clés privées PGP et les mots de passe, de les crypter et de les stocker dans un endroit indépendant en les confiant à une autre organisation en qui elles ont confiance. Ceci évite les problèmes au cas où les individus oublient leur mot de passe ou perdent les clés privées. Cependant, l'endroit où sont stockés les fichiers doit être absolument fiable et des protocoles précis et complets doivent être créés à propos de l'accès à ces fichiers.

Les règles:

1 ◆ NE donnez JAMAIS de privilèges administratifs à un contractant externe. Non seulement il ne sera pas aussi fiable que les membres de l'organisation, mais une personne externe sera aussi plus difficile à joindre en cas d'urgence.

2 ◆ Seules les personnes absolument dignes de confiance doivent détenir les privilèges administratifs.

3 ◆ Déterminez quelles informations doivent être accessibles à l'administrateur: accès à tous les ordinateurs, aux mots de passe pour déverrouiller l'ordinateur, aux mots de passe pour la connexion, aux clés PGP, aux mots de passe pour le cryptage, etc.

4 ◆ Si vous choisissez de confier des copies des mots de passe et des clés PGP à une autre organisation, vous devez créer des protocoles d'accès.

5 ◆ Si une personne quitte l'organisation, ses mots de passe et codes d'accès personnels doivent être immédiatement modifiés.

6 ◆ Si une personne détenant des privilèges administratifs quitte l'organisation, tous les mots de passe et codes d'accès doivent être modifiés immédiatement.

L'administration des logiciels

Utiliser des logiciels piratés peut mettre l'organisation à la merci de la "police des logiciels". La police peut sévir contre une organisation au motif de l'utilisation de logiciels piratés en imposant de lourdes amendes et entraîner de fait une fermeture de l'organisation. L'organisation en question n'obtiendra probablement pas le soutien des médias occidentaux puisque cela ne relèvera pas de l'attaque contre une ONG de droits humains mais de la lutte contre le piratage. Soyez extrêmement vigilants en ce qui concerne les licences de logiciels et ne permettez pas qu'un logiciel soit copié par un membre de l'organisation. Un logiciel piraté peut également représenter un risque de sécurité puisqu'il peut contenir des virus. Utilisez toujours un logiciel anti-virus pour installer des logiciels.

Un administrateur devrait contrôler les nouvelles installations de logiciels pour s'assurer qu'ils soient vérifiés d'abord. Ne permettez pas l'installation d'un logi-

ciel potentiellement non sécurisé, et n'installez que les logiciels dont vous avez besoin.

Installez les listes de signature les plus récentes pour tous les logiciels utilisés, en particulier pour *Microsoft Office, Microsoft Internet Explorer et Netscape*. La plus grande menace de sécurité provient de logiciels et de matériel informatique livrés avec des vulnérabilités connues. Envisagez de passer aux logiciels *Open Source. Open Source* ne base pas sa sécurité sur le principe du secret de la conception de ses logiciels (Security through Obscurity). Au contraire, il invite les experts et les pirates à tester tous ses codes. Utiliser les logiciels *Open Source* et tous les autres logiciels autres que *Microsoft* présente l'avantage supplémentaire de vous rendre moins vulnérable aux virus courants et aux pirates non spécifiques. Moins de virus sont créés pour les systèmes d'exploitation *Linux* ou *Macintosh* car la plupart des personnes utilisent *Windows. Microsoft Outlook* est le programme de messagerie électronique le plus répandu et constitue donc une cible privilégiée pour les pirates.

Les habitudes lors de l'envoi de courriels

Le cryptage des courriels devrait devenir une habitude. Il est plus facile de se souvenir de tout crypter que d'avoir une politique dictant quand il faut crypter et quand non. Sachez que si vous cryptez systématiquement tous vos courriels, la personne qui surveille vos échanges de courriels ne s'apercevra pas que vos communications deviennent plus sensibles à certains moments.

Quelques autres points importants:

- Sauvegardez toujours les courriels cryptés sous leur forme cryptée. Vous pouvez toujours les déchiffrer ultérieurement, tandis que si quelqu'un accède à votre ordinateur les messages sont aussi vulnérables que s'ils n'avaient pas été cryptés.

- Faites preuve de cohérence avec vos correspondants électroniques afin d'être sûr que ces personnes ne décryptent pas leur courrier puis transmettent vos messages sous forme déchiffrée, ou encore qu'ils vous répondent sans crypter leur réponse. La paresse individuelle représente la plus grande menace pour vos communications.

- Vous devriez peut-être créer quelques comptes de messagerie sécurisés pour les personnes travaillant sur le terrain et qui ne soient pas habituellement utilisés afin qu'ils ne soient pas détectés par les serveurs de spam (courriels indésirables). Il faudrait vérifier de manière régulière si ces adresses utilisées seulement par les membres sur le terrain ont quand même reçu de nouveaux courriers. Le cas échéant, vous pourrez détruire les comptes de messagerie qui reçoivent beaucoup de courriels indésirables et conserver, ainsi, sans danger, votre base de contacts.

Conseils généraux sur les cybercafés ou cafés Internet et autres

Les courriels envoyés en texte brut et non chiffrés à travers Internet peuvent être lus par de nombreuses instances pour autant qu'elles en prennent la peine.

L'une d'entre elles peut être votre FAI local (fournisseur d'accès à Internet) ou tout fournisseur par lequel transitent vos courriels. Un courriel transite par de nombreux ordinateurs sur le chemin entre l'expéditeur et le destinataire. Il ignore les frontières géopolitiques et peut transiter par les serveurs d'un autre pays même si vous envoyez des messages à l'intérieur d'un même pays.

Voici quelques éclaircissements sur des malentendus fréquents parmi les utilisateurs d'Internet (les internautes):

- La protection d'un fichier par mot de passe offre une protection si peu efficace du fichier en question que ce n'est pas la peine de l'utiliser pour les documents aux informations sensibles. Elle ne donne qu'une illusion de sécurité.

- Compresser un fichier ne le protège pas de quelqu'un qui voudrait vérifier son contenu.

- Si vous voulez garantir la sécurité d'envoi d'un fichier ou d'un courriel, utilisez la cryptographie (voir www.privaterra.com).

- Si vous voulez envoyer un courriel ou un document en toute sécurité, il faut utiliser le cryptage à toutes les étapes depuis l'envoi jusqu'à la réception par le destinataire et lors de la transmission du destinataire à d'autres personnes. Il ne suffit pas d'envoyer un message crypté depuis un bureau sur le terrain à New York, Londres ou ailleurs pour qu'ensuite il soit transmis à un tiers sans avoir été chiffré.

- Internet est planétaire par définition. Il n'y a aucune différence entre le fait d'envoyer un message entre deux bureaux de Manhattan et celui d'envoyer un message d'un café Internet en Afrique du Sud à un ordinateur d'un bureau de Londres.

- Utilisez la cryptographie autant que possible, même si le message ou les données que vous envoyez ne sont pas sensibles!

- Veillez à ce que l'ordinateur que vous utilisez ait un logiciel de protection contre les virus. Beaucoup de virus sont programmés pour extraire des informations de votre ordinateur, que ce soit les contenus stockés sur votre disque dur ou des fichiers Internet, y compris votre répertoire d'adresses électroniques!

- Veillez à ce que votre logiciel ait une licence légale. Si vous utilisez des logiciels pirates, vous devenez immédiatement un pirate de logiciel et non un militant des droits humains aux yeux des gouvernements et des médias. La meilleure solution est d'utiliser les logiciels Open Source (à accès libre), ils sont gratuits.

- Il n'existe pas de solution à 100% sûre lorsque vous utilisez Internet.

- N'importe qui peut entrer dans votre système sous n'importe quel prétexte en se faisant passer pour quelqu'un d'autre au téléphone ou par courriel. Fiez-vous a votre jugement et à votre bon sens.

- Rappelez-vous que les acteurs intéressés par votre travail n'ont pas attendu les technologies pour essayer d'obtenir des informations vous concernant.

En résumé

De nombreux défenseurs des droits humains sont réticents à utiliser une technologie d'information sûre. Cependant, les procédures de base sont simples.

Les procédures de base simples sont les suivantes: faites montre de discrétion lors de vos communications téléphoniques ou en face-à-face, utiliser le logiciel de cryptage PGP pour la communication par courriels et pour les fichiers sensibles, utiliser des mots de passe pour accéder à votre ordinateur.

Mais disposer du bon logiciel n'est pas tout. **Les utilisateurs représentent souvent le maillon le plus faible, pas la technologie.**

Deuxième Partie

Sécurité de l'Organisation

Introduction:

Dans la deuxième partie de ce manuel, nous aborderons la sécurité du point de vue de l'organisation, c'est à dire les moyens d'améliorer la sécurité au sein des organisations de défenseurs.

La sécurité / protection ne signifie pas avoir simplement un plan de sécurité. Cela exige de s'approprier l'ensemble du processus, en commençant par l'amélioration du niveau de sécurité d'origine de l'organisation, ensuite par la mise en œuvre du processus, et finalement par la gestion du processus d'amélioration lui-même.

L'appropriation du processus fait partie de la sécurité elle-même.

Le processus de sécurité de l'organisation est pragmatique et il inclut tous les membres.

Il doit être réaliste et adapté au profil et aux besoins de l'organisation.

Bien qu'il nécessite dans certains cas des ressources, changer son comportement constitue un élément capital de l'amélioration de la sécurité et ne coûte rien.

Contenu de la deuxième partie:

2.1 Évaluer la performance de l'organisation: la "roue de la sécurité".

2.2 S'assurer du respect des règles et procédures de sécurité.

2.3 Gérer le changement de l'organisation vers une politique de sécurité améliorée.

CHAPITRE 2.1

Évaluer la performance de sécurité de l'organisation: la "roue de la sécurité"

Objectif:

Examiner la façon dont vous gérez la sécurité.

Mesurer l'intégration de la sécurité dans le travail des défenseurs des droits humains.

Pour atteindre cet objectif nous suggérons une approche en deux temps:

- une auto-évaluation par l'organisation de sa performance de sécurité: l'organisation examine la performance de sa sécurité en réunissant des informations objectives. Le processus d'auto-évaluation peut être collectif ou individuel. Il est intéressant de constater que les membres d'une même organisation peuvent aboutir à des conclusions différentes concernant la performance de sécurité de l'organisation entière.

- comment 'les autres' perçoivent l'organisation

Auto-évaluation de la sécurité d'une organisation

La roue de la sécurité

L'auto-évaluation de la sécurité d'une organisation peut être réalisée objectivement à l'aide de la roue de la sécurité et de ses huit rayons.

Pour tourner correctement, une roue doit être ronde; en d'autres termes, tous les rayons doivent avoir la même longueur. Il en va de même pour la roue de la sécurité et ses huit rayons (composants) qui représentent la gestion de la sécurité dans une organisation ou un groupe de défenseurs.

Cette évaluation peut se faire en groupe:

- faites un schéma de la roue
- coloriez les espaces entre les rayons selon le degré estimé de leur développement
- indiquez les raisons pour lesquelles vous pensez (brainstorming) que certains rayons sont moins développés; comme tous les rayons doivent être

aussi longs que le rayon le plus développé, suggérez des méthodes pour parvenir à ce résultat: définissez des objectifs et des processus correspondants, anticipez des problèmes possibles et suggérez des solutions.

- une fois terminé l'exercise, garder la roue. Lorsque vous répéterez l'exercice quelques mois plus tard, vous pourrez comparer les deux roues et vérifier point par point si le niveau global de la sécurité organisationnelle s'est améliorée.

La roue est composée de huit rayons, ou composants:

- **L'expérience sur le terrain et cohésion:** les connaissances pratiques acquises sur le tas et partagées concernant la sécurité et la protection. Votre point de départ et d'arrivée de l'évaluation.

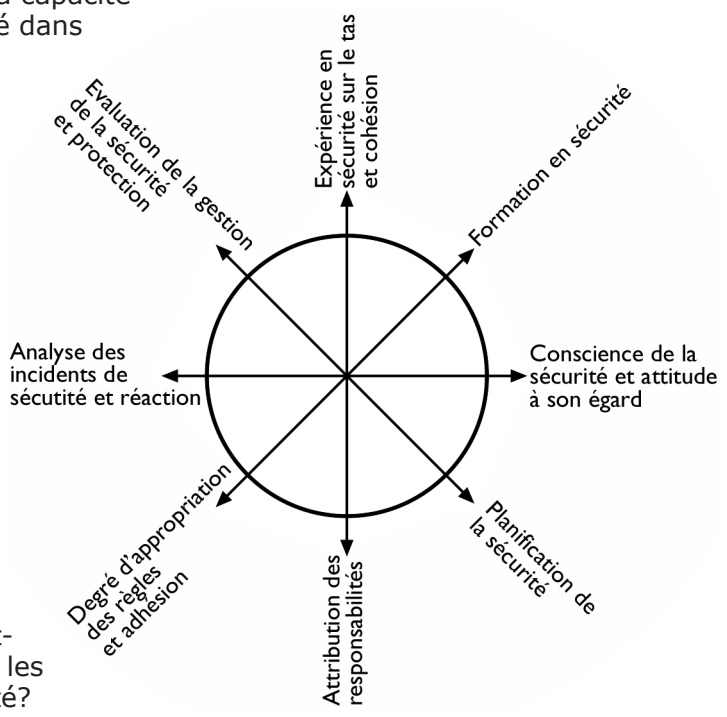
- **La formation:** vous pouvez vous former à la sécurité dans un cours ou à votre propre initiative pendant votre travail.

- **La conscience de la sécurité et l'attitude à son égard:** chaque individu et l'organisation dans son ensemble voient-ils réellement la protection et la sécurité comme des besoins et sont-ils décidés à les mettre en œuvre?

- **La planification:** la capacité de planifier la sécurité dans votre travail.

- **L'attribution des responsabilités:** qui est responsable de quels aspects de la sécurité et de la protection? Et que se passe-t-il en cas d'urgence?

- **Le degré d'appropriation des règles de sécurité et adhésion:** dans quelle mesure les personnes respectent-elles les règles et les procédures de sécurité?



- **Analyser les incidents de sécurité et y réagir:** dans quelle mesure les incidents de sécurité sont-ils analysés? Est-ce que l'organisation réagit de manière adéquate?

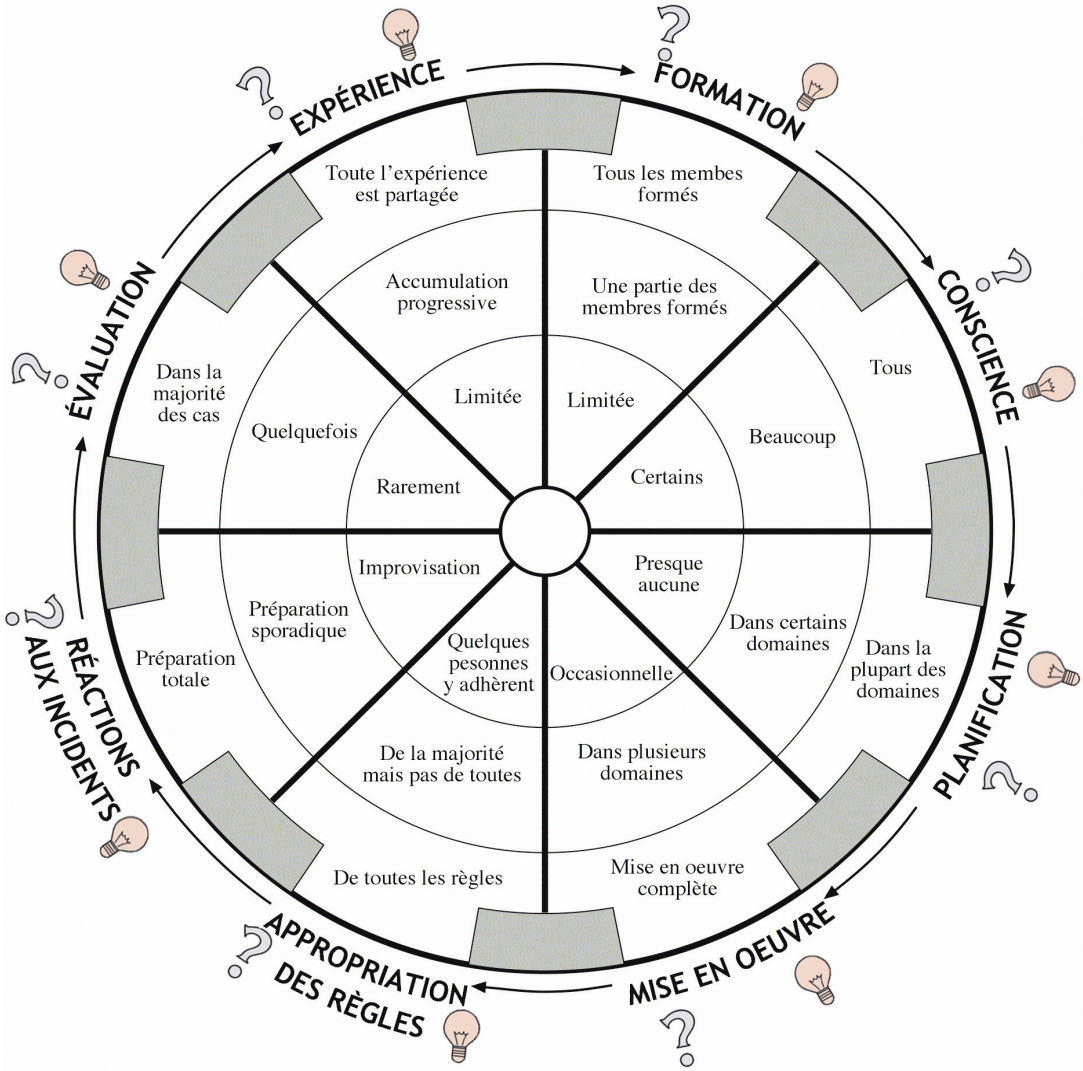
- **Evaluer la gestion de la sécurité et de la protection:** dans quelle mesure l'organisation évalue-t-elle sa gestion de la sécurité et de la protection et dans quelle mesure la met-elle à jour?

Voici un exemple de la roue de la sécurité:

La roue de la sécurité n'est jamais parfaite: certaines parties sont plus développées que d'autres. Il est donc plus utile d'examiner le degré de développement de chaque partie. De cette manière, vous pouvez identifier les types d'actions prioritaires pour améliorer la protection et la sécurité. Chaque ligne partant du centre représente le développement d'un composant de la roue.

Problèmes éventuels se rapportant à ce composant de la roue ...

...et solutions possibles des problèmes.



Photocopiez la roue sur une feuille ou sur un transparent et coloriez les espaces entre les rayons. Ceci illustrera la forme réelle de la roue de votre groupe ou de votre organisation, et fera apparaître plus clairement quelles parties sont plus ou moins développées.

Une analyse étape par étape de "la roue de la sécurité"

Une évaluation complète de la politique de sécurité d'une organisation prend du temps s'il faut examiner la véritable signification de chaque composant de la roue de la sécurité.

1 ● L'expérience acquise sur le tas et la cohésion de toute l'équipe en matière de sécurité et protection:

Le savoir pratique accumulé et la cohésion de l'équipe en matière de sécurité et de protection. Le point de départ et d'arrivée de l'évaluation.

Gardez à l'esprit que l'expérience de quelques membres n'équivaut pas à l'expérience de la sécurité au niveau d'une organisation mais plutôt à la moyenne (l'expérience de quelques-uns divisés par la totalité de ses membres): le partage des connaissances contribuera donc à la cohésion de toute l'équipe.

La somme des connaissances sera reflétée dans les rayons; une fois que vous aurez développé tous les composants à votre convenance, le résultat sera l'augmentation de la somme des connaissances. La connaissance de la sécurité s'en trouvera plus développée et tous les autres rayons devront suivre. C'est une activité sans fin pour la simple raison que les membres d'une organisation vont et viennent, le contexte politique change et avec lui la sécurité. Cependant la bonne nouvelle est la suivante: comme ce rayon résulte des sept autres, ce rayon-ci ne requiert pas d'actions particulières (au contraire des sept autres).

2 ● La formation

Indiquez la formation en matière de sécurité que vous avez reçue soit par le biais d'un cours, soit par votre initiative personnelle durant votre travail quotidien.

Des questions nécessitant d'être plus développées:

Est-ce que des procédures de formation de sécurité sont accessibles à tous? Est-ce qu'elles sont perfectionnées? Quelles difficultés se présenteraient si nous devions former l'ensemble du personnel? Quelles seraient de possibles solutions?

3 ● La conscience de la sécurité et l'attitude à son égard.

Les questions utilisées pour déterminer le niveau actuel de conscience de la sécurité:

Est-ce que tout le monde est réellement conscient de la sécurité et de la protection? Comment pourrait-on atteindre ce résultat? Conscience ne signifie pas conformité (par exemple les fumeurs savent à quel point fumer est dangereux pourtant ils continuent).

Des questions pour accroître le degré de conscience:

Quels facteurs déclenchent la révision de la sécurité?

Quelles sont les histoires racontées et quelle est la connaissance informelle de la sécurité dans l'organisation?

Quels problèmes pourraient survenir en augmentant la conscience de la sécurité? Quelles seraient de possibles solutions?

4 ● La planification de la sécurité:

Des questions pour déterminer le niveau actuel de planification de la sécurité:

- est-ce que nous planifions et intégrons la sécurité et notre travail?
- la question de la sécurité est-elle intégrée dans l'approche institutionnelle et globale? (missions, plans stratégiques, domaines de travail, thèmes transversaux)?
- la sécurité est-elle à l'ordre du jour lors des réunions les plus importantes (et pas à la fin de celui-ci)?
- quelle en est la stratégie budgétaire (est-elle ad hoc pour la sécurité, ou est-elle inclue dans d'autres stratégies?) et la gestion financière?
- procédons-nous à une analyse de l'environnement de travail - dans des groupes de travail - à un niveau local, régional, national?

Est-ce que nous:

- analysons l'impact du travail accompli par l'organisation et comment celle-ci est perçue par des acteurs pouvant constituer une menace?
- réalisons une analyse d'ensemble de tous les risques: menaces, vulnérabilités et capacités?
- réunissons tous les documents relatifs à la sécurité, en révisant leur contenu et en examinant leur utilisation?
- élaborons et mettons à jour les documents relatifs à la sécurité? Vérifions si ils sont à jour et comment atteindre ce résultat? Vérifions si l'impact du travail et des facteurs de risque ont été pris en compte? Est-ce que nous vérifions s'il y a des processus en place pour des consultations quotidiennes relatives à la sécurité?

Avons nous des plans de sécurité qui sont:

- simples et clairs? Contiennent-ils l'information nécessaire dans un langage clair?
- élaborés en collaboration avec les personnes concernées?
- appropriés à tous les contextes de travail?

- améliorés, développés et mis à jour grâce à l'initiative de différentes personnes du groupes de travail prévu à cette fin?
- authentiques et adaptés au "monde réel"?

Est-ce que nos plans de sécurité couvrent:

- tous les sujets requis?
- la communication, l'informatique et la gestion d'information?
- la gestion des ressources humaines (y compris le recrutement)? la gestion du stress?

Est-ce que l'ensemble des personnes concernées est conscient qu'un groupe de travail ayant une bonne structure, une bonne transmission interne des informations, des bonnes relations publiques et une bonne coopération est une nécessité fondamentale en matière de sécurité?

Des questions visant à développer davantage la planification de la sécurité:

Quels problèmes pourrions-nous rencontrer si nous essayions de nous attaquer à chacun des éléments ci-dessus?

Quelles pourraient-être les solutions?

5 ● L'attribution des responsabilités:

Des questions servant à déterminer le niveau actuel concernant les attributions des responsabilités relatives à la sécurité:

- savons-nous clairement qui est responsable de quel aspect de sécurité et de protection? Et en cas d'urgence?
- existe-t-il des responsabilités et des devoirs d'organisation concernant le personnel et les collaborateurs (y compris leur comportement en dehors du travail et de leurs familles)?
- Est-ce que l'ensemble du personnel prend ses responsabilités en matière de sécurité et y a-t-il des responsabilités spécifiques pour différents aspects de sécurité? (Quelles difficultés rencontrons-nous?)

Des questions pour améliorer l'attribution des responsabilités concernant la sécurité:

Quels problèmes pourrions-nous rencontrer si nous voulions attribuer et partager des responsabilités concernant la sécurité?

Quelles pourraient-être les solutions?

L'attribution des responsabilités contribue au partage de la sécurité.

6 ● Le degré d'appropriation des règles de sécurité et adhésion/conformité:

Des questions pour déterminer le niveau actuel du degré d'appropriation des règles de sécurité/conformité:

• dans quelle mesure les personnes respectent-elles les procédures et règles de sécurité?

• dans quelle mesure les individus et l'ensemble du groupe contribuent-ils à l'élaboration du plan de sécurité et se conforment-ils aux règles de protection et de sécurité?

• pouvons-nous savoir si les règles de sécurité ne sont pas appliquées et si oui, pourquoi?

• les collaborateurs se conforment-ils aux règles de sécurité par peur d'un reproche ou parce qu'ils sont convaincus que l'application des règles de sécurité diminuera les conséquences des risques? (par exemple un conducteur peut mettre la ceinture de sécurité par crainte d'une amende ou parce qu'il est convaincu que le port de celle-ci diminuera les effets d'un accident)

Des questions pour améliorer le degré d'appropriation des règles de sécurité et adhésion/conformité:

Quels problèmes pourrions-nous rencontrer en améliorant le niveau de respect des règles?

Quelles sont les possibles solutions?

7 ● Analyser les incidents de sécurité et y réagir

Des questions pour déterminer le niveau actuel de l'analyse des incidents de sécurité et les réactions à celles-ci:

• dans quelle mesure les incidents de sécurité sont-ils analysés et engendrent-ils un retour adéquat par l'organisation? Quels incidents de sécurité ont eu lieu? Comment ont-ils été gérés et quels dommages furent occasionnés?

• faisons-nous des rapports et comment?

• faisons-nous des analyses (comment et à quel niveau?)

• quel est le retour (dates-butoir, procédure de retour, responsabilités?)

• comment évaluons-nous le retour?

• la formation au sein de l'organisation est-elle basée sur les incidents (existe-t-il une formation? existe-t-il des canaux institutionnels pour cela?)

• en résumé, comment les incidents de sécurité sont-ils gérés?

• existe-t-il une procédure pour la collecte, l'enquête sur et l'analyse des incidents de sécurité servant à générer un retour et une base pour nos stratégies et plans?

• les conclusions sont-elles intégrées dans notre travail et nos évaluations (là où c'est nécessaire)?

• en cas d'urgence, existe-t-il des plans clairs et des attributions de responsabilités couvrant les réactions?

• à quel type d'urgences sont-ils applicables?

Des questions pour améliorer l'analyse des incidents de sécurité et les réactions:

Quels sont les problèmes pouvant survenir pour améliorer chacun des sujets énumérés plus haut?

Quelles pourraient être les solutions?

8 ● Evaluer la gestion de la sécurité et de la protection:

Des questions pour déterminer le niveau actuel de l'évaluation de la gestion de la sécurité et de la protection:

• dans quelle mesure l'organisation évalue-t-elle sa gestion de la sécurité et de la protection et dans quelle mesure cette dernière est-elle mise à jour?

• l'évaluation est-elle une activité institutionnalisée?

• sommes- nous conscients que le travail quotidien et les réactions face aux incidents de sécurité nécessitent une évaluation du point de vue de la sécurité pour que celles-ci contribuent à la connaissance et à l'expérience de chaque personne ainsi qu'à l'ensemble de l'organisation?

Des questions visant à améliorer l'évaluation de la gestion de la sécurité et de la protection?

Quels problèmes pourraient survenir en améliorant la gestion de la sécurité et de la protection?

Quelles pourraient être les solutions?

Comment les "autres" perÇoivent l'organisation

La sécurité et notre image

Il est important de considérer l'environnement de l'organisation pour voir comment son image est perçue et si elle correspond à l'image que l'organisation souhaite projeter. Il est également important de découvrir comment d'autres perçoivent la sécurité et la protection de l'organisation. Cette analyse devrait être faite selon les critères suivants:

- du point de vue des personnes avec lesquelles nous collaborons: les contreparties bénéficiaires.

- les collègues et des organisations similaires.
- les institutions contribuant de manière financière et les sponsors (certains peuvent être plus réceptifs que d'autres).
- les autorités avec lesquelles nous sommes en relation.
- d'autres acteurs qui pourraient être des agressseurs potentiels.
- ...

Il est également important d'établir quel niveau de coopération existe en matière de sécurité avec d'autres organisations ou réseaux, avec des homologues, avec les personnes avec lesquelles nous collaborons, etc.

Voici deux listes non-exhaustives avec des sujets utiles concernant ce sujet:

I ◆ L'image de l'organisation et l'impact du travail de celle-ci. Comment l'évaluer?

- Comment s'informer sur l'image de notre organisation?
- Comment parler de notre organisation à d'autres?
- Quel est le but de l'organisation?
- Quelles sont nos activités?
- Comment nos activités affectent-elles les acteurs armés ou d'autres acteurs?
- Quelles capacités ou quel pouvoir avons-nous de maintenir notre espace de travail en activité?
- Que faisons-nous pour le maintenir en activité?
- Comment pensons-nous que notre agresseur potentiel nous perçoit?
- Sommes-nous perçus comme une organisation qui gère bien les questions de protection et de sécurité liées au travail?
- Notre travail est-il observé? ou notre façon de le gérer du point de vue de la sécurité? Pourquoi? Comment pouvons-nous le dire?

II ◆ L'image de l'organisation et l'impact de son travail. Comment sommes-nous perçus?

Essayez de répondre aux questions suivantes envous mettant à la place de l'acteur personne "qui se renseigne" sur vous: (répétez l'exercice pour autant d'acteurs que vous estimez nécessaire: "ils" c'est vous et "nous" est la personne qui enquête).

- Qui sont-ils?
- À quoi s'attendent-ils?

- Quel est leur travail?
- Comment font-ils obstacle à notre travail? Quelles sont les limites de notre travail?
- Que pouvons-nous faire? Comment pouvons-nous nous protéger?
- Comment pouvons-nous obtenir ce que nous voulons?

Une fois que vous avez évalué la perception des autres, vous devrez considérer comment changer votre image si elle ne vous convient pas. Toutes les perceptions ne peuvent pas être changées, bien sûr. Mais il est utile d'en être conscient étant donné qu'elles peuvent avoir un impact sur votre sécurité et votre protection.

En résumé

Pour évaluer votre sécurité vous avez besoin d'une approche en deux temps:

une **auto-évaluation** (un regard sur vous-mêmes) et une évaluation de la manière dont les autres vous perçoivent.

C'est un état des lieux de votre niveau actuel de sécurité et de protection.

Elle permet de développer chaque rayon jusqu'à ce que la roue soit parfaitement ronde.

Pour développer votre roue de la sécurité, vous devez commencer par un inventaire de votre situation actuelle, puis déterminer des objectifs concernant les processus d'amélioration appropriés. Essayez d'anticiper de possibles obstacles tout en progressant vers vos objectifs. Essayez d'anticiper des solutions.

Une évaluation de la manière dont les autres vous perçoivent peut être réalisée en essayant d'imaginer comment ils pourraient parler de vous.

Bien sûr, il est également possible de poser la question à des personnes de confiance.

Vous devez trouver des moyens de changer une perception qui ne vous convient pas. Toutes les perceptions ne peuvent pas être changées, bien sûr. Mais il est utile d'en être conscient vu qu'elles peuvent avoir un impact sur votre sécurité et votre protection.

CHAPITRE 2.2

S'assurer du respect des règles et procédures de sécurité

Objectif:

Etablir pourquoi les membres et les organisations sont incapables ou réticents à respecter des plans et procédures de sécurité. Trouver ensuite les solutions appropriées.

La sécurité est l'affaire de tous

La question du respect effectif des procédures et règles de sécurité par les individus ou par l'organisation est complexe. Il est parfaitement possible d'avoir un bon plan de sécurité avec des règles de prévention et des procédures d'urgence; vous pouvez accorder la priorité à la sécurité lors des réunions importantes, etc., sans pour autant que les personnes appliquent les règles de sécurité de l'organisation.

Cela pourrait paraître incroyable étant donné que les défenseurs subissent constamment des pressions et des menaces. Mais cela arrive.

Si quelqu'un veut savoir quelque chose sur votre travail, il n'essayera pas d'obtenir des informations de la personne la plus prudente de votre organisation. Il ou elle tentera plutôt de se rapprocher d'une personne qui boit souvent le samedi soir. De même, si quelqu'un veut faire peur à votre organisation, il ou elle n'agressera probablement pas une personne qui a pris toutes les précautions nécessaires, mais visera quelqu'un qui néglige généralement sa propre sécurité. Dans la même logique, une personne prudente peut être attaquée parce que une personne négligente a laissé la porte ouverte… Car l'idée est aussi que la négligence d'une seule personne peut mettre tout le monde en danger.

C'est pourquoi la sécurité est une question affectant toute l'organisation, outre les personnes individuellement concernées. Si seules trois personnes sur 12 appliquent les règles de sécurité, l'organisation toute entière, y compris les membres qui les observent, est en danger. Si les choses s'améliorent et que neuf membres commencent à agir en fonction des procédures de sécurité, le risque est réduit. Cependant le risque serait bien moindre si l'ensemble des 12 personnes suivaient ces règles.

La sécurité est une responsabilité de toute l'organisation ainsi que des membres concernés.

Avoir un bon plan de sécurité ne sert à rien s'il n'est pas respecté. Soyons réalistes, beaucoup de personnes ignorent les règles et les procédures. Cette adhésion défaillante est le résultat de l'écart entre les bonnes intentions et la pratique. Il est malgré tout plus aisé de s'attaquer à ce problème qu'à ses possibles conséquences.

Pourquoi ne respecte-t-on pas les règles de sécurité? Comment pouvons-nous éviter cela dès le début?

Tout d'abord, le terme "conformité" évoque la soumission et la docilité et devrait donc être évité. Les personnes ne respectent que les règles qu'elles comprennent et acceptent parce qu'elles peuvent les faire leurs. Le maître mot est donc "l'appropriation".

Pour qu'une procédure de sécurité soit suivie, il faut que chacun au sein d'une organisation y adhère. Cela n'arrive pas du jour au lendemain. Pour que le personnel adhère à une procédure de sécurité il faudrait leur permettre de participer à son élaboration et à sa mise en oeuvre. La formation à la procédure, sa compréhension et son acceptation sont également cruciaux.

Tableau1:
La relation entre les individus et les organisations du point de vue de la sécurité

Idée générale	Démarche: "Chacun doit obéir aux règles!"	Démarche: "Les membres et l'organisation ont convenu des règles!"
Démarche	Orientée sur les règles	Basée sur les besoins de sécurité de l'organisation et des individus
Nature de la relation entre l'individu et l'organisation	Normative ou "paternaliste"	Fondée sur le dialogue
Pourquoi respectons-nous les règles?	Par obligation, pour éviter d'être sanctionné ou expulsé	Pour respecter un accord, qui peut être amendé et optimisé (parce que nous adhérons à l'objectif et au besoin de protéger nos collègues et les personnes avec et pour qui nous travaillons)
Responsabilité de la sécurité	Pas collective	Partagée

L'appropriation ne se borne pas au "respect des règles". Il s'agit bien plus que mettre en place un accord sur les règles qui encouragera les personnes à les appliquer parce qu'elles les comprennent, les jugent adéquates et efficaces et qu'elles y voient un enjeu personnel. Voilà pourquoi les règles devraient aussi correspondre aux valeurs morales et éthiques des individus et à leurs besoins fondamentaux.

S'approprier des règles n'est pas simplement leur "obéir" mais respecter un accord entre l'organisation et ses membres concernant la sécurité.

Afin de préserver l'accord entre l'organisation et les membres du personnel, il est important que les **responsables de la sécurité cultivent l'implication permanente des autres au moyen de briefings,** de rappels sur des aspects précis de l'accord, et en demandant aux autres leur avis sur l'efficacité et l'adéquation des règles dans la pratique.

Impliquer les membres ne vaudra pas beaucoup sans une **culture de la sécurité au sein de l'organisation** qui puisse étayer les procédures tant formelles qu'informelles et les programmes de travail.

Les conditions nécessaires pour que les personnes puissent observer les règles et les procédures de sécurité peuvent être créées en:

- Amenant les membres à comprendre que la sécurité est indispensable pour protéger les victimes, témoins, membres des familles et collègues et qu'elle détermine la poursuite des activités principales de l'organisation.
- En favorisant une culture de la sécurité à l'intérieur de l'organisation et en la valorisant.
- En permettant l'appropriation des règles et procédures de sécurité.
- En veillant à ce que tous les membres conçoivent et améliorent ensemble les règles et procédures de sécurité.
- En formant les personnes aux questions de sécurité.
- En vous assurant que tous les membres du personnel sont convaincus de l'adéquation et de l'efficacité des règles et procédures de sécurité.
- En établissant un accord entre les organisations et les individus sur le respect des règles et procédures de sécurité.
- En impliquant les responsables de la sécurité aux briefings et à la formation des membres. En rappelant les termes de l'accord aux membres et en leur demandant leur opinion sur la pertinence et l'efficacité pratique des règles et procédures de sécurité.

Pourquoi les règles et procédures de sécurité ne sont-elles pas suivies?

Le prototype du défenseur des droits humains ne suivant pas les règles et procédures de sécurité n'existe pas. Beaucoup de personnes au sein d'une organisation observent souvent certaines règles mais pas d'autres, ou bien n'observent les règles que sporadiquement.

Il y a beaucoup de raisons possibles qui poussent les personnes à ne pas suivre les règles et procédures de sécurité. Pour permettre le changement et garantir l'appropriation des règles, il est important d'établir les causes et de trouver les solutions avec les autres personnes concernées. Il sera aussi utile de distinguer les différentes raisons pour lesquelles les personnes ne suivent pas les règles, car elles sont très diverses.

Quelques raisons éventuelles du non-respect des règles et procédures de sécurité:

Involontaires:

- Le défenseur n'est pas conscient des règles.
- Il ou elle n'applique pas les règles correctement.

Délibérées:

Problèmes généraux:

- Les règles sont trop compliquées et difficiles à observer.
- Les procédures ne sont pas à portée de main dans un bureau ou sont présentées d'une manière qui les rend difficilement utilisables au quotidien.

Problèmes individuels:

- Les règles sont en conflit avec les besoins ou les intérêts du membre individuel et ce problème n'a pas été résolu.
- Le membre individuel n'est pas d'accord avec certaines ou toutes les règles et pense qu'elles sont inutiles, inappropriées et inefficaces, par son expérience personnelle, des informations ou une formation antérieure, ou bien en raison de ses convictions personnelles.

Problèmes de groupe:

- La majorité du personnel n'applique pas les règles, les "responsables" du groupe ne les respectent pas ou pas assez, parce qu'il n'y a pas de culture de sécurité au sein de leur organisation.
- Une motivation insuffisante au travail peut amener les membres à ignorer les règles de sécurité.

Problèmes liés à l'organisation:

- Il n'y a pas de ressources financières ou techniques suffisantes pour permettre au personnel de suivre les règles facilement.
- Les règles sont en conflit avec certains domaines d'activité. Par exemple, les règles ont été établies par les responsables de la sécurité mais sont ignorées ou appliquées incorrectement par les personnes travaillant dans les programmes ou à la comptabilité. Certaines règles peuvent être adaptées à un domaine de travail et être en conflit avec d'autres.

- Les membres ont une charge de travail importante, leur temps est limité, et ils ne donnent pas la priorité à certaines ou à toutes les règles.

- Un manque général de motivation, provenant d'un excès de stress, de différends entre collègues, etc.

La culture organisationnelle est à la fois formelle et informelle, et ne doit pas être développée seulement par l'organisation dans son ensemble, mais également au sein des équipes. Une bonne culture de l'organisation se caractérisera par des conversations informelles, des plaisanteries, des fêtes, etc.

Vérifier le respect des règles et des procédures de sécurité

Vérification directe:

Les règles et procédures de sécurité peuvent faire partie d'évaluations générales du travail et de "listes de contrôle", tout comme des réunions avant et après les missions de terrain, des rapports d'activité, des ordres du jour des réunions, etc.

Les équipes concernées peuvent mener des réexamens périodiques de questions comme celles de la conservation des informations sensibles, des copies et des manuels de sécurité, des protocoles de sécurité lors des visites au siège de l'organisation, et de la préparation des missions sur le terrain, etc.

Vérification indirecte:

Demander aux membres si les règles et procédures leur paraissent appropriées et faciles à suivre permettra de constater leur connaissance réelle des règles et s'ils les ont entièrement acceptées ou s'il y a un désaccord qu'il faut lever. L'utilisation de manuels de sécurité et des protocoles et règles en vigueur par le personnel peut également être vérifiée.

Il peut s'avérer très utile de rassembler et d'analyser les avis du personnel et leurs évaluations des règles et procédures de sécurité avec les personnes ou les équipes en question. Ceci peut être fait de manière confidentielle ou anonyme ou encore avec l'aide d'un tiers.

La vérification a posteriori:

Analyser les incidents de sécurité lorsqu'ils se présentent peut être l'occasion de faire un bilan de sécurité. Cela doit être géré avec beaucoup de doigté. Une personne ayant vécu un incident de sécurité peut s'inquiéter d'en être la cause et craindre des sanctions à l'issue de l'analyse. Elle souhaitera peut-être occulter l'incident en taisant l'ensemble ou une partie des faits.

Qui effectue la vérification?

Suivant le fonctionnement interne de l'organisation, quiconque est responsable d'organiser la sécurité, les domaines spécifiques à l'intérieur de la sécurité et des autres responsables de la sécurité, sera aussi chargé de vérifier la sécurité.

Que faire si les règles et procédures de sécurité ne sont pas observées?

1 ◆ Définissez les causes, trouvez des solutions et mettez-les en pratique. La liste des options du tableau 1 ci-dessus peut vous orienter.

2 ◆ S'il s'agit d'un comportement délibéré ne concernant qu'une seule personne, essayez de:

a • lancer un dialogue avec cette personne pour découvrir les ou la cause(s) ou sa motivation.

b • collaborer avec toute l'équipe de l'individu (ceci peut parfois être inadéquat, suivant le cas).

c • mettre en place un système de notification ou d'avertissement pour que la personne soit pleinement consciente du problème.

d • utiliser une échelle progressive de sanctions dont la plus grave pourrait être le licenciement/l'exclusion.

3 ◆ Incluez une clause de respect des règles et des procédures de sécurité dans tous les contrats de travail afin que l'ensemble du personnel soit pleinement conscient de l'importance réelle de la sécurité pour l'organisation.

En conclusion,

Certains estimeront peut-être qu'examiner les raisons pour lesquelles les personnes n'appliquent pas les règles de sécurité est une perte de temps, et qu'il y a d'autres choses plus urgentes ou prioritaires à faire. Ces mêmes personnes sont normalement d'avis que les règles existent pour être observées, un point c'est tout! Les autres sont conscients que ce n'est pas toujours comme cela que le monde fonctionne.

Quelle que soit votre opinion, nous vous invitons maintenant à prendre du recul et à analyser le respect des règles et procédures de sécurité au sein de votre ou de vos organisations. Les résultats pourraient être surprenants et mériter qu'on s'y arrête un instant pour éviter des problèmes plus tard...

En résumé

La sécurité est l'affaire de tous.

La sécurité est un sujet qui touche l'ensemble de l'organisation ainsi que les individus concernés.

Il faut déterminer pour quelles raisons les personnes ne se conforment pas aux règles de sécurité. Ces raisons peuvent être:

involontaires
(un problème individuel).

intentionnelles
(générales,
individuelles,
de groupe,
problèmes organisationnels).

En apprenant à connaître ces raisons on trouvera les moyens appropriés de les gérer.

Il est cependant recommandé d'assurer la supervision et le suivi par un organe spécifiquement désigné à cette tâche.
(La supervision peut-être directe, indirecte et rétrospective).

Le développement d'une culture de la sécurité dans l'organisation est d'une importance fondamentale.

Gérer le changement organisationnel vers une politique de sécurité améliorée

Objectif:

Apprendre à gérer un changement organisationnel vers une politique de sécurité améliorée.

Étapes et problèmes autour desquels ce processus s'articule:

- Améliorer la gestion de la stratégie de sécurité
- Améliorer le processus de mise en oeuvre de la gestion de la sécurité
- Quel est le point d'entrée? Quel organe en est responsable? Quel est le point de départ? Comment faire? Qu'en est-il de la mise en oeuvre? Quels sont les pour et contre? Quels sont les obstacles?

Gérer les défis que pose la sécurité: une gestion de la sécurité pas à pas

La gestion de la sécurité ne s'arrête jamais et est toujours pragmatique, partielle et sélective. Les raisons en sont:

- Il y a des limites au volume d'information que vous pouvez gérer - tous les facteurs influant sur la sécurité ne se laissent pas regrouper et traiter simultanément.

- C'est un processus complexe - du temps et des efforts sont nécessaires pour faire prendre conscience du problème, développer le consensus, former les défenseurs, gérer la fluctuation du personnel, mettre en oeuvre des activités, etc.

La gestion de la sécurité ne permet que rarement une vue d'ensemble intégrée et à long terme. Sa contribution réside dans la capacité à prévenir les attaques et à mettre en évidence le besoin de stratégies organisationnelles pour y faire face. Cela n'est peut-être pas très ambitieux, mais nous ne devons pas oublier que souvent notre attribution de ressources à la sécurité est insuffisante!

En examinant les pratiques de sécurité d'un défenseur ou d'une organisation, vous trouverez sans doute, en vigueur, quelques lignes de conduite, des plans, des mesures ou des modes de comportement. Des tensions risquent d'être

provoquées allant d'idées stéréotypées quant aux pratiques de sécurité jusqu'à la réticence à augmenter les charges de travail existantes en intégrant de nouvelles activités de sécurité.

Les pratiques de sécurité sont par nature un travail fragmentaire et sont soumises à une évolution intuitive. La gestion de la sécurité devrait avoir pour objectif de réaliser des changements pas à pas pour améliorer la performance. Les règles et procédures de sécurité ont tendance à provenir des parties de l'organisation couvrant des domaines de travail spécifiques, comme la logistique, une équipe de terrain particulièrement préoccupée par sa sécurité, ou bien un directeur mis sous pression par les donateurs inquiets de la sécurité, etc.

La gestion de la sécurité pas à pas ouvre la porte à des processus informels et crée un espace pour que de nouvelles pratiques puissent prendre racine. Des événements soudains tels que des incidents de sécurité provoqueront des décisions à court terme prises dans l'urgence, qui, si elles sont bien gérées façonneront des pratiques de sécurité à long terme pour toute l'organisation.

Amélioration de la stratégie de sécurité: les points d'entrée possibles

Une fois que le besoin d'améliorer la sécurité a été établi, il faut le promouvoir. Il existe plusieurs points d'entrée pour cela (soit à l'intérieur, soit à l´extérieur de l'organisation):

À l'intérieur de l'organisation:

- la direction, le comité directeur ou les dirigeants
- le niveau intermédiare /exécutif
- le personnel et la majorité des collaborateurs
- une combinaison des possibilités citées

À l'extérieur de l'organisation:

- les donateurs
- les partenaires et homologues
- des organisations similaires travaillant dans le même réseau

Comparons leurs avantages et inconvénients

Possibles points d'entrée pour promouvoir le besoin de changements?	Avantages	Inconvénients	Solutions Possibles
Points d'entrée à l'intérieur de l'organisation			
Direction, comité directeur ou dirigeants	• peuvent convoquer des réunions ou des assemblées générales • disposent de la mémoire historique • autorité morale • soutien institutionnel • ...	• perçus comme 'imposant la sécurité' et peuvent contribuer à l'indifférence • peuvent la rendre trop formelle, rigide, distante, peuvent être condescendants • voient la sécurité comme n'affectant qu'eux-mêmes • nient l'importance de la sécurité et ne lui accordent pas la priorité • ...	• Réunions ou assemblées générales • ...
Niveau intermédiaire / exécutif	• une vision des échelons supérieurs et inférieurs • facilité d'accès aux deux autres niveaux • canal de communication convivial entre les deux échelons • communication • capacités techniques pour mettre en oeuvre les changements de sécurité • ...	• souvent ce niveau n'existe pas • attention partielle: sur un aspect ou un domaine seulement • distrait par les motivations personnelles de carrière • "trop" technique si pas engagé dans des activités politiques ou de terrain • ...	• Des procédures d'implication (à la fois envers les directeurs et les membres en général). • ...
Personnel et majorité des collaborateurs, ...	• peuvent mobiliser des gens • sont conscients des mécanismes et des détails du travail quotidien • ...	• peuvent avoir des problèmes avec les cadres dirigeants ou la hiérarchie • ...	• En général, en tant que groupe, reconnaitre le problème, le besoin de l'apport de chacun et le besoin de solutions. Ensuite, déléguer la recherche de la solution à un groupe de travail • ...
Points d'entrée à l'extérieur de l'oragnisation			
Donateurs, organisations mères, ...	• plus de distance • pas d'intérêts directs • peut avoir une plus large expérience • peut convoquer des réunions avec l'ensemble des échelons cités plus haut sans conflit d'intérêts • ...	• risque d'avoir des problèmes de crédibilité ou peu de connaissances du travail effectué • l'approche peut être trop technique et approche technique • ...	• Indiquez les intérêts communs en matière de sécurité • Les organisations donatrices préfèrent investir dans une organisation s'occupant de la sécurité plutôt que de risquer de perdre leur investissement dans une organisation négligeant la sécurité • La sécurité inter-organisationnelle dépend des attitudes et règles de sécurité communes • ...

Le processus d'entrée peut être mis en oeuvre par toutes les organisations, indépendamment de leur taille, stabilité ou emplacement.

Quel est l'organe responsable de l'amélioration du processus?

Maintenant que l'entrée a été obtenue (promotion et reconnaissance du besoin), une partie de l'organisation doit prendre en charge ce processus. Quel organe sera responsable du processus d'amélioration de la sécurité? Il y a plusieurs possibilités:

- des membres ad hoc de l'organisation (ils font partie de l'organisation et sont choisis par elle. Ils ont en général d'autres responsabilités). Il peut également s'agir d'un groupe de travail (composé de personnes de domaines divers).
- une personne interne et externe: une personne partiellement impliquée dans le travail et qui collabore étroitement et de façon continue avec les membres de l'organisation (par exemple une personne ayant travaillé pour l'organisation).
- un consultant ou un conseiller: il collabore avec le responsable ad hoc de la sécurité ou avec le groupe de travail (une collaboration à court-terme).

Examinons les avantages et les inconvénients de ces différentes approches

Organe responsable pour le processus d'amélioration	Avantages	Inconvénients	Solutions Possibles
Responsable ad hoc de l'institution	• information centralisée • accès facile à l'information • clarté en termes de responsabilité • prise de décision facile • moins de personnes impliquées • choisi pour ses compétences • ...	• surcharge de travail • engagement collectif moindre • dépendance excessive d'une personne • possible manque de retour concernant les plans et idées. • ...	• distinction entre promotion/coordination et mise en oeuvre • réduction temporaire de la charge de travail pour permettre de se concentrer sur la sécurité • soutien personnel • circulation constante de stratégies pour permettre un retour progressif • ...
Groupe de travail	• partage et approche intégrée du travail en matière de sécurité • expérience large et diversifiée • plus de ressources humaines • distribution des responsabilités: plus de clarté en termes d'initiative et de clarté • plus grande probabilité que les protocoles soient respectés.	• surcharge de travail • lente élaboration d'un consensus lors de la prise de décisions • circulation de l'information moins fluide • plus grand nombre de personnes à être formées à la tâche • ...	• distribution adéquate des compétences et responsabilités • implication de l'échelon de direction • alternance, formation et engagement concernant la circulation proactive du résultat du travail en cours afin d'obtenir un retour et de partager le processus • ...

Une personne interne et externe	• une plus grande objectivité de l'évaluation du risque • une personne compétente, ayant la confiance de l'organisation • engagement total • réceptivité éprouvée • conscience des forces et faiblesses • ...	• discontinuité • peut affaiblir l'engagement du groupe • peut saper l'appropriation légitime du processus entier et du sujet • ...	• formation d'un ou deux membres de l'équipe • circulation continue du résultat du travail en cours et retour de l'ensemble de l'équipe • élaboration d'un consensus et accords • ...
Consultant ou conseiller	• peut former l'équipe • consultation spécialisée • clarté dans le contrôle du processus • conseil reconnu • suivi actif • moins influencé par les questions d'organisation interne • ...	• peut générer une dépendance plutôt que des compétences • peut être vu comme "le préposé à ces tâches" plutôt que comme "la personne qui facilite le travail" • peut saper la confiance nécessaire au sein de l'organisation • augmentation des coûts • les consultants dans ce domaine sont rares • difficultés d'organiser l'emploi du temps • peut avoir des connaissances insuffisantes du contexte • peut produire un plan et des règles inadaptées au contexte de travail • ...	• clarifier autant que possible avec l'ensemble des personnes concernées: expliquer le rôle du consultant et l'étendue de son travail • augmenter le profil de la sécurité avec d'autres organisations en vue de partager les informations et d'y accéder • donner des formations de sécurité aux formateurs dans les organisations et les institutions (facilitateurs) • briefing sur le contexte du travail • ...

Quel est le point de départ du processus?

Maintenant que l'entrée a été effectuée et que l'organe responsable a été déterminé, quel peut être le point de départ de ce dernier?

Le point de départ devrait être l'évaluation du processus de mise en oeuvre de la politique de sécurité de l'organisation entière. En partant de l'évaluation (ou du diagnostic) on déterminera les priorités et les solutions possibles (les meilleures pratiques en accord avec les besoins déclarés, le profil de l'organisation et son mandat). Un plan sera ensuite mis au point visant à structurer le processus d'amélioration. Le plan comprendra des étapes intermédiaires pour contrôler si et comment la progression se fait. De plus, le plan clarifiera le rôle et les responsabilités de chacun, à la fois des personnes chargées du processus et des membres de l'organisation. Le plan comportera également un calendrier. A la fin du processus tel qu'il est prévu, on évaluera la réalisation des objectifs.

Diagnostic ⇨ priorités ⇨ solutions possibles
⇨ plan d'amélioration ⇨ évaluation

Une fois les priorités déterminées, la décision quant à l'ordre de leur mise en oeuvre peut être plus facile si des critères sont établis: une situation d'urgence, les ressources actuellement disponibles, etc.

La flexibilité est un facteur essentiel pendant tout le processus. Cependant, quel sera le minimum nécessaire pour que ce processus d'amélioration ait une véritable chance d'atteindre des résultats positifs? Répondre à cette question avant le début du processus est crucial.

Diagnostic et plan d'amélioration

Le diagnostic peut être effectué en utilisant les outils "évaluation du risque" et "roue de la sécurité" décrits dans les précédents chapitres de ce manuel (toute autre méthode de révision organisationnelle aussi).

Il va de soi que cette étape devrait inclure toutes les personnes et équipes concernées au sein de l'organisation.

Le plan d'amélioration doit être **réaliste** et **adapté** au profil et aux besoins de l'organisation. Voici une proposition de marche à suivre:

1 ◆ Identifiez les attentes de l'organisation et les résultats escomptés du plan d'amélioration de la sécurité.

2 ◆ Diagnostiquez ensemble: obtenez un consensus et partagez les idées concernant la structure actuelle de la gestion de la sécurité (appliquez l' "évaluation du risque" et la "roue de la sécurité"). Notez les progrès, manques et besoins.

3 ◆ Indiquez les meilleures pratiques à mettre en oeuvre pour s'attaquer aux manques et besoins relevés et discutez-en.

4 ◆ Indiquez les objectifs souhaitables et souhaités du plan d'amélioration.

5 ◆ Esquissez les activités requises pour atteindre ces objectifs et ce à quoi on peut raisonnablement s'attendre pour chaque activité (cela permettra de progresser vers les objectifs).

6 ◆ Esquissez les ressources nécessaires (financières, humaines, en temps, techniques). Déterminez les responsabilités et le calendrier.

7 ◆ Définissez les risques découlant de l'atteinte de ces objectifs et des conséquences.

8 ◆ Définissez les indicateurs pour surveiller la progression et les résultats finaux.

9 ◆ Partagez le plan avec toutes les parties concernées afin d'obtenir un retour, de l'améliorer et de générer l'assentiment nécessaire à sa mise en oeuvre.

10 ◆ Mettez en oeuvre le plan et élaborez un calendrier pour surveiller la progression et pouvoir modifier le processus en cours de route.

Le processus: la mise en oeuvre du plan d'amélioration

Le processus comprend une série de réunions et d'interviews avec les personnes et équipes travaillant au sein de l'organisation ou en contact avec celle-ci (dans ce cas, il doit il y avoir un accord préalable de l'organisation, indiquant les personnes et/ou organisations avec lesquelles la sécurité peut être discutée). L'échange peut commencer par une réunion générale d'introduction, qui pourra être suivie d'autres réunions. Celles-ci constitueront l'espace dans lequel on définira les diagnostics et où on discutera de la mise en oeuvre du plan d'amélioration. De plus, les réunions pourront s'attaquer à des points précis ou bien accompagner le travail spécifique de l'organisation du point de vue de la sécurité et de la protection.

Résistance au plan d'amélioration

Maintenant que l'entrée a été effectuée, qu'un organe responsable a été nommé et que les point de départ et le plan du processus ont été déterminés, quelle résistance pourrait surgir de la part des personnes concernées?

Comme tous les processus conduisant à des changements dans une organisation, le plan d'amélioration peut provoquer des résistances. Il trouvera cependant également soutien et approbation. L'idée est donc de voir de quelle façon saisir ce soutien et de quelle façon argumenter contre une possible résistance.

La façon la plus appropriée de saper la résistance est d'être réellement à l'écoute et d'essayer de comprendre le raisonnement sous-jacent. Ici une fois de plus, la participation, l'écoute active de tous les points de vue et attentes est cruciale pour un bon processus.

Il est essentiel que le plan d'amélioration fournisse les moyens de s'attaquer à la résistance possible pour éviter une improvisation ultérieure, courant ainsi le risque de voir le plan échouer simplement à cause d'un déni préalable de la résistance possible.

Ce tableau décrit certains stéréotypes de résistance courants, le raisonnement qui se cache derrière ces stéréotypes et des réponses possibles pour surmonter ces forces de résistance.

Stéréotypes de résistance courants	Raisonnement se cachant derrière ces stéréotypes	Réponses pour surmonter la résistance
"Nous ne sommes pas menacés" ou "notre travail n'est pas aussi exposé ou sujet à controverse que le travail d'autres organisations".	• Le risque reste le même, il ne change pas ou ne dépend pas du fait que le contexte de travail puisse se détériorer ou que le scénario puisse changer.	• Le risque dépend du contexte politique, et le contexte politique est dynamique: tout autant que le risque.

"Le risque est inhérent à notre travail de défenseurs" et "nous sommes déjà conscients de ce à quoi nous sommes exposés."	• Les défenseurs acceptent le risque et il ne les affecte pas dans leur travail. • Ou, le risque ne peut être réduit, il est là, un point c'est tout.	• S'exposer au risque ne signifie pas l'accepter. • Le risque a pour le moins un impact psychologique sur notre travail: il produit au minimum du stress affectant le travail. • Le risque se compose d'éléments objectifs: les menaces, les vulnérabilités et les capacités: les vulnérabilités et capacités appartiennent aux défenseurs et sont des variables sur lesquelles les défenseurs peuvent influer. En réduisant les vulnérabilités et en augmentant les capacités, le risque peut être réduit. Il peut ne pas être totalement éliminé, ce qui ne signifie pas qu'il ne peut être réduit autant que possible.
"Nous savons déjà comment gérer le risque", ou "nous savons faire attention à nous" et "nous avons beaucoup d'expérience".	• La gestion actuelle de la sécurité ne peut être améliorée et ce n'est donc pas la peine d'essayer de le faire. • Le fait que nous n'ayons pas été victimes d'attaques par le passé garantit que nous ne le serons pas à l'avenir.	• La gestion de la sécurité est basée sur des éléments objectifs sur lesquels on peut exercer une influence. • Regardez autour de vous et voyez combien de défenseurs ont subi des violences bien qu'ils étaient très expérimentés.
"Oui, le sujet est intéressant, mais il y a d'autres priorités."	• Il y a des sujets plus importants que la sécurité des défenseurs.	• La vie, c'est la priorité. Si nous la perdons, nous ne pourrons gérer toutes les autres priorités.
"Et comment allons nous financer tout ça?"	• La sécurité est coûteuse et elle ne peut être inclue dans des propositions de recherche de fonds.	• Combien croyez-vous coûte la sécurité? Nombreux facteurs de sécurité sont de l'ordre du comportement et ne coûtent rien. • Les investisseurs préféreront investir dans une organisation gérant la sécurité plutôt que de courir le risque de perdre leur investissement.
"Si nous faisons tellement attention à la sécurité nous ne pourrons pas faire ce qui est réellement important, à savoir travailler avec les gens. Nous le leur devons."	• Le fait que nous soyons affectés par des problèmes de sécurité n'affecte pas les personnes avec lesquelles nous travaillons. La qualité de notre travail pour les gens ne dépend pas du fait de se sentir plus en sécurité.	• La sécurité est une question de vie ou de mort. • Parce que nous le devons aux gens, nous ne pouvons courir le risque de perdre notre vie. • Les gens courent des risques en nous confiant leurs cas et si nous ne nous attaquons pas à notre sécurité cela les affectera en retour; ils pourront choisir une autre organisation qui gèrera sa sécurité de façon adéquate et offrira ainsi plus de sécurité aux gens.
"Nous n'avons pas le temps, nous sommes déjà surchargés."	• Il est impossible de trouver du temps dans notre horaire.	• Combien de temps croyez-vous prend la sécurité? • Combien de temps passons-nous à réagir à des urgences plutôt qu'à la prévention? (probablement plus de temps que nécessite l'intégration de la sécurité dans notre travail).

"La communauté nous soutient: qui osera jamais s'attaquer à nous?"	• Nous faisons partie de la communauté. La communauté n'est pas fragmentée, ne change ni de membres ni d'opinion. • La communauté ne peut être influencée.	• La communauté n'est pas homogène et elle est également composée de ceux qui peuvent être affectés par notre travail.
"Dans notre village, les autorités se sont montrées compréhensives et ont collaboré."	• Les autorités locales ne sont pas affectées par notre travail de droits humains et ne changeront pas d'opinion. • Il n'y a pas de hiérarchie entre les autorités locales et nationales.	• La mémoire historique de l'organisation inclura des exemples d'autorités locales opposant le travail de droits humains lorsque leurs seuils de tolérance auront été franchis. • Les autorités locales doivent mettre en œuvre des ordres venant de leur hiérarchie. • Les autorités sont composées de personnes pouvant avoir un intérêt à protéger des agresseurs. • Les contextes politiques changent.

Maintenant que l'entrée a été effectuée, qu'un organe responsable a été nommé et que les points de départ et le plan du processus ont été déterminés, quels facteurs organisationnels pourraient entraver ou faciliter le changement?

Les facteurs organisationnels pouvant soit faciliter soit entraver les changements au sein de l'organisation en vue d'une meilleure politique de sécurité.

Au sein de l'organisation	Facteurs entravant le changement	Facteurs facilitant le changement
Culture de l'organisation	• Superficialité. Improvisation. Concentration sur l'individu. • Une sécurité non intégrée •...	• Le travail en équipe, la conscience des effets du travail, l'écoute active, la consultation, les procédures de prise décision consensuelles. • L'intégration de la sécurité •...
Attitude de la direction	• Autoritaire et dictatoriale. Orientée sur les résultats. Distante. Importance accordée uniquement aux dirigeants et par conséquent, encline à établir et à respecter des règles répondant uniquement à ses besoins. • L'attente non réciproque que les autres membres sont là pour servir l'organisation. • S'octroyant des privilèges •...	• En contact avec tous les membres. • Reconnaissance de l'importance de la contribution de tous dans la poursuite des objectifs de l'organisation. • Une attention portée aux inquiétudes de l'ensemble du personnel à tous les échelons. • Ouverture. • Respect des règles •...
Structure de l'organisation	• Rigide. • Compartimentée. • Mal adaptée au travai •...	• Une flexibilité adéquate. • Fluidité de la coordination et de la communication entre les échelons. • Reflétant les besoins des personnes et du travail •...

Connaissance des problèmes de sécurité	• Centralisation. Partialité. Une conscience très réduite des problèmes de sécurité sur le terrain. • Absence d'objectivité, connaissance des dossiers et problèmes très peu étoffée •...	• Partage de l'expérience et de la connaissance. Inclusivité. Faits attestés. • Compilation systématique de l'information et mises à jour régulières. •...
Manque de stabilité de l'organisation; lassitude aux changements.	• Renouvellement du personnel. • Absence de mémoire historique. • Tension due à des changements permanents. Absence de continuité dans le travail •...	• Description précise du travail et contrat avec l'organisation attestant l'engagement de notifier de façon adéquate les départs et de transmettre le savoir et les compétences avant le départ. • Des évaluations régulières. • Affectation à des tâches correspondant à la durée pour laquelle le personnel s'est engagé à rester. Introduction et formation.
Surcharge de travail	• Ressources humaines insuffisantes ou inadéquates. Stress. Objectifs progressivement perdus de vue •...	• Établir des priorités et redistribuer du travail. • Un espace pour décompresser. •…
Planification du travail	• La sécurité n'est pas clairement prioritaire. • La sécurité n'est pas prise en compte dans la planification du travail. • La planification du travail est spontanée et ne correspond pas aux objectifs ni au but •...	• Une planification de la sécurité correspondant au travail. La sécurité est intégrée à la planification du travail. • Une attention adéquate est donnée à des activités pour lesquelles la sécurité est vue comme étant insuffisante et les décisions s'ensuivant sont prises pour déterminer si oui ou non elles doivent être réalisées si les conditions de sécurité ne sont pas réunies •...

Les facteurs n'influençant pas spécifiquement le changement de l'organisation afin d'améliorer la politique de sécurité:

- Taille de l'organisation
- Le fait que des personnes responsables pour la sécurité disposent ou non d'une éducation supérieure
- Religion
- Genre
- ...

Normes ou bonnes pratiques de la gestion de la sécurité et de la protection

Maintenant que l'entrée a été effectuée, qu'un organe responsable a été nommé et que les points de départ et le plan du processus ont été déterminés, que la résistance individuelle a été démantelée, que les facteurs organisationnels entravant et facilitant les changements ont étés pris en compte, quelles sont les meilleures pratiques en matière de gestion de la sécurité et de la protection sachant qu'elles dépendent des modèles structurelles de l'organisation?

Il y a différentes options pour gérer la sécurité au sein d'une organisation et il peut être difficile de faire le meilleur choix. Dans le prochain tableau nous allons voir trois modèles, leurs avantages et inconvénients ainsi que quelques solutions.

Modèles structurels	Où est-ce que les décisions de sécurité sont prises	Avantages	Inconvénients	Solutions Possibles
Modèle centralisé	• À l'échelon de la direction, au sein d'un organe spécifique.	• Plus facile de vérifier si l'expérience et le savoir adéquats existent au sein de l'organisation •…	• Surcharge de travail pouvant entraver l'aptitude à prendre les bonnes décisions. • Peut être déconnecté du travail dans certains domaines. •…	• Une personne à l'échelon de la direction investi du pouvoir de décision agissant au nom de la direction. • Un responsable de la sécurité est nommé à l'échelon de la direction mais sans pouvoir de décision. •…
Modèle intermédiaire	• Décisions importantes et globales: à l'échelon de la direction. Décisions spécifiques: prises par les personnes responsables dans chaque domaine concerné.	• La direction n'est pas surchargée. • Combinaison des compétences et d'un niveau adéquat. Plus proche du travail en cours dans tous les domaines. •...	• Des conflits au sujet de la sécurité peuvent naître entre la direction et les différents domaines. •…	• Chaque personne responsable pour un domaine spécifique prend la responsabilité pour la sécurité dans ce domaine. Un consultant en sécurité peut être nommé pour l'organisation entière: une personne liée à un domaine particulier, par exemple l'administration ou la logistique, prend en charge la sécurité et interagit avec les personnes responsables des différents domaines. •…
Modèle décentralisé	• Les décisions de sécurité sont prises à tous les échelons parce que chaque personne en est explicitement responsable.	• Meilleur respect, contribution à la culture de l'organisation concernée par la sécurité. •...	• Les discussions peuvent être plus longues. • Peut s'appliquer principalement à des petites organisations. •…	• Il peut exister ou non des personnes s'occupant uniquement de la sécurité. • Chaque personne peut avoir cette responsabilité dans la description de son poste ou dans son travail précédent. •…

Formation du personnel / des membres

Maintenant que l'entrée a été effectuée, qu'un organe responsable a été nommé et que les point de départ et plan du processus ont été déterminés, que la résistance individuelle a été démantelée, que les facteurs organisationnels entravant et facilitant les changements ont étés pris en compte, que les normes de sécurité et de protection ou les meilleures pratiques ont été déterminées, qu'en est-il de la formation du personnel?

La formation peut être faite avec les ressources internes à l'organisation (il peut y avoir des personnes compétentes en matière de formation de sécurité). La formation peut être également faite en collaboration avec d'autres organisations (envoyer des personnes à des séminaires de formation avec des personnes venant d'autres organisations). Si c'est le cas, développer ses capacités en commun avec d'autres organisations peut faciliter les échanges d'informations de sécurité ultérieurs et même la mise en place de réseaux visant à améliorer la protection. La confiance entre les organisations participant à la formation de sécurité est une condition nécessaire. De plus, il est utile que les organisations partagent les mêmes intérêts et aient des domaines de travail et des environnements similaires: les organisations situées dans des zones rurales et urbaines ont par exemple des besoins de sécurité très différents.

La formation peut être mise en œuvre de nombreuses façons. On peut soutenir que les plus courants sont:

- des ateliers (de préférence en petits groupes de 10 à 15 personnes).
- une formation individuelle (utile pour des tâches complexes ou des responsabilités spécifiques, avec des formations sur le tas).
- des entretiens ou des réunions semi-formelles (orientation, conseils actifs).

Il est recommandé de réaliser au moins une partie des formations à l'extérieur de l'environnement de travail afin de faciliter la concentration et éviter la tension du travail quotidien. Cependant, il est souvent contre-productif de mener ces activités après les heures de travail (par exemple pendant les week-ends), car cela pourrait envoyer un faux signal, c'est-à-dire que la sécurité signifie plus de travail - particulièrement des heures supplémentaires - et qu'elle n'est pas suffisamment importante pour être incluse dans le programme de travail habituel.

Comment améliorer le respect des règles de sécurité

Maintenant que l'entrée a été effectuée, qu'un organe responsable a été nommé et que le point de départ et le plan du processus ont été déterminés, que la résistance individuelle a été démantelée, que les facteurs organisationnels entravant et facilitant les changements ont étés pris en compte, que les normes de sécurité et de protection ou les meilleures pratiques ont été déterminées, que le personnel est formé, comment le respect des règles de sécurité peut-il être amélioré?

Les conditions nécessaires au respect des plans et règles de sécurité sont atteintes par les étapes suivantes:

- L'existence et le développement d'une culture de la sécurité dans l'organisation.

- L'appropriation des plans et règles de sécurité.
La participation à leur conception et au processus d'amélioration.
Une formation pour les clarifier et les comprendre.
Convaincre à la fois de leur adéquation et de leur efficacité.

- Élaborer un accord entre l'individu et l'organisation concernant la conformité aux plans et règles de sécurité.

- Des interventions régulières par les personnes responsables de la sécurité ou des objectifs d'information et de formation, rappelant les personnes à leurs engagements réciproques et réunissant les opinions des personnes concernant l'adéquation et l'efficacité des règles.

Que peut-on faire en cas de non conformité aux plans et règles de sécurité?

I ● Découvrez et résolvez les causes de la non conformité (voir le chapitre 2.2.)

II ● Si la cause de la non conformité est intentionnelle et dépend simplement de la volonté d'une personne, les mesures suivantes peuvent être prises:

a • Parler à la personne (comme point culminant d'un processus préalable visant à résoudre les causes de la non conformité) afin de générer une motivation et un engagement.

b • Abordez le sujet avec l'équipe concernée en présence de la personne concernée (cette mesure peut parfois ne pas être adéquate, selon la situation).

c • Mettez en place un système d'avertissement (entre deux et trois avertissements).

d • Appliquez un système de sanctions graduelles pouvant aller jusqu'au licenciement de la personne.

Il est important d'inclure dans l'accord une clause faisant référence à la conformité aux plans et règles de sécurité, afin que tous les défenseurs soient pleinement conscients de l'importance que l'organisation attribue à la sécurité.

En résumé

Avoir un plan de sécurité ne signifie pas qu'il soit mis en œuvre et respecté. Un processus approprié doit être conçu pour gérer la mise en œuvre, sa conformité et son amélioration. Plus le processus sera intégrateur, plus il sera facile de réunir des informations concernant les besoins de sécurité et plus l'appropriation du processus sera facile.

Il n'y a pas de structure d'une organisation bonne ou mauvaise en soi: chacune a ses avantages et ses inconvénients. Il est donc utile de les analyser pour élaborer un processus approprié et lui donner autant de chances de réussir que possible.

Le plan d'amélioration doit être **réaliste** et **adapté** au profil et aux besoins de l'organisation.

Voici les étapes successives du processus conduisant à une meilleure politique de sécurité:

- il faut admettre la sécurité
- un organe responsable doit être nommé
- l'organe responsable doit trouver le point de départ et planifier le processus
- la résistance individuelle doit être démantelée par une écoute active pour découvrir la logique de la résistance des individus afin de formuler un contre-argument approprié (il n'est pas suffisant de simplement opposer un autre point de vue au stéréotype de résistance car le facteur déterminant est la logique du stéréotype: si le raisonnement de l'individu résistant est juste, sa résistance l'est aussi).
- Les facteurs organisationnels entravant et facilitant le changement doivent être pris en compte
- les normes de sécurité et de protection ou les meilleurs pratiques doivent être définies
- le personnel / les membres doivent être formés
- la conformité aux règles de sécurité doit être améliorée.

TROISIÈME PARTIE

PROTOCOLES, PLANS D'URGENCE ET DAVANTAGE DE POLITIQUES

INTRODUCTION:

Dans la troisième partie de ce manuel nous proposons, à titre d'exemple, quelques protocoles et plans d'urgence pour une utilisation dans des situations spécifiques.

Ils sont basés sur les bonnes pratiques partagées et apprises dans les ateliers que nous animons.

Ils ne sont cependant ni complets, ni une garantie de bons résultats, étant donné que le manuel ne peut reproduire toutes les variables d'un contexte donné.

Ceci est véritablement un travail en cours, et c'est volontiers que nous accueillons votre opinion, ainsi que de nouvelles propositions pour des protocoles et plans.

Nous publierons des mises à jour et des développements sur le site Internet **www.protectionline.org**, pour que les défenseurs puissent en bénéficier aussi vite que possible, et nous inclurons tous les développements dans la prochaine édition de ce manuel. Entretemps, vous pouvez vous référez à l'Annexe IV - Esquisse globale des risques par profil spécifique de défenseur de droits humains.

CONTENU DE LA TROISIÈME PARTIE:

3.1 Comment réduire les risques liés à la perquisition et / ou le cambriolage d'un bureau

3.2 Détention, arrestation, enlèvement et capture d'un défenseur La sécurité et la gestion de l'information

3.3 La sécurité et la gestion de l'information

3.4 La sécurité et le temps libre

CHAPITRE 3.1

Comment réduire les risques liés à la perquisition et / ou au cambriolage d'un bureau

Une perquisition peut être définie comme l'entrée par effraction dans une maison, un bureau ou un espace privé. Une perquisition est légale si c'est l'État la décide et la met en oeuvre conformément aux lois en vigueur. Une perquisition est illégale lorsque l'entrée de force est contraire à la loi (par exemple un cambriolage de nuit, une fouille faite par des forces de sécurité sans le mandat de perquisition correspondant ou une fouille de force à laquelle procède un acteur armé).

Bien que nous traiterons surtout de la perquisition légale, les défenseurs pourront extraire des règles applicables aussi aux perquisitions illégales et de les compléter par l'information contenue dans le chapitre sur la sécurité au travail et au domicile.

L'État est en droit de procéder à des perquisitions légales. La loi en vigueur devra correspondre aux normes internationales relatives aux droits humains et à la protection des libertés démocratiques. Cependant, des perquisitions utilisées comme méthode de harcèlement continu, suivies ou accompagnées de poursuites en justice des défenseurs des droits humains peuvent poser un sérieux problème. Il en va de même pour des mouvements sociaux poursuivis par le biais de perquisitions régulières.

Aucun défenseur ne peut prétendre qu'une perquisition soit un événement "imprévu" (ce qui est valable pour tout autre risque), d'autant plus qu'une perquisition peut être parfaitement légale. Aucun risque ne peut être réduit à zéro. Nous devons réduire autant que possible les conséquences et menaces liées au risque de perquisition.

Comment atteindre cet objectif? En utilisant l'équation du risque et en faisant la liste de toutes les menaces / conséquences (les conséquences peuvent être assimilées aux menaces). Ensuite, pour chaque menace / conséquence, faites la liste des vulnérabilités et capacités correspondantes, et commencez à travailler sur celles-ci...

Menaces / conséquences liées aux perquisitions

Une perquisition génère des menaces / conséquences:

a • La menace de dommages physiques ou psychologiques pouvant être occasionnées pendant une perquisition.

b • La menace que l'information puisse être saisie, perdue ou détruite.

c • Circonstance aggravante, cette information peut ensuite être utilisée de manière inappropriée par des tiers.

d • La menace que des objets litigieux puissent être "cachés" (des armes, des drogues, des documents) afin de poursuivre l'organisation de manière "légale".

e • La menace / conséquence qu'aura le vol d'argent ou la destruction d'objets privés (tels des ordinateurs...).

f • ...

a ◆ La menace que pendant une perquisition quelqu'un puisse subir des préjudices physiques ou psychologiques.

Personne ne peut prédire comment se déroulera une perquisition et quel sera son impact. Cependant, obtenir à l'avance autant d'informations que possible concernant les perquisitions pourrait éviter un comportement et une tension qui favorisent les préjudices physiques et psychologiques. Cela pourrait augmenter la conscience des déclencheurs de risque et aider l'adoption d' un comportement positif.

Vulnérabilités:

- ignorer en quoi consiste une perquisition
- croire que s'y opposer peut nous aider
- l'absence de couverture médicale
- ...

Capacités:

- savoir comment une perquisition légale peut être conduite.
- savoir quelle institution peut émettre des mandats de perquisition et connaître le nom de la personne actuellement responsable des perquisitions (avant et pendant une perquisition légale).
- savoir à quoi ressemble un mandat de perquisition
- savoir quels sont les droits de la personne ou de l'organisation perquisitionnée (y compris le droit de demander à voir le mandat de perquisition et la possibilité de faire appel à un soutien juridique).
- avoir accès à un soutien juridique (pendant et après la perquisition).
- savoir comment ne pas offrir de résistance inappropriée.

- si une perquisition est accompagnée de violence, il est important que les personnes restent en groupe pour réduire le risque d'être maltraités individuellement
- ...

L'organisation devrait envisager d'afficher dans un endroit visible:

- un spécimen de mandat de perquisition.
- l'ensemble de la législation correspondante (droits et devoirs des deux parties).
- une liste avec les noms et numéros de téléphone de l'avocat, du docteur, du psychologue, de l'hôpital le plus proche... (ceci devrait être également affiché dans d'autres parties du bureau pour permettre un accès rapide aux membres du personnel présents).

Cette information est légale et publique. Elle peut donc être accessible par les deux parties. Cela peut ne pas empêcher une perquisition (avec ou sans mandat). Mais cela peut réduire la tension parmi les personnes subissant une perquisition. Cela peut également contribuer à informer l'auteur de la perquisition que la personne ou l'organisation perquisitionnée connaît ses droits et qu'elle le poursuivra si la perquisition dépasse le cadre autorisé par la loi.

b ◆ La menace que l'information puisse être saisie, perdue ou détruite

En général, la plupart des organisations gardent plus d'information que nécessaire. La plus grande partie de celle-ci est rarement utilisée et n'est pas confidentielle. En d'autres termes, seulement une petite partie est confidentielle et elle ne devrait pas être accessible aux personnes faisant une perquisition. L'information absolument confidentielle comprend en général: une liste de personnes (bénéficiaires de projets, témoins); des preuves cruciales dans des affaires judiciaires; des cas spécifiques et leur analyse.

L' information destinée au public ou n'étant pas litigieuse peut être laissée dans les bureaux afin que les personnes procédant à la perquisition la saisissent (comme on fait lorsqu'on voyage avec de l'argent, ne laissant visible que le montant pouvant être dérobé par des voleurs).

Une politique d'information appropriée signifie que la plupart des conséquences liées à la perte, au vol ou à la destruction d'informations sont considérablement réduites.

Cela signifie aussi que le défenseur ne devrait pas ressentir le besoin de prendre le risque de protéger des informations (dans tous les cas, la priorité doit être donnée à la vie); cela diminuera la tension générée par la perquisition, réduisant ainsi le risque de violence et de blessures physiques et psychologiques (s'occuper des menaces / conséquences citées plus haut).

Vulnérabilités:

- l' information non classée en information confidentielle et non-confidentielle au moment de l'archivage.
- l' information sensible archivée sur papier.
- l' information électronique non cryptée (fichiers et pièces jointes).
- une sécurité au travail et au domicile inadéquate: un trop faible nombre de barrières et de filtres pour empêcher la venue de personnes indésirables ou au moins pour laisser le temps d'éteindre un ordinateur ou de dissimuler un document.
- ...

Capacités:

- des copies de sauvegarde régulières de 'information stockée sur ordinateur (au minimum hebdomadaires) et gardées en lieu sûr. Dans le cas d'une perquisition, vous saurez par conséquent quelle quantité d'information est librement accessible (en fonction de la date de la perquisition et la date de la dernière copie de sauvegarde / de l'archivage d'informations).

Comparaison de différents systèmes de sauvegarde informatiques

Support informatique	Avantages	Inconvénients
Graver des CDs/DVDs	De nombreux ordinateurs disposent de graveurs de CD/DVDs. Un transport et archivage facile et plus sûr des DVDs/CDs de sauvegarde	Dans le cas d'une grande quantité d'informations, de nombreux CDs seront nécessaires, ce qui rend le processus plus long et complexe. N'importe qui réussissant à obtenir les CDs aura accès à toutes les données
Mémoire flash	Voir plus haut	Voir plus haut. Bien que plus facile à archiver, la probabilité de tomber entre de mauvaises mains est plus faible
Équipement extérieur	Il peut contenir beaucoup d'informations et le transfert de données ne prend pas beaucoup de temps. Peut être équipé de codes d'accès pour protéger l'information	Coût (200 à 300 US $).
Serveur à distance	Peut contenir toutes les informations, est rapide, ne peut être perdu ou volé.	Vous aurez besoin d'un accès Internet à haut débit et d'un système de cryptage. Les entreprises de serveurs peuvent être forcées de remettre les données aux autorités ('sous prétexte de la sécurité de l'État').

- les copies ou les photocopies, ou encore mieux, les copies scannées, pour garder des traces de documents essentiels dans un endroit sûr. Si c'est nécessaire, elles pourront être redistribuées vers d'autres endroits sûrs.

- une sécurité adéquate au travail et au domicile.

- une alerte donnée au début de la perquisition afin d'obtenir un soutien juridique (avocats) et de faire appel à d'autres organisations pour qu'elles fournissent une assistance et qu'elles soient témoin de la perquisition, au moins de l'extérieur. Cela mettra la pression sur les auteurs de la perquisition dans l'espoir qu'ils se conformeront à loi pendant leur fouille.

- ...

c ◆ La menace / conséquence que l'information soit saisie et utilisée par des tiers.

Il y a une forte probabilité qu'il y ait des conséquences pour l'organisation et pour les personnes mentionnées par l'information.

Conséquences pour l'organisation perquisitionnée

Vulnérabilités:

- absence de procédures de réaction prévues à l'avance.
- négligence de l'éthique, mauvaise comptabilité et logiciels piratés (pouvant déclencher des poursuites judiciaires envers l'organisation).
- ...

Capacités:

- Copies de sauvegarde
- Plan de réaction en vigueur
- ...

Conséquences pour les personnes mentionnées par l'information

Vulnérabilités:

- ne pas avoir discuté cette éventualité avec les personnes concernées
- ne pas pouvoir les joindre rapidement
- ...

Capacités:

- avoir expliqué l'existence d'un risque et s'être assuré autant que possible que ce risque ne se produira pas à cause de la négligence de l'organisation ou de ses membres.

- avoir prévu ensemble la réaction d'urgence (recourir rapidement au plan de réaction, aux mesures de protection, aux cachettes, etc.).
- ...

d ◆ La menace que des objets litigieux puissent être "cachés" (des armes, des drogues, des documents) afin de poursuivre l'organisation en justice par la suite.

Vulnérabilités:

- si l'espace de travail est rempli d'objets et de papiers sans rapport avec le travail (des effets personnels, des magazine éparpillés ça et là...) il est plus difficile de repérer si quelque chose a été volontairement caché pendant la perquisition, ou si un visiteur a laissé / caché au préalable un objet / document qui pourra ensuite être trouvé "par hasard" par les personnes procédant à la perquisition.
- absence d'inventaire du matériel de bureau, encore moins d'un inventaire certifié par un avocat ou un notaire (ce qui est recommandé).
- présence d'un seul membre de l'organisation pendant la perquisition.
- ...

Capacités:

- quand c'est possible (dans le cas d'une perquisition légale),[33] les personnes auront intérêt à se placer dans les diverses pièces et endroits du bureau (par exemple chaque personne à sa place de travail) afin d'être en mesure d'observer le déroulement de la perquisition. De cette manière, il est également plus facile de remarquer si quelque chose est saisi de façon illégale.
- après la perquisition (indépendamment de sa nature), l'organisation procèdera à une vérification complète du bureau ou de l'espace de travail (si possible avec l'assistance d'observateurs externes), en repérant (même par la prise de photos) les objets pour s'assurer que tout objet étranger au bureau soit répertorié et ne soit en aucun cas touché (soyez conscient de l'importance des empreintes digitales). Faites également une liste des objets manquants.
- Déposez plainte auprès de la police et recourez aux dispositions légales en vigueur.
- ...

e ◆ La menace / conséquence qu'auront le vol ou la destruction d'argent et des objets privés (tels que des ordinateurs...).

Une perquisition illégale aura très probablement comme conséquence le vol d'objets.

[33] Si une perquisition est accompagnée de violence, il est important que les personnes restent en groupe pour réduire le risque d'être maltraitées individuellement.

Vulnérabilités:

- une somme importante d'argent et d'objets de valeur dans le bureau.
- des objets non protégés.
- absence d'un inventaire du matériel de bureau, encore moins d'un inventaire certifié par un avocat ou un notaire (ce qui est recommandé).
- absence d'une assurance contre le vol.
- ...

Capacités:

- placez le personnel du bureau à différents endroits afin d'observer la perquisition.[34]
- une alerte donnée au début de la perquisition afin d'obtenir un soutien juridique (avocats) et de faire appel à d'autres organisations pour qu'elles fournissent une assistance et soient témoins de la perquisition, au moins de l'extérieur. Cela mettra la pression sur les auteurs de la perquisition dans l'espoir qu'ils se conformeront à loi pendant leur fouille.
- ...

Comment faire face à la perquisition et en réduire la menace

Si une perquisition correspond aux normes de la législation internationale et a un objectif légal et légitime, il est inutile alors de s'y opposer ou d'en réduire la menace. Vous devez ouvrir la porte et laisser entrer les fonctionnaires. Il vous restera à vous rappeler de la partie "conséquences" traitée plus haut et d'agir en conséquence. Cependant, si les perquisitions sont utilisées de manière systématique pour entraver le travail des organisations sociales et de défense des droits humains, alors il est recommandé d'agir sur la dissuasion.

Afin de confronter et de réduire la menace d'une perquisition légale, la meilleure stratégie est d'en augmenter le coût politique au moyen de campagnes et d'interventions publiques, de préférence en collaboration avec d'autres organisations et institutions.

S'il y a un risque d'une perquisition illégale (ou d'un vol), il est important d'améliorer autant que possible la sécurité du domicile, du bureau ou des locaux professionnels.

Cela s'applique indépendamment de la localisation de votre bureau / domicile, qui peut se trouver dans une zone urbaine ou rurale.

[34] Une fois encore, si une perquisition est accompagnée de violence, il est important que les personnes restent en groupe pour réduire le risque d'être maltraitées individuellement

En résumé

Les manières de réduire le risque d'une perquisition:

Les perquisitions peuvent être à la fois légales et illégales (si elles sont illégales, elles sont équivalentes à une effraction).

Comme pour tout autre risque spécifique, augmentez le coût politique des perquisitions.

Utilisez l'équation du risque et développez chaque élément autant que possible.

Faites la liste des menaces / conséquences et de leurs vulnérabilités et capacités respectives et commencez à travailler sur elles:

a • La menace que durant une perquisition quelqu'un puisse subir des dommages physiques ou psychologiques.

b • La menace que l'information puisse être saisie, perdue ou détruite.

c • Circonstance aggravante, cette information peut ensuite être utilisée de manière inappropriée par un tiers.

d • La menace que des objets litigieux puissent être "cachés" (des armes, des drogues, des documents) afin de poursuivre par la suite l'organisation de manière "légale".

e • La menace / conséquence qu'aura le vol d'argent ou la destruction d'objets privés (tels des ordinateurs...).

f • ...

CHAPITRE 3.2

Détention, arrestation, enlèvement et capture d'un défenseur

"Pas de nouvelles du défenseur"

Lorsque nous ne savons pas où se trouve un défenseur, le premier impératif est de découvrir exactement ce qui lui est arrivé, ce qui peut prendre un certain temps. Plusieurs choses peuvent s'être produites:

- Le défenseur peut ne pas vouloir, ou peut avoir oublié de se mettre en relation avec l'organisation: il ou elle peut avoir décidé de partir pour le week-end en visite sans le dire à qui que ce soit (ou bien il ou elle veut peut être se "changer les idées"). Il ou elle peut se retrouver sans téléphone ou autre moyen de communication, ou n'a peut-être pas pris la peine de se présenter à l'organisation. Il ou elle n'a peut-être pas voulu que quiconque sache ce qu'il ou elle faisait (parfois avec succès). Il ou elle peut (et c'est le cas le moins fréquent) avoir oublié ou ne pas être conscient que ses collègues souhaitent savoir où il se trouve.

- Le défenseur peut ne pas avoir été en mesure de contacter l'organisation pour des raisons techniques: ceci peut se produire si le défenseur n'a pas accès aux moyens de communication dans un lieu isolé de manière imprévisible ou inattendue. Cela peut se produire durant un voyage, lorsque le défenseur se trouve soudain dans un endroit sans moyens de communication, si la route est bloquée, s'il doit prendre un autre itinéraire, ou s'il doit modifier son plan initial, l'amenant à un endroit sans moyens de communication. Il est également possible que les moyens de communication prévus soient endommagés d'une manière ou d'une autre (téléphone portable endommagé, une batterie vide, défaillance du réseau téléphonique local, etc.).

- Le défenseur peut ne pas être en mesure de se présenter à l'organisation en raison d'une maladie ou d'une hospitalisation (due par exemple à un accident de circulation, d'une maladie inattendue, ou bien à l'aggravation d'une maladie existante).

- Le défenseur peut avoir été **emprisonné, arrêté, capturé ou enlevé**. Toutes ces éventualités ont en commun de priver le défenseur de sa liberté de mouvement, l'exposant à tous les risques, d'une pression polie jusqu'à une menace de mort.[35] Dans certains cas, le défenseur peut être en mesure de se présenter à l'organisation, ce qui signifie que l'organisation aura plus d'informations sur la situation.

La détention signifie que les membres de l'organisation sont aux mains d'un groupe de soldats, de miliciens, d'une autorité locale etc. *L'arrestation* est le terme utilisé pour décrire la détention par des forces de sécurité (donc en principe on peut faire appel à la loi). *La capture* fait référence à la saisie et au déplacement forcé réalisé de faÇon illégale pour des raisons politiques. *L'enlèvement* fait référence à la capture et la détention de force avec le but explicite d'obtenir des concessions de la part du captif ou d'autres personnes. Dans ce chapitre nous utiliserons de préférence le terme de *détention* pour des raisons de simplicité.

Dans la plupart des cas, ne pas avoir de nouvelles du lieu où se trouve un défenseur relève habituellement d'une des deux catégories (ne pas vouloir / oublier de communiquer, ou bien ne pas en être en mesure de le faire pour des raisons techniques). Voyons comment prévenir ces situations et y réagir.

Trucs et astuces de prévention pour éviter d'être "sans nouvelles" du lieu de séjour d'un défenseur

Le défenseur ne veut pas, ou a oublié de contacter l'organisation

- Chaque membre de l'organisation et particulièrement les membres les plus exposés au risque doivent être conscients du fait que d'autres s'inquiéteront s'ils ne communiquent pas le lieu où ils se trouvent. S'ils désirent ne pas être contactés, ils devraient en informer leurs collègues, y compris du moment à partir duquel ils seront de nouveau joignables. Dans le cas de défenseurs exposés à un grand risque, il est recommandé qu'ils restent joignables de façon permanente. Le contraire devrait être évité.
- Il est important d'établir des contrôles de routine pour vérifier le maintien du contact régulier avec l'organisation (habituellement avec une ou deux personnes particulières). Cela devient essentiel quand les risques auxquels sont exposés les défenseurs augmentent (parce qu'ils sont en route vers une zone dangereuse, ou qu'ils ont reçu des menaces, etc.).

Le défenseur n'est pas en mesure de contacter l'organisation pour des raisons techniques

- Des heures précises auxquelles on procède à des vérifications devraient être définies et les problèmes de communication devraient être anticipés pour ces heures: si par exemple l'heure à laquelle on doit se présenter coïncide avec un voyage, on devrait penser à quand et comment il sera

[35] Dans ce chapitre, nous utiliserons une partie du manuel de sécurité très utile de van Brabant (2000, chapitre 13).

possible de communiquer (par téléphone portable ou fixe, ou par d'autres moyens) afin d'être sûr que ce sera possible et que l'endommagement, la défaillance, l'expiration du crédit ou un défaut de la batterie n'empêche pas la communication.

- Planifier d'autres moyens de communication (par le biais de tiers par exemple).

Le défenseur n'est pas en mesure de communiquer parce que il ou elle est malade ou est à l'hôpital

- Des listes doivent être tenues avec les numéros de téléphone et les adresses de tous les hôpitaux et centres de santé dans la zone visitée, ainsi que des moyens de se renseigner sur les accidents de circulation (compagnies de bus, police des autoroutes, contacts faits en chemin, etc.).
- Les défenseurs ne devraient pas entreprendre de voyages s'ils ne sont pas en bonne santé.
- Utilisez les moyens de transports les plus sûrs (y compris les bus ou d'autres moyens).
- Les défenseurs doivent avoir des assurances maladie et accident valides.

La prévention de détentions

Il n'est pas facile d'anticiper les façons de prévenir la détention. L'objectif primordial est de réduire les causes et l'exposition au risque de détention d'un membre de l'organisation.

- Un comportement éthique de la part des individus et de l'organisation est capital pour pouvoir raisonnablement exclure des infractions au droit commun. Ces dernières peuvent évidemment être avancées comme prétexte, mais l'avocat de l'organisation connaîtra la marche à suivre. De plus, le défenseur détenu saura quelles mesures seront prises et pourra se les répéter au même moment pour "rester calme" (impact psychologique), sachant qu'à l'extérieur l'organisation fera le nécessaire. Il n'y a pas besoin de défier les autorités ou de leur donner ne occasion d'agir et de s'exposer ainsi à un plus grand risque que celui déjà encouru par le défenseur.
- Dans les cas ou une infraction au droit commun est utilisée comme prétexte à une action politique, une évaluation complète du risque devient nécessaire et une stratégie de limitation des dégâts doit être préparée, en raison du risque accru encouru par les défenseurs.
- La détention légale peut évidemment être un prétexte. Elle peut ou non être le résultat d'une assignation à comparaître et / ou d'un mandat, et se produire au bureau / domicile ou lors d'un voyage. L'objectif serait de prévenir une arrestation quand le défenseur est seul pour réduire les conséquences liées à la détention elle-même. Ce qui en fin de compte est nécessaire, c'est une stratégie d'action politique visant à dissuader les autorités d'arrêter les défenseurs; néanmoins, dans de nombreux pays la tendance semble être de de poursuivre en justice (criminaliser/"judiciariser") les défenseurs et de les emprisonner pour diverses raisons, y compris si elles ne sont pas liées à leur travail.

- Il n'est pas facile de prévenir l'enlèvement. Mis à part une évaluation nécessaire du risque au moment où on suspecte la menace d'enlèvement, il est capital de réduire l'exposition au risque dans des zones dans lesquelles la menace peut être mise à exécution, de s'assurer de n'être jamais seul et de passer au crible toute action pouvant faciliter un enlèvement.
- L'enlèvement peut être exécuté par des criminels de droit commun (qu'il s'agisse d'un prétexte ou non) ou par des acteurs légaux ou para-légaux, par des groupes politiques armés etc. Il peut se produire pratiquement n'importe où, mais il est le plus probable soit lorsque l'occasion est créée par des agresseurs potentiels, soit quand le défenseur la crée malgré lui et de préférence lorsqu'il n'y a pas de témoins. C'est pourquoi l'enlèvement est moins probable sur le lieu de travail pendant les heures ouvrables, au domicile pendant la journée etc. (voir l'exemple de menaces de mort contre le dirigeant d'une organisation au chapitre 1.7.).

  La différence entre des procédures illégales lors d'une détention légale et d'agressions ou d'enlèvements est si minime, que nous conseillons à tous les défenseurs des droits humains de considérer les éléments de l'une et de l'autre non comme s'excluant mutuellement, mais plutôt comme complémentaires. Cependant, nous considérons qu'il est important d'établir la différence entre la signification réelle de la détention et de l'enlèvement pour des raisons psychologiques et pratiques.
- La procédure de prévention de l'agression ou de l'enlèvement devrait prendre en compte le travail quotidien du défenseur dans la zone habituelle de ses activités, celle de ses loisirs etc., et certainement durant ses missions sur le terrain, qu'elles soient dues à l'organisation ou le résultat d'une invitation. Soyez vigilant et vérifiez scrupuleusement toutes les invitations de personnes ou organisation inconnues.

Nous supposons qu'un défenseur a été détenu (ou arrêté, capturé ou enlevé)...

Quand est-ce que nous pouvons supposer qu'un défenseur ait été privé de sa liberté? Et bien, si nous n'avons pas de nouvelles directes du défenseur, nous devons trouver cela suspect si on peut raisonnablement exclure les trois premières options... Il est réaliste de considérer que la procédure de réaction en cas de détention réelle ou supposée est similaire à la procédure de réaction utilisée quand une personne ne se présente pas à l'organisation alors qu'elle le devrait.

Par conséquent, si nous sommes sans nouvelles d'un défenseur, nous devons commencer à faire des recherches pour pouvoir écarter chacune des trois premières options. Il est difficile d'écarter avec certitude chacune des trois premières options. Pour cette raison il est important de fixer un délai avant de considérer une quatrième option: trois heures sans nouvelles, six heures, 12 heures... Dépendant du contexte, des circonstances, du niveau de risque, de la conscience du défenseur de la nécessité de se présenter à l'organisation etc. Plus le délai sera court, plus grand sera le risque de faire une erreur si nous donnons l'alerte; plus il sera long, plus long sera le temps avant de prendre les mesures nécessaires. Ce n'est pas une décision facile à prendre!

Attention: le défenseur peut ne pas avoir fait rapport à l'organisation par oubli ou négligence ou à cause de l'absence de moyens de communications - toutes les possibilités devraient être anticipées au moment de planifier les moments de faire rapport pendant la mission.

Rappelez-vous: nous pouvons réagir à une détention supposée ou confirmée.

Il est capital que les réactions de ceux qui sont détenus et de l'organisation impliquée soient accordées et aient les mêmes objectifs. C'est pour cette raison que tous les membres de l'organisation doivent avoir une bonne connaissance des procédures de réaction.

Détention (arrestation, capture, enlèvement):

Une détention (arrestation, capture, enlèvement) peut être de durée variable et aller de quelques heures à plusieurs années. Elle prend fin quand la personne est libérée. Elle peut se transformer en une situation d'enlèvement si l'objectif souhaité dépasse la simple détention. Dans certains cas graves - la capture - elle peut conduire à des blessures, la mort ou la "disparition".

La détention devrait être gérée de trois points de vue:

- du point de vue de la ou des personnes détenues.
- du point de vue de l'organisation de laquelle les personnes détenues dépendent.
- du point de vue de la famille ou des proches des personnes détenues.

Objectifs globaux lors de la gestion des détentions:

- réduire la probabilité qu'une détention se produise.
- être informé aussi vite que possible de la possibilité d'une détention.
- planifier la réaction à une telle situation:
  - une réaction immédiate
  - une réaction à moyen terme

Pour pouvoir garder ce manuel aussi simple que possible, nous allons aborder la détention (y compris les arrestations) et l'enlèvement distinctement.

Détention d'un défenseur: première réaction

Les objectifs et mesures d'une première réaction à une détention:

Mettre en place un groupe de travail ad hoc pour réagir à la détention.

1 ◆ Protéger la vie et la liberté des membres de l'organisation.

2 ◆ Localiser géographiquement les personnes détenues en utilisant une carte, le plan du voyage, les dernières personnes contactées ou dont la connaissance a été faite, appeler tous les contacts et acteurs sur le terrain etc.

3 ◆ Déterminer quel acteur armé détient la personne, pourquoi et dans quel but.

- En recourant à la localisation géographique de la ou des personne(s) détenue(s) et à la connaissance des circonstances (il est possible que vous deviez déduire les causes de la détention si vous ne les connaissez pas encore):il sera possible de faire une supposition raisonnable de qui détient la personne, ou du moins de faire une liste des suspects possibles.
- En contactant les autorités (si approprié, nécessaire et possible).

4 ◆ Obtenir que le défenseur soit libéré de captivité sain et sauf.

□ En règle générale, il est important de ne pas se concentrer sur l'obtention d'un accord mais plutôt d'obtenir une libération, en remettant les négociations à une période située après la libération du défenseur.

□ Évaluez l'acteur armé concerné (en collaboration avec les autorités régionales quand c'est possible/nécessaire), soit directement si l'acteur est une force de sécurité, ou en utilisant des intermédiaires - ou encore l'assistance d'autres acteurs comme les églises, des dignitaires locaux ou des anciens, le Comité international de la croix rouge, etc. Pour cette raison il est crucial de pouvoir se fier à ces contacts. Cette évaluation aura pour objectif d'établir avec certitude la raison de cette détention et d'essayer d'obtenir la libération immédiate du défenseur détenu.

□ Envisagez d'alerter d'autres défenseurs des droits humains et organisations humanitaires pour les informer et les rendre capables de prendre en commun les mesures nécessaires, leur donnant ainsi un poids supplémentaire. Dans les cas où la capture du défenseur sera probablement accompagnée de blessures (comme dans le cas d'une capture faite par des "hommes de main"), il est important d'agir le plus rapidement possible et de concentrer les mesures autant que possible sur les dirigeants probables (lorsque c'est pertinent) du groupe responsable de la capture, ou sur les acteurs politiques les plus sensibles aux pressions nationales et internationales.

□ Alertez les consulats si la personne détenue vient d'un autre pays.

Détention d'un défenseur: réaction à moyen terme

Si un défenseur est détenu et que nous ne nous attendons pas à sa libération à court terme, les objectifs et mesures à moyen terme doivent être envisagés sans perdre de vue les objectifs à court terme.

Les objectifs et mesures à moyen terme d'une réaction à une détention:

1 ◆ Maintenez l'attention sur les objectifs de la réaction à court terme.

2 ◆ Dans le cas d'une arrestation, en plus d'identifier le plus rapidement possible qui détient le défenseur, essayez d'obtenir un transfert vers une détention légale ou bien vers un service de sécurité influençable. Dans ce cas, essayez d'obtenir un soutien juridique adéquat aussi vite que possible (qui idéalement aura été préparé à l'avance). Le risque de mauvais traitements et de tortures peut ainsi être réduit.

3 ◆ Si la détention du défenseur se poursuit, essayez de subvenir à ses besoins personnels - sécurité, nourriture, santé, contactez sa famille et l'organisation etc. dès le début et pendant toute la durée du processus (ces mesures doivent également être prévues à l'avance - voir plus loin: mesures concernant la famille et les proches).

Réactions des personnes détenues

- Rappelez-vous des mesures et des plans préparés à l'avance pour de telles situations. Il est important de connaître, à l'avance, l'ordre correct des mesures en cas d'une détention ou d'une arrestation en vue de réduire votre incertitude, de maîtriser vos ressources mentales et de planifier des objectifs de résistance simples.
- Gardez votre calme. Le défenseur que vous êtes sait que l'organisation dispose d'un protocole de réaction et quelles mesures seront prises; il pourra se les répéter à lui-même en temps réel et garder son calme.
- Votre vie et sécurité sont prioritaires (ainsi que pour les autres collègues éventuelleñent détenus avec vous): tenez-en compte pour tout ce que vous dites ou faites.
- Établissez, si possible, un contact avec le dirigeant du groupe armé et nouez un dialogue avec lui. Invoquez les arguments fournis par l'organisation dans le but d'obtenir votre la libération et celle des autres personnes détenues avec vous et le retour de tous chez soi, ou bien la libération vers un autre endroit sûr (n'essayez pas de négocier un "accord").
- Si ce n'est pas possible ou autorisé, essayez d'obtenir la permission d'utiliser tous les moyens à votre disposition pour informer l'organisation de votre situation; ne tentez pas d'appeler sans autorisation si vous êtes entre leurs mains car ceci pourrait causer plus de risques que de ne rien faire.
- Si la détention est réalisée par des forces de sécurité, utilisez les arguments juridiques fournis par l'organisation pour ces cas de figure.
- Gardez votre calme et n'oubliez pas que l'organisation déploiera rapidement tous ses systèmes de sécurité à mesure que le temps passe.

Mesures concernant la famille et les proches:

- Informez la famille et les proches si la personne ne sera pas libérée rapidement. Instaurez et maintenez une relation de confiance.
- Développez une approche claire envers la famille. Soutenez-la et tenez-la au courant (nommez une personne de liaison pour la famille).
- La famille aura besoin de temps et d'attention de la part de l'organisation. Attendez-vous à des attitudes changeantes et à des initiatives de la part de la famille.

- Dans le cas d'une arrestation ou d'une incarcération à long terme, il est important de planifier le soutien de la famille du défenseur détenu.

Capture et enlèvement d'un défenseur

Du point de vue de l'organisation

La gestion d'une crise d'enlèvement est un processus changeant qui peut durer de quelques heures à plusieurs mois ou années. Le plus important est de mobiliser une équipe de gestion de la crise; de gérer de la famille, l'autorité et la presse; la communication et la négociation avec les ravisseurs.

Communiquer et négocier avec les ravisseurs

L'enlèvement, tel qu'il est défini ici, est délibéré et sert un but. Habituellement les ravisseurs se manifesteront pour transmettre leurs exigences et dicter leurs conditions.

L'équipe de gestion de crise devrait maintenir le contrôle des négociations, mais éviter d'entrer en contact direct avec les ravisseurs; l'objectif est de mettre en place un délai pour permettre les consultations internes et externes et la prise de décision. Vous pouvez si c'est nécessaire, demander des preuves que le ou les captifs sont en vie, ainsi que des preuves de l'identité des ravisseurs. Il est également possible de demander et d'encourager le bon traitement des captifs.

> Si l'enlèvement est un risque réel, il est important de se mettre d'accord sur certaines règles et procédures liées à la rançon et aux exigences des ravisseurs, si possible en accord avec des organisations similaires, et de les publier. Dans tous les cas, des événements préalables et similaires fourniront des renseignements sur les étapes probables d'un enlèvement.

Du point de vue du défenseur capturé / enlevé

- Les moments les plus dangereux, ceux quand les ravisseurs seront le plus à cran, ont lieu pendant l'enlèvement, lorsque le captif est déplacé d'urgence parce que les ravisseurs craignent la proximité des autorités, en situation de siège et pendant la libération.

- Vos ravisseurs voudront que vous restiez silencieux; on peut vous bander les yeux, vous battre voire même vous droguer pour que vous le soyez. Il ne sert à rien de crier ou de se débattre pour s'opposer à cela: rester calme et silencieux offre la plus grande chance d'éviter ce traitement (à moins que vous puissiez raisonnablement espérer que crier ou hurler pendant un enlèvement pousse d'autres personnes à vous venir en aide).

- L'endroit et les conditions dans lesquelles les captifs sont détenus peuvent énormément varier. Vous pouvez être détenu au même endroit ou bien déplacé plusieurs fois; vous pouvez être seul ou bien avec d'autres captifs. Il arrive que des captifs développent une certaine relation avec leurs ravisseurs et qu'ils s'adaptent difficilement au changement de leurs gardes.

- Obéissez aux ordres de vos ravisseurs sans paraître servile; évitez de les surprendre ou de les rendre méfiants.

- Essayez de garder votre santé physique et mentale.

- Si vous êtes dans un groupe, essayez d'éviter qu'on vous sépare, comme la présence d'au moins une autre personne peut être une source de soutien. Il est cependant important d'être préparé à la séparation et aux changements, et d'une manière générale aux incertitudes que chaque jour peut amener et auxquelles il faudra faire face.

- Ce n'est pas à vous d'obtenir une libération, mais à votre organisation. Ne vous impliquez jamais directement dans les négociations pour votre libération. Cela ne fera que compliquer la situation. Si on vous demande de parler à la radio, au téléphone ou d'être filmé, ne dites que ce que l'on vous demande et refusez de négocier même si vous y êtes poussé par vos ravisseurs.

Procédures de prévention: réduire les risques de détention ou de capture pendant un voyage

Les risques de détention ou de capture sont particulièrement élevés pendant un voyage ou une mission sur le terrain parce que le défenseur est plus exposé au risque, est moins en contact avec son environnement habituel et que ses proches ou collègues peuvent réagir plus tardivement à une menace ou à une attaque. Pour cette raison, nous énumérons les risques liés à une mission sur le terrain parce qu'ils contiennent la plupart des risques et des conséquences liées à l'ensemble du travail des défenseurs.

Par exemple:

poste de contrôle ⇨ arrestation ⇨ détention ⇨ ...
Agression ⇨ capture ⇨ violence ⇨ ...
Perte d'information ⇨ effet sur les témoins ⇨ effet sur l'organisation ⇨ ...
Transport ⇨ public / privé ⇨ ...
Temps de loisir en mission ⇨ baisse de la vigilance ⇨ incidents de sécurité ⇨ ...
Communication ⇨ téléphone ⇨ face à face ⇨ ...

Nous insistons sur le risque d'une détention / capture pendant une mission sur le terrain et recommandons qu'une procédure de prévention pour les missions sur le terrain comprenne au moins:

- la préparation à toutes les missions, aussi bien sur le terrain que dans des zones urbaines comme le voisinage.
- l'interdiction de voyager seul.
- la collecte de renseignements adéquats sur la zone visitée et les acteurs en présence (cartographiez les acteurs, faites une analyse des forces en présence, voir au chapitre 1.1.).
- la connaissance par les défenseurs des itinéraires d'accès et de départ des endroits visités.
- chaque personne faisant partie de la mission doit être munie de ses documents d'identité valables.

- alerte des contacts d'urgence de l'organisation qui sont de garde pendant la durée de la mission sur le terrain (à compter du départ du défenseur jusqu'à son retour).
- préparez la mission en accord avec les procédures: indiquez l'ordre du jour et les activités prévues, lesquels devraient également faire partie du manuel de sécurité de l'organisation.
- planifiez des mises à jour régulières sur l'état de la mission (en général par téléphone, à des heures fixées au préalable). Cela implique, si possible, de vérifier s'il y a des téléphones en chemin et à la destination finale. S'il n'est pas possible de vérifier si un réseau téléphonique est disponible, on peut envisager de recourir à des personnes sur place pour confirmer que l'équipe est bien passée par là.

  Il est important de décider combien de temps la personne de garde doit laisser s'écouler avant que l'inquiétude soit permise, au cas où elle n'arrive pas à joindre l'équipe dans l'attente d'un appel de confirmation. Rappelez-vous qu'il est plus simple de reconstituer une capture après quelques heures qu'après de nombreuses heures.
- Évaluez la sécurité des moyens de transport choisis (par moments, le véhicule de l'organisation et à d'autres, les transports publics, afin d'être entouré de témoins potentiels). En cas de transports publics, évaluez s'il est plus sûr d'être assis ensemble ou séparément en feignant de ne pas se connaître. Cela pourrait donner à un membre de l'équipe au moins la possibilité d'alerter l'organisation. Vous risquez de perdre cette possibilité si vous intervenez.
- Si des voyages sont faits dans un véhicule privé, celui-ci devrait être en état de marche à tout moment (respectez les limitations de vitesse et le code de la route). Ne prenez pas d'auto-stoppeurs.
- Là où c'est pertinent, distribuez des informations appropriées aux autorités civiles, militaires et à celles de la communauté, comme aux responsables de la mission (afin qu'ils assument la responsabilité de la sécurité de la mission et ne répondent pas simplement "on ne savait pas").
- Présentez une description des objectifs et du mandat de l'organisation que vous aurez préparée à l'avance, pour les rendre aussi acceptables que possible aux groupes armés et forces de sécurité auquel vous aurez affaire (il est préférable de ne pas adapter le jugement au groupe armé auquel vous êtes confronté car il pourrait être difficile de les identifier et une erreur dramatique peut facilement se produire).
- Évaluez le moment le plus opportun pour quitter le terrain (quelquefois il peut être préférable de partir à l'aube en raison de la chaleur). Dans le cas d'une attaque survenant juste après avoir quitté le terrain, les contacts d'urgence de l'organisation peuvent ne pas encore être opérationnels; les premiers moments après une capture sont vitaux pour ne pas perdre la piste d'une personne.
- Ne voyagez pas de nuit.
- Ne montrez à aucun moment des objets de valeur (comme des appareils photo ou des caméscopes).
- Comportez-vous de manière appropriée pendant le voyage.

- Faites en sorte que l'organisation obtienne la permission de travailler pour la communauté à laquelle vous rendrez visite (et là où c'est possible, de négocier au moins une tolérance de la part de groupes armés).

Autres choses à faire dans le cas d'une mission sur le terrain après un appel d'une tierce personne:

- Soyez sûrs de l'identité de l'auteur de l'appel (procédez à une vérification auprès d'organisations de confiance).
- Vérifiez auprès d'autres sources les événements cités.
- Évaluez s'il est important d'aller sur le terrain ou s'il ne serait pas plus sûr que l'information remonte jusqu'à l'organisation (voir dans le chap. 3.2. la partie "Une gestion sûre de l'information: procédures de prévention et de réaction").
- Évaluez s'il est nécessaire d'aller sur place à ce moment et à cette heure, juste après l'appel, surtout si l'auteur de l'appel est inconnu (l'information devrait au moins être vérifiée au préalable). On devrait également prendre en considération le fait que la mission sur le terrain ne va pas empêcher les événements comme ils ont déjà eu lieu, d'où l'appel initial. En général, le meilleur conseil est d'éviter l'improvisation et les changements de plan pendant le séjour dans une zone à risque.

En résumé

Nous comprenons que la détention d'une personne peut être une procédure légale. Lorsqu'elle franchit les limites de la légalité, elle peut être considérée comme la privation injustifiée de la liberté d'une personne. Sa durée peut être variable, allant de quelques heures à quelques années...

La détention devrait être gérée de trois points de vue:

- du point de vue de la ou des personnes détenues
- du point de vue de l'organisation de laquelle les personnes détenues dépendent
- du point de vue de la famille ou des proches des personnes détenues

Objectifs globaux lors de la gestion des détentions:

- réduire la probabilité qu'une détention se produise
- être informé aussi vite que possible de la possibilité d'une détention
- planifier la réaction à une telle situation: une réaction immédiate et une réaction à moyen terme

La capture est illégale et peut se produire à tout moment, habituellement quand l'occasion se présente. C'est une des nombreuses conséquences possibles d'une "agression". Les mesures de sécurité seront donc semblables à celles concernant la prévention d'une agression (ch. 1.5.): réduire l'exposition physique autant que possible...

CHAPITRE 3.3

La Sécurité de la gestion de l`information

Les défenseurs des droits humains gèrent des informations qui, dans un environnement hostile, peuvent être utilisées pour affecter la sécurité de l'organisation, d'autres personnes et d'autres institutions. Il est donc crucial d'établir une procédure de gestion des informations et un plan de réaction à tous les incidents affectant la sécurité de l'information détenue par l'organisation.

Une gestion sûre de l'information: la procédure de prévention

Les informations dont disposent les organisations des droits humains peuvent être classées de manière générale en deux catégories, selon leur degré de sensibilité: leur confidentialité élevée, ou leur confidentialité réduite.

Toute information que nous gérons est soumise à quatre étapes distinctes avant de nous parvenir et avant d'être transmise (au destinataire concerné). Nous allons esquisser les mesures de sécurité nécessaires à chacune des étapes.

1 • La source: collecte de l'information au point de rencontre

2 • La transmission des informations

3 • Le traitement et archivage

4 • La distribution

1 • La source - collecte de l'information au point de rencontre

Dans ce cas-ci, le problème principal est la protection de l'information et des personnes concernées par celles-ci.

La personne transmettant l'information aura besoin d'un itinéraire précis entre son domicile / bureau et le lieu de la réunion; d'un lieu de réunion (l'endroit où la personne donnant l'information rencontre un membre de l'organisation); cet endroit peut être situé au domicile ou sur le lieu de travail, dans les bureaux de l'organisation ou à tout autre endroit; ainsi que d'un itinéraire pour quitter le siège de l'organisation (des voyages vers et depuis le lieu de la réunion).

Un lieu et des conditions sûres sont nécessaires à la réunion, ainsi qu'un itinéraire pour que l'information arrive et quitte la source, et également un itinéraire pour l'arrivée et le départ des membres de l'organisation qui à leur tour transmettront l'information.

La sécurité de la gestion de l'information commence *avant* de la recevoir

- L'organisation a-t-elle vraiment besoin d'obtenir cette information?

Est-ce que l'organisation sera en mesure d'utiliser les données pour améliorer son travail ou pour atteindre plus facilement ses buts et objectifs? Si ce n'est pas le cas, il vaut mieux que l'organisation **ne reçoive pas** l'information; si l'information se situe en dehors de son domaine de compétence, l'organisation peut rediriger la personne vers une autre organisation sans accepter ni l'information, ni l'affaire.

- Expliquez qui nous sommes, la nature de nos objectifs et de notre travail et la manière dont l'organisation utilisera l'information à la personne qui la transmet; le type d'information dont nous avons besoin, comment nous la gèrerons et l'utiliserons - et ce qu'elle peut attendre de nous. Il est fondamental et éthique que la personne donnant l'information connaisse au préalable (soit directement ou bien par le biais d'un tiers) les risques qu'elle encourt en transmettant l'information et l'usage que l'organisation peut en faire.

Il n'est pas suffisant de supposer que la personne concernée soit consciente de tout cela. Pour nous, il est important de le lui expliquer pour que nous soyons sûrs qu'elle le sache. Il est également important de définir avec elle de possibles mesures de sécurité.

Le lieu de rencontre doit être aussi sûr et anonyme que possible. Très probablement, le domicile de la personne ne sera pas un endroit sûr, puisque l'arrivée d'un membre de l'organisation sera aisément remarquée. Les bureaux de l'organisation peuvent être plus sûrs (tant que la confidentialité est respectée), ou bien un autre lieu relativement public dans lequel il est normal que des gens vont et viennent (par exemple l'immeuble d'une paroisse, le centre d'une communauté), tant que la confidentialité est respectée, nous insistons sur ce point. Si la rencontre est organisée dans un endroit inapproprié, elle peut être ajournée et déplacée vers un lieu plus sûr en fonction du degré de sensibilité des informations transmises.

On pourrait également envisager de recourir à une version officielle servant de couverture: la personne quitte son domicile sous un prétexte officiel. Elle devra créer le prétexte: une visite chez le dentiste (montrer le mal de dents), une visite chez le médecin (n'importe quelle maladie), des emplettes sur le marché etc. La personne devra revenir à son domicile avec des preuves réelles (des ordonnances et des médicaments, des achats qu'elle n'aurait pas pu trouver chez elle).

N'oubliez pas que la personne fournissant l'information pourra rencontrer des problèmes de sécurité après que la réunion ait eu lieu à l'endroit prévu.

2 ● Transmission de l'information

L'information peut être obtenue par différents moyens: la mémoire, l'imprimante, des notes manuscrites ou bien informatiques, des photos etc.

La méthode courante la plus sûre de transmission d'informations est au moyen d'un ordinateur portable, d'une clé USB ou bien d' un CD-ROM disposant d'un cryptage de sécurité. La rencontre peut être enregistrée, les photos peuvent être archivées et des notes peuvent être prises. Tous les autres moyens sont certainement moins sûrs, ce qui augmente le risque lors de la transmission.

Les informations confidentielles doivent être confiées à des membres de l'organisation qui sont conscients de la valeur de ce qui leur est confié.

Trop souvent les défenseurs des droits humains voyagent avec la totalité de leurs carnets de notes contenant des informations importantes, qui ne sont pas nécessairement liées à la mission spécifique. Ils gardent le même carnet de notes jusqu'à ce qu'il soit rempli, au lieu de voyager uniquement avec le papier ou le matériel dont ils ont besoin. La même chose est valable pour le contenu de clés USB, d'ordinateurs et d'autres supports d'informations.

3 ● Archivage et traitement de l'information

Une fois que l'information a atteint les bureaux de l'organisation, elle est en général plus en sécurité (en fonction des faiblesses du bureau - voir le chapitre 1.8 concernant la sécurité au travail et au domicile).

Les normes ayant une importance particulière pour l'information sont les suivantes:

L'archivage de documents imprimés: ce moyen devrait être utilisé uniquement quand c'est nécessaire; la documentation nécessaire pour des affaires particulières devrait être transmise en personne. L'information sur papier devrait être archivée dans des boîtes de métal à verrous; pour l'archivage des informations, l'utilisation d'une chambre-forte ou d'un coffre-fort devrait être envisagée.

Il est également possible de répartir les papiers entre différents lieux sûrs ou bien de les envoyer à d'autres endroits avec le même soin décrit dans la partie "transmission de l'information". L'information peut être également scannée, cryptée et envoyée à une organisation de confiance (à un homologue international, par exemple).

Les systèmes de cryptage et les codes devraient être utilisés de manière appropriée.

Faites des sauvegardes hebdomadaires et archivez ces copies, également cryptées, dans un lieu sûr comme un coffre-fort ou autre.

4 ● Distribution de l'information

Les critères généraux concernant la distribution de l'information comprennent les points suivants:

- Vérifiez l'information par recoupement.

- Dans les cas où l'organisation est la seule source d'information concernant certains faits, il y aura un risque accru et des plans d'urgence seront nécessaires.

- Il serait utile d'obtenir l'accord de la part des personnes fournissant l'information, en particulier lorsque ces personnes sont la seule source d'information possible à l'échelon local.

- Toute information écrite quittant l'organisation ou des organisations amies devrait être considérée comme "publique", du fait du risque qu'elle tombe entre de mauvaises mains ou en raison des aléas quotidiens des moyens de communication.

- Il est capital pour l'organisation publiant l'information d'avoir une politique de communication dédiée; cela devrait inclure les principales normes de sécurité applicables à la publication de l'information (comme le principe de toujours annoncer une information concernant l'organisation elle-même).

L'accès à l'information par des personnes qui ne sont pas membres de l'organisation (des auxiliaires, des volontaires, etc.).

Pour la sécurité de l'organisation, des tiers, des auxiliaires et des volontaires, l'accès aux archives numériques et physiques doit être restreint (à décider selon le type d'affaire) et doit relever de la responsabilité d'un collaborateur de l'organisation.

Il peut être utile d'incorporer dans le contrat ou l'accord de travail des auxiliaires et des volontaires une clause de confidentialité à laquelle ils seront tenus à tout moment. Cette clause de confidentialité devrait également être incluse dans les contrats du personnel sous-traité par l'organisation.

Une gestion sûre de l'information: procédures de réaction en cas de vol ou de perte de données

Le vol ou la perte de données (il peut être difficile de déterminer s'il s'agit de l'un ou de l'autre) appartenant à l'organisation nous oblige à nous comporter comme si l'information tombait systématiquement entre de mauvaises mains et que dans tous les cas, un usage malveillant en était fait pouvant affecter des tiers (qu'il s'agisse de ceux transmettant les informations ou de collègues, etc.) ou l'organisation elle-même.

Si en dépit de toutes ces procédures de prévention un vol ou une perte d'information se produisait, cela devrait être considéré comme une atteinte sérieuse à la sécurité et les mesures suivantes devraient être prises:

1 ◆ Informez immédiatement des membres de l'organisation.

2 ◆ Évaluez la quantité et le degré de sensibilité de l'information perdue ou volée, en fonction du risque auquel il expose les personnes directement affectées par l'information, des tiers ou l'organisation, et pourquoi (ou les vecteurs du risque). Cette évaluation doit être faite pour tous les types d'informations volées, au cas où plusieurs sortes d'informations ont été volées (par exemple des listes de noms, des références et des informations collectées sur des affaires individuelles).

3 ◆ Évaluez la nécéssité de notifier les personnes et institutions potentiellement affectées pour qu'elles puissent prendre les mesures nécessaires pour se protéger (cela devrait toujours être fait discrètement).

4 ◆ Évaluez la nécéssité de notifier les autorités et de dénoncer les événements.

5 ◆ Lorsque c'est nécessaire, prenez toutes les autres mesures utiles pour éviter des conséquences néfastes au cas où l'information perdue ou volée serait utilisée.

L'organisation devra également décider dans quelle mesure ses membres peuvent se mettre en danger pour protéger l'information: par exemple en cas d'une perquisition violente, on doit avoir évalué jusqu'à quel point cela "vaut la peine" de résister.

En résumé

La sécurité de la gestion de l'information requiert des procédures de prévention et de réaction.

La prévention devrait s'articuler au moins autour de quatre points:

1 • La source - collecte de l'information au point de rencontre.

2 • La transmission de l'information.

3 • Le traitement et l'archivage.

4 • La distribution.

La réaction devrait comprendre au moins les mesures suivantes:

1 • L'information des responsables au sein de l'organisation.

2 • L'évaluation de la quantité et du degré de sensibilité de l'information perdue ou volée.

3 • L'évaluation de la notification des personnes et des institutions potentiellement affectées.

4 • L'évaluation de la notification des autorités et de la déclaration des événements.

5 • Les mesures nécessaires pour éviter des conséquences néfastes au cas où l'information perdue ou volée serait utilisée.

CHAPITRE 3.4

La Sécurité et le temps libre

Réflexion:

D'une manière générale, les règles de sécurité sont respectées tant qu'elles n'interfèrent pas avec des intérêts personnels. Par conséquent, il sera plus facile de s'attaquer à la sécurité au travail qu'à celle concernant le temps libre. Cependant, le temps libre est un élément fondamental de la sécurité à la fois individuelle et organisationnelle. Cela nécessite une discussion et une compréhension des interférences possibles entre les besoins personnels et la sécurité.

Le temps libre

Voici quelques questions et réflexions pour aider l'organisation à élaborer sa politique concernant le temps libre. Il est important, comme avec n'importe quel autre élément de la sécurité, de la pousser aussi loin que possible même si cela peut enfreindre le domaine privé (les incidents de sécurité peuvent également enfreindre le domaine privé).

Nous commençons avec deux réflexions importantes:

- Si quelqu'un désire attaquer une organisation, il n'attaquera probablement pas les personnes les mieux protégées ou ceux qui suivent des règles de sécurité, mais ciblera plutôt celles ayant des points faibles, particulièrement pendant leur temps libre (la nuit, le week-end etc.).
- Si une organisation a dix membres parmi lesquels un ou deux ne se conforment pas aux règles de sécurité durant leur temps libre, c'est toute l'organisation qui est exposée au risque et pas seulement cette ou ces personnes, car c'est l'organisation entière qui serait exposée au risque par une attaque contre ces personnes.

La question sous-jacente est toujours: "Existe t-il un risque de sécurité lié à..." Si la réponse est "non", alors tout est parfait. Si la réponse est "oui", alors il faudra la creuser et décider s'il existe des moyens de répondre à un besoin personnel dans un environnement protégé, ou décider d'accéder à ce besoin à un moment plus sûr, ou s'il faut simplement y renoncer par incompatibilité avec les exigences de sécurité d'un défenseur des droits humains.

Faisons-nous attention à la sécurité seulement durant les heures de travail ou 24 heures sur 24, sept jours sur sept?

Bien qu'il soit difficile de faire une distinction entre les politiques de l'organisation et l'autonomie de chaque membre durant son temps libre, la prévention des attaques et la réaction à celles-ci ne fait pas de différence entre les attaques durant les heures de travail et celles se produisant durant le temps libre... Nous ne devons pas oublier que si une personne décide d'attaquer une organisation à travers ses membres, elle ne le fera pas pendant les heures de travail, mais au moment où les défenseurs sont le plus vulnérables. Une personne préparant une attaque contre un défenseur cherchera une occasion propice. Nous devons également être conscients qu'une attaque de nuit, ou lorsqu'on quitte une boîte de nuit etc., passera plus facilement inaperçue…

Dans les pays où boire de l'alcool est une coutume, est-ce que boire jusqu'à l'ivresse représente un risque pour la sécurité?

L'ivresse dans un endroit public a certainement un impact sur la sécurité. Le défenseur peut parler, son comportement est altéré et il peut ne pas être conscient du fait qu'il est délibérément interrogé ou provoqué. Il y a un impact certain sur l'image de l'organisation, mis à part de l'impact direct sur la sécurité physique du défenseur des droits humains. Rappelez-vous qu'un défenseur ivre donne une occasion dont n'importe quel groupe hostile envisageant une attaque contre l'organisation du défenseur pourrait tenter de profiter (la même chose est valable pour d'autres drogues). L'usage d'alcool et d'autres drogues ne devrait pas être examiné d'un point de vue moral ou de santé, mais comme un fait objectif concernant la sécurité.

Est-ce que des relations et des liaisons secrètes peuvent affecter la sécurité?

- Il y a eu des cas de défenseurs des droits humains qui ne se sont pas présentés à leur organisation parce qu'ils avaient une liaison. L'organisation avait déjà mis en alerte son contact d'urgence, pour ensuite se rendre compte que les défenseurs étaient en parfaite santé et inconscients de l'inquiétude provoquée. Ce genre de situation donne clairement une occasion de discréditer l'organisation et le défenseur concerné en attirant l'attention sur l'image et sur les implications éthiques. Quelques contacts d'urgence pourront même décider de se retirer du système d'alerte anticipé de l'organisation.

- Le problème n'est pas la liaison, mais comment celle-ci peut affecter la communication et la sécurité. Nous répétons qu'il ne s'agit pas d'une question de morale ou de santé mais d'une question de sécurité. Il est important que l'organisation soit capable de gérer ces éventualités d'une façon claire et qu'elle recherche les manières de le faire.

- Que faire si l'ami(e) d'un défenseur était considéré(e) comme suspect(e) par d'autres membres de l'organisation? L'organisation pourrait-elle intervenir?

- De quelle manière l'information peut-elle être transmise aux amis, aux familles et aux proches? Le défenseur des droits humains est-il responsable de la manière dont l'information pourra être utilisée?

La façon dont les défenseurs utilisent leur temps libre a donc un impact potentiel sur la sécurité. Il ne s'agit pas d'interdire les loisirs, qui représentent une nécessité, mais plutôt d'examiner les conditions dans lesquelles on peut les poursuivre.

Toutes les organisations des défenseurs exposées au risque ont besoin d'une politique concernant tous les aspects liés au temps libre, allant des soirées jusqu'aux vacances.

Il est nécessaire d'aborder les questions de la consommation d'alcool en public et d'autres drogues, de la manière dont les relations secrètes peuvent interférer avec la sécurité et de la façon dont le temps libre peut affecter l'image et la sécurité de l'organisation.

Comment gérer la confidentialité de l'information?

Sachant qu'il peut y avoir des fuites d'informations à tout moment, même pendant le temps libre, voici une considération supplémentaire concernant la sécurité de l'information.

L'organisation devrait mettre en place au moins deux niveaux différents de confidentialité de l'information (toujours au sein de l'organisation):

a. Ce que juste un petit nombre de membres devrait savoir.

b. Ce que tous les membres peuvent savoir.

Ce procédé peut réduire le risque de fuites d'informations confidentielles, que ce soit par négligence et / ou par infiltration. Cela peut également permettre à l'organisation de localiser l'origine des fuites.

Certains aspects de notre comportement durant notre temps libre peuvent-ils affecter l'organisation?

- Comment est-ce que d'autres nous perçoivent?
- Dans quelle mesure les collègues savent-ils ce que nous faisons dans notre temps libre?
- Quel est l'impact de l'image de l'organisation sur la sécurité?
- ….

En résumé

Un défenseur exposé au risque doit s'occuper de la sécurité 24 heures par jour, sept jours par semaine, dans tous les aspects de sa vie, y compris durant ses loisirs.

Le temps libre nécessite d'être pris en compte de façon adéquate.

La question sous-jacente est toujours: "Existe-t-il un risque de sécurité lié à..." Si la réponse est "non", alors tout est parfait. Si la réponse est "oui", il faudra creuser le sujet et déterminer s'il y a moyen de satisfaire le besoin en question dans un environnement protégé, ou bien si le besoin doit être remis à une période plus sûre, ou bien s'il faut simplement y renoncer par incompatibilité avec les exigences de sécurité d'un défenseur des droits humains.

Toutes les organisations des défenseurs exposées au risque ont besoin d'une politique concernant tous les aspects du temps libre, allant des soirées jusqu'aux vacances. Il est nécessaire d'aborder les questions de la consommation d'alcool en public et d'autres drogues, de la manière dont les relations sentimentales cachées peuvent interférer avec la sécurité et de la façon dont l'image de l'organisation concernant le temps libre peut affecter la sécurité.

Comme le temps libre comporte des risques, il est important de ne pas oublier d'évaluer le risque.

ANNEXE I

Déclaration de l'ONU sur les Défenseurs des Droits de l'Homme

NATIONS UNIES **A**

Assemblée générale

Distr.
GÉNÉRALE
A/RES/53/144
8 mars 1999

Cinquante-troisième session
Point 110, b, de l'ordre du jour

RÉSOLUTION ADOPTÉE PAR L'ASSEMBLÉE GÉNÉRALE

[sur le rapport de la Troisième Commission (A/53/625/Add.2)]

53/144. Déclaration sur le droit et la responsabilité des individus, groupes et organes de la société de promouvoir et protéger les droits de l'homme et les libertés fondamentales universellement reconnus

L'Assemblée générale,

Réaffirmant l'importance que revêt la réalisation des buts et principes énoncés dans la Charte des Nations Unies pour la promotion et la protection de tous les droits de l'homme et de toutes les libertés fondamentales pour tous, dans tous les pays du monde,

Prenant note de la résolution 1998/7 de la Commission des droits de l'homme, en date du 3 avril 1998,[1] dans laquelle la Commission a approuvé le texte du projet de déclaration sur le droit et la responsabilité des individus, groupes et organes de la société de promouvoir et protéger les droits de l'homme et les libertés fondamentales universellement reconnus,

Prenant note également de la résolution 1998/33 du Conseil économique et social, en date du 30 juillet 1998, dans laquelle le Conseil a recommandé à l'Assemblée générale d'adopter le projet de déclaration,

Consciente de l'importance que revêt l'adoption du projet de déclaration dans le contexte du cinquantenaire de la Déclaration universelle des droits de l'homme[2],

1. *Adopte* la Déclaration sur le droit et la responsabilité des individus, groupes et organes de la société de promouvoir et protéger les droits de l'homme et les libertés fondamentales universellement reconnus qui figure en annexe à la présente résolution;

2. *Invite* les gouvernements, les organes et organismes des Nations Unies et les organisations intergouvernementales et non gouvernementales à intensifier leurs efforts en vue de diffuser la Déclaration

1 Voir Documents officiels du Conseil économique et social, 1998, Supplément no 3 (E/1998/23), chap. II, sect. A.99-77090 /...

2 Résolution 217 A (III).

et d'en promouvoir le respect et la compréhension sur une base universelle, et prie le Secrétaire général de faire figurer le texte de la Déclaration dans la prochaine édition de la publication Droits de l'homme: Recueil d'instruments internationaux.

85e séance plénière
9 décembre 1998

ANNEXE

Déclaration sur le droit et la responsabilité des individus, groupes et organes de la société de promouvoir et protéger les droits de l'homme et les libertés fondamentales universellement reconnus

L'Assemblée générale,

Réaffirmant l'importance que revêt la réalisation des buts et principes énoncés dans la Charte des Nations Unies pour la promotion et la protection de tous les droits de l'homme et de toutes les libertés fondamentales pour tous, dans tous les pays du monde,

Réaffirmant également l'importance de la Déclaration universelle des droits de l'homme [3] et des Pactes internationaux relatifs aux droits de l'homme [4] en tant qu'éléments fondamentaux des efforts internationaux visant à promouvoir le respect universel et effectif des droits de l'homme et des libertés fondamentales, ainsi que l'importance des autres instruments relatifs aux droits de l'homme adoptés par les organes et organismes des Nations Unies, et de ceux adoptés au niveau régional,

Soulignant que tous les membres de la communauté internationale doivent remplir, conjointement et séparément, leur obligation solennelle de promouvoir et encourager le respect des droits de l'homme et des libertés fondamentales pour tous, sans distinction aucune, notamment sans distinction fondée sur la race, la couleur, le sexe, la langue, la religion, l'opinion, politique ou autre, l'origine nationale ou sociale, la fortune, la naissance ou toute autre situation, et réaffirmant qu'il importe en particulier de coopérer à l'échelle internationale pour remplir cette obligation conformément à la Charte,

Reconnaissant le rôle important que joue la coopération internationale et la précieuse contribution qu'apportent les individus, groupes et associations à l'élimination effective de toutes les violations des droits de l'homme et des libertés fondamentales des peuples et des personnes, notamment des violations massives, flagrantes ou systématiques telles que celles qui résultent de l'apartheid, de toutes les formes de discrimination raciale, du colonialisme, de la domination ou de l'occupation étrangère, de l'agression ou des menaces contre la souveraineté nationale, l'unité nationale ou l'intégrité territoriale, ainsi que du refus de reconnaître le droit des peuples à l'autodétermination et le droit de chaque peuple d'exercer sa souveraineté pleine et entière sur ses richesses et ses ressources naturelles,

Considérant les liens qui existent entre la paix et la sécurité internationales, d'une part, et la jouissance des droits de l'homme et des libertés fondamentales, d'autre part, et consciente du fait que l'absence de paix et de sécurité internationales n'excuse pas le non-respect de ces droits et libertés,

Réaffirmant que tous les droits de l'homme et toutes les libertés fondamentales sont universels, indivisibles, interdépendants et indissociables, et qu'il faut les promouvoir et les rendre effectifs en toute équité, sans préjudice de leur mise en oeuvre individuelle,

Soulignant que c'est à l'État qu'incombent la responsabilité première et le devoir de promouvoir et protéger les droits de l'homme et les libertés fondamentales,

Reconnaissant que les individus, groupes et associations ont le droit et la responsabilité de promouvoir le respect des droits de l'homme et des libertés fondamentales et de les faire connaître aux niveaux national et international,

[3] Résolution 217 A (III).
[4] Résolution 2200 A (XXI), annexe.

Déclare:

Article premier

Chacun a le droit, individuellement ou en association avec d'autres, de promouvoir la protection et la réalisation des droits de l'homme et des libertés fondamentales aux niveaux national et international.

Article 2

1. Chaque État a, au premier chef, la responsabilité et le devoir de protéger, promouvoir et rendre effectifs tous les droits de l'homme et toutes les libertés fondamentales, notamment en adoptant les mesures nécessaires pour instaurer les conditions sociales, économiques, politiques et autres ainsi que les garanties juridiques voulues pour que toutes les personnes relevant de sa juridiction puissent, individuellement ou en association avec d'autres, jouir en pratique de tous ces droits et de toutes ces libertés.

2. Chaque État adopte les mesures législatives, administratives et autres nécessaires pour assurer la garantie effective des droits et libertés visés par la présente Déclaration.

Article 3

Les dispositions du droit interne qui sont conformes à la Charte des Nations Unies et aux autres obligations internationales de l'État dans le domaine des droits de l'homme et des libertés fondamentales servent de cadre juridique pour la mise en oeuvre et l'exercice des droits de l'homme et des libertés fondamentales ainsi que pour toutes les activités visées dans la présente Déclaration qui ont pour objet la promotion, la protection et la réalisation effective de ces droits et libertés.

Article 4

Aucune disposition de la présente Déclaration ne peut être interprétée comme portant atteinte aux buts et principes énoncés dans la Charte des Nations Unies ou allant à leur encontre, ni comme apportant des restrictions aux dispositions de la Déclaration universelle des droits de l'homme2, des Pactes internationaux relatifs aux droits de l'homme3 et des autres instruments et engagements internationaux applicables dans ce domaine, ou y dérogeant.

Article 5

Afin de promouvoir et protéger les droits de l'homme et les libertés fondamentales, chacun a le droit, individuellement ou en association avec d'autres, aux niveaux national et international:

a) De se réunir et de se rassembler pacifiquement;

b) De former des organisations, associations ou groupes non gouvernementaux, de s'y affilier et d'y participer;

c) De communiquer avec des organisations non gouvernementales ou intergouvernementales.

Article 6

Chacun a le droit, individuellement ou en association avec d'autres:

a) De détenir, rechercher, obtenir, recevoir et conserver des informations sur tous les droits de l'homme et toutes les libertés fondamentales en ayant notamment accès à l'information quant à la manière dont il est donné effet à ces droits et libertés dans le système législatif, judiciaire ou administratif national;

b) Conformément aux instruments internationaux relatifs aux droits de l'homme et autres instruments internationaux applicables, de publier, communiquer à autrui ou diffuser librement des idées, informations et connaissances sur tous les droits de l'homme et toutes les libertés fondamentales;

c) D'étudier, discuter, apprécier et évaluer le respect, tant en droit qu'en pratique, de tous les droits de l'homme et de toutes les libertés fondamentales et, par ces moyens et autres moyens appropriés, d'appeler l'attention du public sur la question.

Article 7

Chacun a le droit, individuellement ou en association avec d'autres, d'élaborer de nouveaux principes et idées dans le domaine des droits de l'homme, d'en discuter et d'en promouvoir la reconnaissance.

Article 8

1. Chacun a le droit, individuellement ou en association avec d'autres, de participer effectivement, sur une base non discriminatoire, au gouvernement de son pays et à la direction des affaires publiques.

2. Ce droit comporte notamment le droit, individuellement ou en association avec d'autres, de soumettre aux organes et institutions de l'État, ainsi qu'aux organismes s'occupant des affaires publiques, des critiques et propositions touchant l'amélioration de leur fonctionnement, et de signaler tout aspect de leur travail qui risque d'entraver ou empêcher la promotion, la protection et la réalisation des droits de l'homme et des libertés fondamentales.

Article 9

1. Dans l'exercice des droits de l'homme et des libertés fondamentales, y compris le droit de promouvoir et protéger les droits de l'homme visés dans la présente Déclaration, chacun a le droit, individuellement ou en association avec d'autres, de disposer d'un recours effectif et de bénéficier d'une protection en cas de violation de ces droits.

2. À cette fin, toute personne dont les droits ou libertés auraient été violés a le droit, en personne ou par l'entremise d'un représentant autorisé par la loi, de porter plainte et de faire examiner rapidement sa plainte en audience publique par une autorité judiciaire ou toute autre autorité instituée par la loi qui soit indépendante, impartiale et compétente, et d'obtenir de cette autorité une décision, prise conformément à la loi, lui accordant réparation, y compris une indemnisation, lorsque ses droits ou libertés ont été violés, ainsi que l'application de la décision et du jugement éventuel, le tout sans retard excessif.

3. À cette même fin, chacun a le droit, individuellement ou en association avec d'autres, notamment:

a) De se plaindre de la politique et de l'action de fonctionnaires et d'organes de l'État qui auraient commis des violations des droits de l'homme et des libertés fondamentales, au moyen de pétitions ou autres moyens appropriés, auprès des autorités judiciaires, administratives ou législatives nationales compétentes ou de toute autre autorité compétente instituée conformément au système juridique de l'État, qui doit rendre sa décision sans retard excessif;

b) D'assister aux audiences, procédures et procès publics afin de se faire une opinion sur leur conformité avec la législation nationale et les obligations et engagements internationaux applicables;

c) D'offrir et prêter une assistance juridique professionnelle qualifiée ou tout autre conseil et appui pertinents pour la défense des droits de l'homme et des libertés fondamentales.

4. À cette même fin et conformément aux procédures et instruments internationaux applicables, chacun a le droit, individuellement ou en association avec d'autres, de s'adresser sans restriction aux organes internationaux compétents de manière générale ou spéciale pour recevoir et examiner des communications relatives aux droits de l'homme, et de communiquer librement avec ces organes.

5. L'État doit mener une enquête rapide et impartiale ou veiller à ce qu'une procédure d'instruction soit engagée lorsqu'il existe des raisons de croire qu'une violation des droits de l'homme et des libertés fondamentales s'est produite dans un territoire relevant de sa juridiction.

Article 10

Nul ne doit participer à la violation des droits de l'homme et des libertés fondamentales en agissant ou en s'abstenant d'agir quand les circonstances l'exigent, et nul ne peut être châtié ou inquiété pour avoir refusé de porter atteinte à ces droits et libertés.

Article 11

Chacun a le droit, individuellement ou en association avec d'autres, d'exercer son occupation ou sa profession conformément à la loi. Quiconque risque, de par sa profession ou son occupation, de porter atteinte à la dignité de la personne humaine, aux droits de l'homme et aux libertés fondamentales d'autrui doit respecter ces droits et libertés et se conformer aux normes nationales ou internationales pertinentes de conduite ou d'éthique professionnelle.

Article 12

1. Chacun a le droit, individuellement ou en association avec d'autres, de participer à des activités pacifiques pour lutter contre les violations des droits de l'homme et des libertés fondamentales.

2. L'État prend toutes les mesures nécessaires pour assurer que les autorités compétentes protègent toute personne, individuellement ou en association avec d'autres, de toute violence, menace, représailles, discrimination de facto ou de jure, pression ou autre action arbitraire dans le cadre de l'exercice légitime des droits visés dans la présente Déclaration.

3. À cet égard, chacun a le droit, individuellement ou en association avec d'autres, d'être efficacement protégé par la législation nationale quand il réagit par des moyens pacifiques contre des activités et actes, y compris ceux résultant d'omissions, imputables à l'État et ayant entraîné des violations des droits de l'homme et des libertés fondamentales, ainsi que contre des actes de violence perpétrés par des groupes ou individus qui entravent l'exercice des droits de l'homme et des libertés fondamentales.

Article 13

Chacun a le droit, individuellement ou en association avec d'autres, de solliciter, recevoir et utiliser des ressources dans le but exprès de promouvoir et protéger les droits de l'homme et les libertés fondamentales par des moyens pacifiques, conformément à l'article 3 de la présente Déclaration.

Article 14

1. Il incombe à l'État de prendre les mesures appropriées sur les plans législatif, judiciaire, administratif ou autre en vue de mieux faire prendre conscience à toutes les personnes relevant de sa juridiction de leurs droits civils, politiques, économiques, sociaux et culturels.

2. Ces mesures doivent comprendre, notamment:

a) La publication et la large disponibilité des textes de lois et règlements nationaux et des instruments internationaux fondamentaux relatifs aux droits de l'homme;

b) Le plein accès dans des conditions d'égalité aux documents internationaux dans le domaine des droits de l'homme, y compris les rapports périodiques présentés par l'État aux organes créés en vertu d'instruments internationaux relatifs aux droits de l'homme auxquels il est partie, ainsi que les comptes rendus analytiques de l'examen des rapports et les rapports officiels de ces organes.

3. L'État encourage et appuie, lorsqu'il convient, la création et le développement d'autres institutions nationales indépendantes pour la promotion et la protection des droits de l'homme et des libertés fondamentales dans tout territoire relevant de sa juridiction, qu'il s'agisse d'un médiateur, d'une commission des droits de l'homme ou de tout autre type d'institution nationale.

Article 15

Il incombe à l'État de promouvoir et faciliter l'enseignement des droits de l'homme et des libertés fondamentales à tous les niveaux de l'enseignement et de s'assurer que tous ceux qui sont chargés de la formation des avocats, des responsables de l'application des lois, du personnel des forces armées et des agents de la fonction publique incluent dans leurs programmes de formation des éléments appropriés de l'enseignement des droits de l'homme.

Article 16

Les individus, organisations non gouvernementales et institutions compétentes ont un rôle important à jouer pour ce qui est de sensibiliser davantage le public aux questions relatives à tous les droits de l'homme et à toutes les libertés fondamentales, en particulier dans le cadre d'activités d'éducation, de formation et de recherche dans ces domaines en vue de renforcer encore, notamment, la compréhension, la tolérance, la paix et les relations amicales entre les nations ainsi qu'entre tous les groupes raciaux et religieux, en tenant compte de la diversité des sociétés et des communautés dans lesquelles ils mènent leurs activités.

Article 17

Dans l'exercice des droits et libertés visés dans la présente Déclaration, chacun, agissant individuellement ou en association avec d'autres, n'est soumis qu'aux limitations fixées conformément aux obligations internationales existantes et établies par la loi exclusivement en vue d'assurer la reconnaissance et le respect des droits et libertés d'autrui et afin de satisfaire aux justes exigences de la morale, de l'ordre public et du bien-être général dans une société démocratique.

Article 18

1. Chacun a des devoirs envers la communauté et au sein de celle-ci, seul cadre permettant le libre et plein épanouissement de sa personnalité.

2. Les individus, groupes, institutions et organisations non gouvernementales ont un rôle important à jouer et une responsabilité à assumer en ce qui concerne la sauvegarde de la démocratie, la promotion des droits de l'homme et des libertés fondamentales ainsi que la promotion et le progrès de sociétés, institutions et processus démocratiques.

3. Les individus, groupes, institutions et organisations non gouvernementales ont également un rôle important à jouer et une responsabilité à assumer pour ce qui est de contribuer, selon qu'il convient, à la promotion du droit de chacun à un ordre social et international grâce auquel les droits et libertés énoncés dans la Déclaration universelle des droits de l'homme et les autres instruments relatifs aux droits de l'homme peuvent être réalisés dans leur intégralité.

Article 19

Aucune disposition de la présente Déclaration ne peut être interprétée comme impliquant pour un individu, groupe ou organe de la société, ou pour un État, le droit de se livrer à une activité ou d'accomplir un acte visant à détruire des droits et libertés visés dans la présente Déclaration.

Article 20

Aucune disposition de la présente Déclaration ne peut être interprétée comme autorisant les États à soutenir ou encourager les activités d'individus, groupes, institutions ou organisations non gouvernementales allant à l'encontre des dispositions de la Charte des Nations Unies.

ANNEXE II

CONSEIL DE L'UNION EUROPÉENNE

Bruxelles, le 10 juin 2009
16332/2/08
REV 2

PESC 1562
COHOM 138

NOTE

Objet: Garantir la Protection - Orientations de l'Union Européenne concernant les Défenseurs des Droits de l'Homme.

I. OBJET

1. Le soutien des défenseurs des droits de l'homme fait, de longue date, partie intégrante de la politique extérieure de l'Union européenne en matière de droits de l'homme. Les présentes orientations visent à faire des suggestions concrètes permettant d'améliorer l'action de l'UE dans ce domaine. Ces orientations peuvent être utilisées dans les contacts avec les pays tiers, à tous les niveaux, ainsi que dans les enceintes multilatérales compétentes en matière de droits de l'homme, afin d'appuyer et de renforcer les efforts que déploie actuellement l'Union pour promouvoir et encourager le respect du droit à défendre les droits de l'homme. Elles prévoient également des interventions de l'Union en faveur des défenseurs des droits de l'homme qui sont menacés et proposent des moyens concrets de les soutenir et de leur prêter assistance.

Un élément majeur des présentes orientations est le soutien apporté aux procédures spéciales du Conseil des droits de l'homme des Nations Unies, notamment au Rapporteur spécial sur les défenseurs des droits de l'homme et à des mécanismes régionaux appropriés de protection des défenseurs des droits de l'homme. Ces orientations aideront par ailleurs les missions de l'UE (ambassades et consulats des États membres de l'UE et délégations de la Commission européenne) à définir leur approche à l'égard des défenseurs des droits de l'homme. Bien qu'elles aient pour principal objectif de traiter de problèmes spécifiques relatifs aux défenseurs des droits de l'homme, les présentes orientations contribuent également au renforcement de la politique de l'UE en matière de droits de l'homme dans son ensemble.

II. DÉFINITION

2. Aux fins des présentes orientations, la définition des défenseurs des droits de l'homme se fonde sur l'article premier du dispositif de la "Déclaration sur le droit et la responsabilité des individus, groupes et organes de la société de promouvoir et protéger les droits de l'homme et les libertés fondamentales universellement reconnus" (voir annexe I), qui dispose que "Chacun a le droit, individuellement ou en association avec d'autres, de promouvoir la protection et la réalisation des droits de l'homme et des libertés fondamentales aux niveaux national et international".

3. Les défenseurs des droits de l'homme sont des individus, groupes et organes de la société qui promeuvent et protègent les droits de l'homme et les libertés fondamentales universellement reconnus. Les défenseurs des droits de l'homme s'emploient à promouvoir et à protéger les droits civils et politiques et à promouvoir, à protéger et à mettre en oeuvre les droits économiques, sociaux et culturels. Ils promeuvent et protègent également les droits des membres de groupes tels que les communautés autochtones. Cette définition n'inclut pas les individus ou les groupes qui commettent des actes de violence ou propagent la violence.

III. INTRODUCTION

4. L'UE appuie les principes qui figurent dans la Déclaration sur le droit et la responsabilité des individus, groupes et organes de la société de promouvoir et protéger les droits de l'homme et les libertés fondamentales universellement reconnus. Bien que la responsabilité première de la promotion et de la protection des droits de l'homme incombe aux différents États, l'UE constate que les indi-

vidus, les groupes et les organes de la société contribuent tous de manière significative à promouvoir la cause des droits de l'homme. En particulier, les défenseurs des droits de l'homme:

- mettent en évidence les violations;
- leur apportant une aide juridique, psychologique, médicale ou autre; et
- combattent les cultures d'impunité qui servent à masquer les violations systématiques et répétées des droits de l'homme et des libertés fondamentales;
- diffusent la culture des droits de l'Homme et les informations relatives aux défenseurs des droits de l'Homme au niveau local, régional et international.

5. Le travail des défenseurs des droits de l'homme les amène souvent à critiquer les politiques et les actions des gouvernements. Ces derniers ne devraient cependant pas considérer que cela leur porte préjudice. En effet, le principe d'un champ laissé à l'expression d'une pensée indépendante et à un libre débat sur les politiques et les actions d'un gouvernement est fondamental et constitue un moyen éprouvé d'améliorer le niveau de protection des droits de l'homme. Les défenseurs des droits de l'homme peuvent aider les gouvernements à promouvoir et à protéger les droits de l'homme. En participant aux processus de consultation, ils peuvent contribuer de manière significative à l'élaboration de la législation correspondante et à la définition de stratégies et de programmes nationaux en matière de droits de l'homme. Il convient également de reconnaître et de soutenir ce rôle.

6. L'UE constate que les activités des défenseurs des droits de l'homme ont acquis une plus grande reconnaissance au fil des ans. Les défenseurs des droits de l'homme sont parvenus à garantir une meilleure protection aux victimes de violations. Néanmoins, le prix de ce succès est élevé: les défenseurs eux-mêmes deviennent de plus en plus souvent la cible d'attaques et leurs droits sont bafoués dans de nombreux pays. L'UE estime qu'il importe de veiller à la sécurité des défenseurs des droits de l'homme et de protéger leurs droits. À cet égard, il y a lieu d'intégrer le souci d'équité entre les sexes dans le traitement de la question des défenseurs des droits de l'homme.

IV. ORIENTATIONS OPÉRATIONELLES

7. Le volet opérationnel des présentes orientations a pour but de définir les moyens d'œuvrer efficacement, dans le cadre de la politique étrangère et de sécurité commune, en faveur de la promotion et de la protection des défenseurs des droits de l'homme.

Suivi, élaboration de rapports et évaluation

8. Les chefs de mission de l'UE sont d'ores et déjà invités à présenter des rapports périodiques sur la situation en matière de droits de l'homme dans leur pays d'accréditation. Le Groupe "Droits de l'homme" du Conseil (COHOM) a approuvé les grandes lignes de fiches descriptives destinées à faciliter cette tâche. Ces fiches prévoient que, dans leurs rapports, les missions devraient traiter de la situation des défenseurs des droits de l'homme, en précisant notamment les éventuelles menaces ou attaques dont ces derniers font l'objet. À cet égard, les chefs de mission devraient garder à l'esprit que le cadre institutionnel peut avoir une incidence majeure sur la possibilité qu'ont les défenseurs des droits de l'homme d'effectuer leur travail en toute sécurité. Les mesures législatives, judiciaires, administratives et les autres mesures appropriées prises par les États pour protéger toute personne de toute violence, menace, représailles, discrimination de facto ou de jure, pression ou autre action arbitraire dans le cadre de l'exercice légitime des droits visés dans la Déclaration des Nations Unies sur les défenseurs des droits de l'homme sont toutes pertinentes à cet égard.

9. Les chefs de mission de l'UE sont invités à traiter de la situation des défenseurs des droits de l'Homme à l'occasion des réunions des groupes de travail locaux sur les droits de l'Homme. Le cas échéant, les chefs de mission devraient faire des recommandations au Groupe "Droits de l'homme" en vue d'éventuelles actions de l'UE, condamnant notamment les menaces et les attaques à l'encontre des défenseurs des droits de l'homme, et en vue de démarches et de déclarations publiques dans les situations où les défenseurs des droits de l'homme courent un risque immédiat ou grave. Les chefs de mission peuvent décider de mener une action locale urgente afin de soutenir des défenseurs des droits de l'Homme qui courent un risque immédiat ou grave, et de faire rapport de leur action au Groupe "Droits de l'homme" et autres groupes de travail pertinents en formulant des recommandations sur les possibilités de suivi de l'action européenne. Dans leurs rapports, les chefs de mission devraient également examiner l'efficacité des actions entreprises par l'UE. De plus, les missions devraient porter une attention particulière aux risques spécifiques des femmes défenseurs des droits de l'Homme.

10. Sur la base des rapports des chefs de mission et d'autres informations pertinentes, telles que les rapports et les recommandations du Rapporteur spécial sur les défenseurs des droits de l'homme, des autres Rapporteurs spéciaux des Nations Unies, des organes de suivi des traités, du Commissaire aux droits de l'Homme du Conseil de l'Europe et des organisations non gouvernementales, le Groupe "Droits de l'homme" et les autres groupes compétents pourront identifier les situations où l'UE est appelée à intervenir, décider des actions à entreprendre ou, le cas échéant, faire des recommandations d'actions au COPS/Conseil.

Rôle des missions de l'UE dans le soutien et la protection des défenseurs des droits de l'homme

11. Dans de nombreux pays tiers, les missions de l'UE (ambassades des États membres de l'UE et délégations de la Commission européenne) constituent la principale interface entre l'Union et ses États membres et les défenseurs des droits de l'homme sur le terrain. Elles ont donc un rôle important à jouer dans la concrétisation de la politique de l'UE à l'égard des défenseurs des droits de l'homme, Les missions de l'UE devraient donc s'employer à adopter une approche anticipatoire à l'égard des défenseurs des droits de l'homme. Elles devraient parallèlement garder à l'esprit que, dans certains cas, une action de l'UE peut entraîner des menaces ou des attaques à l'encontre de ces défenseurs. Les missions de l'UE devraient donc, le cas échéant, discuter avec les défenseurs des droits de l'homme des actions envisageables. Si des actions devaient être entreprises au nom de l'UE, les missions de l'UE devraient s'assurer que le défenseur des droits de l'Homme concerné et/ou sa famille en soient informés. Les missions de l'UE pourraient par exemple prendre les mesures suivantes:

• élaborer des stratégies locales de mise en oeuvre de ces lignes directrices, en portant une attention particulière pour les femmes défenseurs des droits de l'Homme. Les missions de l'UE garderont à l'esprit que ces lignes directrices portent sur les défenseurs qui promeuvent et protègent les droits de l'Homme, qu'ils soient civils, culturels, économiques, politiques ou sociaux. Les missions de l'UE devront s'employer à impliquer activement les défenseurs des droits de l'Homme et leurs organisations dans l'élaboration et le suivi de la mise en oeuvre des stratégies locales.

• organiser au moins une réunion annuelle réunissant défenseurs des droits de l'Homme et diplomates afin de discuter, entre autres, de la situation locale des droits de l'Homme, de la politique de l'UE mise en oeuvre à ce sujet et de l'application de la stratégie locale des lignes directrices de l'UE sur les défenseurs des droits de l'Homme;

• agir en coopération étroite et échanger des informations sur les défenseurs des droits de l'homme, y compris sur ceux qui sont en danger;

• entretenir des contacts appropriés avec les défenseurs des droits de l'homme, y compris en les recevant dans les missions et en se rendant dans les zones où ils travaillent, la désignation d'officiers de liaison spécifiques, éventuellement sur la base d'un partage des tâches, pouvant être examinée à cette fin;

• apporter, selon les besoins, une reconnaissance visible aux défenseurs des droits de l'homme et à leurs travaux par un recours approprié aux médias y compris Internet et les nouvelles technologies de l'information et de la communication, à la publicité, à des visites ou à des invitations notamment pour remettre les prix qui leurs sont décernés;

• le cas échéant, rendre visite aux défenseurs des droits de l'homme en détention préventive ou assignés à résidence et assister en tant qu'observateurs à leurs procès.

Promotion du respect des défenseurs des droits de l'homme dans les relations avec les pays tiers et au sein des enceintes multilatérales

12. L'UE vise à inciter les pays tiers à satisfaire à leur obligation de respecter les droits des défenseurs des droits de l'homme et à protéger ces derniers d'attaques et de menaces émanant d'acteurs non étatiques. Dans ses contacts avec les pays tiers, l'UE indiquera, lorsqu'elle le jugera nécessaire, qu'il est impératif que tous les pays respectent et observent les normes internationales dans ce domaine, notamment la déclaration susmentionnée des Nations Unies. L'objectif général devrait être de créer un environnement où les défenseurs des droits de l'homme peuvent accomplir librement leur tâche. L'UE fera connaître ses objectifs en tant qu'éléments intrinsèques de sa politique en matière de droits de l'homme et soulignera l'importance qu'elle accorde à la protection des défenseurs des droits de l'homme. Parmi les actions à l'appui de ces objectifs figureront notamment les suivantes:

• le cas échéant, dans le cadre-même de leurs missions dans des pays tiers, la présidence, le Haut Représentant pour la politique étrangère et de sécurité commune, le Représentant personnel du SG/HR pour les droits de l'Homme, les représentants ou les envoyés spéciaux de l'UE, les représen-

tants des Etats membres et ceux de la Commission européenne participeront à des réunions avec des défenseurs des droits de l'homme, au cours desquelles seront évoqués des cas individuels et les questions soulevées par les travaux des défenseurs des droits de l'Homme;

• dans son volet consacré aux droits de l'homme, le dialogue politique de l'UE avec les pays tiers et les organisations régionales s'attachera notamment, le cas échéant, à la situation des défenseurs des droits de l'homme. L'UE soulignera l'appui qu'elle apporte aux défenseurs des droits de l'homme et à leur action et abordera, si nécessaire, des cas individuels préoccupants. L'UE prendra soin d'associer les défenseurs des droits de l'Homme, selon les modalités les plus appropriées, à la préparation, au suivi et à l'évaluation du dialogue conformément aux lignes directrices de l'UE en matière de dialogues sur les droits de l'Homme;

• les chefs de Missions de l´UE et les Ambassades de l'UE rappelleront aux autorités des pays tiers leur obligation de mettre en place des mesures efficaces de protection des défenseurs des droits de l´homme qui sont ou qui risquent d'être en danger;

• travailler en étroite coopération avec d'autres pays partageant la même optique, en particulier au sein du Conseil des droits de l'homme des Nations Unies et de l'Assemblée générale de l'ONU;

• recommander, le cas échéant, aux pays lors de leur passage à l'Examen Périodique Universel du Conseil des droits de l'Homme de mettre leurs législations et pratiques en conformité avec la Déclaration des Nations Unies sur les défenseurs des droits de l'Homme;

• promouvoir le renforcement des mécanismes régionaux existants visant à protéger les défenseurs des droits de l'homme, tels que le point focal sur les défenseurs des droits de l'Homme et les institutions nationales des droits de l'Homme du Bureau pour les institutions démocratiques et les droits de l'Homme de l'OSCE, le Commissaire aux droits de l'Homme du Conseil de l'Europe, le Rapporteur spécial sur la situation des défenseurs des droits de l'homme de la Commission africaine des droits de l'homme et des peuples et l'unité spéciale "défenseurs des droits de l'homme" de la Commission interaméricaine des droits de l'homme, ainsi que la création de mécanismes appropriés dans des régions où il n'en existe pas.

Soutien des procédures spéciales du Conseil des droits de l'homme des Nations Unies, notamment du Rapporteur spécial sur les défenseurs des droits de l'homme

13. L'UE constate que les procédures spéciales du Conseil des droits de l'homme des Nations Unies (et les personnes ou groupes auxquels elles sont assignées: rapporteurs spéciaux, représentants spéciaux, experts indépendants et groupes de travail) apportent un soutien décisif aux efforts déployés au plan international pour protéger les défenseurs des droits de l'homme, en raison de leur indépendance et de leur impartialité ainsi que de leur capacité à agir, à dénoncer les violations dont sont victimes les défenseurs des droits de l'homme à l'échelle mondiale et à effectuer des visites dans les pays concernés. Bien que le Rapporteur spécial sur les défenseurs des droits de l'homme ait un rôle particulier à jouer à cet égard, les mandats relatifs aux autres procédures spéciales concernent également les défenseurs des droits de l'homme. Parmi les actions de l'UE à l'appui des procédures spéciales figureront notamment les suivantes:

• encourager les États à accepter par principe les demandes visant à effectuer une visite dans leur pays dans le cadre des procédures spéciales des Nations Unies;

• promouvoir, par l'intermédiaire des missions de l'UE, l'utilisation des mécanismes thématiques des Nations Unies par des communautés locales agissant dans le domaine des droits de l'homme et par des défenseurs des droits de l'homme, y compris, sans se limiter à cet aspect, faciliter l'instauration de contacts avec les mécanismes thématiques et les défenseurs des droits de l'homme ainsi que l'échange d'informations entre ceux-ci;

• étant donné qu'il est impossible de remplir les missions assignées dans le cadre des procédures spéciales en l'absence de ressources adéquates, les États membres de l'UE soutiendront l'octroi de fonds suffisants, provenant du budget général, au Haut Commissariat des Nations Unies aux droits de l'homme.

Mesures concrètes de soutien aux défenseurs des droits de l'homme, notamment dans le cadre de la politique de développement

14. Les programmes de l'Union européenne et des États membres qui visent à contribuer à la mise en place de processus et d'institutions démocratiques et à promouvoir et à protéger les droits de l'homme dans les pays en développement tel que l'Instrument Européen pour la Démocratie et les

droits de l'Homme appartiennent au large éventail des mesures concrètes de soutien aux défenseurs des droits de l'homme. Ces programmes peuvent comprendre, sans nécessairement s'y limiter, les programmes de coopération au développement des États membres. Parmi ces mesures concrètes figurent notamment les suivantes:

• soutenir les défenseurs des droits de l'homme ainsi que les ONG qui promeuvent et protègent les activités des défenseurs des droits de l'Homme au moyen, par exemple, d'activités visant au renforcement des capacités ou de campagnes de sensibilisation et faciliter la coopération entre les ONG, les défenseurs des droits de l'Homme et les institutions nationales de défense des droits de l'Homme;

• favoriser et soutenir l'établissement et l'action d'instances nationales de promotion et de protection des droits de l'homme créées en conformité avec les principes de Paris, notamment les institutions nationales de défense des droits de l'homme, les bureaux du médiateur et les commissions des droits de l'homme;

• participer à la création de réseaux de défenseurs des droits de l'homme à l'échelle internationale, notamment en facilitant l'organisation de réunions entre ces défenseurs à l'intérieur comme à l'extérieur de l'UE;

• chercher à s'assurer que les défenseurs des droits de l'homme dans les pays tiers ont accès à des ressources, y compris financières, provenant de l'étranger et qu'ils sont informés de la disponibilité de ces ressources et des moyens de les demander;

• s'assurer que les programmes d'éducation aux droits de l'homme promeuvent, entre autres, la Déclaration sur les défenseurs des droits de l'homme;

• prévoir des mesures rapides pour aider et protéger les défenseurs des droits de l'Homme en danger dans des pays tiers, comme par exemple, lorsque cela s'avère opportun, en délivrant des visas d'urgence et en favorisant leur accueil provisoire dans les Etats membres de l'UE.

Rôle des groupes du Conseil

15. Conformément à son mandat, le Groupe "Droits de l'homme" supervisera la mise en oeuvre et le suivi des présentes orientations concernant les défenseurs des droits de l'homme, en coordination et coopération étroites avec d'autres groupes compétents du Conseil. Cette action consistera en particulier:

• à promouvoir l'intégration de la question des défenseurs des droits de l'homme dans les politiques et les actions pertinentes de l'UE;

• à examiner à intervalles appropriés la mise en oeuvre de ces orientations;

• continuer de rechercher, le cas échéant, d'autres moyens de coopération avec les Nations Unies et d'autres mécanismes internationaux et régionaux de soutien aux défenseurs des droits de l'homme;

• à faire rapport au Conseil, par l'intermédiaire du COPS et du Coreper, le cas échéant tous les ans, sur les progrès réalisés sur la voie de la mise en oeuvre des présentes orientations.

ANNEXE I

Déclaration sur le droit et la responsabilité des individus, groupes et organes de la société de promouvoir et protéger les droits de l'homme et les libertés fondamentales universellement reconnus.

Annexe à l'annexe I
Instruments internationaux pertinents

- la Déclaration universelle des droits de l'homme
- le Pacte international relatif aux droits civils et politiques
- le Pacte international relatif aux droits économiques, sociaux et culturels
- la Convention contre la torture et autres peines ou traitements cruels, inhumains ou dégradants
- la Convention relative aux droits de l'enfant
- la Convention sur l'élimination de toutes les formes de discrimination à l'égard des femmes
- la Convention internationale sur l'élimination de toutes les formes de discrimination raciale
- la Convention européenne des droits de l'homme et ses protocoles ainsi que la jurisprudence de la Cour européenne des droits de l'homme en la matière
- la Charte sociale européenne/la Charte sociale européenne (révisée)
- la Charte africaine des droits de l'homme et des peuples
- la Convention américaine des droits de l'homme
- les Conventions de Genève pour la protection des victimes de la guerre et leurs protocoles ainsi que les règles coutumières du droit humanitaire applicables aux conflits armés
- la Convention de 1951 relative au statut des réfugiés et son protocole de 1967
- le Statut de Rome de la Cour pénale internationale
- la Déclaration sur le droit et la responsabilité des individus, groupes et organes de la société de promouvoir et de protéger les droits de l'homme et les libertés fondamentales universellement reconnus

Déclaration sur le droit et la responsabilité des individus, groupes et organes de la société de promouvoir et protéger les droits de l'homme et les libertés fondamentales universellement reconnus

Le 20 novembre 2009, Le troisième Comité de l'Assemblée générale des Nations Unies a adopté une résolution sur les défenseurs des droits humains. Elle exprime son inquiétude quant à la situation précaire des défenseurs dans le monde et invite à adopter des mesures efficaces pour prévenir et éliminer les violations des des droits humains dont sont victimes les défenseurs.

Cf. http://protectionline.org/Document-de-la-Commission-de-DH.html

ANNEXE III

PI formule les recommandations de plaidoyer suivantes pour les DDH en lien avec les missions de l'UE, les ambassades des États membres de l'UE et les représentants spéciaux de l'UE (plus de renseignements sur http://www.protectionline.org)

Depuis l'adoption de la déclaration des Nations Unies de 1998, les mécanismes suivants ont été mis en place pour protéger les défenseurs dans le monde entier:

- **Le mandat du représentant spécial du secrétaire général sur les défenseurs des droits de l'homme**, créé par la Commission des droits de l'homme des Nations Unies.
- Le mandat du **rapporteur spécial de la Commission africaine des droits de l'homme et des peuples**.
- **La résolution sur la protection des défenseurs des droits de l'homme en Afrique** adoptée par la Commission africaine des droits de l'homme et des peuples (ACHPR) lors de sa 35è session ordinaire tenue du 21 mai au 4 juin 2004, à Banjul en Gambie.
- L'**Unité des défenseurs des droits humains de la Commission interaméricaine des droits de l'homme.**
- **Les Lignes directrices sur les défenseurs des droits humains** adoptées en 2004 par l'Union Européenne qui constituent un outil que les missions doivent en principe mettre en oeuvre pour protéger les défenseurs dans des pays tiers.
- La déclaration du conseil des ministres pour la protection renforcée des défenseurs des droits humains adoptée parle **Conseil de l'Europe** le **18 février 2008**.
- **La Commission asiatique des droits de l'homme (AHRC)**.

En 2004, le conseil des ministres de l'UE a adopté les Lignes directrices de l'UE sur les défenseurs des droits humains. Elles réitèrent le contenu de la déclaration des Nations Unies sur les défenseurs des droits humains et adressent des recommandations spécifiques à toutes les missions de l'UE et aux États membres de l'UE. Les recommandations de l'UE visent à:

- adopter des politiques proactives pour la protection des défenseurs des droits humains.
- utiliser les moyens diplomatiques pour obtenir l'engagement du respect intégral des droits des défenseurs des droits humains de la part des gouvernements locaux et nationaux concernés.

Les lignes directrices de l'UE sont également disponibles auprès des bureaux de l'UE et des ambassades des États membres.

Les missions de l'UE (les ambassades des États membres et les délégations de la Commission Européenne de l'UE) constituent le premier point de contact entre les organes de l'UE, les États membres de l'UE et les défenseurs des droits humains locaux.

C'est pourquoi PI recommande au minimum que les défenseurs des droits humains:

- demandent que les lignes directrices de l'UE soient traduites dans la langue des défenseurs des droits humains et distribuées aux organisations de défenseurs et aux autorités locales et nationales.
- envoient des mises à jour régulières concernant leur situation aux chefs de mission de l'UE (CDM) et aux ONG nationales et internationales afin d'accroître la notoriété de leur travail et d'intensifier la coordination entre les acteurs de protection.
- maintiennent un contact régulier avec les missions de l'UE pour être informés sur les lignes directrices de l'UE et des initiatives des missions de l'UE pour la protection des défenseurs. Ce contact régulier permettra aux missions de l'UE d'être au courant à la fois de la situation des défenseurs des droits humains et de leurs recommandations sur les mesures de protection et de soutien.
- demandent aux missions de l'UE de partager et de mettre en oeuvre une pratique cohérente en matière de protection et de stratégies à moyen terme.
- invitent les chefs de mission de l'UE ou les inspecteurs des droits humains à visiter les zones de travail des défenseurs des droits humains, particulièrement là où il sont exposés à un risque accru (par exemple dans les zones de conflit ou les endroits où les défenseurs ont déjà été victimes de menaces ou d'attaques).
- demandent une intervention d'urgence lorsque les défenseurs sont menacés ou arrêtés.
- demandent à ce que les défenseurs exposés au risque aient accès à des endroits sûrs et obtiennent un soutien intégral.
- sollicitent ou acceptent des invitations ainsi que le soutien des missions de l'UE une fois que les défenseurs auront procédé à une évaluation du risque découlant de l'augmentation de leur notoriété. Il est recommandé qu'ils mettent en exergue les conséquences possibles des questions de sécurité et demandent un soutien en matière de protection.
- demandent l'assistance et l'observation par des chefs de mission de l'UE en cas de procès contre les défenseurs des droits humains (cela peut favoriser voire garantir un procès juste et équitable, mais une présence pendant toute la durée de la procédure est nécessaire, soit à partir de la lecture des chefs d'accusation jusqu'à la proclamation de la peine, afin de s'assurer de l'indépendance du tribunal); Qu'ils demandent aux observateurs de l'UE de communiquer avec les défenseurs des droits humains accusés; Qu'ils emandent à ce que des observateurs de l'UE soient présents au procès contre des auteurs de violations des droits humains afin d'éviter que leurs crimes restent impunis.
- soient à jour des visites du pays des défenseurs des droits humains par la présidence de l'UE, PESC - le haut représentant pour la politique étrangère et de sécurité commune, les représentants spéciaux ou les membres de la commission de l'UE, et qu'ils demandent à les rencontrer.
- demandent à ce que la situation des défenseurs des droits humains soit incluse dans l'ordre du jour de la politique de dialogue entre l'UE et les organisations régionales et nationales du pays dans lequel se trouvent les défenseurs des droits humains.
- demandent à ce que les actions politiques avec d'autres acteurs de protection soient coordonnées, particulièrement avec la Commission des droits de l'homme des Nations Unies et l'Assemblée générale des Nations Unies. Il est recommandé qu'ils exigent une coordination avec les organes régionaux pour la protection des droits humains et des défenseurs des droits humains, tels que la Commission africaine des droits de l'homme et des peuples, l'Unité des défenseurs des droits humains de

la Commission interaméricaine des droits de l'homme, la Commission asiatique des droits de l'homme.

- demandent à ce que les rapports des chefs de mission de l'UE soient publics et accessibles aux défenseurs des droits humains.

Recherche de fonds

Les défenseurs des droits humains peuvent collecter des fonds directement auprès des ambassades (programmes de droits humains) et auprès de l'UE à travers l'instrument européen pour la démocratie et les droits de l'homme (IEDDH). L'IEDDH permet à la commission européenne de financer les ONG sans l'accord du gouvernement des pays tiers. (http://ec.europa.eu/europeaid/where/worldwide/eidhr/index_fr.htm ou taper simplement IEDDH dans). Vous trouverez plus d'informations concernant les instruments de financement au même endroit.

De plus:

Bien que les lignes directrices de l'UE couvrent les missions de l'UE, les institutions de l'UE, ses États membres ainsi que leurs ambassades, les défenseurs des droits humains doivent se rappeler qu'un soutien peut également être obtenu par le biais des autres corps diplomatiques et d'autres organisations internationales, puisque la déclaration des Nations Unies sur les défenseurs des droits humains, adoptée par consensus, peut et doit être utilisée par tous les acteurs de protection.

ANNEX IV

Aperçu Général du Risque selon les Profils Spécifiques de Défenseurs des Droits Humains

Objectif:

Définir le risque en fonction du profil spécifique du DDH, de manière àle prendre en compte lors de l'élaboration des plans de sécurité / protection et lors de la promotion d'une politique organisationnelle.

Au-delà des risques communs auxquels sont confrontés tous les défenseurs des droits humains, le chapitre 1.9 illustre comment les spécificités propres à certains groupes de défenseurs doivent être prises en compte au moment de l'élaboration d'un plan de sécurité / protection, que ce soit au niveau individuel, organisationnel ou inter organisationnel.

Le manuel ne peut être exhaustif et explorer tous les profils spécifiques de DDH travaillant dans des contextes politiques différents. Chaque groupe ou situation mériterait que lui soit consacré au moins un chapitre entier, pour ne pas dire un manuel de protection à part entière: institutions religieuses; communautés indigènes; groupes travaillant sur les droits économiques, sociaux et culturels; groupes travaillant sur les droits des enfants; avocats et juristes; journalistes; organisations rurales; environnementalistes; syndicalistes; minorités; LGBTI[1]; …

De plus, cela impliquerait un besoin continu de mise à jour dans la mesure où le contexte politique est dynamique, de même que le risque.

Cependant, il ne faut pas perdre de vue que la logique sous-jacente de l'analyse du risque reste la même pour tous les DDH, groupes et individus. Elle doit juste être mise en œuvre en intégrant les profils spécifiques des DDH et les menaces auxquelles ils sont confrontés, leurs vulnérabilités et leurs capacités.

Le tableau ci-après reprend, de façon non exhaustive, la manière dont chaque donnée spécifique peut être illustrée grâce à un brainstorming. Il peut être considéré comme un point de départ que chaque groupe de DDH devra approfondir et détailler, dans la mesure où chaque élément peut recouvrir des réalités diverses.

Par exemple, les institutions et réseaux religieux peuvent être chrétiens (catholiques, apostoliques, évangélistes, mormons, quakers, …), islamiques (sunnites, chiites, soufis, …), hindous, bouddhistes, juives, etc.; ils peuvent travailler dans des zones urbaines ou rurales; dans des contextes politiques plus ou moins orientés sur les droits humains; sur des sujets plus ou moins controversés; etc.

Une même menace peut prendre des formes différentes, par exemples des menaces d'agression peuvent viser des personnes, des équipements, etc.

Pour chacun des profils, le tableau 3 (pages 32-35) doit être utilisé pour compléter les informations.

[1] Manuel de protection pour les défenseurs LGBTI, PI©2009

Aperçu Général du Risque selon les Profils Spécifiques de Défenseurs des Droits Humains (non exhaustif)

Profils	Domaine d'activité	Menaces liées au travail/impact	Vulnérabilités / Capacités
Réseaux Religieux	• Droits humains, Droit humanitaire international, sécurité alimentaire et valeurs religieuses • Groupe interconfessionnel • (…)	• Discrédit quand étiquetés comme " soutien de groupes armés illégaux " • Agressions du fait de l'étiquette • (…)	• Isolement géographique • Manque de soutien institutionnel • Accès aux réseaux • Travail sur la base d'un élément de convergence (foi religieuse) • (…)
Organisations de droits économiques, sociaux et culturels	• Développement de capacités aux niveaux individuel et organisationnel • Sécurité alimentaire, gestion environnementale et protection, projets agraires, éducation • Identité et droit des minorités • (…)	• Le renforcement organisationnel met à mal l'hégémonie des acteurs armés • Embargos économiques • Infiltration • (…)	• Exposition aux acteurs armés dans les régions où ils travaillent • Isolement géographique • Accès à des réseaux traitant des sujets similaires souvent moins problématiques que dans d'autres domaines des droits humains comme, par exemple, les prisonniers politiques • Accès à l'acceptation dans la mesure où leur travail génère des bénéfices immédiats pour les communautés locales • (…)
Organisations d'avocats ou de juristes	• Défense des DH, souvent par le biais de cas emblématiques • Formation aux DH • Lutte contre l'impunité et pour l'observation de procès • Consultations juridiques et politiques • Dénonciations publiques des violations des DH • Campagnes politiques thématiques • (…)	• Discrédit • Criminalisation • Harcèlement judiciaire • Atteintes à leur image sociale • Infiltrations • (…)	• Distance des autorités civiles et politiques • Soutien politique interne limité • Profil institutionnel relativement élevé • Soutien institutionnel • Accès à des réseaux homologues internationaux • (…)
Institutions religieuses	• Assistance humanitaire • (…)	• Stigmatisation et persécution • (…)	• Exposition • Excès de confiance (volonté divine / protection divine / réincarnation / …) • Légitimation • Réseaux et ressources - Crédibilité • Incidence / influence politique • Hiérarchie • Identité idéologique • (…)

Aperçu Général du Risque selon les Profils Spécifiques de Défenseurs des Droits Humains (non exhaustif)

Profils	Domaine d'activité	Menaces liées au travail/impact	Vulnérabilités / Capacités
Communautés rurales	• Revendication et récupération de la terre • (…)	• Contrôle territorial par des tiers • Déplacement ou confinement • Intimidation par de puissants propriétaires terriens • (…)	• Isolement • Faible leadership • Pauvreté • Compétences pour cultiver les produits • Connaissance du terrain • Compétences organisationnelles • Accès difficile à l'information et à l'éducation • Accès difficile à l'électricité et à l'eau • Territoires agricoles partagés • Intérêts et composition hétérogènes • (…)
Syndicats	• Droits humains liés au travail • (…)	• Discrédit et criminalisation • Licenciements • (…)	• Organisation sociale mondiale avec adhésion déclarée • Exposés à une attitude de protagonistes • Parti pris politique • Travaillent en réseau • Capacité à mobiliser un grand nombre de personnes (militants ou non) • Capacité d'influence dans des domaines clés économiques et sociaux • Reconnaissance sociale • Peu disposés à travailler avec les DDH • Identité politique • Structure hiérarchique • (…)
Journalistes	• Enquêtes et publications sur les violations des DH • (…)	• Discrédit • Agressions • Attaque • Perte de matériel • Perte d'information • Obstructionnisme de la part des média officiels • (…)	• Exposés à la corruption et aux grands groupes de presse • Accès aux réseaux internationaux et aux associations professionnelles de journalistes • Accès aux média • Image publique • Chiens de garde de la démocratie • Individus • (…)

Aperçu Général du Risque selon les Profils Spécifiques de Défenseurs des Droits Humains (non exhaustif)

Profils	Domaine d'activité	Menaces liées au travail/impact	Vulnérabilités / Capacités
LGBTI	• Droits des LGBTI • (…)	• Dénigrement, discrédit et criminalisation • Campagnes publiques anti-LGBTI • Législation anti-LGBTI • (…)	• Exposés à des préjugés moraux / religieux / culturels / sociaux • Accès aux réseaux internationaux • Souvent exclus par les autres DDH • Parfois profil bas • Promotion de leurs droits difficile • Transversal à toutes les organisations de DDH • Facilement reconnaissables • Exposés à l'homo/trans phobie y compris de la part des autorités censées protéger tous les citoyens • Exposés à des pressions psychologiques et au stress • (…)
Groupes d'identités minoritaires	• Droits identitaires • (…)	• Discrédit et exclusion • Restriction de leurs droits civiques • (…)	• Partagent une identité culturelle et ethnique • Peuvent se trouver dans des endroits différents • Tendances à travailler en cercles fermés • Isolement • Accès difficile aux autres groupes de DH • Difficultés à sensibiliser l'opinion sur leur cas • (…)

Bibliographie et ressources supplémentaires

Bibliographie

- Amnesty International (2003): *Essential actors of our time. Human rights defenders in the Americas.* AI International Secretariat (Index AI: AMR 01/009/2003/s).
- AVRE and ENS (2002): *Afrontar la amenaza por persecución sindical*. Escuela de Liderazgo Sindical Democrático. Publié par Escuela Nacional Sindical and Corporación AVRE. Medellín, Colombia.
- Bettocchi, G., Cabrera, A.G., Crisp, J., and Varga, A. (2002): *Protection and solutions in situations of internal displacement.* EPAU/2002/10, UNHCR.
- Cohen, R. (1996): *Protecting the Internally Displaced*. World Refugee Survey.
- Conway, T., Moser, C., Norton, A. and Farrington, J. (2002): *Rights and livelihoods approaches: Exploring policy dimensions*. DFID Natural Resource Perspectives, no. 78. ODI, London.
- Dworken, J.T.: *Threat assessment*. Series of modules for OFDA/InterAction PVO Security Task Force (Mimeo, included in REDR Security Training Modules, 2001).
- Eguren, E. (2000): *Who should go where? Examples from Peace Brigades International,* in *Peacebuilding: a Field Perspective. A Handbook for Field Diplomats*, by Luc Reychler and Thania Paffenholz (editors). Lynne Rienner Publishers (London).
- Eguren, E. (2000): *The Protection Gap: Policies and Strategies* in the ODI HPN Report, London: Overseas Development Institute.
- Eguren, E. (2000): *Beyond security planning: Towards a model of security management. Coping with the security challenges of the humanitarian work*. Journal of Humanitarian Assistance. Bradford, UK. www.jha.ac/articles/a060.pdf
- Eriksson, A. (1999): *Protecting internally displaced persons in Kosovo*. http://web.mit.edu/cis/www/migration/kosovo.html#f4
- Lebow, Richard Ned and Gross Stein, Janice (1990) *When Does Deterrence Succeed And How Do We Know?* (Occasional Paper 8). Ottawa: Canadian Inst. for Peace and International Security.
- Mahony, L. and Eguren, E. (1997): *Unarmed bodyguards. International accompaniment for the protection of human rights*. Kumarian Press. West Hartford, CT (USA).
- Martin Beristain, C. and Riera, F. (1993): *Afirmación y resistencia. La comunidad como apoyo*. Virus Editorial. Barcelona.
- Paul, Diane (1999): *Protection in practice: Field level strategies for protecting civilians from deliberate harm*. ODI Network Paper no. 30.

- SEDEM (2000): *Manual de Seguridad. Seguridad en Democracia*. Guatemala.
- *Sustainable Livelihoods Guidance Sheets* (2000). DFID. London, February 2000
- Sutton, R. (1999): *The policy process: An overview*. Working Paper 118. ODI. London.
- UNHCHR (2004): *About Human Rights Defenders* (extensive information): http://www.unhchr.ch/defenders/about1.htm
- UNHCHR (2004): Human Rights Defenders: *Protecting the Right to Defend Human Rights*. Fact Sheet no. 29. Geneva.
- UNHCHR (2004): *On women defenders*: www.unhchr.ch/defenders/tiwomen.htm
- UNHCR (1999): *Protecting Refugees*: A Field Guide for NGO. Geneva.
- UNHCR (2001): *Complementary forms of protection. Global Consultations on International Protection*. EC/GC/01/18 4 September 2001
- UNHCR (2002): *Strengthening protection capacities in host countries. Global Consultations on International Protection*. EC/GC/01/19 * / 19 April 2002
- UNHCR-Department of Field Protection (2002): *Designing protection strategies and measuring progress: Checklist for UNHCR staff*. Mimeo- Geneva.
- Van Brabant, Koenraad (2000): *Operational Security Management in Violent Environments*. Good Practice Review 8. Humanitarian Practice Network. Overseas Development Institute, London.

Ressources supplémentaires:

Depuis 2000, Protection International-PI- donne des formations et conseils sur la protection et la sécurité pour défenseurs des droits humains. Vous pouvez contacter PI en écrivant soit à pi@protectioninternational.org soit à PI, Rue de la Linière, 11 - 1060 Bruxelles (Belgique).

Tel: + 32 (0)2 609 44 05 +32 (0)2 609 44 07

Fax: +32 (0)2 609 44 06

www.protectioninternational.org

www.protectionline.org

Tactical Technology Collective: **www.tacticaltech.org** (depuis 2003 - expertise technique en sécurité digitale): "NGO in a Box".

Index des chapitres

Avant-propos à la première édition par Hina Jilani 3

Protection International (présentation) 4

Préface 7

Introduction 11

Première partie - Protection et sécurité

Introduction 17

Ch 1.1.- Prendre des décisions fondées de sécurité et de protection 19

Ch 1.2.- Évaluer les risques 29

Ch 1.3.- Comprendre et évaluer les menaces 41

Ch 1.4.- Incidents de sécurité 47

Ch 1.5.- Prévenir les agressions et y réagir 55

Ch 1.6.- Élaborer une stratégie de sécurité globale 67

Ch 1.7.- Préparer un plan de sécurité 77

Ch 1.8.- Améliorer la sécurité au travail et au domicile 85

Ch 1.9.- La sécurité et les défenseurs des droits humains femmes 99

Ch 1.10.- La sécurité dans les zones de conflits armés 113

Ch 1.11.- Sécurité, communication et technologie de l'information 119

Deuxième partie - Sécurité de l'organisation

Introduction 137

Ch 2.1.- Évaluer la performance de l'organisation: la "roue de la sécurité" 139

Ch 2.2.- S'assurer du respect des règles et procédures de sécurité 157

Ch 2.3.- Gérer le changement organisationnel vers une politique de sécurité améliorée 155

Troisième partie - Protocoles, plans d'urgence et davantage de politiques

Introduction 171

Ch 3.1.- Comment réduire les risques liés à la perquisition et / ou le cambriolage d'un bureau 173

Ch 3.2.- Détention, arrestation, enlèvement et capture d'un défenseur ..181

Ch 3.3.- La sécurité et la gestion de l'information 193

Ch 3.4.- La sécurité et le temps libre 199

Annexes

La Déclaration sur les Défenseurs des Droits Humains des Nations Unies..203

Lignes Directrices de L'Union Européenne sur les Défenseurs des Droits Humains 209

Les Recommandations de Promotion de PI pour les Défenseurs des Droits Humains 215

Aperçu Général du Risque selon les Profils Spécifiques de Défenseurs des Droits Humains 219

Bibliographie Choisie et Ressources Supplémentaires 223

Index des Chapitres 225

Index Thématique 227

Index thématique

Adhésion aux règles de sécurité (voir Règles).
Agressions sexuelles, 81, 102, 103, 106, 108
Agressions, comment y réagir, 64
Agressions, déterminer la probabilité d'une agression, 57
Agressions, probabilité d'une agression accidentelle, 60
Agressions, probabilité d'une agression directe, 58
Agressions, probabilité d'une agression par des criminels, 59
Agressions, qui peut s'en prendre à un défenseur?, 55
Agressions, reconnaître qu'une agression se prépare, 56
Alarmes (voir sécurité des bureaux).
Alcool, abus d'alcool et sécurité, 200
Analyse des forces en présence sur le terrain (méthodologie pour analyser le contexte de votre travail), 21
Analyse des risques, 29
Analyse du contexte de votre travail (méthodologies), 19
Armes et les entreprises de sécurité privée, 91
Arrestation d'un défenseur, 187
Artillerie non explosée, 115
Booby-traps (objets piégés), 115
Bureau (emplacement) et sécurité, 86
Cafés Internet et sécurité, 134
Caméras vidéo (voir sécurité des bureaux).
Capacités et vulnérabilités, liste de contrôle, 34-37
Capacités, quelles sont les capacités en matière de sécurité, 31
Capture d'un défenseur, 188
Chiffrage, 124
Ciblage, 31
Clés, serrures (voir sécurité des bureaux).
Communications orales et sécurité (voir Parler).
Contre-surveillance, 62
Courrier électronique, envoyer des courriels en toute sécurité, 125-126
Cryptage, 127

Culture, culture organisationnelle de sécurité de l'organisation, 151, 153, 165
Défenseur, qui est un défenseur, 14
Défenseur, qui peut devenir défenseur des droits humains, 14
Défenseurs, qui est responsable de la sécurité des défenseurs, 15
Détention d'un défenseur, 185
Détention, prévention de détention d'un défenseur, 186, 189
Détention, réactions suite à la détention d'un défenseur, 186-187
Dissuasion et espace sociopolitique des défenseurs, 67-73
Drogue, abus de drogue et sécurité, 200
Enlèvement d'un défenseur, 188
Entreprises de sécurité privée, 91
Espace, espace sociopolitique de travail des défenseurs, 72
Femmes défenseurs des droits humains, besoins de sécurités spécifiques, 99
Image organisationnelle et sécurité, 146
Incidents, comment évaluer un incident de sécurité, 47
Incidents, distinction entre menaces et incidents, 47
Incidents, gérer les incidents y faire face, 49
Incidents, les consigner et les analyser, 49
Incidents, pourquoi peuvent-ils passer inaperçus, 48
Incidents, pourquoi sont-ils si importants?, 48
Incidents, qu'appelle-t-on un incident de sécurité, 47
Incidents, quand et comment les repérer, 47
Incidents, réaction excessive aux, 49
Incidents, réagir de manière urgente, 50
Information saisie, perdue ou détruite, 174, 175, 180
Information, confidentialité de, 201
Information, gestion sûre de, 181
Internet et sécurité, 123-125
LGBTI (Lesbienne, gay, bisexuel, trans-genre et intersexe), 81, 221 and the page just before Bibiography)
Lignes directrices de l'UE sur les DDH, 209
Logiciel, administration des logiciels, 133
Menaces, cinq étapes pour évaluer une menace, 43
Menaces, contingentes, directes et déclarées, 30
Menaces, définition, 41
Menaces, déterminer qui émet une menace, 43
Menaces, émettre une menace par opposition à constituer une menacer, 42
Menaces, établir la probabilité d'exécution de, 43-44
Menaces, modèle de, 43

Menaces, rapport avec l'évaluation des risques, 41
Menaces, suivi et clôture d'un cas de, 44
Mines, 115
ONU, Déclaration de l'ONU sur les Défenseurs des droits humains, 203
Parler, communications et sécurité, 119
Parties prenantes, analyse (méthodologie pour une analyse du contexte de travail), 22
Parties prenantes, classification (principales, détenteurs des obligations, essentielles), 22-23
Performance, évaluer la performance en matière de sécurité, 139
Performance, évaluer la performance en matière de sécurité, 139
Perquisition des bureaux (ou cambriolage), 173
Persuasion et espace sociopolitique des défenseurs, 74
Plaidoyer, recommandations de PI aux DDH quant aux missions EU, 215
Plan, élaborer un plan de sécurité, 77
Plan, mettre en oeuvre un plan de sécurité, 82
Plan, un menu d'éléments à inclure au plan de sécurité, 80
Poser des questions (méthodologie pour une analyse de votre contexte de travail), 20
Procédures d'admission (voir sécurité des bureaux).
Protection, résultats de (lors de la prévention d'une agression), 76
Règles, appropriation des règles de sécurité, 140, 145, 151, 168
Règles, différentes démarches en matière de règles de sécurité, 150
Règles, non respect délibéré des règles de sécurité, 168
Règles, non respect involontaire des règles de sécurité, 153
Règles, pourquoi ne sont-elles pas respectées, 150, 151
Règles, que faire si elles ne sont pas respectées, 153
Règles, vérification du respect des règles de sécurité, 153
Relations (liaisons) secrètes et sécurité, 200
Résistance au plan d'amélioration (de la sécurité), 163
Risques, les gérer, y faire face, 69
Roue de la sécurité, 139, 141
Sauvegarde informatique, systèmes de, 174
Sécurité des bureaux (éclairage et alarmes), 89
Sécurité des bureaux, barrières matérielles et procédures pour les visiteurs, 88, 91, 96
Sécurité des bureaux, clés et serrures, 89, 95, 96
Sécurité des bureaux, listes de contrôle et vérifications régulières, 97
Sécurité des bureaux, livraison d'objets ou de paquets, 93

Sécurité des bureaux, procédures d'admission, 91
Sécurité des bureaux, vulnérabilités, 85
Sécurité des ordinateurs et sécurité des fichiers, 122
Sécurité, amélioration, 158
Securité, gestion de, 157, 166
Sécurité, incidents de (voir Incidents).
Sécurité, plan de, (voir Plan).
Sécurité, règles de (voir Règles).
Stratégies de réponse, 67-68
Surveillance (et contre- surveillance), 62
Téléphones et sécurité des communications, 121
Temps libre et sécurité, 199
Véhicules, voyager dans des zones de conflits armés, 115
Vérification du respect des règles de sécurité (voir règles).
Voyage, prévention de détention pendant un voyage, 189
Vulnérabilités et capacités, liste de contrôle, 34-37
Vulnérabilités, définition des, 31

Luis Enrique Eguren

(Espagne), médecin et expert en protection. Membre de l'Unité de recherche et formation de Protection International. Il a travaillé avec PBI au Salvador, au Sri Lanka et en Colombie. Il a également participé à de courtes missions dans d'autres pays aux côtés d'autres organisations internationales. Consultant, formateur et chercheur, il a publié plusieurs articles et livres sur la protection.

© Maria Dermitzaki

Marie Caraj

(Belgique), interprète et experte en protection. Membre de l'Unité de recherche et formation de Protection International. Elle a travaillé avec PBI et PBI-BEO (1985-2007). Succession de courtes missions en Afrique, Asie et Amérique latine. Consultante, formatrice et chercheuse.

"(...) la gravité des risques encourus au quotidien par les défenseurs des droits humains est telle que leur protection ne pourrait être renforcée sans stratégies additionnelles. A cet égard, j'espère que ce Manuel de protection aidera les défenseurs des droits humains à élaborer leur propres plans de sécurité et mécanismes de protection. De nombreux défenseurs des droits humains se vouent corps et âme à la protection des autres au point d'en oublier leur propre sécurité. Il est essentiel pour nous qui oeuvrons en faveur des droits humains de prendre conscience de l'importance de la sécurité, non seulement pour nous-mêmes mais également pour lespersonnes avec qui et pour qui nous travaillons (...)"

(Hina Jilani, Ex-Représentante spéciale du Secrétaire général des Nations unies sur les défenseurs des droits humains)

"Depuis que nous avons eu cette première formation, il faut reconnaître que bien de choses ont changé dans notre organisation pour la simple et bonne raison que tous les éléments appris au cours de cette formation nous étaient manifestement inconnus. Aujourd'hui, forts de cette formation, nous savons évaluer avec beaucoup plus de compétence les risques auxquels nous sommes exposés quotidiennement en tenant compte des incidents de sécurité, des menaces et l´éventualité de leur exécution."

"(...) La méthode participative que vous avez choisie est un grand atout, elle a permis des échanges. Et nous sommes certains que les résultats seront probants."

"J´ai reçu une formation de qualité pour être un vrai défenseur des droits humains. Je vais changer la façon de travailler après cette formation."

(Défenseurs en République Démocratique du Congo)

"Félicitations pour les efforts et le format car il a été très didactique et il nous a situés dans notre vécu."

(Défenseur au Guatémala)

"J'ai appris énormément sur un univers que je connaissais depuis longtemps, mais que j'avais rarement envisagé sous cet angle auparavant."

(Défenseur au Mexique)

"(...) C'est un sujet entièrement neuf pour moi. Bien que nous travaillions dans un domaine qui comporte toujours une menace pour notre sécurité, nous n'avons jamais pensé avoir besoin d'une telle formation ou bien nous n'avons jamais eu le temps de penser à notre sécurité. Mais après cette formation, je pense personnellement que le sujet doit être maintenu au plus haut niveau avant de lancer un programme quel qu'il soit. En d'autres mots, cette formation est réellement essentielle pour tous."

(Défenseur au Népal)

PROTECTION international

Avec le soutien de:

Bundesministerium für wirtschaftliche Zusammenarbeit und Entwicklung

ROYAUME DE BELGIQUE
Service public fédéral
Affaires étrangères, Commerce extérieur et Coopération au Développement

Koninkrijk der Nederlanden

Initiative Européenne pour la Démocratie et les Droits de l'Homme
IEDDH

Nouveau manuel de protection pour les défenseurs des droits humains
Recherche et texte par Enrique Eguren et Marie Caraj -Unité de recherche et formation- Protection International. Traduction de l'anglais par Hanna et Adrian Garcia Landa

Protection International, Rue de la Linière, 11. B-1060 Bruxelles (Belgique)
Tel: +32 (0) 2 609 44 05 / +32 (0) 2 609 44 07, Fax: +32 (0) 2 609 44 06
E-mail pi@protectioninternational.org / www.protectioninternational.org

Site internet unique sur la protection des défenseurs des droits humains: www.protectionline.org