Manuel De Protection

pour

Les Défenseurs Des Droits Humains

Recherche et texte par Enrique Eguren,
Peace Brigades International, European Office (PBI BEO)

Publié par Front Line
La Fondation Internationale pour la Protection des
Défenseurs des Droits Humains

Publié par Front Line 2005
La fondation internationale pour la protection des défenseurs des droits humains: 16 Idrone Lane, Off Bath Place, Blackrock, County Dublin, Ireland

Des exemplaires de ce manuel peuvent être commandés en écrivant à: info@frontlinedefenders.org et pbibeo@protectionline.org et manual@protectionline.org

Prix EUR20, plus frais de port

Pour commander un manuel, contacter:

PBI-Bureau Européen
11, rue de la Linière, 1000 Bruxelles (Belgique)
Tel +32(0)2 609 44 05, Fax +32(0)2 609 44 06
pbibeo@protectionline.org

Front Line
16 Idrone Lane, Off Bath Place, Blackrock, County Dublin, Ireland
Tel: +353 1212 3750 fax: +353 1212 1001
protectionmanual@frontlinedefenders.org

Ce manuel a été traduit de l'anglais en français, espagnol, russe et arabe par Front Line (et en d'autres langues)

ISBN: 0-9547883-1-1

Avant-propos d'Hina Jilani

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 des 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. 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 saurait 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, non seulement pour nous-mêmes, mais également pour les personnes avec qui et pour qui nous travaillons.

Hina Jilani
Représentante spéciale du Secrétaire général des Nations unies sur les défenseurs des droits humains

[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.

Front line

Front Line a été fondée en 2001 dans le but spécifique de protéger les défenseurs des droits humains, ces personnes qui oeuvrent de manière non-violente pour le respect d'un ou plusieurs droits garantis par la Déclaration Universelle des Droits de l'Homme (DUDH). Front Line vise à aborder certains des besoins identifiés par les défenseurs eux-mêmes, comme la protection, la création de réseaux, la formation et l'accès aux mécanismes thématiques et nationaux de l'ONU et d'autres organisations régionales.

Front Line se concentre essentiellement sur les défenseurs des droits humains menacés, de manière passagère ou constante, du fait de leur travail en faveur de leurs concitoyens. Front Line gère de petits programmes de subvention visant à répondre aux besoins de sécurité des défenseurs. Front Line se mobilise pour faire campagne et exercer des pressions en faveur des défenseurs en danger immédiat. En cas d'urgence, Front Line leur facilite un transfert temporaire.

Front Line dirige des recherches et publie des rapports sur la situation des défenseurs des droits humains dans des pays précis. L'organisation produit également de la documentation et des modules de formation à la demande des défenseurs des droits humains, tout en facilitant les contacts et les échanges entre défenseurs du monde entier. Les projets de Front Line sont habituellement menés en partenariat avec des organisations nationales de droits humains spécifiques.

Front Line promeut la sensibilisation à la Déclaration Universelle des Droits de l'Homme et agit en vue de garantir la diffusion, le respect et l'adhésion aux principes et normes établis par 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 (plus connue sous le nom de déclaration sur les défenseurs des droits humains).

Front Line possède le statut consultatif spécial auprès du Conseil Economique et Social des Nations unies.

Front Line bénéficie du statut caritatif (CHY NO 14029) et est une organisation indépendante et impartiale.

Pour financer ses actions, Front Line compte entièrement sur la générosité individuelle et celle d'organisations. Depuis sa création en 2001, Front Line a eu la chance de bénéficier d'un financement provenant de sources variées et accepte tout don individuel avec gratitude.

Les membres du conseil d'administration sont: Denis O'Brien (président), Mary Lawlor (directrice), Pierre Sané, Kieran Mulvey, Noeline Blackwell, Michel Forst et David Sykes.
Les membres du conseil de direction sont: Hanane Ashraoui, Robert Badinter, Bono, Sa Sainteté le Dalaï Lama, Indai Lourdes Sajor, Wangarai Muta Maathai, Adolfo Perez Esquivel, Desmond Tutu.

Pbi

Peace Brigades International (PBI) est une organisation non-gouvernementale (ONG) qui protège les défenseurs des droits humains et promeut la résolution non violente des conflits.

Sur invitation, PBI envoie des équipes de volontaires dans des régions où sévissent répression et conflits. Ces volontaires accompagnent les défenseurs des droits humains et leurs organisations lorsque ces derniers sont menacés de violence politique. Les auteurs de violations des droits humains ne souhaitent pas en règle générale que le monde soit témoin de leurs actes. La présence physique de ces volontaires en tant qu'observateurs, un vaste réseau de contacts, des activités de sensibilisation et un réseau étendu de soutien international concourent à dissuader l'hostilité et les actions violentes contre les défenseurs. De cette façon, PBI veut créer l'espace nécessaire aux défenseurs pour défendre la justice sociale et les droits humains.
PBI est dotée d'un conseil d'administration international, d'un bureau international à Londres et de groupes nationaux ou de groupes associés dans 17 pays et mène plusieurs projets sur le terrain.

Le bureau européen de Peace Brigades International est situé à Bruxelles (Belgique). Le contenu de ce manuel est le résultat d'un travail de recherche réalisé par son centre de recherche et de formation.

Pour plus d'informations veuillez consulter les sites Internet:
http://www.peacebrigades.org/
www.protectionline.org

Ou le site Internet du Bureau Européen de PBI:
http://www.peacebrigades.org/beo.html

Front Line a été fondée avec la mission exclusive de protéger les défenseurs des droits humains. Malheureusement, notre travail quotidien nous montre combien un renforcement de la sécurité et de la protection des défenseurs des droits humains est nécessaire dans un monde où ils sont de plus en plus la cible de menaces et de violence. Notre préoccupation principale est d'augmenter la pression pour demander des comptes aux gouvernements tenus par le droit humain international à protéger les défenseurs, mais qui sont encore bien trop souvent responsables de violence et de mesures de répression à leur égard. Mais aux dires des défenseurs des droits humains eux -mêmes, on pourrait manifestement faire davantage pour renforcer leurs propres capacités à améliorer leur sécurité.

Nous étions donc enthousiastes d'apprendre l'existence du projet mené par Peace Brigades International sous le titre "Intégrer la protection", et plus particulièrement leur avant-projet de manuel pour les défenseurs des droits humains. Nous leur avons aussitôt suggéré de financer la recherche et la réalisation de ce manuel.

Cela fut un grand plaisir de travailler avec Enrique Eguren, l'auteur de ce manuel. Enrique et ses collègues ont mis leur riche expérience des problèmes de sécurité et de protection à notre disposition. PBI a aussi organisé plusieurs ateliers d'échange et de formation avec les défenseurs des droits humains sur le terrain afin que le manuel puisse bénéficier de l'apport de ceux qui travaillent en première ligne. Deux de ces ateliers ont été organisés en collaboration avec Front Line à Bukavu et à Goma en mai 2004, dans l'est de la République Démocratique du Congo.

En publiant ce manuel, Front Line propose un guide pratique aux défenseurs des droits humains pour élaborer leurs plans et stratégies de sécurité et de protection. Le manuel est conçu dans une large mesure comme un projet évolutif à développer, nous l'espérons, par les expériences communiquées par les défenseurs en milieu hostile. Le contenu tire parti des échanges de vues sur la sécurité et la protection lors des deux premières réunions de défenseurs des droits humains de Dublin, en 2002 et 2003. Le manuel pourra être examiné et commenté en bonne et due forme lors de la troisième réunion de Dublin en octobre 2005.

Le manuel examine en détail l'analyse des risques et menaces et l'élaboration de stratégies et plans de sécurité et de protection efficaces. Il constituera, espérons-le, une référence utile pour les responsables de la sécurité dans les ONG de droits humains et une base pour la formation des défenseurs des droits humains. Nous avons prévu de publier une version

abrégée avec des conseils pratiques et des suggestions en complément du manuel de formation. Front Line participe aussi, aux côtés de Privaterra, à la réalisation d'un manuel et de fiches d'informations sur la sécurité dans les communications électroniques, résumé en partie au chapitre 12 et dont la sortie est prévue en 2005.

Nous souhaitons remercier de leur contribution de nombreuses personnes sans qui ce manuel n'aurait pu être réalisé.

Marie Caraj, Pascale Boosten, Michael Schools et Christophe Klotz, ces collègues estimés du bureau européen de Peace Brigades International : ce projet doit son existence à leur engagement et leur expérience.

Le texte a été révisé et mis en page par Mary Lawlor, Andrew Anderson, James Mehigan et Dmitri Vitaliev (chapitre 12) de Front Line. Kristin Hulaas Sunde a édité une première version du texte.

Le chapitre 12 est basé sur le travail de Robert Guerra, Katitza Rodriguez et Caryn Madden de Privaterra (Canada).

Nous devons beaucoup aux contributions et commentaires apportés à ce projet de manuel par Arnold Tsunga (des avocats du Zimbabwe pour les droits humains), Sihem Bensedrine (Conseil National pour les Libertés en Tunisie, Tunis), le Père Bendan Forde (franciscain itinérant, Colombie), Indai Sajor (ancienne directrice du centre asiatique pour les droits des femmes, Philippines), James Cavallaro (Brésil, directeur associé, programme des droits humains, école de droit d'Harvard), Nadejda Marques (consultante et chercheuse, Centre de justice globale de Rio de Janeiro, Brésil), et par Marie Caraj (Peace Brigades International, Bureau Européen, Belgique).

D'autres collègues ont apporté leur pierre à cet édifice par leur travail. Que soient ainsi remerciés : José Cruz et Iduvina Hernández de SEDEM (Guatemala), Claudia Samayoa (Guatemala), Jaime Prieto (Colombie), Emma Eastwood (Royaume-Uni) et Cintia Lavandera du programme sur les défenseurs des droits humains d'Amnesty International, Londres.

Carmen Diez Rozas a créé la conception du manuel et s'est chargée de la PAO avec l'aide de Montserrat Muñoz qui a collaboré aux illustrations.

Nous sommes également extrêmement reconnaissants du soutien à Development Cooperation, d'Irlande.

Imprimé par "Print and Display".

(Propos de l'auteur) De nombreuses personnes ont également collaboré au recueil d'informations nécessaires à la rédaction de ce manuel. Il est impossible de les citer toutes, cependant nous souhaitons mentionner quelques noms:

Tous les collaborateurs de Peace Brigades International, et tout particulièrement mes anciens collègues proches du projet Colombie, Marga, Elena, Francesca, Emma, Tomás, Juan, Mikel, Solveig, Mirjam et bien d'autres…

Danilo, Clemencia et Abilio et leurs collègues de la commission interecclés iastique pour la justice et la paix en Colombie. Ils m'ont appris à vivre à l'intérieur du coeur des autres.

Les habitants de Santa Marta, San Salvador, et de Cacarica, Jiguamiando et San José de Apartado en Colombie. Ils m'ont, parmi tant d'autres choses, permis de comprendre la dignité des personnes vivant en milieu rural.

Les personnes associées au programme de formation en sécurité des défenseurs des droits humains du projet Counselling Service de Colombie.

Les conseils et les connaissances de départ prodigués par REDR (Londres) et Koenraad van Brabant (Belgique).

Tous les défenseurs rencontrés au Salvador, au Guatemala, en Colombie, au Mexique, au Sri Lanka, en Croatie, en Serbie, au Kosovo, en République Démocratique du Congo, en Ingouchie… Un monde de conversations, de larmes, de sourires, d'apprentissage et d'engagement.

Pour finir, rien n'aurait pu être réalisé sans l'amour, le dévouement et le soutien de Grisela, d'Iker et de mes parents. Merci beaucoup.

Merci à toutes les personnes citées ci-dessus et aux nombreux défenseurs des droits humains avec qui nous avons travaillé et qui nous ont beaucoup appris.
Le texte définitif ainsi que toutes les erreurs qu'il peut contenir sont la responsabilité commune de Front Line et de Peace Brigades International. Nous espérons que ce manuel sera un outil utile d'amélioration de la protection et de la sécurité des défenseurs des droits humains, tout en sachant qu'il n'apporte aucune garantie, et qu'en fin de compte chacun doit assumer sa responsabilité individuelle dans ce domaine. Nous attendons avec impatience tout commentaire.

Front Line
Peace Brigades International
7 mars 2005

Avertissement

Le contenu de ce manuel ne représente pas nécessairement l'opinion de Peace Brigades International et de Front Line (fondation internationale pour la protection des défenseurs des droits humains).

Ni les auteurs, ni l'éditeur ne garantissent que les informations contenues dans cette publication soient complètes et correctes, ils ne peuvent donc pas être tenus responsables des préjudices découlant de l'utilisation de ce manuel. Aucune partie de ce manuel ne constitue une règle officielle ou une garantie et ne saurait être employée sans les éléments nécessaires pour évaluer les problèmes de risque et de sécurité qu'un défenseur des droits humains peut connaître.

Sommaire

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

Les défenseurs des droits humains en péril

Les droits humains sont garantis par le droit international, mais les défendre ainsi que ceux dont les droits ont été violés peut s'avérer une tâche 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 harcèlements, de détentions, de torture, de diffamations, 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 ou "portés disparus".

Au cours des dernières années, il y a eu 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. 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 périlleux où la vie des défenseurs des droits humains peut 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 gratuits. 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 oeuvre 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 sur mesure qui s'appliquent indifféremment à tous les scénarios. Cependant, il s'efforce de proposer 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 en première ligne.

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 est qu'une menace se concrétise en agression réelle. Les agresseurs ont la volonté, les moyens et 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 de nombreuses organisations différentes de défendre le travail extrêmement précieux des défenseurs des droits humains. Ce sont eux qui sont en première ligne, et ils sont également les protagonistes de ce manuel.

Le manuel

L'objectif de ce manuel est de doter les défenseurs des droits humains d'informations supplémentaires et d'outils permettant de mieux comprendre la sécurité et la protection. Nous espérons que ce manuel serve de base à la formation de sécurité et de protection et qu'il aidera les défenseurs à mettre en oeuvre leurs propres évaluations du risque et à définir les règles et procédures de sécurité adaptées à leur cas particulier.

Ce manuel est le fruit d'un projet à long terme de PBI sur la protection des défenseurs sur le terrain. 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 devons 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. 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 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. 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 permettent aux ONG et défenseurs de mieux répondre aux défis croissants de sécurité posés par la défense des droits humains.

Cela dit, nous souhaitons rappeler en premier lieu que les défenseurs des droits humains risquent leur bien-être et leur vie et que c'est une affaire sérieuse. Parfois la seule façon de sauver une vie est de se mettre à l'abri 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 succès.

Améliorons ensemble ce manuel

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 sera 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 ou messages électroniques (e-mails) à :

- protectionmanual@frontlinedefenders.org
- pbibeo@protectionline.org

Et votre courrier à Front Line ou à PBI:

- PBI- European Office
  38, Rue Saint-Christophe, 1000 Bruxelles (Belgium)
  Tel/fax + 32 (0)2 511 14 98

- Front Line
  16 Idrone lane, Off Bath Place, Blackrock, County Dublin, Ireland
  tel: +353 1212 3750 fax: +353 1212 1001

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 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.

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 devenu 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 chargé des défenseurs des droits humains 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".

Pour Front Line, un défenseur des droits humains est « toute personne qui lutte, de manière non-violente, pour le respect d'un ou de plusieurs droits garantis par la Déclaration universelle des droits de l'homme". Front Line s'efforce de promouvoir la Déclaration sur les défenseurs des droits humains des Nations unies (vous trouverez la Déclaration intégrale à la page 123).

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, la représentante spéciale du Secrétaire général des Nations unies sur les défenseurs des droits humains, "dénoncer les violations des droits humains et exiger réparation dépend largement du degré de sécurité dont jouissent les défenseurs des droits humains"[1]. 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.

[1] Rapport sur les défenseurs des droits humains du 10 septembre 2001 (A/56/341).

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.frontlinedefenders.org (Front Line, la fondation internationale pour la protection des défenseurs des droits humains).
- www.peacebrigades.org/beo.html (le bureau européen de Peace Brigades International, dont le siège est à Bruxelles).
- 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 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.humanrightsfirst.org (droits humains d'abord).
- www.urgentactionfund.org (fonds d'action urgente pour les droits humains des femmes).

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.frontlinedefenders.org/manual/fr/index.htm (Front Line, Ireland) pour un manuel sur les instruments internationaux pour les défenseurs des droits humains. Leur page d'hyperliens est très utile: http://www.frontlinedefenders.org/links/
- 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.

CHAPITRE 1

Prendre des décisions fondées de sécurité et de protection

Objectif

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

Apprendre différentes méthodes pour comprendre 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, et qui sont influencés par des procédures décisionnelles profondément politiques. Beaucoup d'événements se déroulent simultanément et chaque événement a une répercussion sur un autre. La dynamique de chaque acteur, ou partie prenante, dans ce scénario aura un rôle significatif à jouer dans les rapports entre l'acteur et les autres. Les défenseurs des droits humains ont donc besoin d'informations non seulement sur les problèmes relatifs à leurs actions mais aussi sur les fonctions des principaux acteurs et des parties prenantes.

Un simple exercice 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 et

aux réactions des différents intervenants. Il est important de considérer les différentes dimensions d'un contexte 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 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 acteurs constituent trois méthodes utiles pour l'analyse du contexte de travail.

Poser des questions

Vous pouvez mieux comprendre votre contexte de travail en 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 votre question serait: "notre cadre socio-politique est-il assez sûr pour travailler?", la possibilité des réponses étant ainsi limitée 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, 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 :

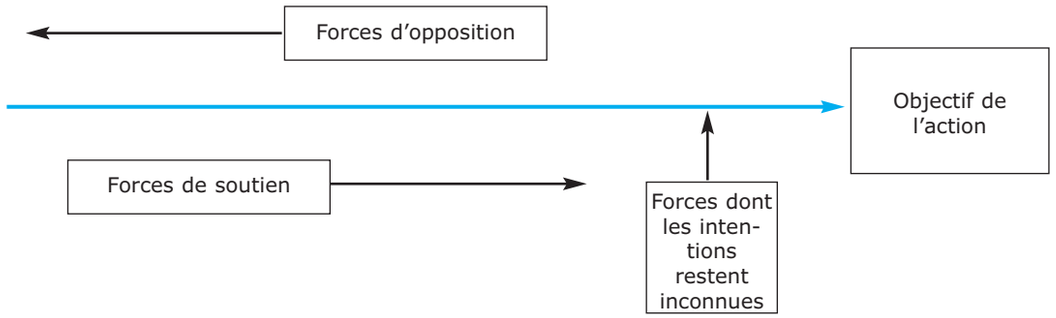
- Quels sont les problèmes majeurs en jeu dans l'arène sociopolitique et économique?
- Qui sont les principaux acteurs liés à ces problèmes majeurs?
- Comment nos actions peuvent-elles influencer de manière positive ou négative les intérêts de ces acteurs principaux?
- Quelle serait notre réaction si 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 des 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. 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.

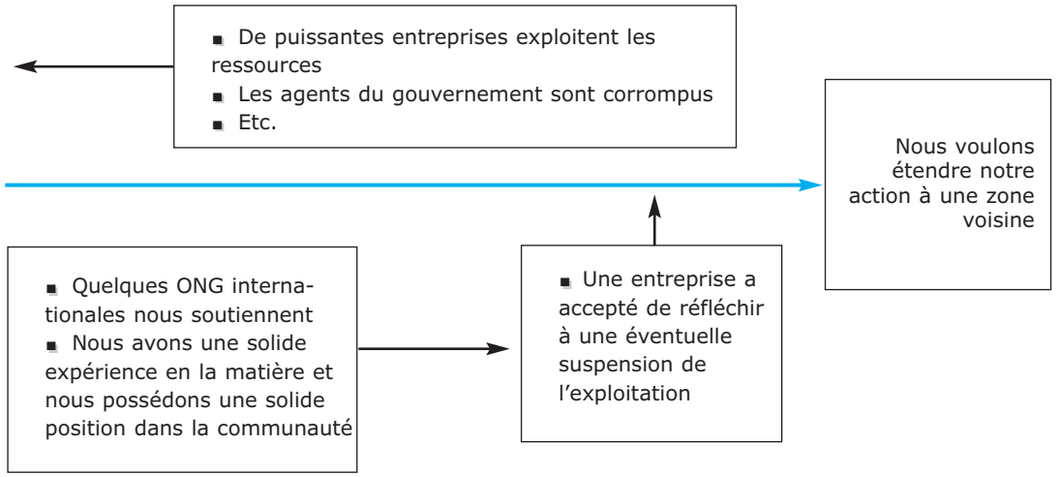
Schéma 1: analyse des forces en présence pour faire le point sur le contexte de travail



Après avoir fini 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 les considérer ou non comme des forces de soutien, 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 à l'accès des populations autochtones 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 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 [1].

L'analyse des parties prenantes est essentielle pour comprendre:

- Qui peut être considéré comme partie prenante et sous 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.

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 etc.)
- Les organes internationaux dotés d'un mandat de protection, comme les organes de l'ONU, les organisations intergouvernementales régionales, les forces de maintien de la paix, etc.
- Dans le cas d'acteurs armés de l'opposition, ils peuvent être tenus de ne pas responsables attaquer les défenseurs des droits humains (en leur qualité de civils), plus particulièrement lorsque ces acteurs contrôlent le territoire.

[1] Adaptation des Sustainable Livelihoods Guidance Sheets No.5.4 (2000)

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 à exercer une pression sur les détenteurs d'obligations qui ne remplissent pas leurs responsabilités (comme les gouvernements, les organes des Nations Unies, le CICR, 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 (autre que les détenteurs d'obligations).
- 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, une des difficultés majeures relève du fait que les relations entre ces différentes parties prenantes ne sont pas explicites et sont parfois même inexistantes. 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. Certaines parties prenantes, qui auraient partagé les mêmes préoccupations de protection, peuvent avoir des conflits d'intérêts, comme dans certains 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.

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 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. En terme de protection, il est important de dégager et de faire attention à ces relations qui forment et transforment les besoins de protection des individus. Il faut alors se pencher sur les `structures et les procédures`.

`Les structures` sont étroitement liées au secteur public, à la société civile ou aux organes privés. On s'y intéresse 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 et l'armée. Les structures peuvent comporter des constituants variés. Par exemple, une commission intersectorielle (composée de membres du gouvernement, d'ONG, de l'ONU et du corps diplomatique) pourrait être 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 manoeuvre déguisée pour les déplacer. L'ONU et les ONG peuvent apporter leur appui à ces personnes lors de cette procédure.

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, quels 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 bien précise de la protection (voir le schéma 2). Inscrivez cette liste dans la première colonne et la première ligne du tableau. Le tableau offre ainsi deux possibilités d'analyse :

- Pour analyser les attributs de chaque partie prenante (objectifs, intérêts, stratégies, légitimité et pouvoir), suivez la diagonale formée par l'interjection de chaque partie prenante avec soi-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						B	
Police			Partie prenante						
Groupes d'opposition armés				A					
ONG nationales de droits humains					Partie prenante				
Églises						Partie prenante			
Autres gouvernements							Partie prenante		
Agences de l'ONU								Partie prenante	
ONG internationales									Partie prenante

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 le problème de protection et en rapport avec les problèmes stratégiques pour chaque partie prenante.

CHAPITRE 2

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

Objectif

Comprendre les concepts de menace, de vulnérabilité et de capacité en termes 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 un risque.

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

- Ce que vous faites peut engendrer des menaces.

- La manière, le lieu et le moment de votre travail 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 se soit, toute personne travaillant sur les droits humains peut être confrontée à un degré courant de risque. Cependant tous ne sont pas vulnérables de la même manière à ce risque courant tout simplement parce 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.

Exemple:

> Il peut exister un pays dans lequel 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 doit faire face un groupe de défenseurs augmente avec les menaces reçues et leur vulnérabilité à ces menaces comme le présente l'équation[1] suivante:

RISQUE = MENACES x VULNÉRABILITÉ

Les menaces sont la possibilité que quelqu'un porte atteinte à l'intégrité physique ou morale ou aux biens d'une autre personne par un acte délibéré et souvent violent[2]. Faire l'évaluation d'une menace signifie analyser les probabilités d'une menace et de son exécution.

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.

Résumé des différents types de menaces :

- Le ciblage : menaces déclarées ou potentielles liées au travail.
- Les menaces exprimées par des agressions ordinaires.
- Les menaces indirectes : liées aux combats dans les conflits armés.

[1] Van Brabant (2000) et REDR.
[2] Dworken (1999).

Les défenseurs peuvent être confrontés à des menaces d'agressions criminelles de droit commun et plus particulièrement si leur travail les mène dans des régions à risque. Bon nombre d'incidents criminels de droit commun sont en réalité des menaces de ciblage.

Les menaces indirectes proviennent des dommages potentiels engendrés par les combats dans des conflits armés, en d'autres termes, du fait d'être au mauvais endroit au mauvais moment. Cela s'applique particulièrement aux défenseurs travaillant dans des zones de conflits armés.

Le ciblage (menaces ciblées) peut aussi être considéré comme un moyen complémentaire. Les défenseurs des droits humains peuvent être sujets à des menaces 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 potentielles lorsqu'un défenseur proche de vous a été menacé et que tout porte à croire que vous serez la prochaine victime.

Les vulnérabilités

Par vulnérabilité on entend le degré de sensibilité 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 liée à la situation géographique. Un défenseur par exemple est plus vulnérable lorsqu'il ou elle se trouve sur la route pendant une visite de terrain que lorsqu'il ou elle se trouve dans un bureau bien connu où il est fort probable que des témoins assistent à une agression.

- Les vulnérabilités peuvent 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.

- Les vulnérabilités peuvent 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, etc.) 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 façon de 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 résulte en 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.

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

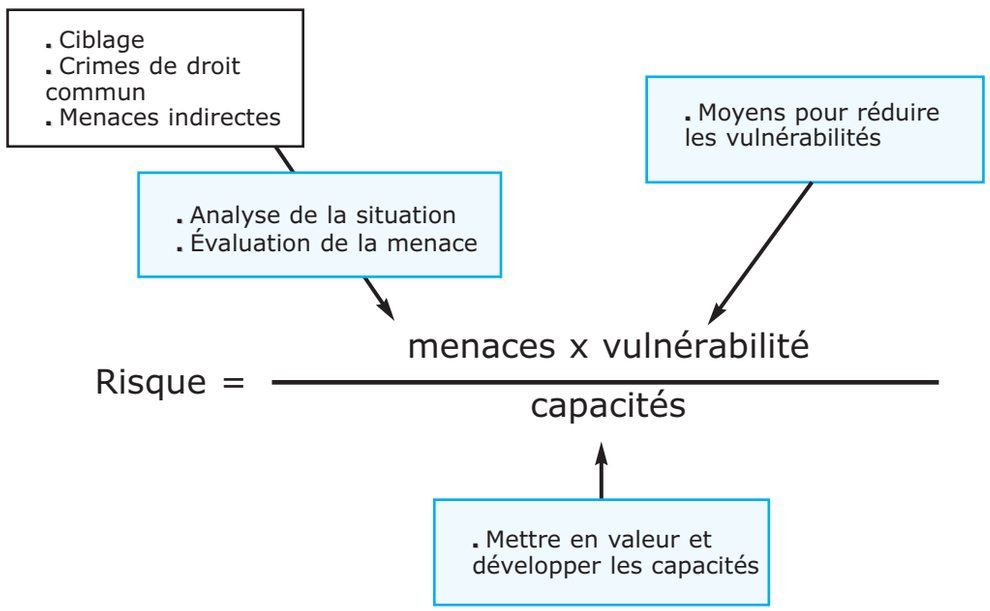
Le danger créé par les menaces et les vulnérabilités peut être diminué si les défenseurs possèdent des capacités suffisantes. Plus il y a de capacités, moins il y a de danger.

$$\text{Risque} = \frac{\text{menaces x vulnérabilité}}{\text{capacités}}$$

En résumé

Afin de réduire le danger à des niveaux acceptables, c'est-à-dire pour assurer la protection, vous devez :

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



Le risque est un concept dynamique qui varie avec le temps et avec les changements de la 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.

La prise de mesures de sécurité, telles que la formation juridique ou les barrières de protection, réduiraient le risque tout 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 la 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).

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

Évaluation des vulnérabilités et des capacités

Mettre au point une analyse des vulnérabilités et des capacités pour un groupe particulier (ou une personne) implique une définition du groupe lui-même (une communauté, une coopérative, une ONG, des individus, etc.), de la région physique où il est localisé et de la période temporelle (votre profil de vulnérabilité évoluera et changera au cours du temps). Pour faire l'analyse dans les

grandes lignes des vulnérabilités et des capacités, utilisez le tableau 3 à la fin de ce chapitre.

À noter : l'analyse des vulnérabilités et des capacités doit être envisagée comme une activité permanente qui vise à se baser sur des informations existantes afin de maintenir une vision exacte d'une situation en constante évolution. Lors de l'analyse des capacités, il est important d'établir les capacités réelles du moment et non pas de faire la liste des capacités potentielles et souhaitables.

Stratégies pour faire face et réagir aux menaces

Les défenseurs et groupes menacés utilisent différentes stratégies pour faire face aux risques qu'ils encourent. Ces stratégies varient complètement suivant le milieu (rural ou urbain), le type de menace, les ressources sociales, financières ou juridiques à leur disposition, etc.

La plupart des stratégies pour faire face peuvent être mises en place immédiatement et répondent à des objectifs à court terme. Elles font alors plus office de tactique que de stratégie de réaction détaillée. Nombre de stratégies peuvent correspondre aux visions subjectives de chaque individu sur le risque, mais peuvent, à long terme, nuire au groupe jusqu'à un certain degré, plus particulièrement si ces stratégies sont irréversibles.

Les stratégies pour faire face sont étroitement liées au type et à la sévérité de la menace et aux vulnérabilités et capacités du groupe.

Lors de la réflexion sur la sécurité et la protection vous devez tenir compte à la fois de vos propres stratégies d'adaptation et de celles des autres. Renforcez les plus efficaces, essayez de limiter les plus préjudiciables et de respecter celles qui restent (spécialement les stratégies d'adaptation liées aux croyances culturelles et religieuses).

Quelques stratégies pour faire face :

- Renforcer les barrières de protection et cacher les objets de valeur.
- Éviter d'adopter un comportement qui pourrait être remis en cause par d'autres acteurs, surtout lorsque le contrôle du territoire dans lequel vous vous trouvez est l'objet d'une dispute militaire.
- Aller se cacher lors de situations de risque, y compris dans des endroits difficiles d'accès comme les montagnes ou la jungle, ou changer de maison, etc. Parfois des familles entières partent se cacher et parfois il ne s'agit que des défenseurs. Parfois cela se déroule durant la nuit et peut durer plusieurs semaines sans aucun contact avec l'extérieur.
- Rechercher la protection armée ou politique d'un des acteurs armés.
- Suspendre ses activités, fermer les bureaux, évacuer les lieux et se mettre à l'abri. Migration forcée (déplacement à l'intérieur du pays ou en tant que réfugié) ou l'exil.
- Compter sur sa « bonne étoile », chance ou avoir recours à des croyances "magiques".
- Se murer dans le silence, y compris avec ses collègues, démentir en refusant de discuter des menaces, abus d'alcool, surmenage, comportement irrationnel.

Les défenseurs ont aussi recours à des stratégies de réaction. Celles-ci peuvent inclure publier des rapports sur une question spécifique, faire des allégations, organiser des manifestations, etc. Dans beaucoup de situations, ces stratégies ne comptent pas comme stratégies à long terme mais relèvent de besoins à court terme. Dans certains cas, les stratégies de réaction peuvent entraîner des problèmes de sécurité plus grands que ceux auxquels ils étaient censés répondre.

Lors de l'analyse des stratégies pour faire face et réagir aux menaces, il convient de tenir compte de :

- La sensibilité : vos stratégies répondent-elles rapidement aux besoins d'un individu ou d'un groupe?
- L'adaptation : vos stratégies s'adaptent-elles rapidement à de nouvelles situations une fois le risque d'agression passé ? Un défenseur peut se trouver devant plusieurs options. Par exemple, il peut avoir à choisir entre se cacher ou vivre chez d'autres personnes pour quelque temps. De telles stratégies peuvent paraître faibles et instables, cependant elles ont fait leurs preuves.
- La durabilité : vos stratégies peuvent-elles survivre à l'épreuve du temps, malgré des menaces ou des agressions non mortelles?
- L'efficacité : vos stratégies protègent-elles de manière efficace les personnes ou le groupe en question?
- La réversibilité : si vos stratégies ne fonctionnent pas ou que la situation évolue, peut-on modifier ou revenir sur ces stratégies?

Faire face au risque après l'avoir évalué

Une fois votre évaluation du risque réalisée, vous devrez étudier les résultats. Comme il est impossible de mesurer la "quantité" de risque encouru vous devrez comprendre le degré de risque.

Différents défenseurs et organisations peuvent estimer différents degrés de risque. Ce qui est inacceptable pour certains défenseurs peut être acceptable pour d'autres, et il en va de même pour les personnes d'une même organisation. Plutôt que de discuter de ce qui "doit" être fait ou de savoir si vous êtes ou non prêt à continuer, les différents seuils de risque des personnes doivent être identifiés : vous devez trouver un seuil acceptable pour tous les membres du groupe. Ceci dit, il y a différents moyens de faire face à un risque:

- Vous pouvez accepter ce risque tel qu'il est car vous vous sentez capable de vivre avec lui.

- Vous pouvez réduire ce risque, en travaillant sur les menaces, les vulnérabilités et les capacités.

- Vous pouvez partager ce risque, en lançant des actions en commun avec d'autres défenseurs afin de rendre les menaces potentielles à l'encontre d'un défenseur individuel ou d'une organisation, moins efficaces.

- Vous pouvez choisir d'éviter ce risque, en modifiant ou en mettant fin à vos activités ou en changeant de démarche afin de réduire les menaces éventuelles.

- Vous pouvez ignorer ce risque, en n'y prêtant pas attention. Il va de soi que ce n'est pas la meilleure solution.

Tenez compte du fait que les degrés de risque varient en général d'une organisation ou d'un individu à un autre et que les agresseurs ont habituellement tendance à s'en prendre aux parties les plus faibles, si bien que vous devez faire attention à ces différents degrés et prendre des mesures spécifiques. Par exemple, prenons le cas d'un paysan assassiné par la milice privée d'un propriétaire foncier. Plusieurs organisations et individus peuvent être impliqués, comme un groupe d'avocats de la ville la plus proche, un syndicat d'agriculteurs locaux et trois témoins (des paysans vivant dans le village d'à côté). Il est crucial d'évaluer les différents degrés de risque pour chacune des trois parties afin de planifier correctement la sécurité de chacun d'entre eux.

Tableau 3:
informations nécessaires à l'évaluation des vulnérabilités et des capacités

(À noter: en règle générale, l'information contenue dans la colonne de droite peut montrer qu'un composant donné, dans la colonne de gauche, est soit une vulnérabilité soit une capacité d'un défenseur ou groupe de défenseur particulier.)

Composants de vulnérabilités ou de capacités	Informations nécessaires à l'analyse des vulnérabilités ou capacités de ces composants
Composants géographiques, physiques et techniques	
L'exposition	Besoin d'être dans, ou de traverser, des zones dangereuses dans le cadre d'activités quotidiennes ou occasionnelles.
Les structures physiques	Les caractéristiques des bâtiments (bureaux, maisons, refuges, etc.); matériaux de construction, portes, fenêtres, placards. Barrières de protection. Veilleuses.
Les bureaux et locaux ouverts au public	Vos bureaux sont-ils ouverts au grand public? Existe-t-il des zones strictement réservées au personnel? Avez-vous affaire à des visiteurs qui vous sont inconnus?
Les lieux de refuge et itinéraires de fuite	Avez-vous des endroits pour vous cacher? Sont-ils faciles d'accès (distance physique) et qui y a accès (individus spécifiques ou groupe entier)? Pouvez-vous 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 de communication 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 de vulnérabilités ou de capacités	Informations nécessaires à l'évaluation des vulnérabilités ou capacités de ces composants
Composants liés au conflit	
Liens avec les parties en conflit	Les défenseurs ont-ils des liens avec les parties en conflit (parents, de la même région, mêmes intérêts) qui pourraient 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 qui pourraient s'avérer précieux aux yeux de groupes armés, et 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 les zones minées	Possédez-vous des informations sur les zones de conflits? Et sur les zones de sécurité pour vous aider à garantir votre propre sécurité ? Possédez-vous 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 ? Ou 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 pirates?
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?

Composants de vulnérabilités ou de capacités	Informations nécessaires à l'analyse des vulnérabilités ou capacités de ces composants
Être témoin ou détenir des informations précieuses	Les défenseurs sont-ils des témoins cruciaux dans des affaires qui mettent en cause des acteurs puissants? Les défenseurs ont-ils les informations pertinentes et uniques sur une affaire, ou une procédure particulières?
Avoir une explication cohérente et acceptable sur vos actions et vos 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?
Composants sociaux et liés à l'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 décisions s'effectuent par une ou plusieurs personnes? Existe-t-il une procédure de suppléance pour la prise de décisions et de responsabilités? Jusqu'à quel niveau la prise de décision reste-t-elle participative? Est-ce que la structure du groupe permet : a) des prises de décisions et mise en application en commun, b) des discussions des problèmes en commun, c) des réunions sporadiques et inefficaces, d) aucune des trois solutions ci-dessus?
Plans et procédures de sécurité	Existe-t-il des règles et procédures de sécurité en place? Existe-t-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).
Conditions de travail	Les contrats de travail sont-ils en règle pour tous? Avez-vous accès aux fonds d'urgence? Assurances?
Recrutement du personnel	Avez-vous des procédures appropriées pour recruter le personnel, les collaborateurs et les membres? Possédez-vous une procédure de sécurité spécifique pour les volontaires temporaires (tels que les étudiants, par exemple) ou visiteurs?
Travail avec les gens ou avec des organisations - interface	Votre travail comprend-il des entretiens directs avec les personnes? Connaissez-vous bien ces personnes? Travaillez-vous avec une organisation interface entre vous et ces personnes?

Composants de vulnérabilités ou de capacités	Informations nécessaires à l'analyse des vulnérabilités ou capacités de ces composants
S'occuper des témoins et des vic times avec qui nous travaillons	Evaluons-nous le risque encouru par les victimes et les témoins, etc., lorsque nous travaillons sur des cas précis? Avons-nous des mesures de sécurité précises lorsque nous les rencontrons dans les bureaux ou à l'extérieur? S'ils sont menacés, comment devons-nous 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)?
Capacité à mobiliser	Les défenseurs sont-ils capables de mobiliser des personnes pour des actions publiques?
Composants psychologiques (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 gens 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 le personnel?
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)?
Ressources de travail	
Capacité à comprendre le contexte de travail et les risques	Les défenseurs ont-ils accès aux 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 les 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 ? Avez-vous accès à des organisations particulières ou à un statut de membre qui améliore vos capacités de protection?
Personnel et charge de travail	Est-ce que les personnes ou le personnel à votre disposition couvrent la masse de travail nécessaire? Pouvez-vous planifier des visites sur le terrain en groupe (au moins deux personnes)?
Ressources financières	Possédez-vous les moyens financiers nécessaires pour assurer votre sécurité? Pouvez-vous manier de l'argent en toute sécurité?

Composants de vulnérabilités ou de capacités	Informations nécessaires à l'analyse des vulnérabilités ou capacités de ces composants
Connaissance des langues et des lieux	Parlez-vous les langues nécessaires à votre travail dans la région? Avez-vous une bonne connaissance de la région? (routes, villages, téléphones publics, centres de santé, etc)
Accès 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? Avez-vous la possibilité de publier des actions urgentes à travers d'autres groupes?
Accès aux médias et la 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:

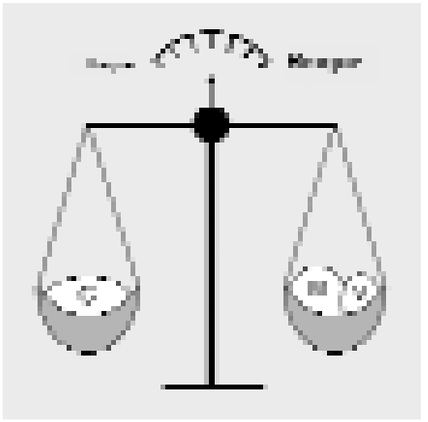


Fig. 1

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

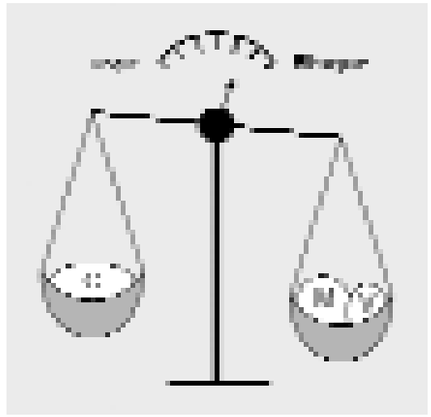


Fig. 2

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

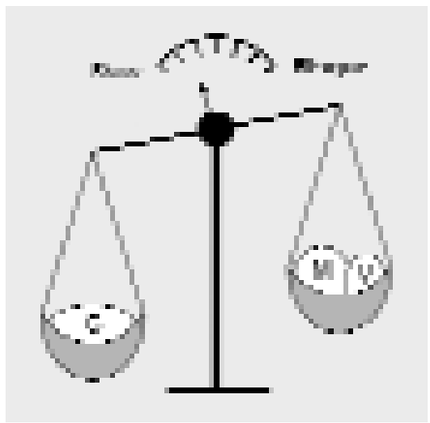


Fig. 3

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.

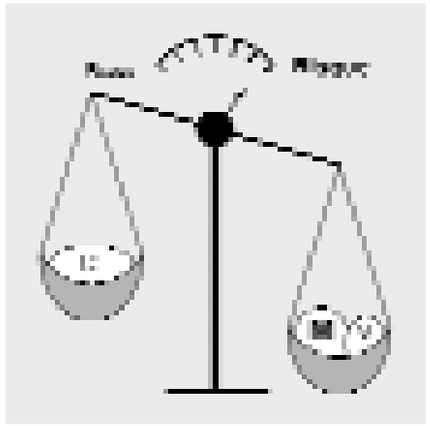


Fig. 4

CHAPITRE 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 au travail. C'est également le sujet 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 possibles (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 (comme par exemple recevoir une menace de mort). Nous allons à présent examiner aux 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 délicates. 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, qui exige un investissement

d'énergie plus important. Pourquoi? Il peut y avoir de nombreuses raisons 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 prix 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 ; dans les deux cas cependant les choses peuvent changer 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 devrions pas oublier qu'il y a une dimension émotionnelle dans toute menace.

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" 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 un 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 votre 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 deux objectifs principaux lors de l'évaluation d'une menace sont:

- D'obtenir 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).

- D'aboutir à une conclusion pondérée quant à la probabilité d'une mise à exécution d'une menace.

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 si les menaces présentent ou non une constante au fil du temps. Si plusieurs menaces sont faites à la suite (comme cela arrive souvent), il est important de chercher une constante, tels que les moyens employés pour menacer, le moment où les menaces se produisent, des symboles, de l'information écrite à la main ou une communication verbale, etc. Il n'est pas toujours possible d'établir de telles constantes, cependant elles sont importantes pour une évaluation correcte des menaces.

3 • Établissez le but de la menace. Puisque habituellement une menace a 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. 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 fausse. Ceci peut être un bon moyen pour l'auteur des menaces d'éviter un prix politique tout en parvenant à sa fin d'effrayer le défenseur et de l'empêcher de poursuivre son travail.

5 ◆ Arrivez à une conclusion 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 qu'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.

Par 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 seront 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 (1éme étape) vers un raisonnement spéculatif. La 2éme étape introduit une légère interprétation des faits que l'on approfondit progressivement dans les 3éme, 4éme et 5éme étapes. Il y a des raisons fondées pour lesquelles il convient d'observer l'ordre des étapes. Si vous commencez directement par la 2éme ou la 4éme 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 que ce sentiment d'inquiétude persiste jusqu'à ce que la menace soit passée. 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 abaisser leur 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 oeuvre 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 debriefing 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 4.

- Une évaluation des menaces déclarées peut vous amener à craindre une agression. Lisez le chapitre consacré à la prévention des attaques, chapitre 5.

CHAPITRE 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 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 pourrait réellement 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, simplement 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. Souvenez-vous : les menaces ont un objectif précis (voir chapitre 2), alors que les incidents surviennent, tout simplement.

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. Maintenant vous êtes en mesure de réagir à cette surveillance.

Les incidents de sécurité représentent "l'unité de base" de la 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 pourrait 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 alors les gens 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, ayant évalué l'incident au sein du groupe après que le défenseur l'a consigné dans le cahier, juge qu'une action n'est 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 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. Tout incident de sécurité remarqué par un défenseur doit être signalé, soit dans un cahier personnel ordinaire, soit dans un cahier accessible à tout le groupe.

2 • Analysez-les. Tous les incidents de sécurité consignés devraient 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 certains incidents (tels que des menaces). Est-il moral et réaliste 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, cependant il est souvent indiqué d'être aussi franc que possible en matière d'échange d'informations et de la gestion des problèmes logistiques, ainsi que des craintes.

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

• Une réaction à l'incident lui-même.

• Des retours d'informations, en termes de sécurité, à propos de votre manière de travailler, vos programmes ou vos stratégies de travail.

Exemple
d'un incident qui permet 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 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, vous modifiez une partie des activités prévues et prévoyez des réunions hebdomadaires pour suivre l'évolution de la situation.

Exemple
d'un incident qui vous permet d'élaborer vos stratégies de sécurité:

Lorsque vouz lancez vos activités de défenseur dans une nouvelle région, vous recevez immédiatement des menaces de mort et un de vos collègues est agressé physiquement. Vous n'aviez pas imaginé une telle opposition à votre travail, et n'aveiz pas prévu de réponse dans votre stratégie globale. Vous aurez donc à modifier votre stratégie afin de faire grandir la tolérance locale à l'égard de votre travail et de dissuader davantage d'agressions et de 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 qu'il a lieu et après qu'il soit passé.

Étape 1. 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) ou à la propriété ?

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

- Une réaction immédiate s'impose afin de porter des secours aux personnes blessées ou pour arrêter 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.
- 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.

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

Des 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, de revenir aux procédures d'organisation internes et de prévoir de meilleures réactions 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. La rapidité de votre action compte, mais il est plus 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 un groupe de défenseurs est informé qu'une de ses 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, 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.

CHAPITRE 5

Prévenir les agressions et y réagir

Objectif

Évaluer la probabilité qu'un certain type d'agression ait lieu.

Empêcher de possibles agressions contre les défenseurs.

Effectuer la contre-surveillance.

Agressions à l'encontre des défenseurs des droits humains

La violence est autant un processus qu'un acte. Une action violente contre un défenseur des droits humains n'a jamais lieu en vase clos. L'analyse détaillée des actions violentes montre qu'elles sont souvent le point culminant de conflits, de différends, de menaces et d'erreurs qui se sont accumulés et accentués 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:

1 ◆ L'individu qui recourt à la violence. 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.

2 ◆ Les antécédents et les déclics qui amènent l'agresseur à envisager la violence comme un moyen d'agir possible. Aux yeux de la majorité d'agresseurs, l'agression est un moyen d'atteindre un but ou de résoudre un problème personnel.

3 ◆ Le cadre qui favorise la violence, l'admet ou ne l'empêche pas.

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

En général, quiconque pense qu'une agression d'un défenseur est un moyen 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'attaquer un défenseur.

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

La menace peut décroître quand la capacité des agresseurs potentiels à organiser une agression est modifiée et que leur conception d'une agression comme acte acceptable change, ainsi que leur probabilité d'être pris et condamnés.

Il est donc vital 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 3).

- 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 (Cf. chapitre 4).

La surveillance des membres ou des bureaux est destinée à l'obtention d'informations et peut jouer des rôles différents:

- déterminer quelles activités sont menées, quand, par ou avec qui.

- utiliser ces informations lors d'une agression ultérieure de membres ou d'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).

- intimider vos alliés ou d'autres personnes avec qui vous collaborez, ou vous intimer de mettre fin à cette collaboration.

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 surgir lorsque l'agresseur voit soudain une occasion de frapper, mais même dans ces cas, l'agression a été préparée.

Souvent, les informations qui permettraient de détecter la préparation d'une agression sont rares. La disparité entre la quantité infime d'études sur ce sujet et le vaste nombre d'agressions contre les défenseurs des droits humains est frappante. Néanmoins, les recherches qui existent sont intéressantes à plusieurs égards[1].

[1] Claudia Samayoa et Jose Cruz (au Guatémala) et Jaime Prieto (en Colombie) ont fourni des études intéressantes sur les agressions à l'encontre des défenseurs des droits humains. Mahony et Eguren (1997) ont analysé de telles attaques.

- Attaquer 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 vital. (Cependant, si les circonstances sont extrêmement favorables à l'agresseur, il pourra agir plus facilement).

- 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. Les agressions ne sont par conséquent ni aléatoires, ni futiles 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 attentats contre des sièges d'ONG ou d'organisations très connues dans les villes provoquent encore davantage de tollés.

- Les choix et les décisions sont arrêtés avant une agression. Ceux qui envisagent une agression contre une organisation de défenseurs doivent décider si 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) et une série d'agressions (visant les membres de l'organisation). Les quelques études sur les agressions contre les défenseurs suggèrent 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 types d'agressions, à savoir les délits et crimes de droit commun, les agressions indirectes (se trouver au mauvais endroit au mauvais moment) et directes (ciblage), à l'aide des trois tableaux suivants[2].

[2] La classification des agressions est identique à celle des menaces : veuillez consulter le chapitre sur les menaces pour de plus amples explications.

Tableau 1: définir le degré de menace d'une agression directe (ciblage)

(AP signifie agresseur potentiel)

Degré de menace dans le cas d'agressions directes (ciblage)			
Facteurs	Degré de menace faible	Degré de menace moyen	Degré de menace élevé
Capacité d'agresser	Les AP ont une marge de manoeuvre 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, liquidités ou autres sources de profit financier (p.ex. la prise d'otages)	L'AP a un besoin clair de matériel ou de liquidités
Mobile politique et militaire	Aucun, votre travail n'est pas lié à leurs objectifs	Intérêt partiel, votre travail réduit leurs objectifs politiques et militaires	Votre travail entrave leurs intérêts, 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 claires
Capacité des forces de sécurité à dissuader des 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

du degré de menace d'agressions directes (ciblage):

Les AP 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.

Le degré de menace d'une agression directe
dans ce cas est donc faible à moyen.

Tableau 2: établir le degré de menaces de délits et crimes

(DC signifie délinquants et criminels)

Degré de menace pour les délits			
Facteurs	Menace faible	Menace moyenne	Menace grave
Mobilité et situation du criminel	Les DC restent habituellement dans leurs zones, évitent les zones des ONG	Incursion des DC dans d'autres zones de nuit (ou à proximité des zones d'ONG)	Les DC agissent partout, jour et nuit
Agressivité des DC	Les DC évitent la confrontation (commettent un crime en prédominance dans des zones où les ONG ne sont pas présentes)	Les DC se livrent à 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	Non armé ou utilisation d'armes non meurtrières	Armes de choc, y compris machettes	Armes à feu ; parfois puissantes
Taille et organisation	Les DC agissent seuls ou à deux	Deux à quatre DC agissant ensemble	Les DC agissent en groupes
Réponse des forces de l'ordre (police) et dissuasion	Réponse rapide, capacité de dissuasion	Réponse lente, peu d'appréhensions sur le fait	Réactions de la police sans la moindre efficacité
Formation et professionnalisme de la force publique	Bien formés et professionnels mais pénurie de ressources	Régulièrement formés, solde maigre, ressources limitées	La police inexistante ou corrompue (collabore avec les DC)
Situation générale de sécurité	Absence de l'Etat de droit mais sécurité relative	Sécurité défaillante	Les droits ne sont pas respectés, impunité totale

Exemple

de l'évaluation du degré de menace représenté par les délits et crimes:

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, et la force publique (police, gendarmerie) n'est pas professionnelle et manque de ressources. Cependant la direction de la police est bien disciplinée. La sécurité est manifestement faible, et si 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'un délit ou d'un crime dans le centre de cette ville est
maximale à moyenne.

Tableau 3: établir le degré de menace des agressions indirectes

(AP signifie agresseaur potentiel)

Degré de menace d'une agression indirecte			
Facteurs	Menace faible	Menace moyenne	Menace 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 des 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	Conflits géographiquement stables, déplacement faible et répertorié	Déplacement relativement fréquent	Déplacement géographique continu, les zones sont imprévisibles
Votre connaissance des régions minées (mines terrestres)	Bonne connaissance ou absence de zones minées	Connaissance approximative	Nulle
Distance de votre lieu de travail aux 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	Connues et répertoriées	Connues et répertoriées avec emploi périodique d'artillerie, d'embuscades et de francs-tireurs	Toutes interviennent sans discrimination: bombardement, artillerie lourde, attentats terroristes ou attaques à la bombe

Exemple

de l'évaluation du degré de menace d'une agression indirecte:

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 indirectes lié au travail dans cette zone est faible.

La prévention d'une possible agression directe

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

Pour empêcher une agression, il est donc nécessaire de :

- Persuader l'agresseur potentiel ou celui qui vous menace qu'une agression représenterait des coûts et des conséquences inacceptables.
- Rendre ces agressions moins réalisables.

Ce genre de prévention d'agressions est similaire à l'analyse effectuée au chapitre 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.

Tableau 4: La prévention des agressions directes et les différents résultats de protection

La prévention des agressions directes : Les différents résultats de protection	
1 • Modification du comportement des agresseurs: dissuader les agresseurs en alourdissant les conséquences négatives d'une agression →	Vous vous attaquez aux menaces et les réduisez (en agissant directement sur la source, ou contre tout fait provenant de cette source.
2 • Changement de l'adhésion des détenteurs des obligations[3] concernés à la déclaration de l'ONU sur les droits de l'homme: dissuader les agresseurs en aggravant les menaces de poursuites à l'encontre des auteurs d'une agression, et en défense des défenseurs →	
3 • Réduire la possibilité d'une agression: réduire l'exposition des défenseurs, améliorer le contexte de votre travail, bien gérer la peur et le stress, mettre au point des plans de sécurité, etc. →	Limiter les vulnérabilités, renforcer les capacités.

[3] Voir chapitre 1. Par exemple, après qu'un défenseur dénonce les menaces, le procureur, la police ou un autre organe enquête sur les faits et cette enquête débouche sur une action contre les individus responsables des menaces. Du moins, il s'agit peut-être de l'objectif d'une réaction pour empêcher une attaque.

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

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 oeuvre 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 ◆ Réduire votre exposition au maximum en vous cachant ou en quittant la zone[4].

c ◆ Tenter de vous assurer une protection armée, à condition qu'elle soit 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 (la réalité montre qu'obtenir une protection armée est extrêmement délicat). Parfois, un gouvernement offre une escorte armée au défenseur à la suite de pressions nationales ou internationales. Dans ces cas, consentir à l'escorte ou la refuser pourrait rappeler l'Etat à ses responsabilités de protection de la sécurité des défenseurs, mais en aucun cas un gouvernement pourra s'estimer délesté de ces responsabilités si le défenseur n'accepte pas l'escorte armée. Les entreprises de sécurité privée peuvent aggraver le risque si elles ont des liens secrets avec la force publique (voir le chapitre 9). Quant au port d'armes par les défenseurs des droits humains, nous devons admettre son inefficacité dans la majorité des cas en situation d'agression organisée. De plus, il fragilise les défenseurs vulnérables car un gouvernement peut avancer ce prétexte pour les réprimer en invoquant la lutte contre le terrorisme ou la répression d'une insurrection.

Les menaces qui peuvent précéder une agression sont plus faciles à gérer dès lors que d'autres acteurs importants ou parties prenantes sont impliqués et qu'ils 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.

4 Il y aura aussi des cas où voyager de nuit exposera le défenseur à un grand risque.

Surveillance et contre-surveillance

La contre-surveillance permet de savoir si vous êtes surveillé. Comme il est difficile de vérifier si vos communications sont placées sur écoute, il vaut toujours mieux le supposer[5]. Cependant, vous pouvez découvrir si vos faits et gestes ainsi que vos bureaux sont 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'installent à proximité de l'entrée de vos locaux, des individus dans les voitures garées à proximité, les visiteurs, etc. pourraient tous vous surveiller en puissance. La surveillance est un moyen de gagner sa vie, elle peut être imposée sous la menace, elle est parfois l'expression de convictions politiques, ou encore 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: 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 en 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 aux mouvements des individus dans votre quartier ainsi qu'aux 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 individus âgés ou très jeunes.

- Si vous soupçonnez quelqu'un de vous suivre, vous pouvez recourir à une tierce partie 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 partie peut observer leurs mouvements de loin lors de votre arrivée, votre départ ou de vos déplacements. Celui ou celle qui vous surveille vous observera en toute probabilité depuis un poste qui permette de vous garder à l'oeil aisément, qu'il s'agisse de votre domicile, des bureaux ou d'autres lieux de travail.

5 Pour plus d'informations sur les mesures de sécurité voir chapitre 12.

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. Faîtes 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 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 (voir chapitre 9).

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 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 certains cas de figure car parfois la surveillance se fait de manière ouverte puisque 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 lorsque ils sont surveillés ou qu'une agression potentielle est préparée à leur intention.

Quand devrez-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 de dénominateur commun entre 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 4.

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

- 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.

CHAPITRE 6

Elaborer une stratégie et un plan de sécurité

Objectif

Apprendre à élaborer une stratégie de sécurité.

Apprendre à établir un plan de sécurité.

Les défenseurs des droits humains qui travaillent dans des environnements hostiles

Trop souvent les défenseurs des droits humains travaillent dans des environnements hostiles. Les raisons en sont multiples. La plupart 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 soient 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 des tentatives de libre expression à des menaces déclarées et des offensives directes. Le degré de tolérance par les acteurs dépend du travail des défenseurs. Les acteurs jugeront qu'ils peuvent accepter certaines activités, et en condamner d'autres. En règle générale, cette indécision de leur part 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 de l'hostilité lors de bouleversements politiques, comme 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 sur des actions socio–politiques permettant d'améliorer le respect des droits humains et l'environnement des défenseurs. 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 lancent des mesures plus efficaces de protection des droits humains. Nous ne pensons habituellement pas que ces activités relèvent de questions de sécurité, cependant elles peuvent favoriser considérablement la protection de l'espace de travail sociopolitique des défenseurs des droits humains lorsque les résultats sont bons.
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 prix ou un ensemble de conséquences».
En définissant certaines conséquences comme «tolérables, et d'autres comme intolérables, le défenseur circonscrit un espace politique défini»[1].

Par exemple, un groupe de défenseurs peut s'occuper d'un cas de 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 mettre de côté le cas provisoirement et améliorer leurs capacités de sécurité dans l'intervalle.

Le concept de risque "tolérable" peut varier au cours 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 sont 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.

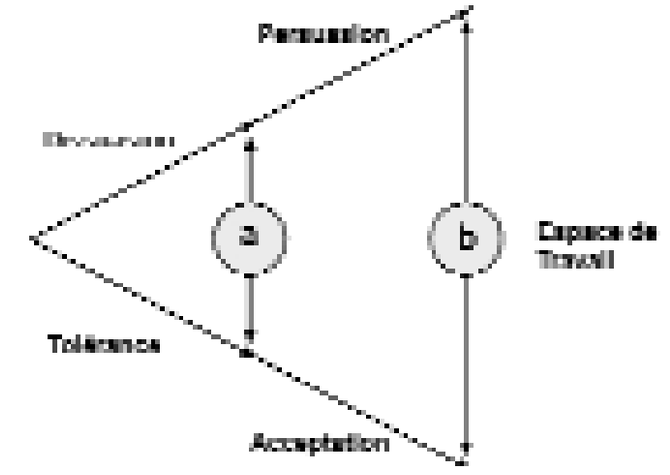
Cet espace politique d'activité, en plus d'être défini subjectivement par ceux qui y évoluent, est très sensible au moindre changement de l'environnement politique national. Il faut considérer qu'il s'agit d'un espace fluctuant et relatif.

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 autorités politiques et militaires ainsi que des groupes armés susceptibles d'être touchés par le travail des défenseurs et décider 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 défendeurs. Il sera plus faible si l'acteur entrevoit des coûts connexes. Dans ce cas, son degré de tolérance dépendra du prix 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 par conséquent causer la malveillance de son adversaire.

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



- La première 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).

- La 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 des 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 des régions de conflit, l'espace se limite généralement à ce que la tolérance des acteurs armés autorise, et découle partiellement du prix politique que représentent les agressions à l'encontre des défenseurs (dissuasion), l'espace étant alors réduit à l'intersection "a".

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 la tolérance à l'égard de votre travail, il est important de limiter l'affrontement à un

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

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 d'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 devriez consentir un effort soutenu pour informer et former de s 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 socio–politique 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 à votre risque et à vos capacités de protection.

- Dans vos stratégies, prévoyez des 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 par la dissuasion et la persuasion

Les défenseurs qui oeuvrent dans des milieux hostiles devraient pouvoir évoquer des 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 un 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 jugé 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 d'induire un adversaire à renoncer à exécuter l'action hostile envisagée. L'argumentation rationnelle, l'appel à la morale, une coopération renforcée, une meilleure compréhension des hommes, 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 ou international. Les défenseurs ne peuvent pas recourir trop fréquemment aux "menaces" directes : la stratégie vise davantage à rappeler aux autres les conséquences possibles de leurs décisions.

La dissuasion à l'oeuvre

Afin de vérifier si notre dissuasion est efficace, il nous faut remplir une série de conditions :

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 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 en vigueur de dissuasion.

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 prix – grâce à la résolution des défenseurs– paraissait plus lourd que les avantages.

Il est difficile pour les défenseurs de persuader un agresseur que la résolution à la dissuasion laisse indifférent. Ceci est le cas quand les gouvernements peuvent faire l'objet de sanctions de la communauté internationale mais 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.

Elaborer le plan de sécurité

Il est simple de rédiger un plan de sécurité. Procédez selon ces quelques étapes :

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

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

Il pourrait s'avérer utile que votre plan de sécurité comporte :

- Des plans et protocoles de prévention pour vous assurer que vos activités de routine répondent aux normes de sécurité, comme lorsque vous préparez une déclaration publique ou une visite dans une région isolée.

- Des plans d'urgence pour réagir à des problèmes spécifiques, p.ex. une détention ou une disparition.

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 dans 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 ◆ Elaborer 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 les menaces de mort explicites; OU la menace la plus probable et grave, à savoir si des organisations similaires à la votre ont été attaquées, vous êtes clairement potentiellement menacé; OU le type de menace auquel vous êtes le plus vulnérable parce que vous le risquez davantage.

- Enumérez les vulnérabilités qui correspondent aux menaces énumérées. Il faut aborder ces vulnérabilités en premier lieu, mais souvenez-vous que toutes les vulnérabilités ne correspondent pas à toutes les menaces. Par exemple, si vous recevez une menace de mort, il pourrait ne pas être très utile de commencer à bien fermer les serrures des placards de votre bureau du centre-ville (à moins que vous puissiez être facilement agressé au bureau, ce qui n'est pas le cas habituellement). Il s'avérera plus utile de réduire votre exposition pendant votre trajet entre le domicile et le lieu de travail ou pendant le week-end. Fermer les placards n'est pas secondaire, mais en soi cela ne réduira probablement pas votre vulnérabilité à la menace de mort.

- Enumérez les capacités qui correspondent aux menaces énumérées

Vous pouvez maintenant aborder les menaces choisies, les vulnérabilités et les capacités de votre plan de sécurité et pouvez être relativement sûr de pouvoir réduire votre risque d'un bon point de 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 d'obtenir un plan "vivant" et « réaliste » et c'est cela qui est compte en matière de sécurité. (Veuillez vous reporter à la liste détaillée de composants de plan de sécurité possibles en fin de chapitre que vous pouvez également utiliser pour évaluer les risques).

Faire face aux problèmes de sécurité : la gestion de la sécurité pas à pas

La gestion de la sécurité n'est jamais finie et reste toujours partielle et sélective :

- Il y a toujours des limites à la quantité d'informations que vous pouvez traiter, tous les facteurs affectant la sécurité ne peuvent être rassemblés et examinés en même temps.

- Il s'agit d'un processus complexe. Il faut du temps et beaucoup d'efforts pour permettre une prise de conscience, développer un consensus, former les gens, gérer le renouvellement du personnel, mettre en oeuvre les activités, etc.

La gestion de la sécurité est pragmatique

La gestion de la sécurité peut rarement prétendre aboutir à une révision exhaustive à long terme. Elle permet de prévenir les agressions et de souligner le besoin de stratégies de l'organisation pour y faire face. Ceci peut paraître peu

ambitieux, mais n'oublions pas que trop peu de ressources sont généralement affectées à la sécurité !

En examinant les pratiques de sécurité d'un défenseur des droits humains ou d'une organisation, vous découvrirez peut-être quelques lignes directrices, des plans, mesures ou types de comportement déjà en application. Il y aura des forces en conflit, depuis des idées arrêtées sur les pratiques de sécurité jusqu'à la réticence d'alourdir la charge de travail existante par des activités de sécurité supplémentaires.

La pratique de la sécurité est l'exemple même d'un projet évolutif fragmenté et intuitif. La gestion de la sécurité devrait avoir pour but d'apporter des changements graduels pour améliorer la performance. Les règles et les procédures de sécurité ont tendance à venir de secteurs d'une organisation chargés de questions précises, comme la logistique, une équipe sur le terrain craignant pour sa sécurité, un gestionnaire sous la pression d'un donateur inquiet pour la sécurité, etc.

Peu à peu la gestion de la sécurité ouvre la voie à des processus informels et permet à de nouvelles pratiques de prendre racine. Des événements imprévus comme les incidents de sécurité exigeront des décisions urgentes à court terme qui, si elles sont gérées correctement, définiront des pratiques de sécurité à plus long terme pour l'ensemble de l'organisation.

Mettre en oeuvre un plan de sécurité

Les plans de sécurité sont importants, mais difficiles à mettre en oeuvre. La mise en oeuvre 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 ainsi que les obstacles et les difficultés.

Un plan de sécurité doit forcément être mis en oeuvre à trois niveaux :

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

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

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

Exemples d'angles d'attaque et de circonstances pour la mise en oeuvre d'un plan de sécurité :

- Plusieurs incidents de sécurité mineurs sont survenus dans votre organisation ou une autre et cela inquiète un certain nombre de membres.
- La situation sécuritaire du pays est préoccupante.
- De nouveaux membres arrivent et peuvent 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 angles d'attaque 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 cruciale 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 effectuent le travail réel, 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 "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 compor-

tent une section consacrée à la sécurité, discutez systématiquement de la sécurité aux 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, des positions et un certain comportement qui affectent la sécurité peuvent avoir des conséquences pour la sécurité des témoins, des membres de la famille des victimes et des collègues. Il faut s'engager collectivement à mettre en oeuvre de bonnes pratiques de sécurité.

- Du temps et des ressources doivent être affectés à la mise en oeuvre du plan puisqu' on ne pourra pas améliorer la sécurité pendant le temps libre des personnes. Pour qu'elles soient perçues comme « importantes », les activités de sécurité doivent figurer à côté d'autres activités «importantes ».

- Tous doivent adhérer visiblement au plan, en particulier les directeurs et les personnes responsables du travail collectif. Il faut que les personnes qui refusent obstinément d'adhérer au plan soient blâmées ou sanctionnées.

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 pouvez choisir et combiner ces idées pour compléter votre plan de sécurité.

- Le mandat de l'organisation, sa mission et ses objectifs généraux.

- Une déclaration de politique de sécurité de l'organisation.

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

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

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

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

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

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

- Les politiques de l'organisation en matière de :

  1-Le repos, le temps libre et la gestion du stress. 2-Les incidents graves, tels que l'enlèvement, la disparition, les blessures personnelles, etc. 3-La sécurité des témoins. 4-La prévention des accidents et en matière de santé. 5-Les liens avec les autorités, les forces de sécurité et les groupes armés. 6-La gestion et stockage de l'information, le traitement de documents confidentiels et de l'information. 7-Votre propre image par rapport aux valeurs religieuses, sociales et culturelles. 8-La gestion de la sécurité dans les bureaux et les domiciles (y compris pour les visiteurs).

- Des plans de prévention et des protocoles sur :

  1-La préparation des missions sur le terrain. 2-Le maniement d'argent liquide et des objets de valeur. 3-Les moyens de communication et protocoles s'y rapportant. 4-L'entretien des véhicules. 5-Les mines terrestres. 6-La réduction du risque d'être la cible de délits et crimes de droit commun, d'incidents armés ou d'agressions sexuelles. 7-La réduction du risque pendant les déplacements ou dans des zones dangereuses.

- Des plans et des protocoles pour réagir aux crises de sécurité, telles que :

  1- Les urgences médicales et psychologiques (y compris sur le terrain). 2-Les agressions, y compris les agressions sexuelles. 3-Les cambriolages. 4-Les réactions appropriées lorsqu'une personne attendue ne se présente pas. 5-L'arrestation et la détention. 6- L'enlèvement. 7- Les incendies et autres accidents. 8-L'évacuation. 9-Les catastrophes naturelles. 10-Les fouilles légales ou illégales ou les effractions dans les bureaux ou les domiciles 11- Si une personne est la cible de tirs. 12- Si une personne est assassinée. 13- En cas de coup d'Etat.

CHAPITRE 7

Evaluer 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.

La roue de la sécurité

Commençons par le plus facile. Pour tourner correctement, une roue doit être parfaitement ronde. Jusque-là, il n'y rien à dire. Mais que se passe-t-il si quelques rayons de la roue sont plus longs que d'autres ? La roue ne serait pas parfaitement ronde et ne tournerait pas correctement.

Il en va de même pour la gestion de sécurité au sein d'un groupe ou d'une organisation. Si les composants principaux de la sécurité ne sont pas conçus d'un seul tenant, on ne peut pas s'attendre à ce que toute la stratégie de sécurité fonctionne bien. En partant de là, vous pouvez dessiner ce que l'on appellera une "roue de la sécurité". Vous pourrez l'utiliser pour examiner la façon dont vous gérez la sécurité, et d'établir dans quelle mesure la sécurité est intégrée au travail d'un groupe de défendeurs.

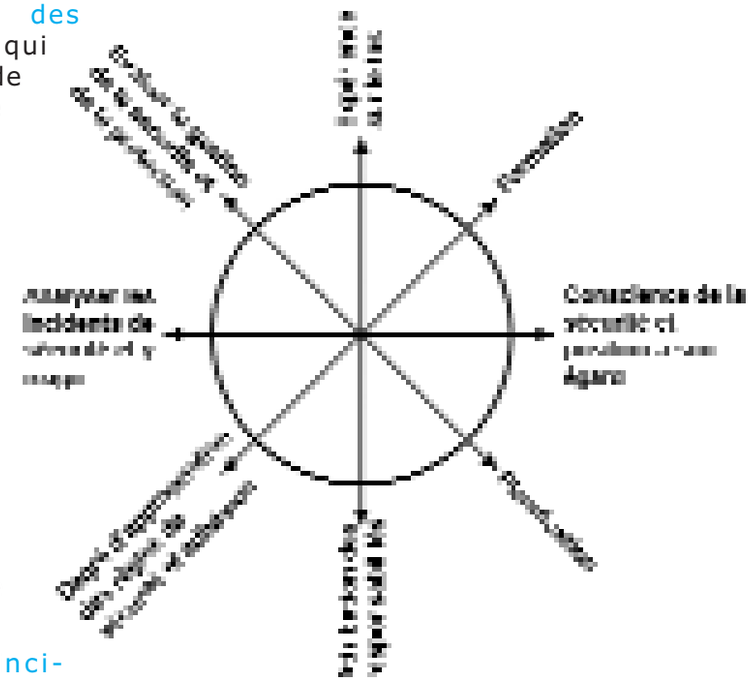
Cette évaluation peut se faire en groupe. Vous pouvez énumérer des explications du manque de développement de certaines parties de la roue, et suggérer de nombreuses façons de résoudre ces problèmes. Une fois les solutions possibles énumérées, vous pouvez vous mettre au travail et choisir celles que vous souhaitez appliquer.

Une fois que vous aurez terminé cette évaluation de votre roue de la sécurité, gardez le résultat et le diagramme. Lorsque vous répéterez l'exercice quelques mois plus tard, vous pourrez comparer les diagrammes ancien et nouveau et vérifier point par point si les choses vont mieux.

Les composants de la roue de la sécurité

La roue est composée de huit rayons, ou composants:

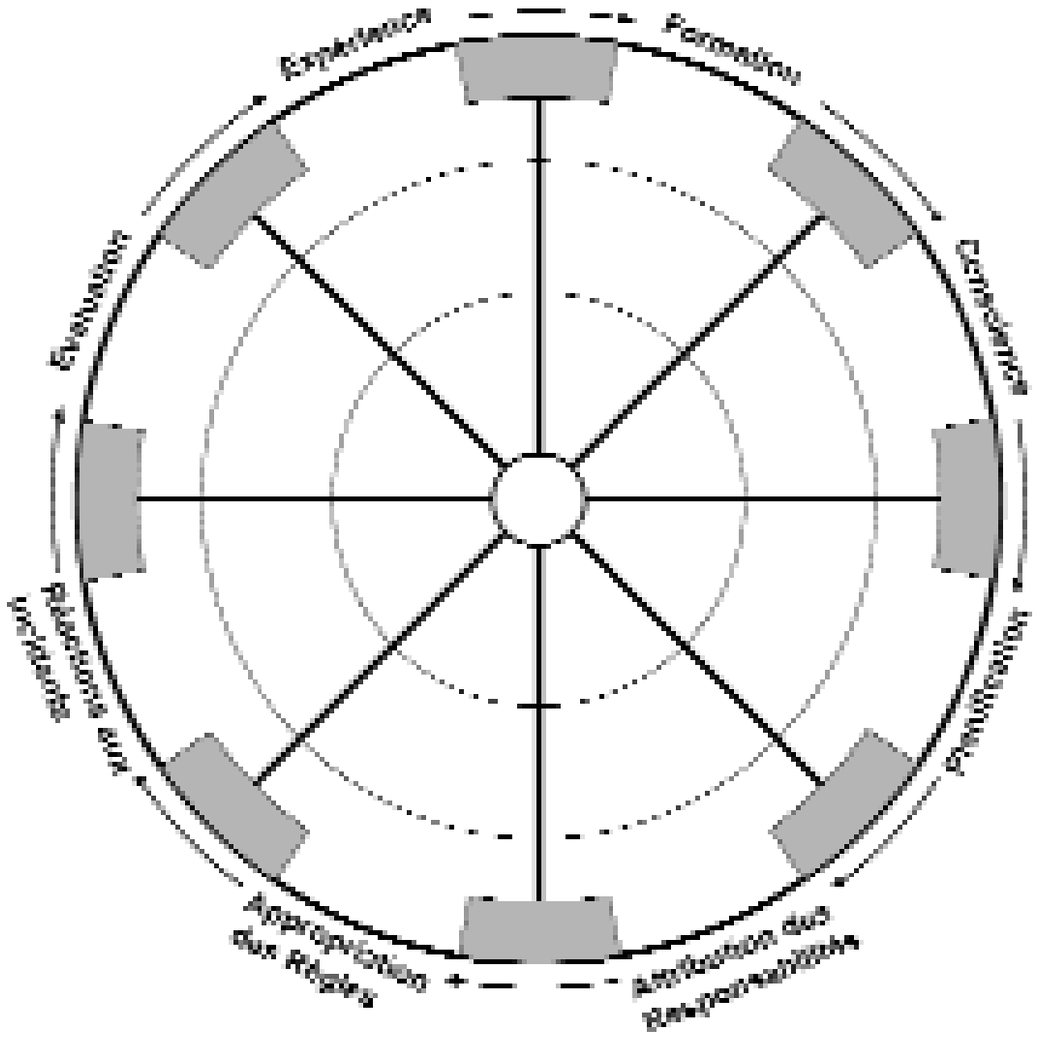
- L'expérience sur le terrain: les connaissances pratiques acquises en sécurité et en protection. Votre point de départ et votre but.
- La formation. Vous pouvez vous former à la sécurité dans un cours ou à votre propre initiative pendant votre travail.
- La conscience de la sécurité et la position à 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 oeuvre?
- La planification: la capacité de planifier en matière de sécurité et de travail. Planifier dans le but de protéger.
- L'attribution des responsabilités: qui est responsable de quels aspects de la sécurité et de la protection? Et dans les cas d'urgence?
- Le degré d'appropriation des règles de sécurité et l'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 la protection : si votre travail quotidien ainsi que les réactions aux incidents de sécurité sont analysés, cela contribuera au savoir et à l'expérience des individus et de l'organisation.

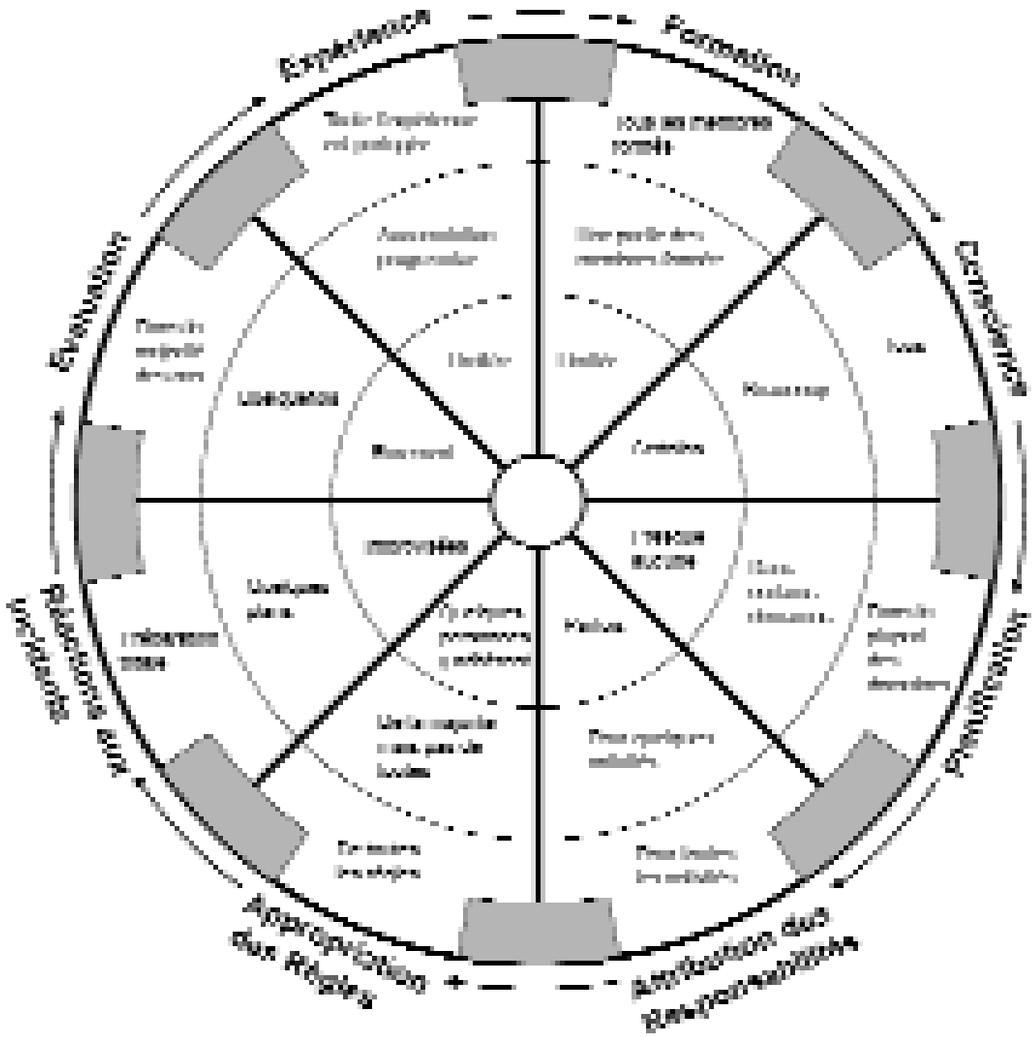
Maintenant que vous connaissez mieux les composants de la roue de la sécurité, essayez de construire un diagramme en ajoutant plus d'informations. Il pourrait ressembler à ceci:

La roue de la sécurité et ses huit rayons ou composants



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.

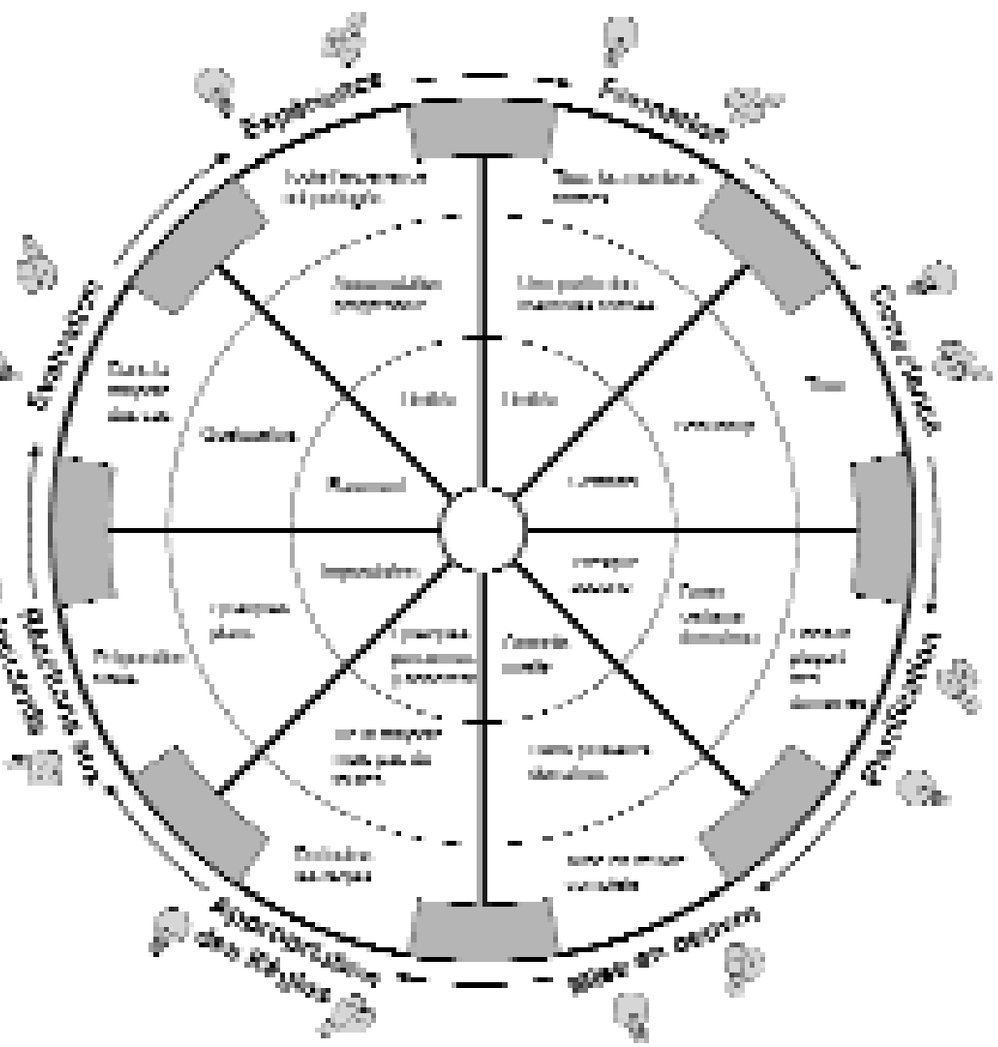


Photocopiez la roue sur une feuille ou sur un transparent et coloriez les espaces entre les rayons. Ceci illustrera la forme réelle de la roue de votre groupe ou de votre organisation, et fera apparaître plus clairement quelles parties sont plus ou moins développées.

Si un des huit composants de la roue est défaillant, vous devrez déterminer:

Les problèmes de cette composante….

...et quelles sont leurs solutions.



CHAPITRE 8

S'assurer que les règles et procédures de sécurité sont respectées

Objectif

Etablir pourquoi les employés et des organisations sont incapables ou réticents de respecter des plans et procédures de sécurité et trouver 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 à 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 beaucoup moindre si les 12 personnes au total 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 l'efficacité réelle. 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 sa mise en oeuvre. La formation à la procédure, sa compréhension et son acceptation sont également cruciaux.

Tableau 1: 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 de 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 pense-bêtes 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 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 déficiente 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 signalera 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 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 per-

sonne 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.

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.

Pour conclure,

Certains estimeront peut-être qu'examiner pourquoi 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 qu'on y obéisse, 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...

CHAPITRE 9

Améliorer la sécurité au travail et au domicile

Objectif

Évaluer la sécurité au travail et au domicile.

Planifier, améliorer et vérifier la sécurité des bureaux et des domiciles.

La sécurité au travail et au domicile

La sécurité du siège de l'organisation ou de ses bureaux, et aux 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 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. Dans de rares cas, il faudra également 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 ne servira pas à grand-chose si on ne prévoit personne pour se déplacer et vérifier ce qui s'est passé. 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.

Cependant il est 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.

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

Si des personnes veulent entrer dans votre bureau à votre insu, ils ne choisiront pas l'accès le plus difficile pour le faire. 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

Les facteurs dont il faudra tenir compte lors de l'installation d'un bureau sont: le voisinage, si les locaux étaient associés à un groupe particulier ou à des activités par le passé, l'accès par les transports publics ou privés, les risques d'accidents, si les locaux se prêtent aux mesures de sécurité, etc (à consulter aussi le risque dans l'évaluation 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 aux habitants des environs. En 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.

Il est tout aussi important de vérifier qui est votre propriétaire. Quelle est sa réputation? Pourrait-il s'avérer sensible aux pressions des autorités? Acceptera-t-il que vous mettiez en place des mesures de sécurité?

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. Il est important de prendre en considération l'accès à ce bureau par transport public – 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 on veut éviter de devoir traverser des zones dangereuses.

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

Liste de contrôle pour choisir le bon emplacement d'un bureau	
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); 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	Incendies, inondations graves, glissements de terrain, déversement de substances toxiques, 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.

Accès au bureau par une tierce partie: barrières matérielles et procédures à suivre par les visiteurs.

L'objectif premier pour la sécurité d'un bureau est de refuser l'accès non autorisé aux personnes. Une ou plusieurs personnes pourraient entrer pour voler, obtenir des informations, cacher quelque chose qui pourrait être utilisé contre vous à une date ultérieure, tels que de la drogue ou des armes, ou pour vous menacer. Chaque cas est différent, mais le but reste le même. Faites tout pour l'éviter.

L'accès à un bâtiment est contrôlé par des barrières matérielles (barrières, portes, grilles), par des mesures techniques (alarmes avec veilleuses) et des procédures d'admission des visiteurs. Chaque barrière et chaque procédure sont un filtre à travers lequel quiconque voulant entrer doit passer. Dans l'idéal, ces filtres devraient être combinés pour former plusieurs niveaux de protection, capables d'empêcher les différentes sources d'entrée non autorisées.

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 autre, au-delà d'un jardin ou d'une cour.

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 visiblement délimité 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.

Le périmètre du bâtiment

Ceci comprend les murs, les portes, les fenêtres et le plafond ou le toit. Si les murs sont solides, toutes les ouvertures et le toit le seront automatiquement. 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 scellées dans la paroi. S'il y a un toit, il 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.

Dans un endroit où il existe un risque d'attaques armées, il faut établir des zones protégées à l'intérieur même du bureau (voir chapitre 11 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.

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'aux membres. 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

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 facile 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 hors de l'accès de l'intrus qui pourrait ouvrir la caméra et détruire la cassette.

Vous devrez éventuellement vérifier que les caméras ne dissuadent pas votre public cible, à savoir des victimes et des témoins, et qu'elles ne soient pas pris pour butin facile attirant les cambrioleurs. Il est de bonne guerre d'avertir les visiteurs qu'ils seront filmés, par une affiche d'information. (le droit à la confidentialité est également un droit humain).

Les entreprises de sécurité privées

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 ces 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. 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 accord 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 l'accord soit respecté.

Par exemple:

> Si vous avez engagé un service de sécurité qui envoie un garde en inspection au cas d'un déclenchement d'une alarme, ce garde pourra éventuellement avoir accès aux zones sensibles de votre bureau et poser des puces dans votre salle de réunions.

Il est préférable que vous ayez le droit de donner votre accord sur les personnes (et que vous les sélectionniez) spécifiques qui travailleront pour vous, 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), cependant 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 probable capacité armée (petites armes à feu) incitera probablement les assaillants à utiliser leurs armes de gros calibre. À ce stade, si vous estimez que vous avez besoin de gardes armés de mitrailleuses, disposez-vous 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 poser des questions ou faire une livraison, et ne demanderont pas nécessairement l'autorisation au préalable. Examinons ceci cas par cas :

Quelqu'un téléphone ou sonne et demande le droit d'entrer pour une raison donnée.

Vous devrez alors suivre trois étapes simples:

1 ◆ Demandez à la personne 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'éviter de devoir ouvrir ou de vous rapprocher de la porte, et il faut donc utiliser tous les moyens, à savoir les judas, les caméras ou l'interphone, pour pouvoir refuser l'entrée le cas échéant ou en cas d'assaut violent ou forcé. Il est donc bon de définir une salle d'attente pour les visiteurs qui soit physiquement séparée de l'entrée interne au 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 dire vouloir entrer pour 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 une garantie de l'authenticité ou de la légalité 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, 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 n'êtes pas sûr(e) du but de leur visite, ne les 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 restreintes.

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, l'heure de son départ, etc. Ceci peut s'avérer particulièrement précieux au moment d'analyser ce qui n'a pas fonctionné après un incident de sécurité.

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 un collègue ou d'autres personnes, ni donner des 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.

Souvent les personnes se présentent par erreur, demandant si un tel 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'un colis piégé. 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 falsifier 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 prendra 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 livré ultérieurement ou qu'il soit gardé à la poste.

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

Durant les réceptions ou les soirées

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

Prenez note des appels téléphoniques et des visiteurs

Il peut également être utile de prendre note des appels téléphoniques et des numéros de téléphone et 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 vont faire des heures supplémentaires tard le soir devraient faire rapport à des heures précises à d'autres membres et faire particulièrement attention lorsqu'ils quittent les locaux, etc.

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 informatique, 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 a 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.

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 pensez qu'il s'agit d'une bombe, ne l'ignorez pas, ne la touchez pas, et contactez la police.

Lors d'un éventuel déménagement de bureau, ou si 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: 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 sachent 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 auraient accès. Ne "cachez" jamais des clés hors de l'entrée du bureau puisque cela les rendrait alors accessibles et non cachées.
- Les procédures d'admission: si un intrus potentiel est autorisé à entrer dans le bureau, les barrières de sécurité n'offriraient 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 les objets vulnérables, comme des informations stockées sur le disque dur, afin de les protéger de tout accès. En cas d'une évacuation d'urgence, emportez-les.
- 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. 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 soient 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 la 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?

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 au 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 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 renouvelées 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?

◆ Faites le bilan de tous les incidents de sécurité attestés 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).

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 à la sécurité? La formation est-elle efficace?

Chapitre 10

La sécurité et les femmes défenseurs des droits humains

Objectif

Examiner les besoins spécifiques de sécurité et les femmes défenseurs des droits humains.

Ce chapitre tente d'aborder certaines questions fondamentales relatives aux besoins de sécurité et les femmes défenseurs des droits humains. Cette question exige une analyse plus approfondie qui s'appuie sur les expériences réelles des femmes défenseurs des droits humains. La réalisation de documents plus détaillés est prévue dans le contexte de la consultation internationale sur les femmes défenseurs des droits humains en 2005.

Les femmes en tant que défenseurs des droits humains

Les femmes ont toujours été des protagonistes importants de la défense et la protection des droits humains. Pourtant, leur rôle n'a pas toujours été reconnu positivement. Les femmes travaillent seules et collaborent avec des hommes pour défendre les droits humains[1]. Beaucoup de femmes appartiennent à des organisations qui s'occupent de personnes disparues ou de prisonniers. D'autres défendent les droits des minorités ou des victimes de violence sexuelle, d'autres encore sont syndicalistes, avocates ou militent en faveur des droits à la terre.

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, la représentante spéciale du Secrétaire général des Nations unies sur les défenseurs des droits humains, déclare que:

> 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

[1] Un guide très utile est disponible sur le site Internet du Haut Comité des Nations unies sur les femmes défenseurs des droits humains http://www.unhchr.ch/defenders/tiwomen.htm. Voyez également "Report : Consultation on Women HRDs with the UN Special Representative of the Secretary General on Human Right Defenders, April 2 – 6 2003", publié par Asia Pacific Forum on Women, Law and Development, ainsi que : "Essential actors of our time. Human rights defenders in the Americas" par Amnesty International.

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 deviennent plus visibles. 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 peut-être 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, non seulement elles pourraient subir des violations des droits humains en raison de leur défense des droits humains, mais ceci d'autant plus qu'elles appartiennent au genre féminin, et que leur travail peut aller à l'encontre de stéréotypes de la société de la nature soumise des femmes, ou encore contester les notions sociétales sur le statut des femmes.

Deuxièmement, 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 de mères, 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.

Troisièmement, 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 du patriarcat et un facteur de perturbation de moeurs 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 de 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 définir plus précisément les besoins spécifiques et souvent variés des femmes défenseurs, 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 de difficultés au quotidien.

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. Voici une liste d'explications possibles:

Les femmes peuvent susciter de l'attention indésirable.

Les femmes défenseurs peuvent susciter de l'hostilité puisque leur double qualité de femmes et de défenseurs des droits humains pourrait braver des valeurs culturelles, religieuses et sociales locales de la féminité et du rôle des femmes. Les femmes défenseurs pourraient subir des violations des droits humains pas seulement par leur travail, mais simplement parce qu'être une femme qui travaille ou défendre les droits humains peuvent heurter les stéréotypes de la société de la nature soumise des femmes et les convictions à propos de leur statut.

Les femmes défenseurs devront peut-être enfreindre des lois patriarcales et des tabous sociaux.

Dans certains pays, défendre le droit des femmes à la vie et à la liberté a amené les femmes défendeurs à voir leur propre vie et leur liberté violées. De même, c'est pour avoir dénoncé des pratiques discriminatoires qu'une éminente avocate des droits de la femme a été poursuivie pour apostasie. Dans beaucoup de cultures, l'obligation pour les femmes de se soumettre aux hommes en public peut les empêcher de dénoncer ouvertement les violations de droits humains par des hommes. Certaines interprétations discriminatoires ou sexistes de textes religieux sont souvent invoquées pour maintenir ou établir des lois ou des pratiques qui ont un impact énorme sur les droits des femmes.

Il existe des types d'agressions spécifiques contre les femmes défenseurs.

L'hostilité, le harcèlement et la répression subis par les femmes défenseurs peuvent être spécifiques au genre et vont d'une violence verbale exclusivement destinée aux femmes au harcèlement sexuel et au viol. Les conséquences de telles agressions peuvent également être spécifiques aux femmes, avec une possible grossesse ou le rejet par la société.

Les femmes défenseurs se verront obligées de "défendre" leur intégrité :

Le professionnalisme des femmes et leur position dans la société peuvent être menacés et discrédités de manières qui leurs sont propres comme lorsque leur intégrité est mise en cause.

Leurs collègues masculins pourront ne pas comprendre, ou même rejeter, le travail des femmes défenseurs.

Les collègues masculins des femmes défenseurs des droits humains peuvent avoir les mêmes préjugés moraux que les personnes extérieures qui les agressent. Les hommes pourraient aussi se sentir menacés par la rivalité professionnelle avec une femme. Ceci peut donner lieu à des tentatives de marginalisation et de sape des femmes défenseurs des droits humains et peut parfois avoir pour résultat du harcèlement et de la violence contre les femmes défenseurs de la part de leurs collègues.

Les femmes défenseurs pourraient être victimes de violence conjugale :

La violence conjugale peut découler de structures de pouvoir changeantes dans les familles. Le rôle professionnel et l'habilitation grandissantes d'une femme défenseur pourraient amener son mari, partenaire ou les membres de sa famille à se sentir menacés et les pousser à vouloir mettre fin à ses activités ou à devenir violents. La violence conjugale à l'encontre des femmes comprend tout préjudice physique, sexuel et psychologique porté au sein de la famille, tels que la maltraitance, le viol conjugal, la mutilation génitale et d'autres pratiques traditionnelles portant atteinte aux femmes (voir ci-dessous).

Des obligations familiales supplémentaires :

Beaucoup de femmes défenseurs doivent s'occuper d'enfants et d'autres parents en plus de leur travail. De telles responsabilités, surtout s'il y a des enfants en bas âge, influenceront de nombreuses décisions de sécurité qu'une femme défenseur sera amenée à prendre dans une situation de risque élevé.

Vers une meilleure sécurité et protection des femmes défenseurs des droits humains

Il faut reconnaître que les femmes défenseurs représentent une grande variété d'êtres humains vivant des problèmes différents, venant d'horizons différents et exigeant des solutions différentes. Retenons avant tout que les femmes sont des défenseurs des droits humains capables d'identifier des problèmes et d'y trouver des réponses, quelles que soient les conditions de sécurité. Afin d'y parvenir, il faut intégrer la participation des femmes, veiller à ce que les aspects spécifiques au genre en matière de sécurité des femmes soient abordés et offrir des formations:

Elargir la participation des femmes défenseurs

En substance, cela signifie garantir la participation à part entière des femmes aux prises de décision à côté des hommes, 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, qu'elles les vérifient et les évaluent.

Garantir l'examen des besoins de sécurité et de protection propres au genre

Comme pour d'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 connaîtront bien les besoins spécifiques des défenseurs femmes. Parfois, il faudra nommer quelqu'un pouvant apporter une connaissance et une compréhension précises à la question. Une personne peut être chargée de la sécurité, mais ensuite l'organisation charge une autre personne formée et compétente de 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 pour tous ceux qui travaillent ensemble au sein d'une organisation des droits humains est la clé pour améliorer la sécurité et la protection et devrait aussi sensibiliser aux besoins spécifiques des femmes défenseurs.

Dénoncer la violence à l'encontre des femmes est encore une pratique trop rare. Une conscience générale de la violence spécifique au genre au sein de l'organisation ou du groupe permet plus facilement aux personnes de parler des menaces ou des incidents spécifiques au genre. Des membres peuvent aussi se porter volontaires comme 'points de chute' pour les défenseurs femmes et hommes qui souhaitent pouvoir répondre aux menaces spécifiques au genre et à la violence qu'eux-mêmes ou d'autres subissent dans l'organisation ou la communauté.

En résumé,

Les différents besoins de sécurité des femmes sont liés à leurs rôles différents, à différents types de menaces 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 spécifiques au genre.

Les agressions sexuelles et la sécurité personnelle

La prévention d'une agression sexuelle peut être semblable à celle d'autres agressions, notamment les agressions liées à la criminalité de droit commun. Les agressions sexuelles peuvent ressembler à une répression du travail des défenseurs, les victimes étant alors des cibles présélectionnées ou correspondant à un intérêt précis.

Tous, hommes et femmes, peuvent être victimes d'une agression sexuelle mais les femmes sont des cibles plus fréquentes. L'agression sexuelle est un crime de pouvoir et de violence, et le contact sexuel n'est qu'un autre moyen pour l'agresseur de démontrer son pouvoir.

Rappelez-vous souvent les femmes emmenées de force à un autre lieu par un agresseur potentiel sont violées (et battues voire assassinées), et que les femmes devraient donc toujours décider de manière énergique et nette de ne pas accompagner un agresseur potentiel à un autre lieu (à moins qu'un tel refus ne mette sérieusement sa vie ou celle d'autrui en danger).

Réagir à une agression sexuelle [2]

Il y a très peu de choix pour répondre 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 sont :

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. Le fait de faire ou de dire quelque chose de désagréable ou de dégoûtant qui coupe l'appétit sexuel de l'agresseur. Dites-lui que vous êtes infectée par le SIDA, que vous avez la diarrhée, faites-vous vomir, etc.

3 ◆ La résistance active. Mobilisez votre force physique comme vous le pouvez pour repousser l'agresseur, que ce soit en frappant, donnant des coups de pied, mordant, griffant, criant ou en vous enfuyant en courant.

Dans tous les cas, faites ce que vous devez pour survivre. Suivez votre instinct. Personne ne sait comment il réagirait dans un cas pareil et votre réaction sera la bonne pour vous vu la situation.

Après une agression sexuelle

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. Le plan de réaction devrait comprendre au moins des soins médicaux efficaces pour la victime, y compris un soutien psychologique (à savoir un dépistage des maladies sexuellement transmissibles immédiatement après l'agression suivi par des contrôles réguliers, la pilule du lendemain, etc.) et des conseils juridiques.

[2] 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 Oecuménique des Églises.

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

Veuillez vous rapporter également au chapitre 5, " Prévenir les agressions et y réagir".

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 ailleurs, 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)

CHAPITRE 11

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 des civils tués sont victimes de pratiques guerrières sans distinction 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 un risque élevé.

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

Le risque d'être pris pour cible

Les types de tirs

Vous pouvez être exposés 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. Les tirs peuvent vous viser plus ou moins directement et vont des tirs d'un franc-tireur ou de l'assaut par hélicoptère de combat par conditions de bonne visibilité aux assauts d'obusiers dirigés ou aux barrages d'artillerie. Il peut s'agir également de tirs de saturation qui visent à "pulvériser" une zone entière.

Plus le tir vise un but précis, plus votre 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 que cela arrive. 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, mais seulement si les bâtiments voisins en sont également équipés, sinon vous risquez d'attirer une attention indésirable.

Si vous n'avez rien d'autre sous la main, le sol ou un enfoncement du sol peuvent vous 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, donc vous ne devez pas être à proximité immédiate pour être touché.

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

Une identification visible de vos bureaux, de votre emplacement ou de véhicules peut être utile, mais sachez que cela n'arrive que dans les régions où vos attaquants respectent normalement votre 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 signaux 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 directement, vous pouvez essayer d'évaluer la situation, mais une évaluation correcte est très difficile dans une telle situation. En général, il est utile de supposer que le véhicule est ou sera 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 d'explosion de réservoirs de pétrole peuvent vous blesser, en plus des tirs directs. Si les tirs ne sont pas trop proches essayez de poursuivre votre route jusqu'à ce que vous trouviez un abri à proximité.

Mines terrestres et artillerie non-explosée (UXO) [1]

Les mines terrestres et l'artillerie non-explosée sont une menace grave pour les civils dans des zones de conflits armés. 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 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.

[1] 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).

La prévention contre les mines et l'artillerie non explosée

Le seul moyen d'éviter les zones minées 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 les mines terrestres en demandant continuellement et activement la population locale ou des experts 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 pistes d'autres véhicules. Ne quittez pas les routes principales avec ou sans votre véhicule et ne roulez pas sur le trottoir ou la bande d'arrêt d'urgence. Les mines ou d'autres pièces d'artillerie non explosées peuvent rester cachées et actives pendant des années.

Les munitions non explosées peuvent apparaître dans les endroits où des combats et des tirs ont lieu et elles peuvent être visibles. 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.

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.

Si une mine explose sous un véhicule ou sous les pieds d'une personne à proximité

Il y a deux règles d'or:

- Une mine annonce toujours d'autres mines.

- N'agissez jamais de manière impulsive même si il peut y avoir des personnes blessées.

Si vous devez quitter l'endroit où vous vous trouvez, rebroussez chemin sur les traces de vos pas s'ils 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 la piste du véhicule.

Si vous vous approchez d'une victime ou que vous quittez une zone minée, le seul moyen est de vous mettre à genoux ou de vous allonger puis de commencer à donner des petits coups très légers avec la pointe d'un 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 trouver un objet solide. Si vous touchez un objet solide, dégagez-en très doucement le pourtour jusqu'à ce que vous puissiez l'identifier clairement. Les mines peuvent aussi être déclenchées par des fils de détente. Ne coupez pas de fils si vous en trouvez.

Tout ceci peut, bien entendu, prendre un temps considérable[2].

[2] 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 12

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

(En collaboration avec 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[1]. Les défenseurs qui n'ont pas accès à des ordinateurs ou à Internet considéreront peut-être que ces informations sont peu utiles dans l'immédiat. En revanche, ils ont d'urgence besoin des moyens et de la formation nécessaires pour employer la technologie de l'information au service de la défense des droits humains.

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

Le savoir c'est le pouvoir, et connaître les problèmes de sécurité susceptibles de toucher vos communications renforcera votre sentiment de 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

L'information ne doit pas passer par Internet pour qu'il y ait un accès illégal. Quand vous parlez de sujets sensibles, réfléchissez aux questions suivantes :

1 - Avez-vous confiance en vos interlocuteurs?

[1] Ce chapitre est basé sur le travail de Robert Guerra, Katitza Rodriguez y 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. Privaterra prépare actuellement un manuel plus détaillé sur les communications électroniques et la sécurité pour le compte de Front Line qui doit paraître en 2005. (Certaines parties de ce texte ont été légèrement adaptées par Enrique Eguren).

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

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 seront onéreux et difficiles à vous 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" (économiques et posés) 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 qui vous accompagnent à tout moment: 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 soient compromises 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 ou d'une chanson populaire pour brouiller la détection et la captation de sons. Seule une technologie onéreuse permet de filtrer le son et d'entendre une conversation.

□ Les grands espaces à plein air sont tant favorables que dangereux. Un rendez-vous à l'écart permet de voir si on vous suit ou 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.

Les téléphones portables

Tous les appels téléphoniques peuvent être écoutés si celui qui écoute a les 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 impliquer des personnes que vous souhaitez protéger.

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 impossible, assurez-vous de pouvoir conserver les dossiers sensibles dans une pièce à accès restreint. Vous devriez 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 [2]

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 la surtension et les variations de courant.

[2] 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.

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 un service compétent 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 parvient 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.

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.

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. 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. Evitez de lancer un virus en ouvrant un fichier exécutable que vous preniez 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 fichers connus ne soit PAS cochée.

Les problèmes de sécurité liés à Internet

Quand vous envoyez votre courrier électronique ou courriel il ne va pas directement sur l'ordinateur de votre destinataire. Il transite par plusieurs noeuds en laissant des informations derrière lui. Ce message peut être intercepté sur l'ensemble de cet itinéraire (non seulement dans ou depuis votre pays !)

Quelqu'un pourrait regarder par dessus votre épaule lorsque vous tapez votre message. C'est particulièrement problématique dans les cybercafés ou cafés Internet. Si vous êtes reliés 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) 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 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 à 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. Ces logiciels se propagent lorsque quelqu'un les installe sur votre ordinateur en votre absence, ou alors 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 votre courrier électronique, en utilisant un logiciel anti-virus, et en tapant votre mot de passe avec votre souris (application souris) plutôt que sur votre clavier. Les key loggers peuvent aussi être mis hors 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 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", vous créez une adresse similaire et la plupart des personnes 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 un de ces menus, éliminez tout l'historique, tous les cookies et videz votre mémoire cache. Pensez à éliminer aussi tous vos ajouts aux signets. Les navigateurs enregistrent tous les sites que vous avez visités sous format de fichiers cache, il faudra donc découvrir 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 toutes les données que vous voulez faire transiter par la toile, y compris les mots de passe et autres données sensibles que vous indiquez dans les formulaires. Installez les listes de signatures les plus récentes pour tous les logiciels utilisés, 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'envoi et la réception de courriers 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 signer vos courriels, avec ou sans vos pièces jointes, 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 HTML, MIME ou du texte riche 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 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 objets 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 de destinataires, et des copies du message à d'autres adresses multiples (champs "Envoyer à" et "CC"). Préférez envoyer le courriel à vous-même en tapant le nom de tous les destinataires dans le champ "CCI". 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. 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.

Le cryptage (cryptographie): questions et réponses

Ce qui suit constitue une liste des questions les plus fréquemment posées (FAQ) et leurs réponses. Vous pouvez vous adresser à nous pour toute question. Contactez 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 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, une plus grande efficacité et leur offre davantage de possibilités. Cependant, tout avantage comporte certains écueils. Ce 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. Si 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 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 alors que vous pourrez parfaitement ne jamais vous en apercevoir. 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. Cependant il existe 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 enregistrement hebdomadaire de tous les fichiers sur disque compact enregistrable, un CD-RW. Ensuite, conservez-le dans un endroit indépen dant et sûr.
- Utilisez des mots de passe que vous pouvez mémoriser mais qui ne peu vent pas être devinés ou déduits par un tiers.
- Restreignez l'accès aux données et aux fichiers en fonction de l'organi gramme 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, pas la technologie. Le cryptage ne fonctionne pas si les individus ne l'utilisent pas de manière systématique, s'ils communiquent leur mot de passe indifféremment ou s'ils le rendent visibles, p.ex. en l'inscrivant sur une note adhésive (Post–it) qu'ils collent à leur écran. Les logiciels de sauvegarde ne vous mettront pas à l'abri d'un incendie ou d'une razzia 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 conscient de la confidentialité et de la sécurité dans vos activités quotidiennes. Nous appelons cela la "paranoïa saine".

Q: Comment est-ce que je fais pour savoir quel logiciel de cryptage je dois 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. 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[3].

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 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 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.

[3] Par exemple, PGP - "Pretty Good Privacy"- est un logiciel bien connu et protégé. Vous pouvez le télécharger depuis www.pgpi.org.

(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. S'ils ne peuvent pas lire vos messages cryptés, ils peuvent distinguer les messages chiffrés des messages non chiffrés (ou clairs). Une soudaine augmentation des messages cryptés peut provoquer une razzia, si bien que c'est une bonne idée de commencer à crypter avant de lancer des projets spéciaux. 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 razzias 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 que la majorité des gouvernements saluent. Les ONG sont des cibles de surveillance plus probables et doivent donc être s'efforcer activement de mettre en place 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 aider les ONG. 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 est simplement incapable de respecter la confidentialité des données. Réexaminez la hiérarchie de vos informations pour être sûr que vous restreignez l'accès à des informations délicates à encore moins de personnes et gardez un oeil 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 razzia.

- 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 unique, 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 votre message en plus de le chiffrer. Votre but est que le destinataire du message sache qu'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 entraîne 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 garantir 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 administratifs. 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 des 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 plus difficile à joindre en cas d'urgence.

2 ◆ Seules les personnes absolument dignes de confiance devraient avoir les privilèges administratifs.

3 ◆ Déterminez quelles informations devraient 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 devraient être immédiatement modifiés.

6 ◆ Si une personne détenant des privilèges administratifs quitte l'organisation, tous les mots de passe et codes d'accès devraient 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 relève 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 logiciel 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 dès le départ avec des failles de sécurité connues. Encore mieux, envisagez de passer aux logiciels Open Source pour lesquels on ne tente pas de garantir la sécurité en occultant sa fabrication selon le principe de la « sécurité par l'ignorance", mais où au contraire les experts de sécurité et les pirates sont encouragés à passer leurs codes au peigne fin. Utiliser le logiciel Open Source et tous les autres logiciels 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 afin qu'ils ne soient pas détectés par les serveurs de spam (courriels indésirables). Il faudrait vérifier de manière régulière si les adresses ont reçu du nouveau courrier sans qu'elles soient utilisées autrement que par les membres sur le terrain. Ainsi vous pourrez détruire les comptes Internet qui reçoivent beaucoup de courriels indésirables sans pour autant endommager votre base de travail.

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. 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 de 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 quiconque 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.org).

- Si vous voulez envoyer un courriel ou un document en toute sécurité, utilisez le cryptage à toutes les étapes depuis l'envoi jusqu'à la réception par le destinataire. Il ne suffit pas d'envoyer un message crypté depuis un bureau sur le terrain à New York ou à 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 pirate, 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. Soyez conscients du fait qu'une personne peut faire de l'ingénierie sociale, c'est-à-dire se faire passer pour un tiers au téléphone ou par courriel pour s'assurer l'accès à vos mots de passe et à votre ordinateur. Fiez vous à votre jugement et à votre bon sens.

La Déclaration sur les Défenseurs des Droits de l'Homme de l'ONU

NATIONS UNIES **A**

Assemblée générale

Distr.
GENERALE

A/RES/53/144
8 March 1999

RÉSOLUTION DE L'ASSEMBLÉE GÉNÉRALE 53/144

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 Voir Documents officiels du Conseil économique et social, 1998, Supplément no 3 (E/1998/23), chap. II, sect. A., 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 Résolution 217 A (III).,

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 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'homme2 et des Pactes internationaux relatifs aux droits de l'homme Résolution 2200 A (XXI), annexe. 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 ?uvre 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,

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 ?uvre 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 intergouverne mentales.

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.

Bibliographie et ressources supplémentaires

Bibliographie

- Amnesty International (2003): "Essential actors of our time. Human right 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. Published by the 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

- ICRC (1983): Fundamental Norms of Geneva Conventions and Additional Protocols. Geneva.

- International Council on Human Rights Policy (2002): "Ends and means: Human Rights Approaches to Armed Groups". Versoix (Switzerland). www.international-council.org

- Jacobsen, K. (1999) "A 'Safety-First' Approach to Physical Protection in Refugee Camps". Working Paper # 4 (mimeo).

- Jamal, A. (2000): "Acces to safety? Negotiating protection in a Central Asia emergency. Evaluation and Policy Analysis Unit, UNHCR. Geneva.

- 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): "Afirmacion 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.

- Slim, H. and Eguren, E. (2003): "Humanitarian Protection: An ALNAP guidance booklet". ALNAP. www.alnap.org.uk. London.

- 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 Managment in Violent Environments". Good Practice Review 8. Humanitarian Practice Network. Overseas Development Institute, London.

- Vincent, M. and Sorensen, B. (eds) (2001) "Caught between borders. Response strategies of the internally displaced". Pluto Press. London.

Ressources supplémentaires

Le Bureau Européen de Peace Brigades International offre des formations et des conseils sur la protection et la sécurité des défenseurs des droits humains depuis 2000, en fonction du temps et des ressources disponibles.

Veuillez contacter pbibeo@protectionline.org, ou écrivez au PBI-Bureau Européen, 11, rue de la Linière, 1000 Bruxelles (Belgique)
Tel +32(0)2 609 44 05, Fax +32(0)2 609 44 06
www.peacebrigades.org/beo.html
www.protectionline.com

Front Line subventionne les formations et les capacités en sécurité et protection des défenseurs des droits humains et produit des manuels et des matériels.

Pour plus d'informations consultez www.frontlinedefenders.org ou contactez info@frontlinedefenders.org ou écrivez à Front Line,16 Idrone Lane, Off Bath Place, Blackrock, County Dublin, Ireland
tel: +353 1212 3750 fax: +353 1212 1001

Index Thématique

Manuel de protection pour les défenseurs des droits humains

Luis Enrique Eguren

(Espagne, 1962), médecin et expert en protection, membre de l'Unité de recherche et formation du Bureau européen de PBI. 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. Consultant, formateur et chercheur, il a publié plusieurs articles et livres sur la protection.