Humanitarian Practice Network

Le **Réseau des pratiques humanitaires** (**Humanitarian Practice Network – HPN**) est un forum indépendant sur lequel les agents de terrain, les gestionnaires et les décideurs du secteur humanitaire échangent information, analyses et expérience

Le but du HPN est d'améliorer la performance de l'action humanitaire en contribuant à l'apprentissage individuel et institutionnel.

Les activités du HPN comprennent :

- Une série de publications spécialisées : le magazine Échange humanitaire, les Dossiers thématiques et les Revues des bonnes pratiques.
- Un site de ressources sur www.odihpn.org.
- Des séminaires et ateliers épisodiques qui rassemblent praticiens, décideurs et analystes.

Les membres et le public du HPN comprennent des individus et des organisations qui jouent un rôle actif dans le secteur humanitaire. Ils sont répartis dans 80 pays et travaillent pour des ONG du nord et du sud, l'ONU et d'autres organisations multilatérales, des gouvernements, donateurs, institutions universitaires et bureaux de consultants. Les publications du HPN sont rédigées par un éventail tout aussi varié de personnes.

Le HPN est situé dans les locaux du Groupe de travail sur les politiques humanitaires (Humanitarian Policy Group – HPG) de l'Overseas Development Institute (ODI), un groupe de réflexion sur la politique humanitaire et du développement. Les ressources du HPN sont préparées et rédigées par un large éventail d'individus et d'organisations et sont publiées par le HPN afin d'encourager et de faciliter le partage des connaissances dans le secteur. Les opinions exprimées dans les publications du HPN ne représentent ou ne reflètent pas nécessairement celles du Groupe de travail sur les politiques humanitaires ou de l'Overseas Development Institute.

Cette RBP a bénéficié de l'appui d'USAID, de DFID et de SIDA.

USAID FROM THE AMERICAN PEOPLE

UKaid from the Department for International Development

Sida

Humanitarian Practice Network (HPN)
Overseas Development Institute
111 Westminster Bridge Road
London, SE1 7JD
Royaume-Uni

Tél : +44 (0)20 7922 0331/74
Fax : +44 (0)20 7922 0399
Email : hpn@odi.org.uk
Site Web : www.odihpn.org

Composition : Design To Print Solutions Limited. Imprimée et reliée au RU par Charlesworth.

Gestion opérationnelle de la sécurité dans des contextes violents

Réseau des pratiques humanitaires
HPN
Géré par le
Groupe de travail sur les politiques humanitaires

À propos du HPN
Le Réseau des pratiques humanitaires (HPN) de l'Overseas Development Institute (ODI) est un forum indépendant sur lequel les agents de terrain, les gestionnaires et les décideurs du secteur humanitaire échangent information, analyses et expérience. Les opinions exprimées dans les publications du HPN ne représentent ou ne reflètent pas nécessairement celles du Groupe de travail sur les politiques humanitaires ou de l'Overseas Development Institute.

odi **Premier groupe de réflexion indépendant de Grande-Bretagne** sur le **développement international** et les **questions humanitaires**

Overseas Development Institute
111 Westminster Bridge Road
Londres SE1 7JD
Royaume-Uni

Tél. +44 (0) 20 7922 0300
Fax. +44 (0) 20 7922 0399

Email HPN : hpn@odi.org.uk
Site web HPN : www.odihpn.org

Numéro 8 (Nouvelle édition)
Décembre 2010

Revue des bonnes pratiques

Gestion opérationnelle de la sécurité dans des contextes violents

Commandée et publiée par le Réseau des pratiques humanitaires de l'ODI

Humanitarian Practice Network (HPN)
Overseas Development Institute
111 Westminster Bridge Road
London, SE1 7JD
Royaume-Uni

Tél : +44 (0)20 7922 0331/74
Fax : +44 (0)20 7922 0399

Email : hpn@odi.org.uk
Site web : www.odihpn.org

Imprimée et reliée au Royaume-Uni
Composition et production : Design To Print Solutions

ISBN : 978 1 907288 32 6

Prix unitaire : £10.00 (hors frais de port et d'emballage).

Gestion opérationnelle de la sécurité dans des contextes violents

Revue des bonnes pratiques 8
Édition révisée

Revue des bonnes pratiques

Gestion opérationnelle de la sécurité dans des contextes violents

décembre 2010

Revue des bonnes pratiques 8
Édition révisée
Réseau des pratiques humanitaires
Overseas Development Institute

Table des matières

Auteurs et remerciements ix
Déclaration de non-responsabilité xiii
Glossaire des termes de sécurité xv
Introduction 1

PARTIE 1
CONCEPTS ET PRINCIPES FONDAMENTAUX

Chapitre 1 Concepts et principes fondamentaux de la gestion de la sécurité 7
1.1 Pourquoi gérer les risques de sécurité ? 7
1.2 Gestion de la sécurité organisationnelle 12
1.3 Gestion de la sécurité entre organisations 18
1.4 Transférer les risques de sécurité 23
1.5 Le pays d'accueil et la gestion de la sécurité 25

PARTIE 2
APPROCHES STRATÉGIQUES ET OPÉRATIONNELLES DE LA GESTION DE LA SÉCURITÉ

Chapitre 2 Évaluation des risques 29
2.1 L'importance d'une évaluation des risques systématique 29
2.2 Définitions essentielles 30
2.3 Analyse du contexte : connaissez votre lieu d'action 32
2.4 L'analyse du programme : sachez qui vous êtes et ce que vous voulez réaliser 38
2.5 Évaluation des menaces 42
2.6 Évaluation de la vulnérabilité 45
2.7 Analyse du risque 50

Chapitre 3 Stratégie de sécurité 59
3.1 Élaborer une stratégie de sécurité 59
3.2 L'acceptation 61
3.3 Protection 77
3.4 Dissuasion et protection armée 79

Chapitre 4 Évacuation, hibernation, gestion d'un programme à distance et retour 91
4.1 L'évacuation et la relocalisation 91
4.2 L'hibernation 102

4.3 Gestion de programmes à distance 104
4.4 Retour 109

Chapitre 5 Rapport d'incident et gestion d'un incident critique 111
5.1 L'importance du rapport et du suivi d'un incident critique 111
5.2 Gestion d'un incident critique 113
5.3 Gestion post-incident 118

PARTIE 3
LE PERSONNEL EN CHARGE DE LA GESTION DE LA SÉCURITÉ

Chapitre 6 Le personnel en charge de la gestion de la sécurité 123
6.1 Les responsables de la sécurité sur le terrain 123
6.2 Compétences personnelles 126
6.3 Compétence des équipes 130
6.4 Différencier les menaces et les risques pour différentes catégories de personnel 133
6.5 Ressources humaines 139
6.6 Le stress et sa gestion 143

PARTIE 4
SÉCURITÉ DE LA COMMUNICATION

Chapitre 7 Gérer la sécurité de la communication 155
7.1 Télécommunications 155
7.2 Protéger l'équipement de communication 169
7.3 Sécurité de l'information 169
7.4 Communiquer avec les médias 175

PARTIE 5
GÉRER DES SITUATIONS DE MENACES ET DE RISQUES SPÉCIFIQUES

Chapitre 8 Sécurité des voyages et des déplacements 181
8.1 Sécurité à l'arrivée 181
8.2 Véhicules et sécurité routière 183
8.3 Déplacements sur la route : préparation et réponse à un incident 193
8.4 Voyager en avion et en bateau 196
8.5 Liste de contrôle pour la préparation du personnel 197

Chapitre 9 Sécurité du site 199
9.1 Choix d'un site pour les bureaux 199
9.2 Renforcement du périmètre physique 203

9.3 Gestion de la sécurité du site 206
9.4 Zones sous menace terroriste 212
9.5 Contre-surveillance 214
9.6 Sites de distribution 215

Chapitre 10 Foules, bandes et pillage 217
10.1 Suivi et analyse de la situation 217
10.2 Action préventive 218
10.3 Protection 103

Chapitre 11 Sécurité de l'argent liquide 223
11.1 Réduire l'utilisation d'argent liquide 223
11.2 Discrétion 223
11.3 Limiter l'exposition 224
11.4 Sécurité électronique de l'argent 226
11.5 Utilisation d'argent liquide dans les programmes 228

Chapitre 12 Agression sexuelle 229
12.1 Définition et cadre 229
12.2 Réduction du risque 230
12.3 Survivre à une agression sexuelle 234
12.4 Gestion de la crise 236
12.5 Préparation et formation 244

Chapitre 13 Détention, arrestation et enlèvement 247
13.1 Terminologie 247
13.2 Réduction du risque 248
13.3 Répondre à un incident et gestion de crise 249

Chapitre 14 Rapt et situations d'otages 253
14.1 Définitions 253
14.2 Stratégies de réduction du risque 253
14.3 Survivre à une situation de rapt ou de prise d'otages 257
14.4 Gestion d'incident critique 260
14.5 Communiquer et négocier avec les ravisseurs 269
14.6 Gérer les suites d'un rapt 273
14.7 Préparation et formation 275

Chapitre 15 Menaces liées aux combats et débris de guerre 279
15.1 Questions essentielles 279
15.2 Tirs d'obus et bombardements 280
15.3 Feux croisés et tirs de précision 285
15.4 Mines, objets piégés et munitions non explosées 287

15.5 Phosphore blanc 295
15.6 Les Débris de guerre : un rappel 296

Annexes

Annexe 1 Tendances générales concernant la sécurité du travailleur humanitaire 301
Annexe 2 Le système de gestion de la sécurité des Nations Unies 307
Annexe 3 Sauver des vies ensemble : un cadre de collaboration pour la sécurité 313
Annexe 4 Prestataires privés de sécurité 319
Annexe 5 L'assurance 325
Annexe 6 Financement des donateurs et gestion de la sécurité 331
Annexe 7 Ressources supplémentaires 335

Auteurs et remerciements

Cette édition révisée de la Revue des bonnes pratiques (RBP) a été réalisée avec la participation d'un grand nombre de spécialistes dans le domaine de la gestion de la sécurité opérationnelle.

Koenraad van Brabant, principal auteur de l'édition de 2000, a rédigé des notes de travail et de multiples documents de travail pour un grand nombre de chapitres et d'annexes de l'édition révisée. Adele Harmer, Abby Stoddard et Katherine Haver se sont chargées de la gestion du projet et de la co-rédaction de la publication de la RBP. Adele, Abby et Katherine sont toutes trois des associées de chez Humanitarian Outcomes, Wendy Fenton, coordinatrice du Réseau des pratiques et politiques humanitaires (HPN), a supervisé la production de la RBP et Matthew Foley, rédacteur en chef pour le Groupe de la politique humanitaire, en a adapté le manuscrit.

Des contributions et conseils importants ont également été fournis par un groupe conseil comprenant:

Frédéric Bardou	référent sécurité, Action Contre la Faim.
Shawn Bardwell	coordinateur de la sûreté et de la sécurité, Bureau d'assistance en cas de catastrophe à l'étranger, USAID.
Oliver Behn	coordinateur exécutif, European Interagency Security Forum.
Alexandre Carle	conseiller en sécurité pour l'Afrique, CARE.
Pascal Daudin	directeur de la sûreté et de la sécurité, CARE International.
Christopher Finucane	consultant en recherche, Groupe de la politique humanitaire.
Anthony Val Flynn	Direction générale de la Commission européenne pour l'aide humanitaire et la protection civile.
Pierre Gallien	directeur technique et du développement, Solidarités.
Andrew Gleadle	consultant indépendant.
Heather Hughes	conseillère en sécurité, Oxfam GB.
Melker Mabeck	délégué adjoint pour les questions de sécurité, Comité international de la Croix-Rouge.
Maarten Merkelbach	directeur de projet, Initiative de gestion de la sécurité, Nouvelles questions sur les programmes de sécurité, Centre pour la politique de sécurité, Genève.
Mamadou Ndiaye	directeur général, OFADEC.
Erin Noordeloos	directeur des programmes internationaux, RedR UK.

Michael O'Neill	directeur principal, Service de la sûreté et de la sécurité, Save the Children.
Robert Painter	spécialiste principal en sécurité : Liaison ONG, Division des opérations régionales, Département des Nations Unies pour la sûreté et la sécurité.
Jean S. Renouf	chercheur et consultant dans le domaine des conflits armés et de la sécurité.
John Schafer	Directeur de la sécurité, InterAction
Mike Tomkins	directeur associé (Opérations), Bureau de la sécurité, World Vision International.
Équipe de sécurité	Fédération internationale de la Croix-Rouge et du Croissant-Rouge.

Nous tenons également à remercier nos collaborateurs et pairs évaluateurs :

Yan Bui	chargé de comptes, Assurance des entreprises, Clements International.
Pete Buth	consultant indépendant.
Andries Dreyer	World Vision International.
Patricia Dunbar	conseillère en sécurité, UNICEF.
Ben Emmens	directeur du service RH, People In Aid.
Matthew Freedman	directeur général, Indigo Telecom USA.
Bruce Hickling	directeur pays pour la Somalie, International Rescue Committee.
Trevor Hughes	directeur de la sécurité, International Medical Corps.
Rafael K. Khusnutdinov	directeur associé, service de la sûreté et de la sécurité, Save the Children.
Gerald Kloski	directeur de la sécurité, CHF International.
Terry Lewis	directeur de la formation et des publications, Mango.
Randy Martin	directeur des opérations d'urgence, MercyCorps.
Steve McCann	directeur, Armadillo At Large.
Auriol Miller	directrice pays pour Oxfam GB, Russie.
Josh Miller	directeur général, Mexique, Amérique centrale et Caraïbes, Control Risks Group.
Julian Neale	division conflits, aide humanitaire et sécurité, DFID.
Michael Niedermayr	coordinateur de la sécurité, zone Asie-Pacifique, Fédération internationale de la Croix-Rouge et du Croissant-Rouge.

Manual Novoa	conseiller en stress, GTZ.
Rupert Reid	directeur général, Security Exchange Ltd.
Norm Sheehan	directeur de la sécurité, Academy for Education Development.
Julie Spooner	formatrice en sensibilisation à la sécurité (pour les femmes), Programme alimentaire mondial.
Simon Springett	coordinateur humanitaire régional pour le Moyen-Orient, l'Europe de l'Est et la Communauté des États indépendants, Oxfam GB.
Hine Sullivan	responsable sécurité pour la zone Pacific Development Group (Papouasie Nouvelle-Guinée, Iles Salomon et Vanuatu) et le Timor oriental, World Vision.
Hernan del Valle	chef de mission, Médecins Sans Frontières, Papouasie Nouvelle-Guinée.
Amy West	responsable de programme, Academy for Education Development.)

Enfin, nous tenons à remercier les personnes suivantes pour le temps qu'elles ont généreusement consacré aux entretiens :

Felix Ackebo	directeur par intérim du bureau de la zone est, UNICEF, RDC
John Adlam	directeur d'équipe, CHASE OT, DFID
José Luis Barreiro	responsable du programme Protection et chargé de la sécurité en Colombie, Oxfam GB
Sophie Battas	assistante technique, ECHO, Tchad
Tom Karl Bil	GTZ
Reiseal Ni Cheilleachair	agent de soutien au programme de Somalie, Concern, Nairobi
Robin Coupeland	Insecurity Insight
Marie-Jose D'Aprile	chercheur SMI
Michel Emeryk	conseiller en sécurité mondiale, Croix-Rouge britannique
Paul Farrell	siège UNICEF
Susannah Friedman	directrice des urgences, Save the Children UK, Somalie (basée à Nairobi)
Anne Garella	chef de mission, ACF Afghanistan
Eric le Guen	conseiller en sûreté et sécurité mondiale, CRI
Patrick Hamilton	Comité international de la Croix-Rouge
Roland Van Hauwermeiren	directeur de pays, Oxfam GB, Tchad

Kevin Henry	vice-président, Réponse mondiale, Hiscox USA
Alfred Kamara	coordinateur de programme, 'Hands empowering the less privileged (HELP)', Sierra Leone
Sureka Khandagle	représentante de pays, OFDA/USAID, Soudan
Kai Leonhardt	GTZ
Christoph Leudi	chef de délégation régionale, CICR, Nairobi
Sean McDonald	conseiller en sécurité internationale, Joint NGO Safety Office, Timor-Leste
Rebekka Meissner	siège Medair International
Perry Metaxas	liaison ONG, ONU-DSS, Darfour
Ron Mortensen	conseiller régional par intérim, OFDA/USAID, Dakar
Abdi Rashid Hadi Nur	directeur de pays, Programme Somalie, Concern
John Prideaux-Brune	Oxfam GB, directeur de pays, Territoires palestiniens occupés et Israël
Lara Puglielli	ancienne directrice de la sûreté et de la sécurité du personnel, Catholic Relief Services
David Richards	SPAS, Somalie
Tom Rogers	USAID/OFDA
Hussein Ali Salad	conseiller en politiques, CICR, Somalie
Nuwa Serunjogi	conseiller en plaidoyer humanitaire, Christian Aid
Stefanie Sobol	OFDA/USAID, Dakar
Alain Ondias Souna	responsable de la sécurité, WVI Sri Lanka
Barry Steyn	CARE Bangkok
Marcel Stoessel	directeur de pays, Oxfam GB, RDC
Hine Sullivan	responsable de la sécurité pour Pacific Development Group (Papouasie-Nouvelle-Guinée, Iles Salomon et Vanuatu) et Timor-Leste, World Vision
Nathan Taback	Insecurity Insight
Fergus Thomas	chef de bureau, Goma, Concern, RDC
Christina Wille	Insecurity Insight
Nigel Young	personnel de soutien humanitaire, actuellement directeur de pays par intérim pour le Nord-Soudan, Oxfam GB

Traduction Brigitte Clark.

Relecture Alexandre Carle

Déclaration de non-responsabilité

Aucune condition n'est exprimée ni sous-entendue et aucune garantie n'est donnée ni sous-entendue quant à la qualité et à la durée de validité de cette Revue des bonnes pratiques (RBP) publiée en décembre 2010, ni quant à son utilité à des fins particulières ou dans des conditions spécifiques. Les informations contenues dans cette RBP sont présentées par l'ODI uniquement en tant que conseils généraux en matière de gestion de la sécurité. Elles ne doivent pas être considérées comme constituant une déclaration adéquate ou valable sur les procédures opérationnelles standard et/ou les caractéristiques des menaces dans un pays particulier, ni sur la gestion de la sécurité d'une ou plusieurs organisations.

Bien que l'ODI se soit efforcée de s'assurer de l'exactitude et de la qualité des informations présentées dans cette RBP, elle ne sera pas tenue responsable dans toute la mesure permise par la loi, d'éventuels dommages, pertes ou difficultés résultant de l'utilisation des informations contenues dans cette RBP ou de l'impossibilité de les utiliser, ni de leur interprétation. L'ODI déclinera toute responsabilité et ne pourra être tenue responsable envers qui que ce soit des dommages, quels qu'ils soient, découlant de décisions ou d'actions prises sur la base des informations qui y sont contenues.

Cette RBP peut inclure l'opinion et les recommandations de tierces personnes et ne reflète pas nécessairement l'opinion de l'ODI ni n'indique l'adoption d'une ligne de conduite particulière.

Glossaire des termes de sécurité

Accoutumance au danger : phénomène d'adaptation, généralement inconscient, de son seuil de risque acceptable, résultant d'une exposition régulière ou constante au danger ; en conséquence, l'évaluation objective du risque et de ses conséquences potentielles est réduite, ce qui peut entraîner une prise de risque accrue par une exposition non contrôlée.

Agression sexuelle : acte ou menace de viol, d'attaque et intimidation sexuelles, harcèlement sexuel ou attouchements non désirés.

Analyse d'incident : étude plus approfondie et plus décisive sur les facteurs structurels, opérationnels et contextuels qui ont donné lieu à un incident de sécurité ; consiste à questionner l'efficacité des diverses dimensions et mesures de la gestion de la sécurité et à demander si et dans quelle mesure l'organisation ou l'un ou plusieurs des membres de son personnel pourraient être jugés avoir « été à la source de l'incident ».

Approche d'acceptation : composante d'une stratégie de sécurité qui tente de diminuer l'exposition à une menace en créant des relations avec les communautés locales et les parties prenantes concernées dans la région d'intervention, de manière à obtenir leur acceptation de la présence de votre organisation et leur consentement à son travail.

Approche de protection : composante d'une stratégie de sécurité qui met l'accent sur l'utilisation de procédures et de dispositifs de protection pour diminuer la vulnérabilité aux menaces existantes ; cette approche n'a aucun effet sur le niveau de la menace.

Armes légères : armes utilisées pour l'autoprotection et le combat rapproché ou à courte distance.

Atténuation du risque : objectif de votre gestion de la sécurité, vise à réduire la menace et/ou votre vulnérabilité.

Audit de sécurité : évaluation des forces et des faiblesses de la gestion et de l'infrastructure d'une organisation en matière de sécurité afin d'en apprécier son efficacité et d'identifier les domaines à améliorer.

Bande : groupe organisé de personnes agressives ayant des intentions destructrices, criminelles, crapuleuses ou violentes.

Clan : groupement social de personnes unies par des liens de parenté, c'est-à-dire pensant avoir un ancêtre commun.

Connaissance du terrain : être attentif et comprendre l'environnement physique et social dans lequel on évolue, connaître la source de dangers potentiels, d'aide et d'abri.

Contre-surveillance : action de surveiller si quelqu'un vous épie. Stratégie pour détecter si vos déplacements, systèmes et/ou installations sont étudiés par des personnes ayant des intentions malveillantes, p. ex. un rapt, un bombardement ou un vol à main armée.

Convoi : groupe de véhicules (ou de navires) se déplaçant ensemble de manière organisée et sous la commande d'un chef afin de se soutenir et se protéger mutuellement.

Coordination civil-militaire : liaison entre acteurs militaires (y compris pour les opérations de maintien de la paix) et acteurs civils déployés sur un même terrain, en particulier ceux qui sont issus de la communauté humanitaire et du développement.

Création de scénarios : prévoir comment la situation pourrait se développer à court et moyen termes et comment les menaces qui existent dans votre environnement pourraient évoluer ; examiner les hypothèses de vos plans et envisager ce que vous feriez si elles ne se réalisaient pas.

Détection : technique essentielle utilisée pour sortir d'un terrain soupçonné d'être miné, selon laquelle le sol est très soigneusement examiné avant d'y poser un pied.

Détention : action de retenir une personne en captivité sous l'autorité (p. ex. police, gardes-frontières).

Déterminer le profil des incidents : visualisation, généralement sur une carte mais également possible dans un cadre temporel, du moment, du lieu et du type des incidents survenus afin de déterminer les tendances et d'identifier de possibles tendances telles que les zones et/ou périodes à haut risque.

Détournement de voiture : vol d'une voiture, lorsque le chauffeur est au volant.

EEI : Engin Explosif Improvisé. Bombe pouvant être placée pratiquement n'importe où, par exemple sur le bord d'une route, dans un véhicule, un sac, un colis, une lettre ou des vêtements.

Embuscade : attaque soudaine lancée depuis une position dissimulée, généralement constituée d'un élément d'arrêt et d'un élément de destruction. Terme souvent employé dans le contexte d'attaques sur une route/de véhicules/de convoi.

Engins non explosés (UXO) : tout type de munitions (balle, grenade à main, obus de mortier, etc.) qui ont été amorcées (préparées au tir) mais pas utilisées, ou qui ont été tirées mais qui n'ont pas explosé et qui sont instables et dangereuses.

Enlèvement : action d'emmener une personne contre son gré. À distinguer du « rapt », qui implique que le ravisseur demande une contrepartie (p. ex. une rançon) pour libérer la victime.

Enquête sur incident : collecte d'informations situationnelles et circonstancielles au sujet d'un incident qui a eu lieu, en complément des faits de base énoncés dans le rapport d'incident.

Équipe de gestion des incidents critiques (EGIC) : Groupe créé dans le but de gérer la réponse organisationnelle aux situations de crise. Équipe généralement composée de membres spécifiques du personnel, identifiés et formés au préalable, et ayant une bonne connaissance des procédures et protocoles de gestion des incidents critiques mis en place par leur organisation.

Établir la cartographie des menaces : visualiser et illustrer les menaces sur une carte géographique.

Évacuation : mise en sécurité du personnel en le faisant sortir d'un pays.

Évaluation/analyse des menaces : tentative d'examiner plus systématiquement la nature, l'origine, la fréquence et la concentration géographique des menaces.

Évaluation/analyse du risque : tentative de considérer le risque de manière plus systématique en termes de menaces dans votre environnement, vos vulnérabilités particulières et vos mesures de sécurité pour réduire la menace et/ou réduire votre exposition.

Evasan : Évacuation sanitaire – transfert d'un patient par voie routière, maritime ou aérienne afin d'obtenir un traitement médical dans un autre lieu.

Extorsion : utilisation de la contrainte ou de l'intimidation pour obtenir de l'argent, un bien ou un acte de favoritisme.

Fournisseur/ société / prestataire privé de sécurité : entité privée fournissant des services de sécurité à des personnes ou des organisations contre rémunération. Ces services peuvent aller d'une sécurité « douce » (p. ex. consultations, formation et soutien logistique) à une sécurité « dure » (services de garde, protection armée) et à la gestion des risques et des crises, la formation des forces armées et même au commandement opérationnel et au combat.

Harcèlement : attitude abusive, que ce soit verbalement ou physiquement, à l'encontre d'une personne et qui provoque détresse ou embarras.

Hibernation : processus de s'abriter sur place jusqu'à ce que la menace et/ou le danger passe, qu'une assistance soit fournie ou qu'il soit possible de se déplacer en sécurité.

Incident critique : incident de sécurité dont la sévérité perturbe considérablement la capacité d'une organisation à exercer son activité ; met généralement en danger de mort ou provoque la mort.

Menace : danger dans votre environnement d'intervention.

Mentalité ghetto : tendance des membres d'une organisation à évoquer et à analyser l'environnement externe entre eux, dans les limites protectrices de leur « enclos », sans grande consultation ni interaction avec les divers acteurs de l'environnement externe.

Phases de sécurité (d'alerte) : résumé de la classification de différents niveaux possibles de risque et d'insécurité dans votre environnement, chacun nécessitant un ensemble spécifique de procédures de sécurité obligatoires.

Piège : système explosif improvisé ou spécialement conçu, généralement attaché à des objets ordinaires ou dissimulés sous des objets (peluche, poupée, objet militaire…), servant à dissuader, blesser ou tuer les personnes qui s'approchent de la zone piégée.

Planification d'urgence : outil de gestion employé pour une préparation adéquate à diverses situations d'urgence potentielles spécifiques à un contexte.

Point focal : agent de liaison en matière de sécurité, ayant généralement la responsabilité d'un groupe de personnes dans une zone géographique définie ; le point focal est un « nœud » important de l'arbre de communication et s'assurera aussi que toutes les personnes placées sous sa responsabilité suivent les procédures de sécurité adoptées.

Procédures opérationnelles standard : procédures officiellement établies pour mener certaines interventions ou pour agir dans certaines situations, ici plus particulièrement pour éviter qu'un incident ne se produise (aspect préventif) ou pour survivre à un incident, ou procédures à observer dans le cadre de la gestion d'un incident/d'une crise d'une organisation (aspect réactif).

Protection : employé ici de façon distincte de « sûreté » et de « sécurité » et fait référence à la « sécurisation » des civils et des non-combattants qui ne font pas partie du personnel de l'organisation d'aide humanitaire.

Rapt : enlèvement et détention d'une personne par la force dans le but explicite d'obtenir une contrepartie (argent, équipement ou certains actes) pour la vie et la remise en liberté de la personne.

Référence sociale : recommandation ou « garantie » personnelle concernant le recrutement possible d'une personne, sans avoir nécessairement travaillé avec elle mais en ayant connaissance de sa position et de sa réputation dans une communauté.

Règles d'engagement : directives destinées à tout combattant ou garde armé précisant dans quelles conditions et dans quelles limites ils peuvent employer la force en faisant usage de leurs armes à feu.

Relocalisation : retrait du personnel d'un lieu d'opérations vers un lieu plus sûr, généralement à l'intérieur du pays.

Réseau de communications : Ensemble d'éléments de même nature reliés les uns aux autres pour communiquer rapidement des informations, telles qu'une alerte à la sécurité. Selon ce système, une personne/organisation informe une liste prédéterminée d'autres personnes/organisations qui, à leur tour, en informent d'autres sur leur liste, etc.

Risque : probabilité et impact potentiel de faire face à une menace définie.

Sécurité : être à l'abri du risque ou des atteintes provenant de la violence ou d'autres actes intentionnels.

Seuil de risque acceptable : point au-delà duquel vous considérez que le risque est trop élevé pour poursuivre l'intervention (proportionnellement a l'impact de votre action) et que vous devez quitter la zone de danger ; influencé par la probabilité qu'un incident se produise et par la gravité de l'impact s'il se produisait.

Situation d'otages : situation dans laquelle une personne ou un groupe de personnes est dans un état de siège dans un lieu connu. Comme dans le cas d'une situation de rapt, la sécurité et la remise en liberté ultérieure des personnes sont généralement soumises à certaines conditions. Celles-ci peuvent inclure une demande politique ou financière.

Stratégie de dissuasion : composante d'une approche de la sécurité qui tente de prévenir une menace en utilisant une contre menace. Celle-ci peut, sous sa forme la plus extrême, être une protection armée.

Stratégie de sécurité : philosophie, combinaison des approches et utilisation des ressources qui globalement définissent la gestion de la sécurité d'une organisation.

Stress : état de tension physique et/ou émotionnelle, inquiétude profonde ou prolongée. « État ou sentiment d'une personne lorsqu'elle sent que les demandes excèdent les ressources personnelles et sociales qu'elle est en mesure de mobiliser ». (Richard S Lazarus)

Sûreté : être à l'abri du risque ou des atteintes provenant d'actes non intentionnels (accidents, phénomènes/catastrophes naturels ou maladie).

Surveillance de quartier : programme communautaire plus ou moins officialisé entre voisins ayant pour objectif de surveiller les personnes suspectes et de lutter contre la criminalité dans leur zone d'influence ou résidentielle.

Survivre sur les champs de bataille : mesures visant à atténuer le risque de mort ou de blessure lorsqu'une personne est sous le feu de l'ennemi, ou dans une zone de tir, quel que soit le type d'arme utilisé.

Terrorisme : actes destinés à infliger des blessures spectaculaires ou mortelles à des personnes civiles et à créer une atmosphère de peur, généralement pour poursuivre un objectif politique ou idéologique.

Triangulation : recoupement des informations ou détails en comparant l'opinion ou la version de différentes sources.

Trouble de stress post-traumatique (TSPT) : trouble psychologique dont peuvent souffrir les personnes ayant subi un traumatisme émotionnel sévère et qui peut occasionner perturbations du sommeil, retours en arrière, angoisse, fatigue et dépression.

Violence basée sur le genre : violence à l'encontre d'une personne basée sur le genre, le sexe. Inclut les menaces et/ou les actes qui infligent des souffrances physiques, mentales ou sexuelles, la contrainte ou autres privations de liberté. Bien que des personnes des deux sexes et de tous âges puissent en être victimes, les femmes et jeunes filles en sont les principales victimes en raison de leur statut de subordination.

Note : Un point de référence utile pour la terminologie est l'organisation internationale pour la standardisation (ISO – International Organisation for Standardization) ISO 31000 Guide 73:2009 sur « Risk Management – Vocabulary », disponible chez www.iso.org.

Introduction

La première édition de cette Revue des bonnes pratiques sur la *Gestion opérationnelle de la sécurité dans des contextes violents* (également appelée RBP 8) a été publiée en 2000. Elle est, depuis, un document novateur en matière de gestion de la sécurité opérationnelle humanitaire et on lui attribue d'avoir facilité la compréhension des bonnes pratiques dans ce domaine pour l'ensemble de la communauté des organisations opérationnelles. Elle a présenté des concepts fondamentaux de gestion de la sécurité et a mis en relief les bonnes politiques et pratiques des diverses approches de la sécurité opérationnelle dans les contextes humanitaires. Au moment de sa publication, la majorité des organisations d'aide humanitaire commençait tout juste à prendre en considération les réalités et les difficultés de l'insécurité opérationnelle. Peu d'organisations internationales ou nationales avaient des postes désignés à la gestion de la sécurité ou des politiques et protocoles sur la gestion des risques de violence intentionnelle à l'encontre de leurs personnels et de leurs opérations. La RBP a donc comblé un important vide concernant la politique et la pratique de la gestion de la sécurité.

Bien qu'une grande partie de la RBP 8 reste valable, le contexte mondial a beaucoup changé au cours des dix dernières années. L'augmentation de la violence vis à vis des travailleurs humanitaires, notamment un plus grand nombre de rapts et d'attaques mortelles, a eu de graves implications pour l'assistance humanitaire internationale. Les attaques avaient des motifs politiques et traduisaient également des niveaux croissants de banditisme et de criminalité. Cette augmentation de la violence a généré une meilleure sensibilisation aux difficultés en matière de sécurité et a donné lieu à de nouvelles adaptations et stratégies de gestion de la sécurité. Cela a également généré un professionnalisme et une sophistication des pratiques de sécurité humanitaire et dans la coordination entre organisations. Globalement, au cours de la dernière décennie, les changements survenus dans les contextes opérationnels ainsi que les politiques indiquent qu'une révision et une mise à jour de la première RBP sont nécessaires et justifiées.

Cette édition révisée de la RBP actualise le texte original et présente également de nouveaux sujets. Elle propose, en particulier, une approche plus détaillée et plus élaborée de l'évaluation des risques. Celle-ci est spécifiquement destinée aux travailleurs sur le terrain. Elle décrit également une méthode plus approfondie de mettre en œuvre une approche « d'acceptation active » et examine en détail les stratégies de dissuasion et les stratégies de protection, telles qu'opérer sans se faire remarquer ou utiliser une protection armée. Les nouveaux sujets couvrent les questions relatives à la sécurité lors de la

« gestion à distance des programmes», les bonnes pratiques de coordination de la sécurité entre organisations et comment localiser, partager et analyser les informations liées à la sécurité. La RBP présente une approche beaucoup plus détaillée de la gestion des incidents critiques, en particulier le rapt et la prise d'otages. Les questions relatives à la menace de terrorisme sont évoquées dans un certain nombre des nouveaux chapitres et ont été intentionnellement intégrées dans le texte général plutôt que limitées à un chapitre. Une série d'annexes examine les questions telles que l'évolution du contexte dans lequel opèrent les acteurs humanitaires, le rôle des prestataires privés de sécurité, la fourniture d'assurance et le rôle des bailleurs de fonds institutionnels pour financer la gestion de la sécurité.

Lecteurs cibles

La première RBP a été utilisée par un très grand nombre de personnes et d'organisations, aussi bien comme guide de référence opérationnel que comme base ou modèle pour les politiques et procédures de gestion de la sécurité spécifiques à leur organisation.

Cette RBP révisée a avant tout été écrite pour les cadres opérationnels qui supervisent et soutiennent directement les opérations dans des contextes violents. Cela inclut non seulement les conseillers en sécurité sur le terrain mais également les hauts représentants dans un contexte opérationnel donné, notamment les responsables et les coordinateurs de programmes. Un grand nombre d'autres personnes, des personnels locaux à la haute direction de l'organisation, pourront également l'utiliser. Bien que son contenu vise en particulier les organisations non gouvernementales (ONG), internationales et nationales, d'autres organisations pourront également la trouver utile.

Cette RBP porte principalement sur la sécurité, définie comme étant liée à des actes de violence et de crime politique. Cependant, l'insécurité, n'est pas le seul type de risque qui peut avoir une incidence sur la vie ou le bien-être des acteurs humanitaires. Les risques de santé et de sûreté, y compris les maladies, les accidents, les incendies et les dangers environnementaux, constituent également de graves menaces, mais ils font l'objet d'autres consignes. Les communautés locales qui reçoivent une assistance peuvent être exposées à des risques de violence aussi importants, sinon plus, et peuvent nécessiter une assistance et une protection essentielles. Cette RBP n'aborde pas ces difficultés de protection, en particulier parce que les stratégies employées pour protéger la population générale sont souvent très différentes de celles employées pour protéger les travailleurs humanitaires.

Bonnes pratiques versus pratiques exemplaires

Cette RBP décrit les bonnes pratiques, non pas les pratiques exemplaires, et n'offre guère de procédures opérationnelles ni de listes de contrôle d'usage. Ceci est intentionnel. Il existe, sans aucun doute, un certain nombre de mesures de sécurité qui sont quasiment toujours applicables, comme par exemple verrouiller les portes la nuit, installer une protection antivirus sur les ordinateurs, dire à quelqu'un où vous allez et quand vous comptez être de retour et mentionner tous les incidents de sécurité et tous les accidents évités de justesse. Prendre ces précautions de base est déjà une bonne initiative. Les listes de contrôle de base incluses dans ce guide doivent être considérées comme des aide-mémoire pour s'assurer que les mesures de base sont et restent en place.

Mais un aspect important de la gestion de la sécurité opérationnelle consiste à agir de manière appropriée dans les circonstances données. Selon les circonstances, cela peut signifier faire quelque chose de très différent, ou même à l'encontre de ce qui pourrait être considéré comme une bonne pratique dans la plus grande partie du monde. Autrement dit, une grande part de la gestion de la sécurité dépend d'un jugement sur la situation, des connaissances que l'on possède et de l'aptitude à évaluer l'efficacité relative de différentes options de sécurité.

Les bonnes pratiques de la gestion de la sécurité impliquent également une gestion responsable. La gestion responsable (de soi-même et d'autrui) signifie de ne pas exposer les personnes et les biens à des risques inutiles ou à des risques disproportionnés à l'impact potentiel de l'aide que vous pourriez tenter de fournir. Les sauveteurs en montagne ne vont pas à la recherche de personnes prises dans une avalanche si le temps ou les conditions de neige peuvent les exposer à un très grand risque. Une bonne gestion de la sécurité opérationnelle exige de se demander si le risque est justifié compte tenu des avantages potentiels offerts par le projet ou le programme. Il est également nécessaire de voir si tout a été fait, dans la mesure du possible, pour réduire le risque et l'impact potentiel d'un incident.

Enfin, de bonnes pratiques supposent d'intégrer la gestion de la sécurité à tous les niveaux de l'organisation. Il ne s'agit ni d'un élément accessoire ni d'un luxe. Le manque de temps est la raison que l'on donne souvent pour ne pas consacrer suffisamment d'attention à un grand nombre de choses, notamment la gestion de la sécurité. Il faut savoir remettre en question cet argument. Il devrait être inacceptable que quelqu'un soit gravement blessé ou tué parce que son organisation n'a pas pris le temps de mettre en œuvre de bonnes pratiques. Les organisations, sans exception, prennent le temps de mettre en place des vérifications et contrôles financiers. Pourquoi la protection de la vie

des personnels ne mériterait-elle pas une telle attention ? Le temps manque-t-il réellement et les charges de travail sont-elles réellement si lourdes, ou est-ce plutôt le reflet d'une culture organisationnelle qui encourage le personnel à juger qu'il est sous pression constante, à se précipiter d'une crise à l'autre sans avoir le temps de faire une pause et de reprendre son souffle ? Au bout du compte, la gestion de la sécurité des opérations dans les zones à haut risque est une obligation à la fois morale et légale. Les organisations doivent prendre le temps de veiller à ce qu'elle soit faite comme il se doit et de manière satisfaisante.

Il importe de noter que les bonnes pratiques de gestion de la sécurité sont étroitement liées aux bonnes pratiques plus larges de gestion des programmes et du personnel, sur lesquelles elles s'appuient et qu'elles renforcent. Il ne s'agit pas de tâches ni de charges de travail séparées ; il y a un effet multiplicateur positif important. Une bonne gestion de programme nécessite une compréhension du contexte opérationnel, de l'impact de la présence et du travail de votre organisation, la création de bonnes relations, une bonne gestion du personnel international / national et une collaboration efficace avec d'autres organisations.

Comment utiliser cette RBP

Le guide est structuré de la manière suivante. La partie I (chapitre 1) explore les concepts et principes fondamentaux de la gestion de la sécurité. La partie II (chapitres 2 à 5) souligne les approches stratégiques et opérationnelles de la gestion de la sécurité, notamment l'évaluation des risques et une stratégie de la sécurité organisationnelle. La partie III (chapitre 6) évoque les questions relatives au personnel, entre autres le recrutement, la composition du personnel et la gestion du stress. La partie IV (chapitre 7) couvre la gestion de la communication. La partie V (chapitres 8 à 15) examine diverses situations spécifiques de menace et de risque ainsi que les manières de les gérer, y compris les déplacements, la sécurité du site, l'argent liquide et réagir face aux bandes et aux foules. Elle étudie également les questions relatives à l'agression sexuelle, à la détention, à l'arrestation, à l'enlèvement, au rapt et aux situations d'otages.

Certains utilisateurs auront une vaste expérience de la gestion de la sécurité ou feront partie d'organisations ayant une forte culture de sécurité et les capacités correspondantes. D'autres auront peu ou pas d'expérience en la matière, ou travailleront dans des organisations qui n'ont pas consacré beaucoup de temps à la gestion de la sécurité. Les utilisateurs potentiels de cette RBP se trouveront dans des positions très différentes et étudieront donc la question de la gestion de la sécurité opérationnelle sous différents angles et avec différents besoins et priorités. Nous espérons que ce guide pourra satisfaire les besoins de nombreux et différents lecteurs.

Partie 1
Concepts et principes fondamentaux

Chapitre 1
Concepts et principes fondamentaux de la gestion de la sécurité

1.1 Pourquoi gérer les risques de sécurité ?

Gérer la sécurité n'est pas une fin en soi. L'intérêt principal est de pouvoir fournir une assistance humanitaire de manière impartiale, ce qui pourrait nécessiter d'établir et de maintenir une présence dans des contextes très dangereux. Un haut niveau d'insécurité compromet ou entrave la réalisation de cet objectif. La gestion de la sécurité est donc un moyen pour une fin opérationnelle. Parallèlement, la gestion de la sécurité signifie protéger et préserver la vie et le bien-être du personnel de l'organisation (et éventuellement de ses partenaires) et protéger les actifs de l'organisation ainsi que ses programmes et sa réputation. Ceci est valable à deux points de vue :

- D'un point de vue pragmatique, la perte temporaire ou permanente de biens ou les dommages corporels subis par un membre du personnel réduisent la capacité opérationnelle et peuvent même conduire l'organisation à suspendre son programme ou à se retirer.
- Moralement, les organisations ont un devoir de diligence envers leurs employés et collègues. Bien que le travail humanitaire implique un certain niveau de risque, les organisations doivent s'assurer que toutes les mesures raisonnables sont prises pour atténuer ce risque.

Obligation légale de l'employeur, le devoir de diligence est de plus en en plus important. Dans de nombreux pays, le droit du travail impose aux employeurs l'obligation de garantir la sûreté sur le lieu de travail. Bien que ces obligations aient rarement été prises en considération dans le contexte de l'aide humanitaire internationale, les organisations humanitaires s'exposent à des problèmes juridiques si elles n'informent pas leur personnel comme il se doit des risques associés à une mission particulière ou si elles ne prennent pas toutes les mesures nécessaires pour réduire ces risques.

Il est donc essentiel, du point de vue opérationnel, moral et légal, de gérer les risques de sécurité de manière efficace. L'objectif est de protéger le personnel et les biens, tout en faisant parvenir l'aide à certaines des personnes dans le monde qui en ont le plus besoin.

1.1.1 Combiner les risques de sécurité et d'autres risques

La gestion des risques ne porte pas entièrement sur les risques de sécurité : lorsqu'elles se penchent sur la question des risques, les organisations et les personnes tiennent compte d'autres facteurs. Une organisation qui décide d'aller ou de rester dans un environnement où les risques de sécurité sont très élevés peut avoir des motivations financières. Souvent, des considérations de réputation entrent également en jeu. Dans certains cas, les organisations ont de fortes raisons liées à leur réputation et leurs finances d'être actives dans une crise à grand retentissement, même si elle est dangereuse. Le personnel, surtout le personnel national, pourrait accepter individuellement de travailler dans des contextes très dangereux à la vue des motivations économiques qui autrement ne lui seraient pas accessibles. Un autre type de considération, qui mérite une plus grande attention, est le besoin auquel les organisations tentent de répondre. Quelles seraient les conséquences, pour des personnes dans le besoin, de mettre fin à un programme ? Quelle peut être l'efficacité d'un programme dans ces conditions ? Combien de personnes peuvent réellement être secourues ? Quelle est la gravité de leurs besoins matériels et de leurs besoins de protection ? Ces questions sont évoquées en détail dans les chapitres suivants.

1.1.2 Cadre de base de la gestion des risques de sécurité

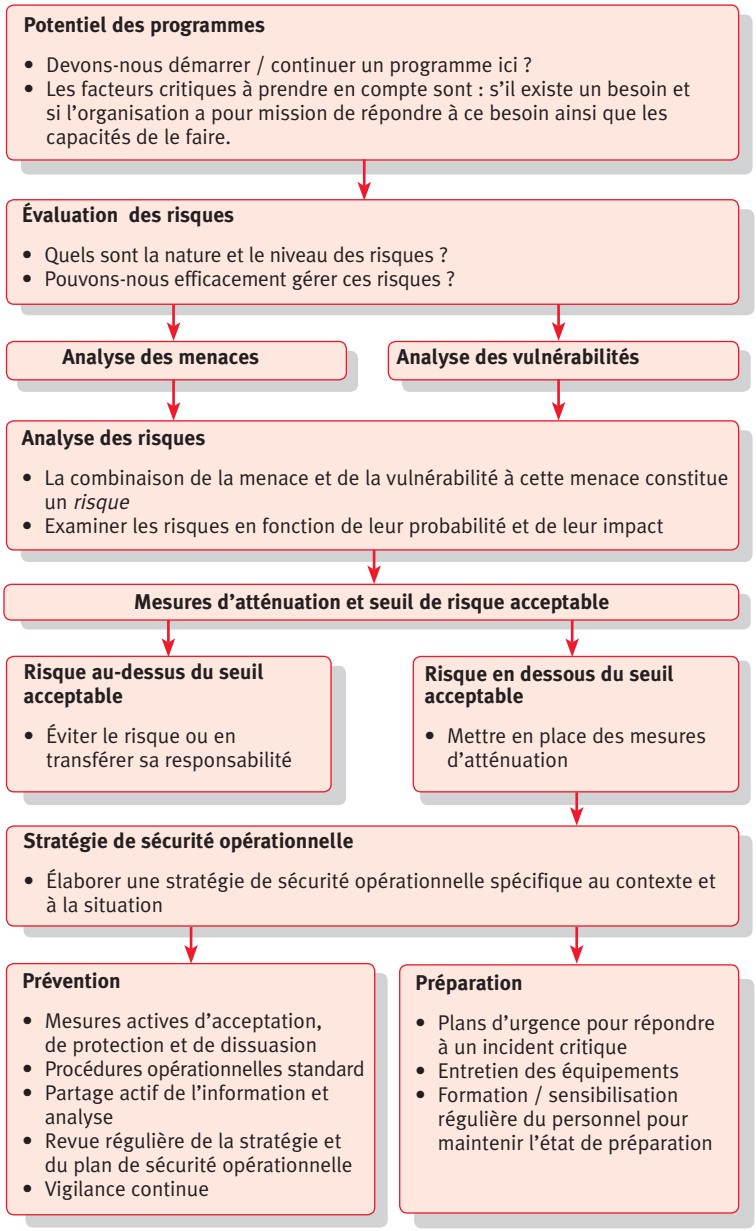
La figure 1 montre le cadre de base de la gestion des risques de sécurité.[1] La logique fondamentale de ce cadre est la même que celle du cycle de la gestion d'un projet : évaluer, planifier, mettre en œuvre (et ajuster si nécessaire), analyser et réévaluer. Notez que ce modèle comporte la possibilité de ne pas mettre en œuvre un programme si les risques étaient jugés trop élevés, de le modifier radicalement si les risques changeaient ou d'y mettre fin.

Les principales étapes du processus de gestion de la sécurité sont :

- Identifier un programme potentiel : un besoin existe et l'organisation a la mission, ou le mandat, et les capacités d'y répondre.
- Évaluer de manière exhaustive les risques de sécurité et les capacités de l'organisation (ressources humaines, financières et temporelles) pour gérer ces risques. (Le processus d'évaluation des risques est abordé au chapitre 2).
- Déterminer le seuil de risque acceptable. Ce seuil peut être différent selon les avantages potentiels d'une présence et d'un programme, et selon la mission de l'organisation.
- Demander si les risques dépassent les moyens dont dispose l'organisation pour les gérer : si c'est le cas, n'exécutez pas le programme (ou bien

1 Cette figure comprend des éléments du guide de l'IASC Security Risk Management (Gestion des risques de sécurité) (Washington DC : InterAction Security Advisory Group, 2010), p. 7.

Figure 1
Cadre de gestion des risques sécuritaires



« transférez » les risques à un autre acteur qui peut les gérer). Si la capacité de gestion de la sécurité est suffisante pour réduire les risques jusqu'à un niveau acceptable, lancez le programme.

- Élaborer une stratégie de sécurité opérationnelle spécifique au contexte et à la situation (les concepts d'acceptation, de protection et de dissuasion sont expliqués au chapitre 3).
- Une gestion de la sécurité responsable exige non seulement de prendre des mesures préventives pour éviter un incident mais également d'investir dans la capacité de gérer une situation de crise réelle et les conséquences d'un incident critique. Cela nécessite aussi une évaluation constante des conditions de sécurité afin de déterminer si la stratégie de sécurité reste appropriée aux menaces qui existent dans ce contexte et si les risques restent acceptables.
- Établir des procédures pour répondre à un incident critique. Même avec les meilleures approches et mesures de prévention, un incident peut se produire. Les personnes touchées par un incident devront faire leur possible pour survivre (un facteur important sera leur préparation, ou manque de préparation), alors que l'organisation mobilisera une réponse immédiate à un incident critique.
- Fournir un soutien après l'incident. Les survivants d'un incident critique, et peut-être aussi d'autres membres du personnel et/ou des membres des familles du personnel concerné, auront besoin d'un soutien.
- Effectuer des analyses après l'incident (« analyses après action »). Analysez de manière objective et honnête comment l'incident s'est produit, comment les risques ont été évalués et si les mesures de sécurité étaient appropriées et efficaces. Évaluez la qualité de la réponse et la préparation générale à l'incident critique. Ces analyses et évaluations donneront peut-être lieu à des modifications de la stratégie de gestion de la sécurité, ou conduiront peut-être à la conclusion que les risques sont à présent trop lourds à gérer et que des modifications plus importantes du programme doivent être effectuées, ou bien que les activités doivent être suspendues.

1.1.3 Principaux acteurs de la gestion de la sécurité

Les autorités nationales sont responsables de la sécurité de toutes les personnes civiles se trouvant sur leur territoire. Dans la pratique, cependant, de nombreux gouvernements ne sont pas en mesure d'assumer cette responsabilité (voir l'explication ci-dessous dans la section 1.4). Cela ne signifie pas que les autorités doivent être ignorées, mais que des mesures supplémentaires seront nécessaires pour gérer la sécurité de manière efficace.

Comme indiqué, les organisations ont, en tant qu'employeurs, une responsabilité officielle envers leur personnel. Un concept fondamental à cet égard est le « devoir de diligence ». Le devoir de diligence d'une organisation envers ses

employés doit être défini dans sa politique de sécurité. Il incombe aussi à l'organisation d'informer de manière proactive ses employés, les employés potentiels et le personnel associé tel que les consultants, des risques de sécurité. Cela permet aux personnes de donner leur « consentement éclairé », c'est-à-dire d'accepter un certain degré de risque après avoir été pleinement informé de l'étendue du risque. L'organisation est également responsable de veiller à ce que les risques soient réduits jusqu'à un niveau acceptable.

Les responsables de l'organisation ont également une responsabilité envers leur personnel. Si l'organisation est accusée de négligence en ce qui concerne la sécurité, et si cette négligence a porté atteinte à un membre du personnel ou a causé sa mort, les cadres supérieurs ou les représentants sur le terrain peuvent, dans certains cas, être poursuivis individuellement pour réparation juridique. Un « cadre de responsabilisation », qui peut couvrir des questions autres que la sécurité, est un moyen de préciser aux responsables à tous les niveaux quelles sont leurs responsabilités et leurs obligations de répondre de leurs actes. Il est également important de préciser à *tout* le personnel, des gardes et chauffeurs aux hauts responsables de programme, que chaque personne est responsable de sa propre sécurité et de la sécurité de l'équipe dans son ensemble, ainsi que des biens de l'organisation. Tout le personnel doit prendre part à des discussions et activités régulières, y compris des formations, sur le thème de la sécurité. Une organisation pourrait aussi devoir assumer la responsabilité de personnes autres que son personnel. Les personnes à charge (dépendants) font partie de cette catégorie, tout au moins en ce qui concerne le personnel international. Définissez soigneusement et clairement les responsabilités et assurez-vous que les personnes comprennent l'étendue de leurs responsabilités ainsi que les procédures de sécurité qu'elles doivent suivre. Pour le personnel international, les ambassades des pays concernés pourraient avoir un rôle à jouer pour alerter leurs ressortissants sur des risques possibles. En règle générale, les ambassades ont un seuil de sécurité très bas pour les visiteurs et pour les personnes qui n'opèrent pas dans un cadre de sécurité particulier. Bien qu'il soit important de connaître les recommandations de l'ambassade, une organisation pourra peut-être opérer en sécurité sans observer ces recommandations si elle possède un système efficace de gestion de la sécurité. Les organisations ont également la responsabilité de communiquer les informations vitales en matière de sécurité aux autres organisations actives au même endroit. Ne pas alerter d'autres personnes qu'un membre de son personnel a évité de justesse une embuscade sur une route particulière, par exemple, pourrait rendre inutilement ces personnes victimes d'un violent incident.

Beaucoup d'organisations internationales emploient des conseillers en sécurité globaux pour apporter un soutien aux bureaux sur le terrain. Certaines ont également des conseillers en sécurité régionaux, qui supervisent une

zone opérationnelle à haut risque spécifique et fournissent une capacité de mobilisation instantanée aux programmes. Dans d'autres organisations, la gestion de la sécurité est intégrée dans la gestion générale et il n'y a pas de conseillers spécifiques en sécurité. Dans le pays, la responsabilité de s'assurer que les politiques et procédures organisationnelles sont mises en œuvre et observées incombe au haut représentant (autrement dit le directeur national), bien que dans la pratique un grand nombre de tâches de gestion de la sécurité puissent être déléguées à un conseiller en sécurité (étant donné les sensibilités concernant le mot « sécurité », dans certains pays le terme « conseiller en sûreté » est plutôt utilisé pour cette fonction). La décision de nommer un conseiller en sécurité (soit à plein temps ou, à mi-temps lorsque l'agent de liaison en matière de sécurité a d'autres responsabilités) doit être basée sur diverses considérations, notamment sur l'indice de risque pour cette zone, le champ de travail et les ressources disponibles.

De nombreuses organisations délèguent l'autorité décisionnelle au directeur national et à son personnel sur le terrain, plutôt que de confier cette responsabilité à un bureau régional ou au siège international. Cependant, la responsabilité absolue incombe au directeur exécutif ou, dans certains cas, au conseil d'administration. Ces responsabilités doivent être clairement énoncées dans les descriptifs de postes. Des décisions spécifiques pourront aussi nécessiter l'accord officiel d'une autorité plus haute que celle du haut représentant sur le terrain. Celles-ci comprennent :

- réduire l'indice de risque d'un pays ou d'une zone d'un pays ;
- retourner dans une zone après avoir relocalisé le personnel hors de cette zone pour raison de sécurité ;
- adopter une approche de « discrétion » et retirer les logos et drapeaux des bureaux et des véhicules ; et
- utiliser une protection armée
- utiliser un prestataire privé de sécurité.

Les incidents majeurs, comme le rapt ou la prise d'otages, nécessitent également l'intervention constante de la haute direction de l'organisation. Les bailleurs de fonds officiels peuvent avoir imposé des obligations contractuelles concernant la visibilité (identification par leur marque/logo) de l'assistance qu'ils financent, auquel cas l'organisation pourra devoir demander leur autorisation officielle de ne pas observer cette exigence.

1.2 Gestion de la sécurité organisationnelle

Bien que la plupart des organisations délèguent la prise de décisions à des personnes en poste aussi proches du terrain que possible, la gestion

opérationnelle de la sécurité est liée, de manière complexe, à des pratiques et prises de décisions organisationnelles plus larges, entre autres :

- L'élaboration d'une politique de sûreté et de sécurité et des conseils pratiques sur la gestion de la sécurité pour l'ensemble de l'organisation.
- Des compétences et responsabilités organisationnelles pour certains incidents graves, y compris la création d'une équipe de gestion d'incidents critiques dans le bureau régional et/ou au siège mondial (pour les organisations internationales).
- L'établissement et le maintien d'un système centralisé de rapports pour rassembler toutes les traces d'incidents de sécurité et d'incidents évités de justesse, afin de permettre une analyse globale des incidents de sécurité qui touchent l'organisation.

Les décisions concernant le lancement d'opérations dans un certain pays et le choix du type de programme à effectuer incombent généralement au siège. L'organisation pourra aussi demander aux hauts responsables du siège de prendre les décisions concernant certaines questions majeures de sécurité, comme indiqué plus haut. De plus, une grande partie du travail concernant les médias, les communications et la collecte de fonds pour les programmes sur le terrain pourra être effectuée au siège. Les questions relatives aux ressources humaines, comme l'établissement de polices d'assurance, sont en général également traitées par l'ensemble de l'organisation plutôt que par une personne au niveau opérationnel.

Une organisation humanitaire qui déploie des personnes dans des zones à haut risque doit avoir les politiques, procédures et capacités pour gérer de telles opérations. Ces politiques pourraient être énoncées dans la liste de documents qui suit. Ces documents ont une compétence à l'échelon de l'organisation, ils sont élaborés au siège et par le siège et constituent des ressources de référence générales.

- Mandat, énoncé général de mission ou énoncé des valeurs et principes de l'organisation.
- Politique générale de sécurité pour l'ensemble de l'organisation et, le cas échéant, déclarations de principe sur des questions spécifiques de sécurité, telles que l'utilisation de protection armée, de prestataires privés de sécurité et de protection des informations.
- Structure de responsabilisation de la direction, énonçant clairement à qui incombent les responsabilités de gestion de la sécurité et des incidents critiques et les responsabilités décisionnelles (en faisant la distinction entre le siège et le terrain).

- Guides et manuels généraux de référence, par exemple sur l'utilisation de la radio.

1.2.1 Planification de la sécurité et préparation

Sur le terrain, la pierre angulaire de la gestion de la sécurité est le plan de sécurité. La qualité d'un plan de sécurité opérationnelle dépend de la qualité du processus de planification. Une planification d'équipe - mettant en jeu le personnel national et international - est préférable à la planification individuelle, car elle exploite les connaissances et expériences collectives et facilite l'adhésion au produit final. Un bon processus de planification doit être complété par des analyses périodiques ; le plan devra être adapté aux changements qui surviennent dans le contexte en question.

Chaque organisation produit son propre plan de sécurité qui reflète ses besoins organisationnels, le contexte et ses politiques et procédures organisationnelles. Un bon plan de sécurité pourra être composé des éléments essentiels suivants :

- Un résumé du contexte du pays, y compris du conflit, s'il y a lieu.
- Les objectifs spécifiques de la mission dans le pays.
- Une évaluation des risques de sécurité (pour une explication détaillée, voir chapitre 2).
- Le seuil de risque acceptable : cette information doit indiquer comment ce seuil a été défini (voir chapitre 2).
- Une déclaration des responsabilités en termes de gestion de la sécurité.
- Les mesures préventives. Certaines mesures seront couvertes dans les procédures opérationnelles standard car elles porteront sur des questions telles que la sécurité du site, les déplacements et les communications (voir parties IV et V). Certaines de ces procédures opérationnelles standard peuvent paraître sous forme de listes de contrôle. D'autres mesures préventives ne sont pas incluses dans des procédures opérationnelles standard ni dans des listes de contrôle, par exemple les efforts pour obtenir une meilleure acceptation parmi les acteurs locaux.
- Une clarification des rôles et responsabilités en matière de réponse aux incidents et de gestion des crises. Dans certains cas, l'intervention du bureau régional ou du siège peut être nécessaire ou obligatoire (pour un exposé détaillé sur la gestion d'incidents critiques, voir chapitre 5).
- La procédure de la déclaration d'incident et de l'analyse d'une réaction en cas d'incident.
- Un plan de repli (hibernation, relocalisation, évacuation).
- Une déclaration de principes concernant la collaboration en matière de sécurité avec d'autres acteurs actifs dans le même contexte, comme par exemple reconnaître l'interdépendance des prestataires d'aide et les

responsabilités minimales correspondantes, notamment donner l'alerte à d'autres acteurs et éventuellement collaborer dans les domaines de l'analyse et de l'évaluation des risques, et la mise en commun ou le partage de ressources ou de la logistique en cas de retrait.
- Une déclaration indiquant quand le plan a été établi ou examiné pour la dernière fois, comment il a été établi (le processus de planification et qui y a participé), qui l'a approuvé et quand il sera de nouveau examiné.
- Des cartes du lieu d'opérations, indiquant entre autres l'emplacement des bureaux.

Un certain nombre de points sont à prendre en considération concernant les plans de sécurité :

- Un plan est une feuille de papier. Le papier ne réduit aucun risque. Les plans doivent être partagés, expliqués et mis en œuvre.
- Un bon plan aujourd'hui pourrait ne plus être approprié dans six mois. Si la situation évolue, réexaminez l'analyse et les plans.
- Les personnes qui ne connaissent pas bien les plans et procédures de sécurité ne peuvent les observer. Tous les membres du personnel et tous les visiteurs doivent être informés de ces plans et procédures dès leur arrivée et chaque fois que des modifications importantes y ont été apportées.
- Une bonne mise en œuvre dépend des compétences. Le meilleur des plans s'effondre s'il n'existe pas les connaissances et les aptitudes pour le mettre en œuvre. Certains aspects de la gestion de la sécurité exigent des connaissances ou compétences spécialisées.
- Une gestion efficace de la sécurité repose, dans une certaine mesure, sur l'entraînement pratique. Il est essentiel de s'entraîner avec des simulations et des formations.

1.2.2 Revoir les plans de sécurité

Même dans un contexte calme et sûr, les plans de sécurité doivent être revus une fois par an. Dans les situations à hauts risques, ils doivent être revus plus fréquemment pour s'assurer qu'ils reflètent les risques présents et que les informations qu'ils contiennent sont à jour.

Quand revoir les plans ?

- Lorsque des changements notables sont intervenus dans le contexte externe, en particulier suite aux actions de protagonistes majeurs.
- Lorsqu'une autre organisation a été touchée par un incident, plus particulièrement dans la même zone opérationnelle ou à proximité de cette zone.
- Lorsqu'un autre acteur est touché par un incident qui, de par sa nature ou son intensité, semble introduire un nouvel élément dans l'évaluation des risques initiale.

Que revoir

Pratiquement tout peut être revu :

- Le contexte et l'analyse situationnelle au sens large.
- L'évaluation des menaces.
- L'évaluation des risques.
- La stratégie de sécurité.
- Les procédures opérationnelles standard de prévention/contrôle des risques.
- Les choix de programmes et/ou la stratégie de mise en œuvre.
- La politique d'emploi et les critères de recrutement.
- Les choix de véhicules et de transport.
- Les dispositions/pratiques du partage des informations de sécurité entre organisations.
- Les contacts et relations utilisés pour maintenir l'acceptation.

Si l'examen indique une détérioration importante de la sécurité, le personnel pourra être réuni et informé de la nouvelle évaluation de la situation et de ce qui peut être fait, de façon réaliste, pour atténuer les risques. Les membres du personnel doit pouvoir réévaluer la situation en fonction de leur propre seuil de risque acceptable et reconfirmer, ou pas, leur « consentement éclairé ».

1.2.3 Développer une culture de sécurité

Généralement, la gestion de la sécurité porte, en grande partie, sur des besoins opérationnels spécifiques, tels que les politiques et plans de sécurité. Mais il est également nécessaire de faire un pas en arrière et d'étudier comment développer une culture de sécurité au sein de l'organisation, et entre autres comment renforcer les capacités. L'une des priorités les plus importantes est de s'assurer que tout le personnel connaît l'organisation et sa mission dans un contexte, quel qu'il soit. Il n'est pas rare qu'une grande partie du personnel, y compris le personnel national, ne sache pas grand-chose au sujet de l'organisation qu'il représente. Le personnel doit être informé de la raison d'être de l'organisation. Les questions clés comprennent :

- Pourquoi cette organisation est-elle là ?
- Que fait-elle-là ?
- Où obtient-elle ses fonds ? À quelle fin utilise-t-elle ses fonds ?
- Qui dirige ses activités ?
- Sert-elle des intérêts politiques étrangers ?
- Quel est son programme politique ?
- Souhaite-t-elle changer la société, la culture, les valeurs ou la(les) religion(s) locales ?

- Prend-elle le parti du gouvernement (ou d'un autre acteur politique dans ce contexte) ?

Envisagez de fournir aux membres du personnel des documents écrits dans leur(s) propre(s) langue(s), et étudiez-les avec eux de manière interactive, réunissez-les périodiquement pour savoir quels types de questions et commentaires ils reçoivent le plus régulièrement des membres de la communauté et comment ils y répondent. De plus, faites de la sécurité une priorité pour tout le personnel, ne la considérez pas comme un problème de gestion délicat, à évoquer en privé, par quelques membres du personnel seulement. En particulier :

- Assurez-vous que tout le personnel connaît le contexte, les risques et les engagements de l'organisation en matière de réduction des risques et de gestion de la sécurité.
- Assurez-vous que tous les membres du personnel comprennent leurs responsabilités individuelles en ce qui concerne la sécurité, le travail d'équipe et la discipline.
- Conseillez et aidez les membres du personnel à se préoccuper de leur situation médicale et financière et de leur assurance personnelle avant d'être déployés dans une zone à hauts risques.
- Expliquez clairement quelles sont les attentes concernant les responsables et les styles de gestion dans des circonstances normales et dans des situations de grand stress.
- Faites de la sécurité un point permanent (de préférence le premier point) de l'ordre du jour de toutes les réunions de direction et des réunions régulières du personnel.
- Exigez des examens et, si nécessaire, des mises à jour des recommandations de sûreté et de sécurité de base, ainsi que des plans de sécurité à l'échelle d'un pays et spécifiques à une région, comme décrit plus haut.
- Investissez dans le développement des compétences. Il n'est pas rare que des organisations humanitaires se précipitent pour organiser une formation sur la sécurité lorsqu'une situation se détériore. Il faut investir dans le développement du personnel, notamment dans les compétences de réduction des risques de sécurité, en périodes de calme et de stabilité.
- Veillez à ce que la sécurité soit une considération essentielle de toute planification de programme.
- Faites effectuer des inspections périodiques de l'équipement par une personne qualifiée, entre autres les radios, les trousses de secours, les détecteurs de fumée, les extincteurs d'incendie, les alarmes anti-effraction et les gilets pare-balles
- Effectuez des analyses après action. L'objectif est d'évaluer ce qui s'est produit et comment l'équipe a réagi dans cette situation, et non

pas d'évaluer les responsabilités individuelles. Il s'agit d'un exercice d'apprentissage collectif.

Intégrer une culture de sécurité, aussi bien au niveau des membres individuels du personnel qu'au niveau de l'organisation, signifie tenir compte des implications de sécurité dans tout ce que fait l'organisation (ou tout ce qu'elle choisit de ne pas faire) depuis les discussions sur la conception de programmes et les communications au public jusqu'aux décisions concernant le financement et le recrutement de prestataires externes. Les gens « pensent sécurité » et agissent en conséquence parce qu'ils comprennent son importance, et on les respecte pour cela. L'importance de la sécurité est continuellement renforcée, non seulement dans les politiques écrites mais aussi dans les actions. Le haut personnel est tenu responsable des décisions qui ont un impact positif ou négatif sur la sécurité globale du personnel. Les organisations ont également commencé à effectuer des audits de sécurité annuels de leurs bureaux sur le terrain par rapport à une série de critères. Ces audits sont généralement annoncés à l'avance, mais pas toujours. Ils peuvent avoir lieu après un incident critique, à des périodes ou dans des lieux à risque accru, ou périodiquement dans n'importe quel environnement dangereux.

1.3 Gestion de la sécurité entre organisations

1.3.1 Collaboration et interdépendance

La gestion de la sécurité dans le monde de l'aide humanitaire est, dans une large mesure, axée sur les organisations, et ce pour des raisons évidentes : en tant qu'employeur, l'organisation doit assumer la responsabilité de la sûreté et de la sécurité de son personnel, et les ressources seront naturellement affectées à cet effet ; les mandats ou missions diffèrent selon les organisations et celles-ci peuvent donc déterminer différents seuils de ce qu'elles considèrent comme « un risque acceptable » et poursuivre différentes stratégies de sécurité. Parallèlement, les organisations actives dans le même environnement de violence, ont aussi de bonnes raisons de coopérer. Les modes de coopération comprennent :

- L'alerte collective : si une organisation subit ou évite de justesse un incident on doit présumer que d'autres organisations courent le même risque, sauf s'il est prouvé que l'organisation était directement ciblée. Mentionner rapidement l'incident à d'autres organisations dans la région est une responsabilité collective.
- L'interdépendance directe : si une organisation dispose de la capacité à obtenir un avion ou un navire pour évacuer son personnel et que d'autres acteurs n'ont pas cette possibilité, les organisations concernées devront se mettre d'accord au préalable sur les critères et procédures d'évacuation.

- L'interdépendance indirecte : les stratégies de sécurité d'une organisation peuvent avoir des répercussions sur d'autres organisations. Si une organisation offre des pots-de-vin aux postes de contrôle par exemple, cela créera des problèmes pour celles qui ne le font pas. Si un certain nombre d'organisations travaillent dans un district et que la majorité décide d'utiliser des gardes armés, cela accroîtra la vulnérabilité d'autres organisations, qui deviendront de ce fait une cible « facile ». Si une organisation décide de « suspendre » son aide dans un certain district parce que l'un de ses véhicules a fait l'objet d'un vol à main armée, cela pourra avoir un impact sur d'autres organisations qui travaillent à cet endroit.

La collaboration entre organisations peut offrir des avantages notables :

- Un meilleur système d'alerte : les organisations obtiennent une vue plus complète des menaces de sécurité réelles ou possibles dans leur environnement, ce qui augmente leurs chances d'éviter un incident. Ce système peut être facilité par un « réseau de communications » utilisant des téléphones portables, l'e-mail et la radio. Il peut également être facilité par une chaîne de radio d'urgence commune.
- Une meilleure évaluation des risques : un fichier central de tous les incidents et incidents évités de justesse dans un contexte opérationnel donné est, pour l'évaluation des risques, une meilleure base que des documents partiels ou incomplets.
- Un suivi et une analyse stratégiques et tactiques de l'environnement opérationnel et de ses implications de sécurité : toutes les organisations doivent suivre cette procédure. Généralement elles contacteront d'autres acteurs non officiellement pour obtenir des informations. Lorsque la confiance règne et que la confidentialité est respectée, il est possible de collaborer de manière plus structurée.
- Une capacité ou des services supplémentaires, financièrement avantageux : des spécialistes peuvent être utilisés de manière collective pour éviter à chaque organisation de subir individuellement les coûts d'obtenir ou de recruter des compétences supplémentaires. Le coût d'un événement de formation en matière de sécurité peut également être partagé.
- Une liaison et un engagement avec les autorités : les organisations peuvent potentiellement mieux défendre ensemble leur position qu'individuellement, et de manière plus cohérente.
- Un plaidoyer auprès des bailleurs de fonds : si la situation sécuritaire se détériore et que plusieurs organisations concluent qu'elles ont besoin de ressources financières supplémentaires pour prendre un plus grand nombre de mesures d'atténuation, elles pourront peut-être mieux défendre leur position auprès des bailleurs de fonds de manière collective.

1.3.2 Mécanismes de sécurité inter organisations

Au siège

Au siège, la coordination entre ONG et entre ONG et l'ONU a progressé au cours des dernières années. Il existe aujourd'hui deux forums régionaux de sécurité entre les organisations non gouvernementales : le Security Advisory Group (Groupe de conseil en sécurité) (SAG) d'InterAction, basé à Washington DC, qui répond aux besoins de la communauté des ONG américaines, et le European Interagency Security Forum (Forum européen de sécurité inter organisations) (EISF), basé à Londres, qui est utilisé par la communauté des ONG européennes. Ces structures sont des forums de partage d'informations, de sensibilisation, de plaidoyer et de formation. Ils sont jugés utiles pour encourager et promouvoir les bonnes pratiques ainsi que pour partager les leçons tirées et fournir des informations spécifiques concernant un pays en temps réel ou quasi réel. L'initiative « Sauver des vies ensemble » fournit un cadre pour la collaboration entre l'ONU et des ONG en matière de sécurité (voir annexe 3). Depuis 2007, le HCNUR et OCHA ont co-présidé un groupe de travail de l'IASC sur les difficultés que rencontre l'espace humanitaire.[2]

Mécanismes de sécurité sur le terrain

Il n'existe pas de modèle standard de mécanisme de sécurité entre organisations. Dans la pratique, les mécanismes de collaboration se sont présentés sous diverses formes, notamment :

- Un travail en réseau non formel, par exemple des réunions périodiques ou un réseau non formel d'agents de liaison en matière de sécurité.
- Des mesures de sécurité entre organisations, par exemple un réseau de surveillance résidentielle partagée, le partage d'agents de liaison en matière de sécurité sur le terrain ou la formation relative à la sécurité.
- L'introduction de la sécurité comme thème dans les groupes de travail inter organisations existants.
- Des bureaux de sûreté et de sécurité inter organisations, pouvant obtenir des ressources et être dirigés indépendamment, ou pouvant être accueillis par des ONG de manière permanente ou temporaire.

Un mécanisme de sécurité inter organisations peut avoir plusieurs fonctions, notamment :

- Organiser des réunions sur la sécurité.
- Donner des alertes de sécurité, recouper les informations non confirmées et faciliter la diffusion des informations.
- Effectuer des évaluations des risques et des analyses des caractéristiques

2 V. V. Tennant, B. Doyle et R. Mazou, *Safeguarding Humanitarian Space : A Review of Key Challenges for UNHCR* (Protéger l'espace humanitaire : Étude des principales difficultés pour le HCR) (Genève : HCNUR)

Exemples de mécanismes de sécurité interorganisations sur le terrain[3]

- L'Afghanistan NGO Safety Office (Bureau de sûreté des ONG en Afghanistan) (ANSO). ANSO a été établi à la fin 2002. Il comprend un personnel de sécurité international et national.
- Le bureau de sécurité de l'ONG Coordinating Committee for Iraq (Comité de coordination des ONG en Irak) (NCCI). Le NCCI est un organisme autonome qui s'est développé d'un forum général de coordination pour les OING travaillant en Irak en 2003. À la fin 2004, le NCCI s'est relocalisé à Amman en Jordanie pour des raisons de sécurité, de même que la plupart des organisations humanitaires internationales, et le bureau de sécurité a suspendu sa surveillance des incidents. Au début 2010, le NCCI avait construit un vaste réseau d'informations constitué d'ONG locales à l'intérieur du pays ainsi qu'un nouveau système de surveillance des incidents de sécurité. Le NCCI commence, avec certaines ONG internationales, à redéployer du personnel à l'intérieur de l'Irak.
- Le consortium d'OING du Balochistan - Security Management Support Project (Projet de soutien à la gestion de la sécurité) (BINGO) a été créé au début 2004 par des organisations basées à Quetta au Pakistan. Le consortium a utilisé des agents de sécurité nationaux et internationaux. À la fin 2005, BINGO a fermé ses portes dû, en partie, à la pression exercée par les autorités pakistanaises et en partie parce que les ressources des OING ont été affectées à de nouvelles priorités pour l'intervention suite au tremblement de terre.
- Le NGO Safety Program (Programme de sûreté des ONG) (NSP) en Somalie. Le NSP a été établi par un plus grand consortium d'ONG en Somalie à la fin 2004. Il est situé à Nairobi mais a des liens dans les régions somaliennes. Le projet utilise des agents de sécurité internationaux et nationaux.
- L'Initiative ONG Sécurité (IOS)-Haïti. IOS-Haïti a été créée à la fin 2005 et son personnel comprenait un agent de sécurité national. IOS a fermé en 2009 mais a été réactivée pour répondre au tremblement de terre en janvier 2010.
- Le Gaza NGO Safety Office (Bureau de sécurité des ONG à Gaza) (GANSO). GANSO a été établi en 2008 pour fournir des informations et une analyse aux ONG actives à Gaza.
- OASIS, au Tchad, fournit des logiciels, aide à gérer les données relatives aux incidents, développe l'apprentissage et soutient les flux d'informations entre organisations actives au Tchad. Il est actuellement accueilli par iMMAP et utilise son logiciel de cartographie spécifiquement créé. Il est soutenu par des bailleurs de fonds internationaux.

3 La plupart de ces mécanismes de sécurité sont accueillis par une OING et obtiennent leur soutien financier de bailleurs de fonds internationaux.

et des tendances, et en communiquer les résultats dans des rapports relatifs aux menaces.
- Fournir des instructions de sécurité élémentaires, une assistance et des conseils techniques ainsi qu'une formation aux organisations individuelles.
- Gestion des crises : fournir un soutien pour la planification d'urgence et faciliter une aide in-extremis ; par exemple si une organisation subit un incident critique tel qu'un rapt, cette structure pourrait être en mesure de fournir une analyse et un soutien supplémentaires par le biais de réseaux locaux.
- Liaison avec les autorités gouvernementales, les forces militaires internationales et nationales, y compris les forces du maintien de la paix des Nations Unies, et les sociétés privées de sécurité.

Souvent, la structure inter organisations est hébergée par une organisation particulière, qui lui donne l'identité légale dont elle a besoin pour recevoir et dépenser des fonds. L'organisation hôte signe les contrats et assume la responsabilité légale. La plupart de ces structures de sécurité sur le terrain agissent entre ONG et en principe n'incluent pas les agences des Nations Unies, bien que les informations et les analyses puissent être partagées. Dans les cas où la collaboration est plus formelle, la relation peut être plus directe, surtout lorsque des membres du personnel de sécurité des Nations Unies ont été désignés en tant qu'agents de liaison pour ONG. Autrement, dans le cadre de l'initiative Sauver des vies ensemble, les ONG peuvent identifier un agent de sécurité qui fera partie des équipes de gestion de la sécurité des Nations Unies.

Certaines organisations très à cheval sur les principes humanitaires tendent à rester en dehors de structures de sécurité formelles, bien qu'elles puissent partager des informations dans diverses mesures. La majeure partie des structures de sécurité sur le terrain fonctionnent entre ONG internationales et on ne sait pas au juste dans quelle mesure les ONG nationales y participent et en bénéficient.

Entraves et facteurs propices

Les facteurs qui gênent ou facilitent la collaboration entre organisations en matière de sécurité sont en grande partie les mêmes facteurs qui gênent ou facilitent la collaboration entre organisations humanitaires en général, même si le thème de la sécurité en soi peut révéler des sensibilités particulières.

Il est important de savoir qu'une organisation pourrait développer une dépendance excessive envers un mécanisme inter organisations au point qu'elle remplace les mesures internes visant à maintenir activement sa propre gestion de la sécurité. Il faut s'assurer que le mécanisme fournit à l'organisation une capacité additionnelle mais qu'il ne la supplante pas.

Tableau 1: Obstacles et facteurs propices à la collaboration en matière de sécurité

Facteurs pouvant entraver la collaboration en matière de sécurité	Facteurs pouvant faciliter la collaboration en matière de sécurité
• Manque d'engagement et de soutien de la part de l'organisation. • Différences d'approches, par exemple concernant la sécurité armée. • Gouvernance inefficace. • Manque ou perte de transparence et de confiance, par exemple parce que les informations sensibles ne sont pas traitées avec discrétion. • La suspicion et l'ingérence des autorités. • Les problèmes de recrutement et de rétention du personnel. • Des priorités rivales et des charges de travail générales lourdes. • Un financement insuffisant.	• Collaboration déterminée et gérée par les ONG, bonne adhésion. • Buts et objectifs communs et réalistes. • Appropriée à la situation. • Direction et gouvernance efficaces. • Personnel, capacités et ressources appropriés. • Mécanismes d'établissement de rapports faciles à utiliser. • Informations traitées avec délicatesse et confidentialité. • Analyse opportune et détaillée fournie aux participants. • Une détérioration du contexte de la sécurité conduit les ONG à remettre en question leur gestion de la sécurité. • Accès à un financement adéquat et prévisible pour la sécurité.

1.4 Transférer les risques de sécurité

Dans le travail humanitaire, il est courant qu'une partie ou que la totalité d'un programme soit conçue et « possédée » par une organisation mais mise en œuvre par une autre. Travailler avec et par le biais d'autres organisations ou associations, que ce soit des ONG, des organisations communautaires ou des prestataires privés, pourrait être plus rentable, ou pourrait faire partie d'une stratégie intentionnelle de renforcement des capacités locales. Le transfert des risques devient un élément constitutif d'une stratégie de sécurité opérationnelle lorsqu'une organisation recherche sciemment un autre acteur pour entreprendre certaines activités dans un contexte très dangereux.

Il existe une distinction fondamentale entre transférer un risque au personnel national de l'organisation (qui est clairement sous la responsabilité légale de cette organisation) et transférer le risque à des entités ayant leur propre identité légale. Dans le premier cas, l'organisation pourrait conclure que les risques posés au personnel national et au personnel international sont relativement similaires et que ni l'un ni l'autre ne doit être déployé dans des zones jugées trop dangereuses. Ou bien, l'organisation pourrait déterminer, en se basant sur une ferme évaluation des risques, que les personnels

national et international sont exposés à des risques différents. L'évaluation des risques effectuée par une organisation peut confirmer que le personnel international est exposé à un risque plus élevé. La décision pourra être de retirer le personnel international et de laisser le personnel national en place pour gérer et superviser le programme. Le personnel national aura souvent ainsi une plus grande autorité, ce qui pourrait augmenter les pressions qu'il subit et les risques auxquels il est exposé. Il est important que les organisations déterminent à quel moment la situation dépasse le seuil de ce qui constitue un risque acceptable. Ceci est beaucoup plus difficile à établir si le personnel international (et éventuellement le personnel national mais non local) n'est plus présent. De même, il est difficile de déterminer quand la situation de sécurité s'est suffisamment améliorée pour permettre au personnel international et national non local de retourner sur les lieux.

Les entités ayant leur propre identité légale sont uniquement responsables de la gestion de la sécurité de leur personnel et de leurs biens, ainsi que de l'atténuation des risques. En ce sens, l'organisation qui transfert les risques n'a pas la responsabilité légale de fournir un soutien en matière de sécurité. Cela n'exclut cependant pas la possibilité d'une responsabilité éthique et morale, de même que la responsabilité pratique de s'assurer que les besoins opérationnels et de sécurité sont abordés afin que le travail puisse être effectué. Les options pour fournir un soutien à un partenaire d'exécution comprennent :

- Une évaluation commune, avec le partenaire d'exécution, des risques de sécurité et du seuil de risque acceptable, afin que les acteurs aient tous deux un tableau précis des risques possibles, ce qui permet au partenaire d'exécution (et à son personnel) de donner son consentement éclairé. Cette évaluation devra faire l'objet d'une analyse commune périodique de l'évolution de la situation de risque.
- Une évaluation commune de la capacité du partenaire d'exécution à gérer les risques de sécurité et, au besoin, un renforcement des capacités, par exemple par la formation, le détachement d'un conseiller en sécurité et des analyses communes périodiques des mesures d'atténuation des risques de sécurité et des procédures de gestion des incidents critiques.
- Un effort soutenu pour accorder au personnel du partenaire d'exécution, ou tout au moins au personnel le plus exposé aux risques, une couverture assurance appropriée pour la protection médicale et la protection contre les actes malveillants.
- Une initiative pour transférer les capacités de sécurité au partenaire d'exécution sous forme d'apport de matériel (par exemple un équipement de communication et des véhicules), des informations, analyses et formations.

Un processus devra également être approuvé dans les cas où l'une ou l'autre organisation pense que son seuil de risque acceptable a été atteint. Si l'organisation dirigeante est inquiète au sujet des risques potentiels posés à son partenaire d'exécution mais ne peut lui offrir une aide pratique pour les atténuer, elle pourrait décider de ne pas demander à son partenaire d'entreprendre le travail.

1.5 Le pays d'accueil et la gestion de la sécurité

Un aspect de la gestion de la sécurité souvent oublié est le rôle du pays d'accueil. Théoriquement, les autorités de l'État sont responsables de la sécurité de leurs citoyens et de toutes autres personnes respectueuses de la loi de passage ou vivant sur leur territoire. Dans les contextes de guerre, cette protection est consacrée par les Conventions de Genève et par les principes du Droit international humanitaire (DIH). Les États ont le devoir de faire connaître le DIH, d'enseigner au personnel militaire et civil comment l'appliquer et comment gérer les personnes soupçonnées de violation. Un certain nombre d'autres conventions et cadres clés, essentiellement dirigés par les Nations Unies, cherchent à rendre compte de la situation de sécurité pour les travailleurs humanitaires et des responsabilités de l'État dans ce domaine.

Conventions, cadres et résolutions clés sur la sécurité du travailleur humanitaire

- Convention sur la sûreté des Nations Unies et du personnel associé (1994)
- Déclaration présidentielle du Conseil de sécurité sur la protection du personnel des Nations Unies dans les zones de conflit (2000)
- Sûreté et sécurité du personnel des Nations Unies - Rapport du Secrétaire général (octobre 2000)
- Résolution 1502 du Conseil de sécurité, qui condamne toute forme de violence à l'encontre des personnels qui participent aux opérations humanitaires et qui demande instamment aux États de veiller à ce que les crimes commis contre ces agents ne restent pas impunis (2003)
- Résolution 59/211 de l'Assemblée générale sur la sûreté et la sécurité du personnel humanitaire et la protection du personnel des Nations Unies (2004)
- Protocole facultatif 60/123 de l'Assemblée générale (2006)

La relation entre les organisations d'aide et l'État peut être délicate, en particulier lorsque l'État est un belligérant. Les organisations, en grande partie, ne souhaitent pas que l'État se charge directement de la protection des travailleurs humanitaires ; elles préfèrent faire la distinction entre la

fourniture d'une sécurité ambiante (l'environnement général de sécurité dans lequel ce travail humanitaire est effectué) et une sécurité immédiate (comme les escortes lors de déplacements et la protection de la propriété). Des mesures d'État surprotectrices envers les organisations humanitaires peuvent accroître l'insécurité car elles peuvent donner une impression de partialité et peuvent rendre la tâche plus difficile aux organisations qui tentent de répondre aux besoins avec impartialité, en faisant d'une présence policière ou militaire une condition de l'accès à l'aide. N'oubliez pas que les organisations d'aide ne sont pas obligées d'accepter la protection armée des autorités, peuvent penser que la police locale ne peut pas ou ne souhaite pas agir à l'encontre des bandes criminelles et pourraient hésiter à impliquer les autorités pour résoudre une situation de rapt ou de prise d'otages. D'autres aspects essentiels à connaître sont entre autres :

- L'analyse du contexte pourrait être ressentie comme étant une activité excessivement politique.
- Les évaluations de la sécurité et le suivi des menaces pourraient être ressentis comme une indication que les autorités ne peuvent pas maintenir l'ordre public. Ce qui est plus problématique c'est que ces évaluations pourraient être ressenties comme une activité de collecte de renseignements.
- Les forces du gouvernement engagées dans des opérations sur le champ de bataille pourraient créer des risques de sécurité pour les organisations d'aide.
- Les autorités pourraient interdire à une organisation d'aide de déployer un équipement de télécommunications, en particulier des radios, que l'organisation considère comme essentiel pour sa gestion de la sécurité.
- Des forces du gouvernement mal équipées et mal payées pourraient être indignées par la richesse relative des organisations d'aide et tenter de réquisitionner ou de piller leurs biens.
- La décision d'évacuer le personnel, en particulier le personnel international, a des connotations politiques et pourrait inquiéter les autorités.

Partie 2
Approches stratégiques et opérationnelles de la gestion de la sécurité

Chapitre 2
Évaluation des risques

Une évaluation des risques est une composante essentielle d'une bonne gestion de la sécurité, et un domaine dans lequel les organisations humanitaires ont fait d'énormes progrès au cours des dernières années. Le raisonnement actuel sur les bonnes pratiques soutient que les organisations doivent effectuer une évaluation des risques de sécurité (ERS) avant de démarrer des opérations dans un nouveau lieu, et que cette évaluation devra guider la conception du programme dès le début. L'objectif de l'exercice est de pouvoir déterminer le niveau de risque associé au lancement d'un programme et d'évaluer ce risque par rapport aux bénéfices que la population tirera de ce programme. Une ERS n'est pas un document à remplir et à ranger sur une étagère, mais plutôt un document que l'on doit considérer comme vivant, consulter fréquemment et réviser au fur et à mesure des évolutions de la situation. L'ERS et l'analyse risques-avantages qui en découlera, changeront donc avec toute évolution majeure dans le contexte opérationnel (politique, économique, démographique), lorsque les programmes commenceront, finiront ou s'élargiront à d'autres régions, ou encore avant des événements spéciaux.

Ce chapitre fournit des recommandations sur l'évaluation des risques, basées sur les récentes pratiques du secteur. Il s'appuie sur un certain nombre de modèles actuellement utilisés, en particulier l'ERS des Nations Unies qui a été adoptée (et adaptée) par les grandes ONG opérationnelles.

2.1 L'importance d'une évaluation des risques systématique

L'évaluation des risques doit être effectuée de manière structurée et disciplinée car, en tant qu'êtres humains, nous sommes généralement enclins à être subjectifs. Cette subjectivité peut créer une image déformée et refléter notre partialité inconsciente. Une étude de psychologie a révélé que les êtres humains :

- Exagèrent les risques spectaculaires mais rares, et minimisent les risques plus fréquents et plus courants.
- Réagissent intensément aux menaces immédiates mais réagissent mollement face aux menaces à long terme.
- Réagissent rapidement aux changements soudains et spectaculaires, mais s'adaptent lentement aux changements qui surviennent peu à peu, au fil du temps (syndrome de la grenouille).
- Ont du mal à estimer le risque dans des situations et des expériences inhabituelles.

- Surestiment les risques dont on parle continuellement et sous-estiment les risques qui sont si courants qu'ils n'attirent quasiment pas l'attention (par exemple les accidents de voiture).
- Sous-estiment les risques qu'ils sont prêts à prendre et surestiment les risques dans des situations dont ils n'ont pas le contrôle.
- Surestiment les risques qui se présentent à leur propre communauté et sous-estiment les risques qui affectent les autres.

Ce guide a pour objectif d'aider les travailleurs sur le terrain à gérer les risques. La gestion des risques débute par une tentative d'évaluation disciplinée et bien argumentée. L'intuition n'est pas suffisante. Par ailleurs, la gestion des risques ne doit pas se raréfier et devenir le domaine exclusif et spécialisé du cadre qui en a la charge. Cette personne devra s'assurer que le système est inclusif et qu'il suscite les perspectives et informations de tout le personnel afin de créer une compréhension commune du risque et un sentiment de responsabilité commune pour prendre les mesures de sécurité nécessaires.

2.2 Définitions essentielles

2.2.1 Comprendre le concept du risque

Le risque est une mesure de vulnérabilité aux menaces qui existent dans un contexte. En d'autres termes, le risque est le potentiel d'une atteinte : la probabilité que quelque chose de néfaste se produise et l'étendue de cette atteinte si cela se produisait. Les concepts fondamentaux sont ici « la menace », « la vulnérabilité », « le risque » et « l'atténuation/la réduction du risque ». Dans le contexte de la gestion de la sécurité, une menace est tout ce qui peut porter atteinte ou causer une perte, alors que la *vulnérabilité* fait référence à la *probabilité* de se trouver face à une menace et aux *conséquences* ou à l'impact si cela se produit, quand cela se produira. La combinaison de la menace et de la vulnérabilité à cette menace constitue le *risque*.

Les mesures *d'atténuation des risques* ou de *réduction des risques* sont des actions qui visent à réduire les risques. Il existe essentiellement trois façons de procéder, et aucune n'est parfaite :

- Éliminer ou diminuer la menace même.
- Réduire l'exposition à la menace.
- Prendre des mesures pour faire en sorte que l'impact soit limité lorsque l'on fait face à la menace.

Identifier les menaces qui peuvent se présenter, et la vulnérabilité à ces menaces, nécessite une évaluation complète du contexte dans lequel l'organisation

opère et de ce qu'elle peut accomplir dans ce contexte. Les sections qui suivent portent sur les composantes de base de ce processus analytique :

- Analyse contextuelle, comme cadre général et essentiel pour comprendre les menaces potentielles.
- Analyse du programme, pour clarifier les objectifs prioritaires de l'organisation dans ce lieu et déterminer ses capacités.
- Analyse des menaces, pour identifier et comprendre celles qui pourraient porter atteinte à l'organisation ou à ses programmes.
- Analyse de la vulnérabilité, pour comprendre l'exposition de l'organisation aux menaces, ses points de faiblesse et de quelles façons l'organisation pourrait être affectée.

Toutes ces informations sont utilisées pour produire une analyse du risque, conçue pour permettre à l'organisation de déterminer si le niveau de risque dans un environnement donné est acceptable. Le processus d'évaluation décrit dans ce chapitre aboutit à une grille qui trace la courbe des risques en fonction de leur probabilité et de leur impact ; un exemple est donné ci-dessous.

Tableau 2: d'Analyse du risque

		Impact				
		Negligeable	Mineur	Moyen	Grave	Trés grave
Probabilité	Très probable	Faible	Moyen	Élevé	Très élevé	Très élevé
	Probable	Faible	Moyen	Élevé	Élevé	Très élevé
	Moyennement probable	Très faible	Faible	Moyen	Élevé	Élevé
	Peu probable	Très faible	Faible	Faible	Moyen	Moyen
	Très peu probable	Très faible	Très faible	Très faible	Faible	Faible

Source : InterAction, Security Risk Management : NGO Approach (Gestion de la sécurité des risques : Approche ONG) 2010

Les modèles d'évaluation des risques varient d'une organisation à l'autre en complexité et niveau de détail. Il n'existe pas de modèle universel. Cette section vise à expliquer les éléments de base et à présenter les outils jugés utiles par les responsables de la sécurité et le personnel sur le terrain des organisations humanitaires. Le modèle d'évaluation des risques qui convient à votre organisation est celui qui, selon vous, sera à la fois compris et systématiquement utilisé par votre personnel sur le terrain et qui ajoutera de la valeur au processus de gestion de la sécurité.

2.3 Analyse du contexte : connaissez votre lieu d'action

Une bonne gestion de la sécurité, tout comme une bonne programmation, exige de bien comprendre l'environnement local et le rôle, à la fois réel et perçu, que les organisations d'aide y jouent. Idéalement, l'organisation tentera d'obtenir, à des fins de programmation, des connaissances contextuelles profondes pour chaque situation, mais si ce n'est pas le cas, la gestion de la sécurité peut être l'élément moteur légitime pour le faire. Cette compréhension peut grandement contribuer à la capacité d'une organisation d'anticiper les menaces.

Développer et entretenir des connaissances détaillées du contexte a des conséquences pratiques. Par exemple, cela signifie investir le temps nécessaire au personnel pour l'analyse initiale et le suivi régulier, et inclure ces connaissances dans les présentations données aux nouveaux arrivants et aux successeurs. Le manque de temps lors d'une urgence extrême et le renouvellement constant du personnel sont des obstacles à surmonter, et en aucun cas des excuses. Dans la pratique, le développement de connaissances contextuelles est un processus continu et itératif, mais il est présenté en étapes dans ce chapitre. (Notez que la plupart des modèles d'évaluation des risques opérationnels omettent l'acquisition de connaissances contextuelles profondes suggérée ici et commencent par la seconde étape : évaluation/analyse du programme. Cependant, elle est incluse ici comme exemple de bonne pratique, bien qu'elle ne soit sans doute réalisable que dans une période prolongée, dans une situation donnée.)

Investir dans une bonne analyse du contexte ne signifie pas « se politiser » ou compromettre le principe de neutralité qui sous-tend l'entreprise humanitaire. La question fondamentale n'est pas la « neutralité » autoproclamée d'une organisation mais comment ses actions et ses paroles sont perçues par les acteurs qui ont de l'importance. Si les organisations veulent être considérées comme neutres, elles doivent faire preuve de bon sens et comprendre les intérêts, inquiétudes et perceptions des nombreux acteurs dans leur environnement opérationnel – et gérer leur propre position et leur propre image de manière active et constante.

2.3.1 Analyse du contexte général

L'analyse du contexte général débute avec des connaissances de base sur les origines de l'État moderne et son histoire, y compris son héritage colonial, le cas échéant ; ses relations avec ses voisins principaux et avec les grandes puissances étatiques ; et la situation politique nationale globale, notamment la nature du gouvernement, la situation relative aux partis politiques, la conduite des élections et la façon dont la population moyenne interagit avec le gouvernement et en ressent la présence dans sa vie. D'autres questions à prendre en considération sont :

- Tous problèmes sociaux entre groupes ou régions en matière de ressources, de territoire ou de contrôle gouvernemental, ou toutes plaintes relatives à la discrimination ou l'exclusion.
- Les groupes d'identité (fondée sur la religion, l'appartenance à une caste, classe ou ethnie, par exemple) et comment l'idéologie, les idées reçues et les symboles ont été utilisés pour mobiliser ces groupes.
- La religion et l'idéologie sociale et politique : croyances, symboles et domaines principaux de sensibilité et de respect.
- Les structures sociales traditionnelles utilisées pour gérer le conflit et veiller au respect des normes ; fonctionnent-elles toujours ou ont-elles une influence ?
- Les normes et codes sociaux qui gouvernent le comportement public, l'habillement et l'interaction entre les hommes et les femmes.

2.3.2 Analyse détaillée du conflit et de la violence

Après avoir obtenu une vue d'ensemble, une analyse plus détaillée du conflit et de la violence permettra de faire la lumière sur les motivations et les sources de menace. Ceci dit, l'origine d'un conflit peut souvent paraître déconcertante à des étrangers, et quoi qu'il en soit, comprendre comment un conflit a commencé n'explique pas toujours pleinement ce qui se produit aujourd'hui. L'analyse du conflit doit aussi identifier d'autres problèmes plus immédiats. Ainsi, la cause première du problème palestinien dans les territoires occupés n'explique pas ce qui a provoqué la violente confrontation entre Hamas et Fatah ces dernières

Analyser la violence en Algérie

Les organisations humanitaires qui interviennent suite à une inondation ou un tremblement de terre en Algérie, ou qui ont un bureau dans ce pays, ont tout intérêt à comprendre la nature complexe de la violence sociale et politique. L'un des épisodes cruciaux en Algérie est bien sûr la violente guerre civile (1991-2002) entre l'État soutenu par l'occident et les insurgés islamistes. Ceci faisait suite à la victoire islamiste aux élections locales de 1990. Le conflit, qui a causé la mort d'un grand nombre d'Algériens, a également frappé des cibles occidentales. Pourtant la violence politique en Algérie contient d'autres chapitres importants, entre autres la guerre brutale entre les Français et le mouvement pour l'indépendance de l'Algérie ainsi que le traitement des « collaborateurs » aux mains de l'État algérien après l'obtention de l'indépendance. Un autre aspect a trait à la récente apparition en Algérie d'une aile d'Al-Qaida au Maghreb Islamique, qui résulte de la guerre civile algérienne mais qui a aussi des liens avec les réseaux islamistes radicaux mondiaux. Al-Qaida a revendiqué le bombardement du bureau des Nations Unies à Alger en décembre 2007.

années. Parfois, de multiples conflits sont intimement liés. Les tensions et les flambées de violence dans une ville comme Karachi au Pakistan peuvent éveiller la dynamique des relations chiites-sunnites, les tensions entre les citadins autochtones et « immigrants » (c'est-à-dire ceux qui sont arrivés pendant la partition), le commerce des armes et de la drogue, l'arène politique nationale pakistanaise ou l'Islam radical. L'un ou l'autre ou l'ensemble de ces sujets peut être source de menaces. Une bonne analyse du conflit ne porte pas uniquement sur les endroits où la violence est visible. La violence est précédée de tensions qui peuvent être moins visibles : les « divisions profondes » et les « lignes de faille » dans une société. Ces aspects doivent également être explorés et compris.

Comprendre la nature et la structure de la violence permet d'anticiper où elle pourrait éclater et avec quelle intensité. Cela permet également d'évaluer la probabilité que les acteurs humanitaires puissent en être affectés. Il ne s'agit cependant pas d'une science exacte. Dans les contextes « traditionnels » de conflit, où les lignes de front sont bien définies, comme entre l'Éthiopie et l'Érythrée, en Angola ou dans les Balkans, il est plus facile d'anticiper les menaces que lors d'un conflit type guérilla. Cela même si le risque d'une embuscade, d'un raid éclair, d'une mine placée sur une route ou d'un massacre de civils, existe dans les deux cas. Il est cependant sans doute plus aisé de juger et d'anticiper dans le premier cas que dans le second. Il s'agit de se poser les questions qui permettront de mieux appréhender un contexte particulier et d'aller au-delà d'une impression généralisée de la violence qui est souvent partout la même.

Une question clé est de savoir si la violence est aléatoire et décentralisée ou au contraire organisée et ciblée. Qui est ciblé et pourquoi ? La violence est-elle généralement perpétrée par des groupes armés organisés, des individus, de petits groupes ou des bandes ? Est-elle motivée par une volonté de gain politique ou criminel/économique ou les deux ? L'intensité de la violence a-t-elle augmenté ou cause-t-elle un plus grand nombre de morts ? Les raids (contre des habitations et des bureaux) et le banditisme sur les routes sont deux types différents de menace et peuvent tous deux comporter des niveaux de violence variables, allant de peu ou pas de violence, jusqu'au meurtre. Au Darfour, un grand nombre d'organisations humanitaires ont remarqué une augmentation de la sévérité de la violence à l'encontre des chauffeurs, orchestrée par des bandits, pendant le déroulement du conflit, alors qu'auparavant, la majorité des incidents ne gêneraient pas de blessés.

Dans les Balkans, le viol a été utilisé comme une arme dans les actes d'épuration ethnique afin de démoraliser l'adversaire. En général, le personnel international était moins à risque que le personnel local. En revanche, en Sierra Leone le viol était largement répandu, moins comme tactique de guerre que pour subjuguer et terroriser les communautés civiles et pour brutaliser les (enfants) soldats qui le

commettaient. Dans un tel contexte, le personnel international sera tout autant à risque que le personnel national, surtout si l'opinion politique internationale (occidentale) est peu prise en compte. Bien que peu de cas figurent au nombre des incidents signalés, les violentes attaques sexuelles contre les travailleurs humanitaires dans l'est de la RDC et au Darfour indiquaient l'intention de cibler/terroriser la communauté de l'aide internationale.

La violence n'est pas toujours liée au conflit. Par exemple, bien que le conflit au Guatemala ne soit plus actif, le taux d'homicide y est plus élevé que durant la guerre civile, et la violence, majoritairement liée au crime, y est très répandue. Étudiez les tendances générales de criminalité dans le contexte et déterminez quelles sont les principales menaces criminelles (rapt, viol, vol à main armée, détournement de voiture). À certains endroits, la violence peut présenter un élément de saisonnalité. Au Tchad, par exemple, les principales attaques ne sont généralement pas lancées pendant la saison des pluies. Paradoxalement, la période juste après la fin d'un conflit peut être particulièrement difficile à gérer car un certain nombre d'anciens combattants pourraient se retrouver sans source de revenu.

2.3.3 Analyse des acteurs

L'analyse des acteurs porte essentiellement sur les principaux acteurs/groupes pouvant potentiellement avoir un impact sur la sécurité. Elle peut être effectuée en deux étapes : tout d'abord, faites une liste de tous les acteurs pertinents, puis envisagez leurs relations mutuelles. Il s'agit d'un exercice d'exploration, qui devra être effectué de manière continue et qui soulèvera sans doute initialement plus de questions qu'il n'apportera de réponses. Les acteurs concernés comprendront les divers groupes armés impliqués dans le combat ainsi que les participants nationaux et internationaux s'efforçant officiellement d'atténuer le conflit et de jouer un rôle de médiateur. Dressez la liste des objectifs déclarés (s'ils sont connus) de chacun de ces acteurs. Les acteurs nationaux ou locaux pourraient également inclure la classe moyenne urbaine, les groupes d'étudiants radicaux, les syndicats, les grands propriétaires terriens, les militants religieux ou les radicaux nationalistes, les médias locaux, les ONG locales ou les dirigeants traditionnels. Des acteurs régionaux et internationaux potentiellement pertinents pourraient être les puissances voisines, les organisations intergouvernementales, les corporations transnationales, les diplomates et les organisations humanitaires et celles qui luttent pour les droits de l'homme, ainsi que les diasporas.

Des lignes peuvent être tracées entre les différents acteurs de manière à illustrer les interactions. Ces lignes représentent les différents types de relations, en indiquant par exemple, qui les finance, quels groupes sont hostiles les uns envers les autres et qui se dispute le territoire dans une région

particulière. Encore une fois, bien que les réponses soient susceptibles de ne pas être connues, la première étape est de poser des questions pertinentes. Ne soyez pas surpris si les interprétations de ces relations varient selon les personnes. Les relations sont complexes et différentes dimensions seront mises en évidence à divers moments.

Au fur et à mesure que l'analyse s'approfondira, vous pourrez vous apercevoir que les groupes alliés, ou que les acteurs individuels, ne sont pas aussi monolithiques ou homogènes qu'ils le paraissaient. Des factions et des luttes de pouvoir pourraient exister au sein du gouvernement ou d'un mouvement de résistance ; les opinions et perspectives pourraient varier selon les différentes organisations des Nations Unies et ONG ; des acteurs politiques internationaux pourraient jouer des coudes pour prendre la direction de la gestion du conflit. Plus l'on aura de renseignements sur la position d'une organisation ou d'une personne dans ce qui semble être un groupe d'intérêt commun, plus la relation qui pourra être entretenue sera nuancée. Cet exercice constituera également un outil pratique pour informer les nouveaux venus et les successeurs sur le contexte d'opération.

2.3.4 Comprendre les groupes armés

Comprendre les groupes armés est une tâche difficile et très délicate. Il est également crucial de comprendre comment et pourquoi votre présence et vos programmes pourraient être manipulés ou menacés. De nouveau, des éclaircissements pourraient n'apparaître que progressivement. Penchez-vous sur :

- L'idéologie d'un mouvement/d'une organisation. Comprendre un peu la vision du monde qu'ont les acteurs clés du conflit sera utile dans les discussions et les négociations, et peut-être aussi dans la lecture et l'interprétation des déclarations et des communications publiques pouvant inclure un « avertissement » implicite à l'organisation et à ses activités. Quelles raisons et justification avancent-ils pour leur lutte et comment les organisations d'aide et les acteurs politiques internationaux sont-ils dépeints dans cette perspective ? Quels symboles et quelles idées reçues utilisent-ils ?
- L'organisation et la chaine de commandement et de contrôle. Essayez de déterminer comment un certain groupe est organisé : s'il y a une hiérarchie claire, qui sont les dirigeants et si la prise de décisions est centralisée. Avec quelles personnes est-il souhaitable de négocier et quels résultats pratiques peut-on escompter d'un accord formel avec ces personnes ?
- Le « contrat social » entre un groupe armé et la population civile. Plus les groupes armés maltraitent les civils qui se trouvent sous leur contrôle, plus la tâche de l'organisation qui apporte de l'aide sera difficile et dangereuse.

Enfin, si la présence et les programmes d'une organisation humanitaire sont ressentis comme menaçant ou affaiblissant le contrôle qu'un groupe armé exerce sur la population civile, celui-ci pourrait tenter d'intimider l'organisation ou user de représailles envers elle.

2.3.5 La base de ressources et l'économie de guerre

La présence d'une organisation dans un endroit pourrait générer de potentielles ressources pour un groupe armé ou pourrait les menacer. En plus des armes et munitions, pour poursuivre leurs objectifs les groupes armés ont besoin de nourriture, de médicaments, de moyens de transport et d'autres matériels, ainsi que d'argent. Un grand nombre de conflits modernes ont été financés et entretenus par des « économies de guerre », notamment par le commerce illégal et quasi légal des armes, de la drogue, des diamants, du pétrole, des minéraux et autres produits. Des groupes armés pourraient menacer des organisations d'aide pour s'emparer de leurs biens, ou encore menacer des bénéficiaires et/ou les communautés locales pour s'emparer de leurs ressources. Lorsqu'il existe peu d'autres ressources, les organisations d'aide jouent un plus grand rôle dans l'économie de guerre et sont ainsi plus vulnérables. Dans certaines circonstances, ces organisations pourraient être considérées comme gênantes ou comme témoins indésirables. C'est notamment le cas si elles ont une présence ou des activités dans une zone sensible où les ressources naturelles sont exploitées et soutiennent l'économie de guerre, ou si elles longent des voies d'export/import. Les programmes d'aide humanitaire pourraient également compliquer l'action de recrutement de manière directe ou indirecte. Par exemple en introduisant des programmes générateurs de revenus pour les anciens combattants (action directe), ou en soutenant la réhabilitation scolaire et la reconstruction agricole et en offrant ainsi d'autres moyens d'existence aux jeunes hommes (action indirecte) .

2.3.6 L'histoire des interventions d'aide humanitaire dans le pays

Beaucoup de pays connaissent une longue histoire de présence des travailleurs humanitaires internationaux sur leur sol. Les Afghans connaissent sans doute la violence et la guerre depuis 30 ans et beaucoup bénéficient de l'aide internationale depuis au moins 25 ans. Et ceci aussi bien en Afghanistan que dans les camps de réfugiés au Pakistan et en Iran. La population haïtienne a été témoin d'interventions internationales répétées pour stabiliser le pays et le remettre politiquement et économiquement sur la bonne voie. Pourtant, beaucoup d'Afghans et d'Haïtiens se plaignent d'être plus pauvres que jamais. Beaucoup de populations reconnaissent que, à un moment ou un autre, elles ont reçu des avantages tangibles mais elles sont sceptiques, sinon cyniques, quant à l'efficacité de l'aide à long terme et aux motifs des organisations qui ont distribué de l'aide. De plus, les élites politiques locales pourraient être indignées de la prédominance d'une « communauté

internationale » qui proclame un attachement de pure forme à l'adhésion et aux priorités nationales mais qui peut aussi parfois être ressentie plutôt comme un pouvoir colonial. L'histoire de l'aide humanitaire et la façon dont elle a été ressentie historiquement par les bénéficiaires et les communautés hôtes est donc une autre considération importante. Il en va de même des façons d'opérer des organisations dans le pays ou la région en question. Certaines organisations opèrent dans les mêmes lieux depuis des décennies, et cet historique sera donc vital pour comprendre le contexte et pour analyser le programme. Ce thème est abordé dans la section qui suit.

2.4 L'analyse du programme : sachez qui vous êtes et ce que vous voulez réaliser

Une appréciation générale des risques de sécurité doit figurer dans la décision de démarrer ou de continuer un travail programmatique dans un contexte donné. Les considérations cruciales suivantes sont la mission et le mandat, les priorités spécifiques de programmation et la capacité de gérer les risques de sécurité. Les sous-sections qui suivent couvrent les composants essentiels de l'analyse de programme : pourquoi, où et quoi analyser.

2.4.1 Mission et mandat

La distinction entre « mandat » et « mission » prête un peu à confusion. Les organisations non gouvernementales se sont généralement attribué elles-mêmes un objectif qui reflète les valeurs sous-jacentes de l'organisation et sa raison d'être. Nous pouvons les appeler « la mission de l'organisation », souvent reflétée dans un « énoncé de la mission ». Un mandat diffère d'une mission en ce sens qu'il est attribué par quelqu'un d'autre. Les entités multilatérales telles que les Nations Unies ou l'Organisation pour la Sécurité et la Coopération en Europe (OSCE) ont un mandat qui leur a été attribué par les États membres. Ce mandat peut être très spécifique : le HCNUR, par exemple, a pour mandat de travailler pour les réfugiés et le Haut commissariat aux droits de l'homme (HCDH) a pour mandat de travailler pour les droits de l'homme. Clarifier cette distinction n'est pas simplement un divertissement : si une organisation a un mandat, on s'attend beaucoup plus à ce qu'elle soit présente à un certain endroit/moment ; pour les organisations dont la mission est auto-attribuée, le choix de rester en dehors d'une situation difficile et dangereuse leur appartient plus. Le HCNUR doit être présent dans les lieux où il y a une forte population de réfugiés ; le HCDH doit porter son attention sur les endroits où il existe de fortes violations des droits de l'homme ; l'UNICEF doit jouer un rôle dans les contextes où il y a un nombre important d'enfants dans le besoin.

La façon dont les organisations comprennent leur mandat ou leur mission organisationnelle a une influence sur leur tolérance générale du risque.

Lorsque la situation dans une région s'enflamme, certains acteurs pourront y affluer : le CICR, MSF, le HCNUR, les journalistes et les défenseurs des droits de l'homme par exemple. D'autres, qui ont essentiellement un objectif de développement et qui travaillent par le biais de structures gouvernementales, pourront suspendre leurs opérations ou se retirer. Quelques agences des Nations Unies et une grande partie des grandes ONG effectuent une programmation de l'aide dans des contextes de problèmes humanitaires et de développement. Ces organisations changeront généralement leurs modes de programmation lorsqu'une urgence surviendra ou que l'instabilité grandira. Ceci nécessite souvent des modifications dans les opérations et dans les profils de recrutement pour disposer des compétences appropriées. Les missions et les mandats peuvent aussi créer des vulnérabilités.

Le terme « mission » est également utilisé dans un sens plus précis pour décrire ce que les organisations souhaitent accomplir dans un contexte particulier. Nous pouvons appeler cela « la mission sur le terrain ». Cette mission fournit également des critères d'action : si sa mission est de fournir des services de santé d'urgence dans une zone de conflit ou une formation professionnelle dans une zone instable, une organisation pourra décider de suspendre ses opérations ou de se retirer lorsque les circonstances deviennent telles qu'elle ne peut plus remplir sa mission : des quantités trop importantes de médicaments et d'équipements médicaux sont pillées, ou bien la situation s'est détériorée au point que les emplois pour lesquels l'organisation fournit une formation ne sont plus disponibles.

2.4.2 Objectifs

Du point de vue de la sécurité, une organisation pourrait avoir ou pas l'option de demander si elle doit partir ou rester dans une zone dangereuse. Choisir d'être présente dans une zone dangereuse implique, pour l'organisation, de demander si les risques encourus ont un lien avec ce que l'organisation souhaite accomplir. Qui part et qui reste et où les ressources existantes doivent être affectées doit être décidé en fonction de l'urgence et de la gravité des besoins humanitaires. Cela doit être mis en balance avec le devoir de diligence d'assurer la sécurité du personnel. Si la mission prévue ne sauve pas de vies ou ne cherche pas à remédier à de grandes souffrances, il est raisonnable de bien réfléchir si cela vaut la peine de continuer à opérer dans des conditions de danger extrême. Il est nécessaire de déterminer si les programmes sont cruciaux sur le plan de l'aide fournie. Le programme sauve-t-il réellement des vies ou favorise-t-il le bien-être ? Quelles seraient, pour les bénéficiaires directs, les conséquences de le suspendre ? Quelles seraient les conséquences pour d'autres organisations (p. ex. d'autres ONG, les installations de santé locales) qui dépendent de ce programme? Ces questions sont également pertinentes en ce qui concerne la décision

d'entrer dans un pays, d'y retourner après une évacuation ou d'élargir un programme géographiquement (et thématiquement) à l'intérieur d'un pays.

2.4.3 Lieu

Où les programmes seront-ils effectués ? Il est essentiel de bien préciser le rayon géographique de la présence opérationnelle. Regroupez les activités en fonction de leur lieu géographique et assurez-vous de prendre en considération toutes les installations soutenues ou visitées par le personnel ainsi que les habitations et routes utilisées. De plus, il est important de noter quelles autres organisations d'aide (combien et le nombre approximatif de personnel) et quels autres acteurs internationaux et nationaux sont présents et actifs dans le même environnement, et quels types de programmes ils mettent en place à cet endroit.

2.4.4 Capacités

Un ensemble fondamental de capacités est nécessaire pour la gestion des risques de sécurité, notamment : ressources financières, compétences clés, personnel et temps de gestion.

- *Ressources financières*. La gestion des risques de sécurité n'est pas sans frais. Les coûts financiers associés à une gestion performante de la sécurité devront être correctement évalués et figurer au budget. De plus, les personnes chargées de la planification devront être sûres qu'elles pourront mobiliser les fonds nécessaires au moment voulu.
- *Compétences*. Bien qu'il soit possible d'obtenir des compétences spécifiques en recrutant des consultants externes, il est important, en matière de gestion de la sécurité, de développer des compétences fondamentales à l'intérieur de l'organisation. Il faut faire une distinction entre sensibilisation et connaissances d'une part et compétences réelles, basées sur l'expérience d'autre part. Confier des responsabilités de gestion à quelqu'un qui a bénéficié d'une sensibilisation mais qui a des connaissances limitées et qui n'a aucune expérience pratique est malavisé dans un environnement à hauts risques. Avoir une faible proportion de personnel expérimenté par rapport au personnel inexpérimenté dans un contexte dangereux est tout aussi irréfléchi et révèle vraiment la nécessité d'apporter une attention au développement du personnel.
- *Personnel et temps de gestion*. La disponibilité des fonds et du personnel ne signifiera pas grand-chose si les personnes ne consacrent pas du temps à la gestion des risques de sécurité. Ceci est une responsabilité essentielle qui doit figurer dans leur description de poste. Externaliser la planification de la sécurité n'est pas un substitut pour prendre le temps de développer et de maintenir une stratégie et des plans de sécurité efficaces.

2.4.5 Rester – ou partir ?

Les considérations mentionnées plus haut peuvent être résumées dans une simple liste de questions :

- Le « mandat » ou la « mission » de l'organisation permet-il de penser qu'elle doit opérer dans ce contexte ?
- Avec une présence et des opérations, les programmes satisferont-ils des besoins humains cruciaux ?
- S'il est nécessaire et approprié que l'organisation soit présente à cet endroit, a-t-elle les capacités (financières et compétences) de gérer les risques de sécurité ?
- Si ce n'est pas le cas, peut-elle les développer ou les obtenir de l'extérieur en temps voulu ?
- Une fois les ressources financières et humaines en place, peut-on consacrer suffisamment de personnel et de temps pour gérer les risques.

Si la réponse à au moins une question sur la liste est « non », réfléchissez sérieusement avant de décider de lancer l'opération, en tout cas jusqu'à ce que la situation s'améliore ou que des capacités suffisantes (argent, personnes compétentes et temps) soient disponibles pour gérer les risques. Outre la présence physique d'un programme, il existe d'autres options valables, entre autres aiguiller le financement disponible ou d'autres ressources vers des organisations mieux placées pour opérer en sécurité dans le contexte en question.

2.4.6 Les éléments moteurs de la prise de décisions

Tous les points mentionnés plus haut pourraient paraître évidents, pourtant beaucoup d'organisations démarrent des programmes dans des contextes à hauts risques sans les fonds ni les compétences nécessaires (dans les lieux où le besoin humanitaire est important, les organisations sont susceptibles d'avoir une plus grande tolérance vis-à-vis des risques). Il y a aussi les organisations qui ont les fonds et les compétences internes mais d'autres priorités les éloignent constamment de la gestion des risques de sécurité. En réalité, il y a d'autres considérations qui, à tort ou à raison, peuvent primer dans une situation où les risques de sécurité sont élevés et où les capacités de gestion des risques sont faibles. Mais l'opportunité financière est un autre facteur fréquent et influent dans la prise de décision. Les organisations sont présentes dans un endroit parce qu'il existe un besoin mais aussi parce que des fonds sont disponibles. Ignorer les risques parce qu'il y a une opportunité financière pourrait être justifié sur le plan de la survie et de la croissance de l'organisation, mais est-ce responsable envers son personnel et ses collègues, surtout si les besoins ne sont pas majeurs ? Une évaluation objective des motifs d'une organisation demanderait d'ajouter une dernière question à la liste de contrôle donnée plus haut :

Tableau 3: Grille d'analyse de programme

Description du programme	Lieu	Activité	Cadre temporel	Impact positif	Impact négatif
	• Où travaillons-nous ? • Quelles menaces sont présentes ou pourraient apparaître ? • Espace humanitaire : en diminution ou stable ?	• Indispensable ? • Pertinente ? • Urgente ? • Besoins • Méthode d'exécution	• Opérations actuelles et futures • Depuis combien de temps sommes-nous présents ?	• Renforce la crédibilité et l'acceptation ? • Réduit le risque en stabilisant la communauté ? • Répond aux besoins de la communauté ?	• Ressenti comme ne bénéficiant qu'à certaines parties de la communauté ? • Exige que le personnel se déplace dans des zones à hauts risques ? • Sources de financement

Source : World Vision International. (Note : cette grille est utilisée avec l'autorisation de World Vision International et toute reproduction autre que cette publication (RBP) doit faire l'objet d'une autorisation expresse de World Vision International.)

- L'organisation est-elle excessivement influencée par la pression des bailleurs de fonds ou par des incitations financières pour opérer dans le contexte en question ?

Il pourrait être utile, pour cet exercice, d'utiliser une grille d'analyse de programme, comme celle donnée en exemple ici, utilisée par l'ONG World Vision International.

2.5 Évaluation des menaces

Nous avons jusqu'à présent examiné le contexte opérationnel – le cadre général, la nature et le niveau de la violence ainsi que les acteurs entrant en ligne de compte – et nous avons clarifié la mission et les objectifs prioritaires dans ce contexte ainsi que les capacités à gérer la sécurité. La prochaine étape est de se pencher spécifiquement sur les menaces auxquelles l'organisation et ses programmes sont susceptibles de faire face, et sur leurs vulnérabilités. Par menaces on entend les facteurs et événements *externes* pouvant porter atteinte, tandis que les vulnérabilités sont plutôt *internes*, et peuvent résulter de la façon dont une organisation est perçue, de son mode d'opération, des personnes qu'elle embauche et de ses procédures et installations.

Les menaces peuvent être divisées en deux grandes catégories : générales et spécifiques. Une analyse contextuelle donne une idée des menaces générales, telles que le crime, les attaques terroristes et les activités de combat ou militaires. Outre celles-ci, il pourrait y avoir des menaces spécifiques. Des scénarios de menaces spécifiques sont donnés en exemple ci-dessous.

- Crime
  - Détournement de voiture
  - Banditisme sur la route
  - Vols/agressions dans la rue
  - Vols/raids à main armée
  - Rapt
- Attaque terroriste
  - Engins explosifs improvisés (EEI) au bord de la route
  - Bombes dans une voiture/un camion
  - Kamikazes dans des véhicules
  - Bombardements ou fusillades dans des lieux publics
  - Attaque à la grenade dans une enceinte
  - Prise d'otages
- Activités de combat/militaires
  - Bombardements
  - Feux croisés d'infanterie
  - Mines antipersonnel

Certaines menaces peuvent être dirigées contre une organisation spécifique (ou contre les organisations humanitaires en général) et certaines peuvent être indirectes ; le personnel peut ne pas être directement ciblé lors d'une attaque envers une installation gouvernementale ou un bureau des Nations Unies, mais il peut être blessé s'il est présent lorsque l'attaque a lieu. Au moment d'évaluer une menace potentielle émanant d'une source humaine (adversaire), déterminez si la menace a les trois caractéristiques suivantes :

- Historique – un incident ou un type d'attaques envers des organisations similaires dans le passé.
- Intention – des menaces spécifiques, une intention ou une mentalité à attaquer démontrée.
- Capacité – les moyens nécessaires pour perpétrer une attaque.

2.5.1 Sources d'informations et analyse

Une évaluation des menaces dépendra dans tous les cas des informations sur lesquelles elle est basée. Ces informations pourront provenir de diverses sources, qui ne seront pas nécessairement toutes fiables.

Établir la tendance et faire l'analyse des incidents à partir d'une surveillance approfondie des incidents de sécurité (de votre organisation ou d'autres organisations) dans le lieu en question peut jouer un rôle vital pour identifier les menaces et déterminer les tendances de la violence et la probabilité d'une attaque (voir chapitre 5). Une autre source est celle des structures de coordination de la sécurité des Nations Unies et des ONG : les bureaux

nationaux des NU, les agents sur le terrain du Département de la Sûreté et de la Sécurité des Nations Unies (DSS) et les consortiums de sécurité pour les ONG sur le terrain, lorsqu'ils existent, ainsi que les soldats de la paix. Les bureaux locaux des organisations des droits de l'homme pourraient aussi surveiller les incidents mettant en jeu les travailleurs humanitaires.

Les représentants locaux et les autorités locales doivent être consultés. Ces personnes sont, entre autres : les représentants gouvernementaux, le chef de police local, le personnel de l'ambassade, les commandants de l'armée de terre, les commandants des groupes armés et les dirigeants/anciens des villages. Certaines de ces sources pourraient être bien informées et désireuses de partager ce qu'elles savent, tandis que d'autres pourraient être mal informées ou pourraient donner intentionnellement une image faussée de la situation. C'est également une opportunité d'informer d'autres personnes sur votre organisation, ses objectifs et ses rôles.

L'intelligentsia locale – les universitaires, journalistes, enseignants, missionnaires, activistes sociaux, dirigeants religieux, activistes politiques – est en général plus souvent consultée par les organisations luttant pour les droits de l'homme et visant à résoudre les conflits que par les organisations humanitaires. Cette Intelligentsia peut avoir des choses intéressantes et utiles à dire. Certaines de ces personnes pourraient se trouver parmi le personnel de l'organisation. De même, certaines seront mieux informées et feront une analyse plus perspicace et plus objective que d'autres, et en connaitront probablement plus sur le contexte, de façon plus large, que sur les risques précis de sécurité. Dans certains endroits, les réseaux locaux, comme les chauffeurs de taxi, les commerçants, les négociants, les banques et les sociétés d'assurance pourraient surveiller les conditions de sécurité dans leur quartier et auront probablement des inquiétudes similaires concernant les risques et la sécurité. Le personnel recruté localement pourrait connaître ces réseaux ou pourrait connaître des personnes ayant de bonnes relations et pouvant obtenir une bonne évaluation actuelle de zones particulières.

Les médias locaux et internationaux sont une autre ressource importante d'information. La presse internationale, et plus particulièrement les sites Internet des grands organismes de radio et de télévision, présente parfois une analyse des incidents de sécurité à l'aide de graphiques et de cartes. Les médias locaux peuvent être fiables ou sensationnalistes, mais il est relativement facile de savoir si un incident a été correctement signalé, quel que soit l'embellissement pouvant être ajouté. Surveiller les médias de langue locale est très utile car ils peuvent donner une meilleure idée de ce que la population locale est susceptible d'entendre et de lire, que les médias locaux qui sont écrits dans une langue internationale et qui n'atteignent donc qu'une petite partie de

la population. Enfin, les sociétés de sécurité internationales fournissent une analyse des caractéristiques et des tendances de la violence. Cela peut être utile pour la macro analyse, mais en général cela ne donne pas le genre de détails quotidiens dont ont besoin les organisations sur le terrain.

2.5.2 Informations et rumeurs

Les rumeurs sont en quelque sorte une catégorie de source d'informations à part. Le problème pratique des rumeurs est de savoir si on peut se fier à elles ou pas. Pour toutes informations obtenues de manière privée, la question doit être divisée en deux parties :

- La source d'informations est-elle fiable ?
- Les informations sont-elles valables ?

Tableau 4: Évaluer les sources d'information

Fiabilité de la source	Validité des informations
• Bien informée, ayant un accès direct aux informations • Bien informée mais sans accès direct aux informations • Généralement fiable • Généralement non fiable • Sans avis	• Mentionnées par plusieurs sources indépendantes • Très probablement valables • Probablement valables • Probablement non valables • Probablement fausses • Sans avis

Source : InterAction Security Action Group.

Au fil du temps, et probablement avec l'aide de personnes locales fiables, il est possible d'apprendre à apprécier les deux. N'oubliez pas de mentionner pendant les passassions quelle source est fiable et quelle source ne l'est pas. La grille ci-dessous est utile pour évaluer la fiabilité des informations que l'on « entend », plutôt que ce que l'on a vécu ou vu.

2.6 Évaluation de la vulnérabilité

Les vulnérabilités sont des facteurs qui augmentent l'exposition de l'organisation aux menaces ou qui augmentent la probabilité de conséquences graves. Des exemples spécifiques peuvent être :

- Avoir une présence très visible dans une zone à forte criminalité.
- Disposer de biens de grande valeur.
- Ne pas avoir de mur d'enceinte ou de clôture.
- Avoir de multiples points d'accès au bâtiment/à l'enceinte.

- Difficultés de communication.
- Manque de personnel expérimenté.
- Manque de soutien de la part d'autorités hostiles ou non coopératives.
- Transporter régulièrement du personnel, des biens ou de l'argent liquide.
- Emprunter toujours les mêmes routes.

Les questions clés comprennent :

- *Personnes*. Qui, dans l'organisation, est susceptible d'être exposé à des menaces ou d'être ciblé, quand et où ? Une analyse différenciée (expliquée dans le chapitre 6 sur « Les personnes dans la gestion de la sécurité ») sera nécessaire. Le concept fondamental, ici est celui du risque différencié. Les menaces seront différentes et par conséquent les niveaux de risque le seront aussi selon les types de personnel (expatriés ; membres de la population nationale/locale de différentes appartenances politique, religieuse ou ethnique ; hommes ; femmes ; différents postes dans l'organisation).
- *Lieux*. Les lieux des opérations (et les mouvements entre ces lieux) accroissent-ils l'exposition aux menaces ?
- *Biens*. Quels biens sont susceptibles d'être vulnérables, et où ? Les biens sont généralement vulnérables au vol, au pillage, à l'endommagement ou à la destruction (suite à des catastrophes naturelles, des actes de guerre, des actes criminels et des actes terroristes). Réfléchissez aux différents lieux où les biens pourraient être ciblés : au bureau, dans les logements, les entrepôts, en déplacement (le mouvement physique d'argent, de véhicules et de biens sur la route, entre points de distribution).

L'inverse des vulnérabilités est, bien entendu, les forces. Ce sont des facteurs qui réduisent l'exposition aux menaces et qui atténuent les résultats. Il est utile de préciser aussi les forces dans l'évaluation des risques. Par exemple, le personnel est-il bien formé et sensibilisé aux questions de sécurité ? Les questions relatives à la sécurité sont-elles évoquées de manière régulière ? L'organisation est-elle présente dans cette région depuis longtemps et a-t-elle de solides réseaux locaux qui la tiennent informée des changements dans la situation ?

Dans le travail d'une organisation, les aspects suivants peuvent être sources de vulnérabilité :

2.6.1 Présence/lieu

Les emplacements des bureaux, les routes principales utilisées et/ou les activités principales du programme peuvent engendrer un risque, simplement parce qu'ils placent l'organisation dans une zone de danger (potentiel) ou à proximité de cette zone. Posez-vous les questions suivantes :

- Les programmes placent-ils le personnel sur la trajectoire des opérations militaires, insurrectionnelles ou anti-insurrectionnelles ? Les opérations ont-elles lieu trop près de cibles politiques ou militaires potentielles ? Les voies d'entrée et de sortie peuvent-elles être affectées ?
- L'organisation opère-t-elle dans des camps de réfugiés qui servent aussi de base pour l'arrière-garde des insurgés ?
- Les programmes ont-ils lieu dans des régions importantes pour la guerre, l'économie illicite ou le commerce illégal (p. ex. l'exploitation forestière illégale) qui s'y pratiquent ?
- Les activités du programme ont-elles lieu dans des zones à forte criminalité (p. ex. zones de culture d'opium ou de cocaïne), ou sur des routes de transit utilisées par les trafiquants de drogue ou de personnes ?
- Si la violence sectaire est un problème, les bureaux ou les activités du programme sont-ils près d'un lieu ayant une forte valeur sociale et symbolique pour un groupe d'identité et pourraient-ils donc être une cible ?

2.6.2 Identité, présence et programmation

Les vulnérabilités en matière de sécurité peuvent aussi naître du contenu des missions et des mandats, ainsi que des programmes et de la façon dont ils sont mis en œuvre. Ces vulnérabilités « inhérentes » sont souvent plus difficiles à reconnaître. Certains aspects de cette question sont donnés ci-dessous.

- *Mission/mandat*. Une organisation pourrait être exposée à des menaces en raison d'un manque d'acceptation de sa mission ou de son mandat, surtout si des valeurs religieuses ou sociopolitiques sont considérées comme secondaires à l'action de fournir de l'aide aux personnes qui en ont besoin. Des exemples sont une ONG chrétienne soupçonnée de faire du prosélytisme dans un pays musulman, ou une organisation mandatée par un gouvernement pour poursuivre des objectifs d'aide associés au soutien de résultats politiques spécifiques.
- *Identité perçue*. La façon dont une organisation est perçue peut suffire à créer de la suspicion et même de l'hostilité. On peut penser du fondateur et directeur d'une ONG nationale ou d'une association de la société civile qu'il a des ambitions politiques personnelles, ou qu'il est un critique véhément d'autres membres de la société, ce qui peut engendrer de l'animosité envers l'organisation nationale dans son ensemble. En fait, toute identification religieuse – ou inversement une position laïque déclarée – peut avoir des connotations négatives dans certaines situations.
- *Programmes controversés*. Les programmes peuvent-ils prêter à controverse, et si c'est le cas, pourquoi et par qui ? Portent-ils sur une source de conflit, comme la reconstruction d'habitations dans des villes ayant subi une épuration ethnique (aux Balkans), la reconstruction agricole qui crée des disputes concernant la propriété foncière (au nord de l'Irak), ou

l'alimentation en eau dans des environnements arides (le Sahel ou la Somalie) ? Ou bien, les programmes peuvent-ils devenir une nouvelle source de conflit dans un environnement faisant déjà l'objet d'un différend, par exemple une proposition de construire un centre de santé sur un territoire contrôlé par un groupe ou une autorité et qui sera ensuite revendiqué par un rival ? Le programme remet-il en question des normes sociales et culturelles ou des principes religieux, par exemple les programmes pour autonomiser les femmes, pour la scolarisation des filles ou l'élargissement d'une éducation laïque ? Comment peut-on obtenir la légitimité de ces types de programmes ?

2.6.3 L'impact sur l'économie politique, locale ou plus large

Il pourrait arriver que le travail d'une organisation influence la balance du pouvoir entre différentes parties adverses, de sorte que celles qui craignent d'être perdantes deviennent une source de menace. Par exemple :

- Reconstituer les troupeaux de pasteurs peut être contesté par des agriculteurs indignés parce que les animaux envahissent leurs champs.
- Fournir des installations de stockage et des informations actualisées sur le marché dans des contextes ruraux isolés peut être contesté par les intermédiaires qui contrôlent le flux des informations et monopolisent l'entreposage.
- Réorganiser un système de distribution pour que les biens soient délivrés directement aux bénéficiaires prévus pourrait écarter le comité du camp, le « commandant » local ou le conseil du village et supprimer ainsi des opportunités de parrainage.
- Si des violations des droits de l'homme et des atrocités sont commises, l'organisation pourrait être considérée comme témoin indésirable par les auteurs des crimes.
- La présence même d'organisations internationales peut être un facteur de stabilité et pourrait aller à l'encontre des intérêts de ceux qui tirent un avantage de l'instabilité constante. Les programmes qui visent spécifiquement à contribuer à l'édification de la paix et à la construction d'un État peuvent créer l'antagonisme.
- La source de financement du programme d'aide dans un contexte donné peut suffire à créer la méfiance.

2.6.4 Impartialité dans l'allocation de ressources limitées

La plupart des organisations humanitaires souscrivent au concept d'impartialité dans l'allocation d'assistance. Cela signifie que les ressources doivent être allouées uniquement en fonction du besoin, et non pas selon des considérations politiques ou autres. Dans la pratique, c'est rarement le cas et d'autres facteurs, comme l'accès, la visibilité et l'efficacité par rapport au coût,

jouent un rôle dans les décisions d'allocation. De plus, les ressources sont limitées, alors que souvent les besoins ne le sont pas. Dans ces conditions, le biais et la partialité perçus en faveur d'un groupe plutôt que d'un autre peuvent entraîner le mécontentement. Un moyen d'atténuer ce risque est d'expliquer la base de l'allocation de l'aide et les obstacles pratiques imposés par des ressources limitées. Il pourrait être utile également de demander aux communautés bénéficiaires mêmes quels critères elles utiliseraient.

Un facteur clé à ce sujet est de comprendre qui est exclu ou oublié et comment ces personnes pourraient réagir. Il est généralement accepté que les organisations ne peuvent concentrer toute leur aide sur les populations de réfugiés aux dépens des communautés hôtes par exemple. D'autres groupes, potentiellement dans le besoin, pourraient inclure les personnes vivant le long de routes de transit ou dans des villes, qui pourraient être mécontentes d'être exclues de l'assistance ou des opportunités d'emploi que l'action d'apport et de distribution de l'aide crée. De même, une organisation qui dirige sa propre opération de logistique pourrait entrer en concurrence avec les sociétés locales de transport ou les empêcher de faire des affaires.

2.6.5 Transparence et responsabilisation des intermédiaires

Une organisation qui met en œuvre des programmes par le biais d'un intermédiaire (un prestataire ou partenaire local) pourrait avoir des différends avec ce collaborateur ou pourrait être tenue responsable des actes et omissions de celui-ci. Définir clairement les attentes dès le départ peut permettre d'éviter les problèmes ou de faciliter leur gestion s'ils surgissent et peut également éviter qu'ils ne conduisent à la violence. Une allocation précise des tâches et responsabilités réduira également le risque d'être mis en cause et peut même être menacé en raison des actions et des omissions du collaborateur. Évoquez au préalable, peut-être dans un forum ouvert avec suffisamment de « témoins », les normes de transparence et de responsabilisation attendues ainsi que les procédures qui seront suivies si ces normes ne sont pas observées et/ou si des abus ou de la corruption sont identifiés.

2.6.6 Provoquer la colère et le mécontentement

Outre les perceptions de biais et de partialité, les causes fréquentes de colère et de mécontentement comprennent :

- La lassitude face aux évaluations et aux demandes de renseignements : encore une autre mission d'évaluation par une organisation posant les mêmes questions, sans aucun programme tangible réalisé, ou : encore un nouveau membre du personnel de l'organisation posant les mêmes questions pour lesquelles les bénéficiaires ont donné des réponses à trois de ses prédécesseurs.

- Des délits non traités : par exemple, le véhicule d'une organisation percute et tue la vache d'un villageois local mais ne s'arrête pas pour régler le problème.
- Des promesses non respectées, réellement ou perçues comme telles : promesses sur un projet qui ne s'est jamais concrétisé ou qui s'est réalisé plus lentement ou sur une échelle plus petite que prévu.
- Une programmation tout simplement mauvaise : incompétence, gaspillage, objectifs non atteints.
- Des trains de vie « luxueux » : le personnel fréquente des bars, des clubs ou des restaurants qui sont hors d'atteinte pour la plupart de la population.

Notez que souvent les personnes externes ne font pas la distinction entre une organisation ou une autre, si bien qu'une organisation pourrait faire face à un problème créé par une autre organisation.

2.7 Analyse du risque

Le risque est la combinaison des menaces et de la vulnérabilité. Évaluer les risques signifie essentiellement classer les menaces selon leur gravité sur la base de leur *impact* et de leur *probabilité*. Pour effectuer cela systématiquement, il peut être utile de suivre les étapes ci-dessous ; il ne s'agit pas d'une formule scientifique, mais plutôt d'apporter une structure et une discipline à la façon dont l'analyse est effectuée.

2.7.1 Impacts

Il est utile de penser aux impacts directs et indirects.

Impacts directs :

- Pour le personnel/les personnes (y compris les familles et amis) : blessure physique temporaire ou permanente, atteinte psychologique temporaire ou à plus long terme, mort.
- Pour les organisations : perte ou endommagement des biens, inefficacité opérationnelle, perte de qualité du programme ou suspension totale, perte de réputation, perte de financement.
- Pour le programme et ses bénéficiaires : réduction de la qualité du programme, suspension temporaire du programme, suppression forcée du programme.

Il y a également des coûts indirects à plus long terme pour l'organisation. Ceux-ci pourraient inclure :

- Coût des traitements médicaux et du soutien psychologique
- Frais légaux.

Tableau 5: Évaluer les impacts potentiels

	Impact prévu sur les activités de l'organisation		
	Opérations	**Personnel**	**Biens**
Négligeable	Perturbations mineures	Pas de blessures	Pas de dommages
Mineur	Faibles retards	Blessures mineures/ stress possible	Dommages ou pertes possibles
Moyen	Retards	Blessures non mortelles/ stress important	Certaines pertes
Grave	Perturbations graves	Blessures graves	Pertes graves
Très important	Annulation des activités	Mort et blessures graves	Pertes importantes ou totales

Source : InterAction, Security Risk Management : NGO Approach (Gestion de la sécurité des risques : Approche ONG) 2010

- Primes d'assurance plus élevées.
- Démoralisation du personnel : perte de confiance possible du personnel en la direction, pouvant conduire à un plus grand renouvellement du personnel.
- Atteinte à la réputation de l'organisation, avec des conséquences possibles sur la collecte de fonds.

Il doit exister, au sein de l'organisation, une compréhension commune du niveau de sévérité des impacts possibles. À cette fin, faites une liste des impacts potentiels et classez-les de négligeable (par exemple un vol mineur) à crucial (une attaque de l'enceinte à main armée au cours de laquelle des membres du personnel sont tués).

2.7.2 Probabilité

Une analyse de la probabilité permet de hiérarchiser les menaces potentielles, faisant la différence entre ce qui est possible et ce qui est probable. Dans une large mesure, il s'agit d'un jugement basé sur l'expérience des décideurs, mais plus les informations fournies par l'évaluation des menaces seront importantes (notamment les informations statistiques sur les tendances des incidents), plus les décideurs disposeront d'éléments de prise de décision. Comme le mentionne la section sur l'évaluation des menaces (voir section 2.5), il est important de se demander si un adversaire particulier a déjà exercé une menace spécifique, s'il en a déjà eu l'intention et s'il en est capable. Si c'est le cas, on peut considérer que l'événement est probable.

Le tableau suivant montre les catégories qui peuvent aider à classer la probabilité de différents événements.

Tableau 6: Classer la probabilité des événements

Description	Définitions de « probabilité »
Improbable	Il est jugé que l'événement n'a pas de réelle probabilité de se produire
Moyennement probable	Il est jugé que l'événement a une probabilité raisonnable de se produire
Probable	Il est jugé que l'événement a une forte probabilité de se produire.
Très probable	Il est jugé que l'événement a une très forte probabilité de se produire.
Certain/Imminent	L'événement se produira et est imminent.

Source : World Vision International. (Note : ce tableau est utilisé avec l'autorisation de World Vision International et toute reproduction autre que cette publication (RBP) doit faire l'objet d'une autorisation expresse de World Vision International.)

L'évaluation de la probabilité et de l'impact

Essayez de classer les différentes menaces selon deux critères : quelle est la probabilité que quelque chose (une menace) se produise, et si cela se produisait, quelle serait la gravité de l'impact ? Dans la grille ci-dessous, les colonnes représentent la probabilité qu'un incident se produise dans un délai donné, disons dans les six prochains mois. Les lignes horizontales représentent la sévérité de l'impact. Il est important de clarifier ce qu'est un impact dans ce contexte. Un viol, par exemple, aura un impact grave pour la personne concernée, mais ne conduira sans doute pas l'organisation à suspendre ses programmes. Si des émeutiers endommagent les logements de membres du personnel international, cela sera probablement moins grave pour ces personnes (qui, après tout, louent leur logement et ont la majeure partie de leurs biens à l'étranger) que des dommages causés aux habitations des membres du personnel national (qui auront peut-être investi toutes leurs économies dans leurs logements).

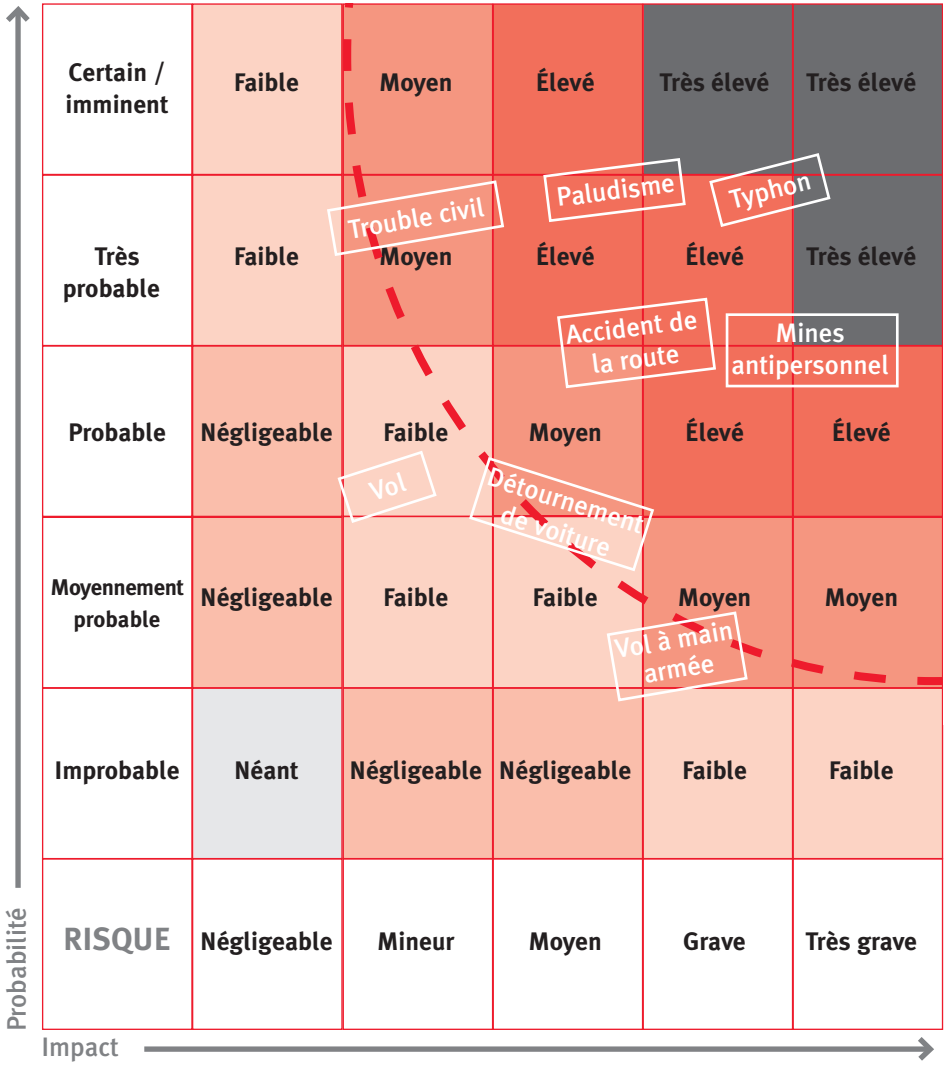
Cette évaluation permet d'identifier les priorités dans la gestion des menaces, autrement dit les risques qui sont les plus susceptibles de

Tableau 7: Grille d'évaluation de la probabilité/susceptibilité et de l'impact d'une menace

Probabilité	Impact				
	Négligeable	Mineur	Moyen	Grave	Tres grave
Tres probable					
Probable					
Moyennement probable					
Peu probable					
Tres peu probable					

se réaliser et, s'ils se réalisaient, la gravité de leur impact. Elle permet également de déterminer quand un risque est devenu trop élevé pour la continuation des opérations.

Tableau 8: Analyse des risques



Source : World Vision International. (Note : ce tableau est utilisé avec l'autorisation de World Vision International et toute reproduction autre que cette publication (RBP) doit faire l'objet d'une autorisation expresse de World Vision International.)

2.7.3 Mesures d'atténuation et seuil du risque

Le diagramme ci-dessous illustre les conclusions suivantes, issues d'une discussion d'une équipe sur le terrain :

- La probabilité d'un trouble civil dans la région est relativement forte, mais son impact sur le personnel et sur le programme serait limité.
- Le risque de vol à main armée pourrait être de moyen à faible, mais son impact sur le programme serait considérablement plus fort, en termes de blessures graves et de stress important infligés au personnel ainsi que de pertes importantes de biens.

Ces deux facteurs peuvent être considérés comme se trouvant à un seuil de risque acceptable par l'organisation, comme indiqué par la ligne en pointillés. En revanche, la menace de mines antipersonnel, ayant à la fois une forte probabilité et un impact grave à très grave, est au-delà du seuil de risque acceptable de l'organisation et demande des mesures immédiates pour atténuer le risque. Les couleurs représentent les niveaux généraux de risque, allant de faible (vert) à élevé (noir). Les pointillés représentent le « seuil de risque » de l'organisation, au-dessus duquel le risque est considéré comme trop élevé.

La prochaine étape consiste à se demander ce qui peut être fait pour réduire les risques à un niveau acceptable. En termes généraux, il y trois modes d'action :

- *Réduire la menace*. Si c'est faisable, établissez le dialogue avec des adversaires potentiels ou demandez à d'autres personnes de négocier en votre nom.
- *Réduire les conséquences/atténuer l'impact de la menace*. Ces actions pourraient très bien être nommées « mesures d'urgence », comme les protocoles de premier secours, les procédures de réponse à une crise, l'évacuation préventive in extremis et les recommandations sur la façon de se comporter dans l'éventualité d'un accident grave.
- *Réduire ou éliminer l'exposition* en adoptant des mesures de protection additionnelles ou en changeant de lieu, par exemple. Une version extrême de cette action serait « d'éviter le risque », c'est-à-dire soustraire entièrement l'organisation à la menace, soit de façon permanente soit de façon temporaire.

Un moyen de réduire ou d'éliminer l'exposition au risque est de le faire passer à un autre acteur (transfert du risque).

- *Transfert du risque*. Utiliser d'autres entités pour entreprendre le travail et accepter les risques du programme, par exemple sous-traiter à un partenaire local ou à un prestataire de services local. L'assurance (des véhicules et d'autres biens) est une forme de transfert de risque, mais uniquement en ce qui concerne les conséquences financières d'un incident

Tableau 9: Définir des mesures d'atténuation des risques

Réalités						Problèmes			Solutions	
Évaluation de la menace		Évaluation du programme		Évaluation de la vulnérabilité		Analyse du risque			Recommandations	
Menace	Situation	Lieu	Activité	Faiblesses	Forces	Impact	Probabilité	Niveau du risque (actuel)	Mesures d'atténuation	Niveau du risque résiduel (futur)

Source : InterAction, Security Risk Management : NGO Approach, 2010.

survenu. Cependant, lorsque le risque concerne le potentiel de blessures ou de mort, le transfert devient un gros problème éthique.

Il est temps, ensuite, de retourner à l'analyse des capacités initiales, afin de déterminer si les ressources financières et les compétences sont disponibles pour mettre en œuvre ces stratégies et ces mesures spécifiques aux menaces. Il faudra ensuite vérifier si le temps et l'attention nécessaires peuvent être consacrés à cette tâche. La responsabilité de gestion des risques doit être spécifiquement attribuée et des personnels devront rendre des comptes à ce sujet. L'exemple de fiche de travail qui suit pourrait être utilisé pour déterminer les mesures d'atténuation des risques basées sur l'évaluation des risques.

Il est important d'être réaliste quant à l'efficacité des mesures d'atténuation des risques : même des installations bien protégées peuvent être vulnérables à des attaques bien planifiées par un groupe ayant une ferme intention. Dans certains cas, il pourrait être possible de réduire le risque à un niveau acceptable mais, à moins de quitter la région, il sera probablement impossible de le supprimer totalement. Il reste un *risque résiduel*. Après avoir identifié tous les risques dans le contexte opérationnel et après avoir évalué objectivement et avec réalisme l'efficacité des mesures de réduction du risque, il est nécessaire de se demander si le risque résiduel est acceptable ? Trop peu d'organisations ont clairement défini des seuils et critères de risque pour éclairer ces décisions. Au bout du compte, si le risque résiduel n'est pas acceptable, et qu'aucune mesure d'atténuation supplémentaire ne peut être prise, la présence du programme devra être modifiée ou supprimée.

Seuil de risque acceptable

Le travail humanitaire dans des contextes de conflit implique la volonté de prendre certains risques. Les débats des organisations d'aide le reconnaissent. Un exercice visant à déterminer le seuil de risque acceptable tente de rendre cette tolérance du risque concrète et explicite, et de définir les implications des décisions de gestion concernant l'action à prendre face à un risque. Les points suivants décrivent trois moments importants où le seuil de risque acceptable doit être évoqué.

- Pour décider d'entrer dans un environnement dangereux ou d'élargir un programme dans un tel environnement.
- Pour déterminer des seuils individuels de risque acceptable.
- Pour tirer un trait lorsqu'une situation se détériore.

Dans le premier cas, une analyse de la menace doit donner un sens plus ou moins objectif de ce que les risques sont susceptibles d'être. La question à poser est : ces risques sont-ils acceptables ? Décider ce qui constitue un

risque acceptable nécessite des critères et des conditions explicites pour assurer un processus décisionnel discipliné et transparent.

Dans le second cas, déterminer des seuils individuels de risque acceptable est important parce que la tolérance au risque diffère selon les personnes. De même, l'impact d'une menace n'est pas nécessairement le même pour une personne que pour une organisation et peut aussi être différent selon les individus. On ne peut donc présumer que tous les membres du personnel existant et potentiel ont le même seuil de risque acceptable. Un climat de confiance dans l'organisation permet aux personnes d'exprimer un malaise si une situation dépasse leur niveau de tolérance du risque. De même les personnes qui entrent dans un environnement à haut risque doivent le faire après avoir été informées des risques présents. Parallèlement, des personnels pourraient se sentir obligés de prendre des risques au-delà de ce qu'ils peuvent personnellement tolérer, souvent pour des raisons économiques ou professionnelles : par exemple, ne pas y aller impliquerait de ne pas avoir le poste ou de perdre l'opportunité de se distinguer et de remplir les conditions requises pour recevoir une promotion.

Dans le troisième cas, le but est d'éviter le syndrome de la grenouille dans la marmite : l'eau est chauffée progressivement, la grenouille ne reconnaît pas le danger, ne sort pas à temps, et lorsque l'eau atteint l'ébullition c'est trop tard. « L'accoutumance au danger » est fréquente chez les travailleurs humanitaires. Bien que les personnes soient conscientes que la situation se détériore, elles ne s'en éloignent pas ou ne renforcent pas leurs mesures de sécurité, sauf après un incident. De plus, de nombreux travailleurs humanitaires témoignent qu'ils baissent continuellement leur seuil de risque acceptable au cours de leur travail. Cette situation nécessite une supervision externe et ne serait justifiable que si des mesures de sécurité étaient considérablement renforcées et améliorées. Il est manifeste que ce sont les besoins qui justifient les risques plus élevés (là ou le programme est crucial), et ceux qui restent dans un environnement à hauts risques peuvent gérer le stress et ont correctement réévalué leur seuil personnel de risque acceptable.

2.7.4 Les phases de sécurité

Certaines organisations, notamment les Nations Unies, gèrent la sécurité par une « classification du risque », ou encore par des « niveaux » ou « phases ». En général, les organisations ont quatre ou cinq phases de sécurité, allant de risque faible à risque très élevé. Chaque phase contient un ensemble de mesures prédéterminées à prendre; la dernière sera en général le retrait de tout le personnel. La grille qui suit montre un moyen de structurer les pratiques de la gestion de la sécurité selon les phases de sécurité.

Indicateurs	Phase/niveau	Impact sur les activités du programme	Mesures de sécurité à prendre
	Phase 1 (« normale »)		
	Phase 2		
	Phase 3		
	Phase 4		

L'avantage de travailler avec des phases de sécurité est que, une fois déclarées, elles sont censées déclencher un ensemble d'actions sans autre hésitation ni discussion. Cela apporte également une certaine cohérence dans la réponse face à une augmentation du risque. Les phases pourraient être particulièrement utiles en tant que baromètre simplifié permettant au siège de suivre le risque de près. La décision de passer à une phase de sécurité plus élevée appartient généralement aux hauts responsables sur le terrain, tandis que placer la situation à une phase de sécurité inférieure nécessite l'autorisation d'une autorité organisationnelle en dehors du contexte opérationnel.

Utiliser des « phases » de sécurité comme outil de gestion peut donner un faux sens de robustesse et de prévisibilité, et il est important de comprendre les limites de cette approche :

- Des informations incomplètes et les difficultés associées à l'interprétation correcte d'une réalité complexe pourraient poser des difficultés pour décider de passer à un niveau d'alerte différent. Quoi qu'il en soit, identifier la phase de sécurité adéquate et mettre en œuvre le plan sont deux choses différentes.
- Les classifications par phases peuvent parfois être trop larges pour saisir les gradients de la menace ou les différentes catégories de personnes en danger dans un même lieu. Par exemple, certaines organisations en Somalie ont décidé de diviser la classification des phases en deux, l'une pour le personnel international et l'autre pour le personnel national (ou même de les diviser entre personnel national « local » et « relocalisé »), en raison des risques très différents auxquels ces groupes sont exposés.
- Dans la pratique, les situations ne se dégradent ou ne s'améliorent pas toujours progressivement : une situation peut soudain se détériorer en raison de conditions pouvant correspondre à celles des Phases 1 à 5.
- Plusieurs organisations peuvent interpréter la même situation différemment et peuvent donc se placer dans des phases de sécurité différentes et prendre diverses mesures correspondant à ces phases. L'évacuation dans des moments de crise nécessite généralement une collaboration inter organisations, qui pourrait être compliquée par différentes appréciations du risque. De plus, le fait que certaines organisations procèdent à une évacuation et d'autres pas, pourrait changer le risque et accroître la vulnérabilité de ceux qui restent.

Chapitre 3
Stratégie de sécurité

3.1 Élaborer une stratégie de sécurité

La première édition de cette Revue des bonnes pratiques identifiait trois approches générales de la sécurité ou positions qui définissent la stratégie de gestion de la sécurité d'une organisation, c'est-à-dire l'acceptation, la protection et la dissuasion.

- Une approche d'**acceptation** tente de réduire ou de supprimer les menaces en renforçant l'acceptation (le consentement politique et social) de la présence d'une organisation et de son travail dans un contexte particulier.
- Une approche de **protection** utilise des dispositifs et procédures de protection pour réduire la vulnérabilité à la menace, mais n'a aucun effet sur la menace même. En termes de sécurité, on appelle cela durcir la cible.
- Une approche de **dissuasion** vise à supprimer la menace par une contre menace. Elle peut impliquer des sanctions légales, économiques ou politiques (pas nécessairement de la part des organisations humanitaires) et même la menace d'utilisation ou l'utilisation de la force.

Les concepts d'acceptation, de protection et de dissuasion constituent pour les organisations une gamme d'options et d'actions de sécurité, allant de « douces » à « dures ». Celles-ci sont souvent associées et varient en fonction des cultures et conditions de sécurité locales. L'édition de 2000 de cette Revue des bonnes pratiques présentait les trois approches comme ce qui est communément appelé : le triangle de la sécurité. Au fil des années, cependant, sa signification et son application pratique ont donné lieu à une certaine confusion.

Le modèle du triangle n'était pas censé impliquer qu'une organisation humanitaire décide tout simplement, au niveau institutionnel, quelle approche est préférable (ou la position de l'organisation dans le triangle) et quelles opérations conduire en conséquence. La réalité est beaucoup plus fluide. Tout d'abord, une approche particulière ne peut être efficace que si elle est adaptée à son environnement, et si l'organisation a les capacités et compétences de gérer cette approche. Deuxièmement, dans tout environnement opérationnel donné, une organisation choisira probablement une combinaison d'approches. Au fur et à mesure que les risques évoluent, l'organisation devra s'adapter en modifiant l'équilibre des approches. En particulier, adopter une approche de protection ne signifiera *pas* généralement abandonner une approche d'acceptation ; les deux composantes peuvent être conjuguées. Durcir la

cible pourrait nécessiter une *plus grande* action sur le terrain afin de créer la confiance et d'obtenir l'acceptation. Troisièmement, l'efficacité d'une approche sera influencée par l'action d'autres organisations. Enfin, aucune approche, seule ou conjuguée, ne réduira le risque à néant.

En raison de leur mission et de leurs valeurs, les organisations jugent que l'acceptation est, de loin, la stratégie de sécurité la plus souhaitable. Certes, l'acceptation peut et doit être le fondement de toutes les stratégies de sécurité. Mais l'acceptation ne sera pas efficace contre toutes les menaces. Dans les contextes où la criminalité ou le banditisme sont très répandus, dans les situations où les belligérants poursuivent des objectifs nationaux ou même mondiaux, et dans celles où la mission et les objectifs des organisations signifient peu pour certains acteurs, une approche d'acceptation seule pourrait ne pas être viable.

Cependant, les approches de protection et de dissuasion ne sont pas nécessairement plus efficaces dans tous les cas et peuvent elles-mêmes être accompagnées de difficultés. Une approche de protection porte principalement sur l'organisation en tant que cible potentielle et, à l'inverse de l'acceptation, n'agit pas sur les auteurs de la menace. Elle peut aussi engendrer une « mentalité de ghetto ». Il est ainsi plus difficile de développer des relations avec d'autres acteurs. De ce fait,, il devient plus ardu d'obtenir des informations sur le contexte et de communiquer de manière efficace avec des interlocuteurs locaux. De mauvaises relations ou des relations inexistantes permettent à la suspicion, au mécontentement et à l'hostilité de s'enraciner.

Une approche de dissuasion peut également créer des difficultés supplémentaires. Si les organisations font preuve de force, par exemple en se déplaçant en voiture avec des escortes armées ou en recrutant des gardes armés pour leurs bureaux, il leur sera peut-être plus difficile de communiquer des principes de non-violence et d'indépendance. Les membres des communautés ou les acteurs armés pourraient penser que l'organisation est en quelque sorte connectée avec des groupes belligérants et l'acceptation pourrait en être compromise. Dans certains contextes, comme en Somalie, les organisations humanitaires se sont également aperçues que les gardes armés contrôlent un marché de la sécurité de facto et il est très difficile de ne plus les employer après les avoir recrutés.

Dans la pratique, une bonne stratégie de sécurité nécessite une combinaison d'approches flexible. Cultiver l'acceptation et de bonnes relations avec la population locale et ses dirigeants, ainsi qu'avec les acteurs armés, gouvernementaux ou non, doit être la base de toute activité de programme. Dans des contextes plus dangereux comportant des risques identifiés pour les

organisations d'aide, certaines mesures de protection, en particulier contre le crime, pourraient être inévitables. Dans les contextes très dangereux, qui comportent d'importants risques identifiés , des mesures de dissuasion pourraient être nécessaires si elles sont le seul moyen de protéger le personnel et de continuer à fournir une assistance cruciale. L'essentiel est que la gestion de la sécurité soit proactive, ce qui implique des choix délibérés quant à la combinaison d'approches utilisée en fonction des menaces identifiées et des approches adoptées par d'autres organisations.

Enfin, il est important de ne pas oublier que les différentes approches ont des implications diverses en matière de ressources. Elles entraînent toutes un coût financier. L'acceptation est sans doute l'approche la plus difficile à mesurer en termes financiers, mais ne doit pas nécessairement être considérée comme peu onéreuse. Si elle est activement poursuivie, l'acceptation peut nécessiter un temps considérable et sans doute de nouvelles initiatives de programmes, telles qu'une action médiatique sur le terrain. Les dispositifs et matériels de protection comportent un coût financier direct, et les procédures de protection (par exemple l'imposition de couvre-feux ou toujours se déplacer à deux voitures) peuvent alourdir le budget et /ou limiter la capacité opérationnelle. Une approche de dissuasion peut avoir de petites ou de grandes implications en matière de ressources, auxquelles il pourrait être difficile ou impossible de se soustraire à long terme.

3.2 L'acceptation

Traditionnellement, une approche d'acceptation a différentes significations selon les organisations. Obtenir le consentement des parties belligérantes est, historiquement, un aspect fondamental des principes de l'action humanitaire du mouvement de la Croix-Rouge et du Croissant-Rouge. Obtenir l'acceptation générale des communautés, par le biais de bonnes actions et de l'observation des principes humanitaires est au cœur de la mission et des principes d'un nombre beaucoup plus important d'organisations humanitaires.

Pour la majeure partie des organisations humanitaires, l'acceptation est le type d'approche de la gestion de la sécurité le plus souhaitable. Pourtant, ce qui est souvent mal compris, c'est que l'acceptation ne peut être présumée ; elle doit être obtenue et maintenue. À l'inverse des organisations des droits de l'homme et des journalistes, qui sont plus conscients que leur travail ne plaira probablement pas à tout le monde, les organisations humanitaires s'attendent en général à être acceptées avec empressement, en raison de leurs activités. Dans certaines parties du monde, ce n'est cependant plus le cas pour des raisons diverses. Depuis la première analyse de l'approche d'acceptation dans la RBP de 2000, de nombreux faits concourent à indiquer que, dans un certain

nombre de contextes, l'acceptation est aujourd'hui plus difficile à obtenir (voir l'annexe 1). L'acceptation peut-elle être obtenue, quand et par qui ? Il est aujourd'hui nécessaire de se poser ces questions opérationnelles.

Un grand nombre d'organisations ont aujourd'hui des politiques organisationnelles et des politiques de sécurité qui sont ancrées dans le concept d'une approche d'acceptation. Cependant, elles n'ont pas souvent de lignes directrices sur les mesures pratiques à prendre pour cultiver et maintenir l'acceptation, ou pour évaluer si elle est obtenue ou pas. Dans le passé, les organisations présumaient tout simplement qu'en n'adoptant pas d'approche de protection ou de dissuasion, en n'ayant pas de relations avec certains acteurs internationaux ou en n'acceptant pas de fonds de certains donateurs, elles adoptaient une approche d'acceptation. C'est une attitude malavisée ; l'acceptation ne peut être définie à la forme négative ou adoptée par défaut. Les sections qui suivent abordent donc les éléments essentiels d'une approche « d'acceptation active » et soulignent que l'acceptation est quelque chose que l'on doit favoriser et continuellement tenter d'obtenir – et non pas une attitude statique de l'organisation.

3.2.1 Composantes essentielles d'une approche d'acceptation active

Qu'entend-on par une approche d'acceptation active ? Les éléments composants clés comprennent une action de proximité active auprès d'un large éventail de parties prenantes ; un investissement considérable en temps de personnel, ayant d'excellentes compétences sociales, politiques, de relations interpersonnelles et de communication ; et le développement et maintien de messages fondamentaux concernant le mandat, les objectifs et les programmes de l'organisation. Mais le plus important est sans doute qu'elle implique une action conforme à cet exposé.

Créer et entretenir des relations avec les parties prenantes clés

Dans une approche d'acceptation, les parties prenantes clés correspondent à toutes personnes pouvant officiellement ou pas, exercer une influence utile sur la capacité d'une agence à travailler en sécurité dans un environnement donné. Elles pourraient inclure des acteurs armés gouvernementaux et non gouvernementaux, des représentants du gouvernement, les autorités locales, les dirigeants de la communauté, les médias locaux et internationaux ainsi que des personnes du milieu des affaires ou du secteur privé. Certains acteurs pourraient être difficiles à identifier (parfois parce qu'ils ne souhaitent pas être identifiés), ou il pourrait être difficile de les joindre. Connaître ces parties prenantes nécessite d'établir leur profil et de les analyser. Ceci est un exercice que les personnels nationaux et expatriés doivent effectuer ensemble.

L'acceptation doit être obtenue de toutes les parties concernées, y compris celles qui, pour des raisons économiques, culturelles, religieuses, militaires

ou politiques, pourraient se méfier de l'organisation, se sentir menacées par elle ou ressentir une hostilité active envers elle. Ces personnes doivent être identifiées au cours de l'analyse de la situation/des risques. Il est important de déterminer l'influence que chaque partie possède. Dans certaines situations, être accepté par des personnes influentes et clés peut suffire s'il est impossible d'être accepté par tout le monde, tandis que dans d'autres situations ce n'est pas le cas. Le personnel national peut jouer un rôle essentiel pour déterminer avec quelles parties prenantes communiquer et entrer en contact. Dans des contextes difficiles, un personnel national chargé de la « liaison » pourrait être nécessaire. Dans certains cas, le fait d'utiliser un intermédiaire respecté (par exemple un dirigeant religieux ou un chef de la communauté) peut doter l'organisation de respectabilité dans la région où elle est présente.

Une stratégie d'acceptation active peut ne pas se limiter aux acteurs locaux. Des progrès dans les télécommunications et le transport ont amélioré l'interconnectivité. Ceci signifie que les parties prenantes peuvent être dispersées géographiquement. Pour les atteindre, l'organisation doit faire preuve de volonté, de compétence et de ressources financières. Une ONG, par exemple, a commencé à communiquer avec des membres de la diaspora somalienne sur la mission et les valeurs de l'organisation dans le but d'encourager l'acceptation.

Il pourrait être utile, pour s'assurer que tous les acteurs clés sont pris en compte, de remplir le tableau suivant. La précision est ici essentielle. Les termes : « gouvernement », « communauté chiite » ou « militaires » ne sont généralement pas suffisants. Il y aura probablement différentes opinions, différents faiseurs d'opinions et différents centres de pouvoir dans chaque catégorie. Même s'il n'y a pas de réponses précises, la valeur de cet exercice réside fortement dans la discussion qu'il engendre. Cette discussion pourrait se concentrer sur quelques acteurs cruciaux, ou sur les actions qui pourraient être mises en place pour accroître l'acceptabilité.

Acteur	Niveau d'acceptation (aucun, faible, suffisant, fort)	Pourquoi?	Que peut-on faire pour obtenir une plus grande acceptation ?

Obtenir l'acceptation des populations locales

Une approche d'acceptation active prend en compte non seulement les membres de la communauté qui bénéficient directement du programme d'aide, mais également, et peut-être surtout, ceux qui n'en bénéficient pas. Ces derniers peuvent se trouver aussi bien à l'intérieur de la zone du programme que dans les régions traversées par le personnel pour s'y rendre.

Il est important de comprendre la différence entre la simple tolérance de la présence du programme et la pleine acceptation d'une organisation. Quelquefois, la population accepte la présence uniquement parce qu'il y a un profond besoin. D'autres fois, la population peut utiliser l'aide comme source de soutien mais peut ne pas se sentir activement responsable du bien-être de l'organisation. Écouter ce que la population veut et répondre à ses besoins, la traiter avec respect, agir avec transparence et avec responsabilité peut encourager un plus grand niveau d'acceptation. Cela peut même compter davantage que la dimension matérielle. Une organisation pourrait se trouver dans l'impossibilité d'apporter une bonne assistance ou, périodiquement, une quelconque assistance, et être malgré tout acceptée grâce à la qualité des relations qu'elle entretient. Ceci dit, il est important de ne pas créer des attentes que l'on ne saurait satisfaire. Par exemple, pendant l'intervention suite au tsunami de l'Océan Indien, trop promettre et ne pas tenir tous ses engagements a été un problème pour un certain nombre d'organisations humanitaire.

S'il y a un grand niveau d'acceptation, les membres de la communauté peuvent faire des suggestions pour réduire les risques. Par exemple, en Afghanistan on demande parfois aux personnels médicaux de passer la nuit chez des membres de la communauté plutôt qu'au poste de santé. En Somalie, les membres de la communauté ont quelquefois prévenu les ONG de quitter la région avant qu'une menace ne les atteigne. Dans d'autres cas, les habitants locaux ont aidé à récupérer des biens volés et ont donné des informations dans des cas de rapt. Mais ne surestimez pas le pouvoir de la communauté locale. Dans d'autres circonstances, les communautés ne seront pas en mesure de réduire les risques de sécurité. Elles n'auront peut-être pas le pouvoir d'influencer d'autres acteurs, pourront négliger ou mal évaluer de nouvelles menaces ou bien juger qu'elles ont intérêt, à long terme, d'être en relations avec un autre acteur très influent, peut-être armé, plutôt qu'avec un prestataire d'aide temporaire.

L'acceptation peut diminuer au fil du temps, au fur et à mesure que les besoins et les attentes de la population évoluent. Après la stabilisation d'une situation, de nouvelles aspirations naissent souvent. En Afghanistan, par exemple, au bout d'un certain temps les Afghans se sont mis à définir la « paix » en termes « d'électricité et d'emplois » plutôt qu'en termes de protection contre des

atteintes physiques.[1] L'incapacité des organisations d'aide à satisfaire ces besoins à si long terme pourrait conduire à un désintérêt et à une moins grande acceptation de la part de la population.

Entretenir des relations avec les acteurs armés

Nouer des liens ou négocier avec des groupes armés sera souvent inévitable. Une organisation qui travaille dans une région où un certain groupe détient le contrôle devra probablement de facto lui signaler sa présence et avoir son assurance que son travail est acceptable et qu'on ne portera pas atteinte à son personnel. Cependant, lorsque vous nouez le dialogue avec des acteurs armés, procédez avec prudence, et préparez-vous. Les questions à envisager sont :

- Quelles sont les relations entre le groupe armé et les civils que l'organisation tente de secourir ?
- Quelle est la structure de commandement, la discipline, les buts et objectifs du groupe armé ?
- Quelle influence les négociations avec ce groupe armé auront-elles sur les relations avec d'autres acteurs (notamment le gouvernement) ?

Comprendre cette dynamique et ces risques nécessite la capacité proactive de les analyser. Il sera souvent judicieux de travailler avec d'autres acteurs (p. ex. OCHA, une autre agence des Nations Unies ou un groupe d'ONG) pour partager les ressources et permettre une approche commune, ou tout au moins pour s'assurer que des approches différentes n'entravent pas les efforts d'autres acteurs.[2]

Maintenir des communications cohérentes

Les communications doivent être claires et homogènes pour toutes les parties prenantes. Une organisation doit savoir et être en mesure d'expliquer, dans un langage succinct et facile à comprendre, qui elle est, pourquoi elle se trouve là, ce qu'elle veut réaliser et comment elle maintient des rapports avec autrui.

La cohérence doit être à la fois externe et interne. Étant donné qu'aujourd'hui un plus grand nombre de personnes dans le monde ont accès aux médias internationaux, elles peuvent obtenir des informations sur une organisation par Internet ainsi que les actualités internationales et locales. Certaines communications peuvent être légèrement adaptées pour différents publics, mais

1 A. Donini et al., *Mapping the Security Environment : Understanding the Perceptions of Local Communities, Peace Support Operations and Assistance Agencies*) (Établir le profil du contexte de sécurité : Comprendre les perceptions des communautés locales, des opérations de soutien de la paix et des organisations d'aide) (Medford, MA : Feinstein International Famine Centre, 2005). p. 8.
2 Pour obtenir plus de détails à ce sujet, consulter M. Glaser, Humanitarian Engagement with Non-state Actors : The Parameters of Negotiated Access (Coopération humanitaire avec des acteurs non gouvernementaux : Les paramètres d'un accès négocié), HPN, Dossier thématique 51 (Londres : ODI, juin 2005).

le message global doit rester le même. Cela nécessite une cohérence interne, de sorte que le site Internet, un porte-parole au siège et un membre du personnel s'adressant aux médias locaux sur le terrain tiennent tous le même discours.

Tout le personnel, des hauts responsables aux gardes et chauffeurs, doit être en mesure de comprendre et de communiquer les buts et principes de l'organisation. Bien entendu, au quotidien le personnel subalterne aura probablement plus de relations avec les représentants du gouvernement, les acteurs armés aux barrages routiers et d'autres membres de la population locale. Rédiger une simple liste de questions et de réponses est un moyen de s'assurer que le personnel peut communiquer ces messages.

Parvenir à des accords formels

Les accords formels, par exemple avec le gouvernement ou avec certains groupes armés, sont utiles en ce sens qu'ils permettent une reconnaissance officielle et un accord explicite sur des sujets spécifiques. Mais ils peuvent aussi être problématiques s'ils ne sont valides que pour une période limitée, s'ils attirent l'attention sur des régions où les autorités pourraient tenter à tort de régir ou d'entraver les activités des organisations d'aide, ou encore si le temps qu'on leur consacre est excessif par rapport à ce qu'ils représentent.

Avoir des termes relativement généraux permet une certaine flexibilité, mais cela pourrait aussi faire plus de tort que de bien si cela donne à l'autre partie la possibilité d'ignorer ses responsabilités. En ce qui concerne la sécurité, les accords doivent énoncer clairement les responsabilités précises, notamment les procédures à suivre en cas de problèmes de sécurité. Mais attention : les accords écrits n'ont pas la même valeur dans tous les milieux sociaux. Par exemple, la parole d'honneur de la personne adéquate pourrait être plus importante. L'obligation qu'elle implique sera probablement observée plus strictement si tout le monde sait qu'une personne respectée a donné sa parole.

Conduire des réunions et avoir des relations sociales

Les messages sont communiqués non seulement lors de réunions mais aussi par le type de réunion qui a lieu. Qui demande la réunion, qui y est invité, où elle a lieu, quelle est l'attribution des sièges, sont des aspects bien connus de la diplomatie et jouent tous un rôle pour développer un certain type de relations. Convoquer des anciens de la communauté au bureau de l'organisation par exemple, plutôt que d'aller leur rendre visite dans leur propre environnement, transmet un message différent. Des personnes pourraient venir au bureau pour faire des demandes qui rapidement se révèlent inacceptables, mais il pourrait être judicieux de passer plus de temps qu'il n'est nécessaire avec elles pour leur donner une réponse. Il est important de ne pas paraître brusque ou impoli. Ralentir, prendre le temps

de rencontrer et d'avoir une conversation avec les gens, expliquer, écouter et en général faire preuve de politesse et de respect élémentaires peut être important pour obtenir l'acceptation.

Entretenir des relations sociales pour développer des rapports cordiaux et personnels est une pratique courante en diplomatie : les représentants du gouvernement sont invités à des dîners ou à des soirées privés chez le représentant de l'organisation, et les membres du personnel de l'organisation peuvent accepter l'hospitalité d'un chef de tribu, qui fera tuer une chèvre ou un mouton en leur honneur. Créer des relations demande plus que des réunions rares, brèves et non officielles. Un accord formel pourrait n'être qu'une simple feuille de papier s'il n'y a pas d'autre contact pour entretenir la qualité des relations. Parallèlement, avoir des relations sociales ne doit pas compromettre la distance essentielle que les organisations doivent garder si de réels problèmes surgissaient.

Négocier et faire des déclarations publiques

Prêtez attention aux différents styles de relations et de négociations des divers groupes sociaux. Les membres du personnel national pourront être particulièrement utiles car ils auront généralement une connaissance plus approfondie que les personnels expatriés. S'ils sont de la même région, ils comprendront peut-être aussi la langue locale, les messages non verbaux et les codes de comportement social. Pour vous préparer à d'importantes réunions, posez-vous les questions suivantes. Que sait-on des interlocuteurs ? Quelles positions et arguments seront-ils censés utiliser ? Quelle sera la position de l'organisation ? Quel style et quelles tactiques adoptera-t-elle ? Dans certains contextes, il pourrait être conseillé de demander à un expatrié de communiquer les messages et les décisions susceptibles de déplaire à un interlocuteur. En effet, l'expatrié pourrait être moins influencé par les pressions et les intimidations et serait probablement moins susceptible de représailles qu'un membre du personnel national. Avant les négociations, précisez clairement les rôles de chacun.

Les déclarations publiques de prise de décisions sont rarement reçues avec gratitude. Il est important d'envisager :

- Les raisons de faire des déclarations publiques plutôt que de communiquer des messages plus discrètement.
- Si le destinataire du message doit être informé avant de communiquer le message au public (aussi).
- Comment formuler la déclaration : qu'est-ce qui peut être documenté et étayé si l'on était questionné et est-il possible d'utiliser une formulation moins provocatrice ?

- Si possible, contrôlez la version finale qui sera rendue publique : par exemple, il est plus facile de contrôler le contenu d'un communiqué de presse écrit qu'une conférence de presse qui autorise les questions, ou encore qu'une interview en direct.

Attention aux déclarations « divulguées » : une déclaration « en confidence » sera-t-elle réellement gardée confidentielle ? Les déclarations confidentielles faites dans un forum ouvert, par exemple lors d'une réunion de coordination inter organisations, le resteront-elles ? Toutes sortes de raisons peuvent expliquer pourquoi une déclaration pourrait être plus ou moins déformée lorsqu'elle est divulguée.

3.2.2 Gérer les perceptions

Les aspects politiques du profil général du personnel

Le profil du personnel est important du point de vue de la sécurité pour deux raisons : il influence la façon dont l'organisation est perçue et donc les rapports que la population aura avec elle ainsi que l'ampleur des contacts et des canaux d'informations informels que l'organisation pourra établir et maintenir.

Dans certains contextes de conflit, il pourrait être nécessaire de nommer des membres du personnel international aux postes clés, sinon il sera difficile d'être considéré avec neutralité et impartialité. Dans d'autres cas, il pourrait être judicieux d'écarter certaines nationalités, par exemple, certaines ONG ne placeraient pas des citoyens américains, britanniques et autres dans leurs programmes en Irak en raison des déploiements militaires dans ce pays. Dans un contexte où il existe des clivages ethniques, il pourrait être désirable de s'assurer que tous les groupes ou clans ethniques majeurs sont représentés parmi le personnel national. Ailleurs, des clivages importants peuvent exister, fondés sur les sympathies de certaines personnes pour l'un ou l'autre des partis politiques. Avoir un personnel tiré entièrement ou en grande partie d'un seul parti politique est mal avisé, mais cela pourrait ne pas être apparent jusqu'au moment où une crise politique éclate, comme cela a été le cas pour certaines ONG pendant l'agitation politique au Kenya en 2007-2008. Un autre clivage fréquent est celui qui existe entre des personnes issues d'un milieu urbain et celles issues d'un milieu rural. Cela peut créer des problèmes dans les endroits où les environnements urbains et ruraux constituent des milieux sociaux très différents et où les citadins peuvent être considérés comme des étrangers.

Le profil idéal des personnels de la mission est une combinaison justifiable de membres issus de divers groupes. Lorsque cela n'est pas possible, essayez de créer une présence opérationnelle équilibrée composée de différents groupes et, si possible, ayez un personnel varié au bureau central de la capitale du pays où vous opérez. Une stratégie de combinaison justifiable à des fins d'acceptation

(pour des raisons programmatiques et sécuritaires) peut primer sur une politique de recrutement fondée uniquement sur les compétences et l'égalité des chances. Autrement dit, une organisation pourrait intentionnellement rechercher des personnes appartenant à une certaine catégorie, ou donner la préférence à ces personnes, même si elles ne sont pas les mieux qualifiées. Si votre personnel est issu de différents groupes entre lesquels il existe des tensions ou même un conflit déclaré, attendez-vous à ce que ces tensions soient présentes aussi dans l'organisation. Ce n'est pas quelque chose à éviter à tout prix, mais à gérer de manière constructive.

Apparence et comportement

L'apparence est importante. Les styles de coiffure, les ornements corporels et la façon de s'habiller peuvent avoir d'importantes significations sociales et politiques. L'apparence comprend les boucles d'oreilles, les tatouages, le maquillage, le style de lunettes et la pilosité sur le visage, de même que les vêtements et quelles parties du corps ils couvrent ou révèlent. Bien qu'un comportement inapproprié ne constitue pas en lui-même une menace, il pourrait aggraver des suspicions et des tensions existantes et pourrait être un terrain propice pour ceux dont l'objectif est de créer de l'animosité. N'oubliez pas :

- Quel type de comportement est considéré comme approprié ou inapproprié dans un milieu social/culturel particulier et quelles connotations possibles il a avec la position, le sexe et l'âge. Par exemple, dans certains milieux sociaux, certaines catégories d'homme sont censées faire preuve d'une très grande assurance. D'autres environnements sociaux mettent en exergue le besoin de faire preuve de sang-froid et de maîtrise de soi.
- Beaucoup de milieux sociaux comportent des normes implicites sur la consommation de stimulants tels que l'alcool. Si sa consommation n'est pas désapprouvée, son acceptation est généralement limitée à des endroits, heures et occasions particuliers. Accepter la consommation d'alcool ne doit pas être confondue avec accepter l'ébriété, surtout en public. Consommer de l'alcool avec d'autres personnes peut être un rite important, mais les consommateurs seront censés pouvoir garder le contrôle (et bien entendu le risque de parler ou d'agir de manière inappropriée augmente au fur et à mesure que la maîtrise de soi diminue).
- Exprimer la colère ou l'irritation en public donne toujours lieu au mécontentement et peut être provocateur. Dire non avec fermeté ne fera généralement aucun mal si cela est fait correctement et poliment. Mais l'arrogance, réelle ou ressentie, tend à créer du ressentiment.
- Se montrer distant (se tenir à l'écart dans la voiture, au bureau, avec de nombreuses barrières et garde-barrières) peut aussi être mal perçu mais cela doit correspondre aux politiques organisationnelles concernant les déplacements et la sécurité du site (voir les chapitres 8 et 9).

Dimensions du genre

Un grand nombre de sociétés patriarcales expriment leur intégrité morale et communautaire par la « pureté » des femmes, dont les codes d'habillement et de comportement constituent un indicateur fort. En période de conflit, lorsque les identités de groupes sont souvent redéfinies ou réaffirmées, ces codes peuvent être appliqués encore plus fermement. Le port de shorts, de jupes courtes, de chemisiers à col ouvert et de chemises sans manches peut être jugé provocateur et offensif et provoquer au mieux la désapprobation, au pire le harcèlement sexuel, voire plus. Le personnel féminin doit garder ces considérations à l'esprit. Cependant, les hommes aussi doivent se demander si la façon dont ils s'habillent inspire le respect ou au contraire si elle est perçue comme irrespectueuse.

Il est également important d'être attentif et prudent au sujet des normes sociales qui régissent les relations hommes / femmes en dehors de la famille immédiate. Il en va de même avec les notions d'espace public et d'espace privé. Beaucoup de milieux sociaux ont des codes plus restrictifs sur la manifestation d'un comportement intime en public, comme se tenir la main, s'enlacer et s'embrasser. Au Pakistan, par exemple, une ONG a été mise en garde « nous n'approuvons pas que vous logiez votre personnel masculin et féminin dans la même enceinte », et l'ONG a donc construit un mur pour séparer les hommes des femmes.

Considérations culturelles et religieuses

Dans de nombreux contextes, les normes culturelles et religieuses nécessiteront une attention toute particulière. Au Sri Lanka, par exemple, il est jugé irrespectueux d'utiliser une image ou une statue de Bouddha en fond d'une photo de quelqu'un. Bien que ce type de comportement inapproprié ne donne pas nécessairement lieu à une menace, il pourrait aggraver des suspicions et des tensions existantes. Les organisations religieuses doivent être particulièrement prudentes dans la gestion de leur profil et envisager des mesures de sécurité supplémentaires pendant les périodes de tensions religieuses.

Activités de programme

Il est important de se demander si les programmes renforcent la sécurité ou augmentent le risque. Une question importante est de savoir si le travail est effectué sur une échelle suffisamment grande pour être utile à la population affectée. Un autre élément à examiner est comment les programmes qui ne sont pas strictement vitaux, notamment ceux qui ont pour objectif d'effectuer des changements sociaux au sens large, peuvent être perçus. Cela inclut, par exemple, les projets qui soutiennent l'autonomisation des femmes dans les sociétés traditionnelles, ou ceux qui ne répondent pas aux besoins les plus

urgents, comme une campagne de vaccination dans une région souffrant de forte insécurité alimentaire. Comprendre ces questions nécessite d'écouter la population et de réagir en conséquence. Même si un programme est accepté par une grande partie de la communauté, il peut aussi mécontenter d'autres parties prenantes locales. Cela est vrai dans pratiquement tous les secteurs. Par exemple, un programme d'aide alimentaire pourrait contrarier les commerçants locaux en réduisant leurs profits ; fournir des services de santé gratuits pourrait éloigner les patients des centres de santé qui fournissent des soins payants, et aller à l'encontre des représentants locaux de la santé ; enregistrer les menaces contre la protection de la population pourrait rendre furieux les responsables de la violence.

Une autre considération à prendre en compte est la stratégie de sortie. Souvent, les organisations dirigent de bons programmes, mais une stratégie de sortie mal exécutée compromet l'attitude favorable qui avait été développée pendant la durée du programme. Cela signifie que les organisations pourraient devoir faire face à une tâche ardue si elles retournent dans la région pour offrir de l'assistance après une autre catastrophe.

3.2.3 Difficultés d'acceptation

Dans certains contextes opérationnels, la poursuite d'une approche d'acceptation peut être particulièrement difficile. Les difficultés sont entre autres :

- Les contextes profondément fragmentés, avec une multitude d'acteurs armés, où les chaines de commandement et de contrôle ne sont pas claires (p. ex. certaines parties de l'est de la RDC, le Darfour, la Somalie et l'Afghanistan).
- Les contextes où les acteurs armés accumulent des avantages stratégiques grâce au chaos et à l'instabilité (p. ex. l'est de la RDC, l'Afghanistan et l'Irak).
- Les contextes où il y a une profusion d'acteurs internationaux (militaires, politiques, humanitaires) et où l'on juge que tous les étrangers ne font qu'un (p. ex. l'Afghanistan, l'Irak et certaines parties du Pakistan).
- Les contextes où le gouvernement et/ou les acteurs armés et parfois même les communautés rejettent ou se méfient de ceux qui ont des liens avec l'Occident ou avec les interventions qui en émanent, y compris les organisations humanitaires (p. ex. l'Afghanistan, l'Iraq, certaines parties du Pakistan, la Birmanie, la Corée du Nord et le Zimbabwe).
- Les périodes de grand changement dans les rôles et positions des acteurs armés gouvernementaux et non gouvernementaux (p. ex. l'Irak après la défaite du régime de Saddam Hussein en 2003 et certaines parties de l'est de la RDC après l'intervention du Rwanda en 2009).
- Les environnements urbains où le taux de criminalité est élevé (p. ex. Port Moresby, Nairobi, Johannesburg ou Haïti).

- Les contextes où il existe des bandes locales ou des réseaux de crime organisé cherchant à protéger les lieux où ils opèrent (p. ex. les trafiquants de drogue en Colombie)

Environnements difficiles pour l'acceptation

Dans certaines parties du monde, l'acceptation générale des organisations (occidentales) humanitaires est devenue plus problématique car aujourd'hui ces organisations sont vues en tant qu'instruments de la politique étrangère occidentale ou de ses valeurs. Le cas le plus évident est celui où la « guerre contre le terrorisme » a eu lieu (Irak, Afghanistan, certaines parties du Pakistan). Mais c'est aussi le cas ailleurs : le gouvernement sri lankais éprouve, depuis longtemps, une grande méfiance envers les organisations d'aide étrangères (notamment envers les Nations Unies) par rapport à son conflit avec les Tigres de libération de l'Eelam tamoul ; les autorités birmanes se méfiaient de l'influence des organisations d'aide étrangères après le cyclone Nargis ; et le gouvernement de Mugabe au Zimbabwe rend périodiquement difficile la présence et les programmes des organisations d'aide occidentales. Au Soudan, la méfiance du gouvernement envers les organisations internationales a augmenté et les restrictions qu'il leur impose se sont durcies après la mise en examen du président Omar al-Bashir par la Cour pénale internationale en 2009.

La façon dont une organisation est perçue peut également porter sur les sources de son financement. La suspicion que ceux qui contrôlent l'argent exercent tous les pouvoirs se répand de plus en plus. Cela crée d'importants problèmes pour la grande majorité des organisations qui dépendent, au moins en partie, de financements gouvernementaux. Cela sera d'autant plus sensible si le gouvernement financeur est est un belligérant dans le contexte particulier.

L'acceptabilité de nombreuses organisations internationales d'aide a également été compromise par les efforts de certains gouvernements occidentaux pour combiner leurs stratégies humanitaires et leurs stratégies militaires. Dans la période qui a précédé l'invasion de l'Irak en 2003, par exemple, des hauts officiers américains ont fait des déclarations dépeignant les ONG comme des instruments de politique étrangère, des « multiplicateurs de force » et des sources de renseignements. Cela a incité certains dirigeants irakiens à déclarer que les organisations humanitaires étaient des ennemis de l'islam. Plus généralement, lorsque des armées étrangères mettent en œuvre des projets d'assistance, cela contribue aux perceptions locales que les organisations et les armées d'aide ne sont qu'une et même entité.

Périodes de changement rapide

Dans son analyse des attaques qui ont eu lieu en Irak et en Afghanistan, une organisation d'aide a conclu que, dans les deux situations, elle n'avait pas

été consciente des implications d'un changement rapide et profond dans les rôles et places des acteurs. Dans les deux pays, les acteurs avec lesquels l'organisation avait traité ont rapidement adopté des rôles d'opposition, en même temps que de multiples nouveaux acteurs sont apparus sur la scène. Dans les situations de profond changement, le fondement d'une stratégie d'acceptation peut souvent disparaître, tout au moins temporairement, et les contacts et relations devront être reconstruits. Dans l'intervalle, les organisations feront probablement face à une période de risque plus élevé, pouvant nécessiter l'adoption d'une plus forte protection et peut-être même d'approches de dissuasion, ou elles pourraient compter beaucoup plus sur la coopération avec des acteurs locaux. Le champ du travail humanitaire pourrait également être réduit.

Objections juridiques

Dans certains contextes, les gouvernements hôtes, de même que les gouvernements donateurs étrangers, pourraient ne pas souhaiter que des organisations négocient l'accès et l'acceptation avec des groupes armés non gouvernementaux ou autres. Les gouvernements hôtes pourraient désapprouver ou décourager de telles négociations, et la législation anti-terroriste pourrait imposer des pénalités aux organisations qui nouent le dialogue avec des groupes jugés être des acteurs terroristes, y compris les TLET au Sri Lanka, le Hezbollah au Liban, le Hamas en Palestine, Al-Shebab en Somalie, le parti communiste au Népal et l'Armée de Résistance du Seigneur en Ouganda. Pourtant, il pourrait être très difficile d'éviter ces groupes s'ils ont des liens étroits avec la population locale et ont un fort soutien local, ou lorsqu'ils contrôlent une région donnée. Cela a été le cas pendant les guerres au Liban et à Gaza en 2006, au cours desquelles de nombreuses ONG, en particulier celles qui étaient financées par les USA, éprouvaient des difficultés pour faire face à des conditions de terrorisme.[3] Les organisations qui décident d'accepter un financement avec des clauses antiterroristes devront veiller à prendre toutes les mesures raisonnables pour les respecter, y compris contrôler les nouvelles recrues et maintenir de bons systèmes de surveillance financière, sans compromettre la mission humanitaire. À plus long terme, le plaidoyer avec les gouvernements donateurs pourrait conduire à une plus grande clarté dans ce qui demeure un domaine ambigu du droit.

Le plaidoyer et exprimer son opinion

Rechercher et préserver l'acceptation peut exiger que les organisations restent silencieuses au sujet des abus des droits de l'homme. Faire entendre sa voix pourrait créer des risques de sécurité sur le terrain ou entraîner l'expulsion de l'organisation. Cela place les organisations devant un dilemme moral évident : une organisation pourrait se sentir obligée de s'exprimer contre les

3 Voir K. Thorne, « Terrorist Lists and Humanitarian Assistance » (Listes de terroristes et aide humanitaire), *Humanitarian Exchange*, nº 37, 2007

abus, mais au risque d'écourter son assistance et à l'avenir de ne plus pouvoir agir contre les abus. À quel moment, et sur quels critères, une organisation doit-elle décider de ne *pas* faire passer l'acceptation au-dessus de toute autre considération ? Bien que chaque situation doive être jugée selon ses mérites, il sera utile d'élaborer un ensemble de consignes permettant de structurer les questions et d'évaluer les considérations clés les unes par rapport aux autres. Si la décision est de faire entendre sa voix, il faudra en tenir compte par rapport à des besoins de sécurité. Une bonne politique organisationnelle n'est jamais de faire n'importe quelle déclaration publique sur une situation particulière sans avoir préalablement reçu le feu vert de ses collègues sur le terrain.

3.2.4 Indicateurs d'acceptation

Il n'existe pas de moyen simple de savoir comment une organisation est perçue et si (et pourquoi) elle est acceptée. Cela est d'autant plus vrai dans les situations où la population est divisée. Mais il est important de tenter d'évaluer cela, plutôt que de présumer que l'organisation est acceptée. Des signes positifs d'acceptation sont si les acteurs ou groupes locaux :

- Collaborent activement aux activités de l'organisation (p. ex. les communautés locales accueillent une clinique mobile ou en aident la logistique), ou les groupes armés laissent passer le personnel de l'organisation aux postes de contrôle pour lui permettre d'atteindre les zones du programme.
- Avertissent l'organisation que quelqu'un a posé des questions à son sujet ou qu'une certaine menace est probable.
- Aident à obtenir la liberté d'un membre du personnel victime de rapt ou à récupérer des biens volés.
- Expliquent ce qui les gêne dans le programme, chez son personnel ou chez un sous-traitant local.
- Admettent qu'ils ne sont pas d'accord avec la politique étrangère du gouvernement du pays d'origine de l'organisation, mais peuvent faire la distinction entre l'organisation et le gouvernement de son pays.
- Identifient une différence positive entre l'organisation et d'autres organisations d'aide.
- S'excusent si des membres d'un groupe portent atteinte à l'organisation.

Si, à l'inverse d'autres organisations dans le même contexte opérationnel, une organisation ne subit aucun incident violent, cela pourrait indiquer qu'elle est acceptée mais cela pourrait aussi être une coïncidence. Il est donc préférable de ne pas se fier à cela comme indicateur. Il est utile aussi de garder à l'esprit que les interlocuteurs pourraient mentir, et prétendre accepter la présence d'une organisation uniquement si cela sert leurs intérêts. D'autres indicateurs comprennent la fréquence des réunions avec les parties prenantes clés ainsi que le niveau et la nature des relations avec les acteurs principaux. Essayez de

mesurer les niveaux d'acceptation (p. ex. haut, « pas suffisant », faible) par rapport aux types de critères d'objectifs énoncés plus haut : se fier à l'intuition n'est pas suffisant. Les évaluations de l'acceptation pourraient être incorporées dans les audits de sécurité sur le terrain ou dans les plans de sécurité nationaux.

3.2.5 Les implications pratiques de l'acceptation

L'acceptation a des implications pratiques sur le plan des ressources humaines, financières et administratives.

Besoins en ressources humaines

Une approche d'acceptation active nécessite un personnel ayant certaines compétences clés, entre autres :

- La capacité d'établir le profil des principaux acteurs et de créer un large réseau de parties prenantes.
- Une bonne compréhension de la mission et des valeurs de l'organisation.
- De fortes compétences diplomatiques et en négociation.
- Parler couramment la langue locale (c'est l'une des raisons d'obtenir la participation du personnel national) et d'excellentes compétences en communication.
- La capacité d'analyser l'évolution des conditions politiques et de sécurité.
- La capacité d'utiliser et de mettre systématiquement à jour les outils tels que les audits et plans de sécurité.

Beaucoup d'organisations se sont aperçues qu'en définitive, le succès d'une approche d'acceptation doit être la responsabilité du très haut personnel. Ces personnes doivent donc avoir non seulement les compétences requises mais aussi suffisamment de temps pour assumer leurs autres responsabilités. Au CICR, par exemple, le chef de délégation a la responsabilité essentielle d'établir et de maintenir l'acceptation et n'est pas censé passer du temps sur la gestion programmatique et financière détaillée. Dans de nombreuses ONG, en revanche, les hauts responsables sont principalement chargés de la gestion opérationnelle quotidienne. De ce fait, le travail en réseau externe est limité aux autorités du gouvernement, aux bailleurs de fonds et à d'autres organisations d'aide. Bien que cette différence soit en partie expliquée par la nature du mandat du CICR, qui est de promouvoir le droit humanitaire international, ainsi que sans doute par un niveau de ressources différent, elle reflète le haut degré de priorité que le CICR donne au maintien de la sécurité opérationnelle dans les contextes dangereux.

Implications financières et administratives

L'acceptation n'est pas sans frais. Les coûts opérationnels sont considérables et comprennent entre autres :

Exemples de ressources humaines nécessaires pour obtenir l'acceptation

Le CICR avait une équipe de trois à cinq personnes à temps complet chargée de créer des relations et des communications externes pour retrouver l'acceptation en Irak et dans les pays voisins après le bombardement du siège de l'organisation à Bagdad en 2003.

Une organisation médicale qui travaillait dans la région depuis plusieurs années a déployé du personnel pour visiter plusieurs pays du Moyen-Orient et rencontrer un large éventail de personnalités politiques, de dirigeants sociaux et religieux ainsi que d'hommes et de femmes d'affaires pour expliquer le travail de l'organisation ou renforcer la compréhension qu'ils en avaient. Cela a généré un large réseau de contacts.

- Le temps du personnel, notamment le recrutement de personnel de sécurité supplémentaire, l'action de proximité ou les responsabilités médiatiques.
- La formation du personnel sur la façon de communiquer la mission et les valeurs de l'organisation, sur la communication interculturelle et sur les compétences en diplomatie et en négociation.
- Les déplacements supplémentaires nécessaires (véhicules, carburant, temps du personnel) pour rencontrer les parties prenantes.
- La traduction des documents ou des messages organisationnels dans les formats et langues appropriés aux lieux concernés.
- L'utilisation de la radio et de la télévision locales, le cas échéant.
- Le temps supplémentaire nécessaire durant la phase de conception d'un programme (parfois appelé « Plan de gestion de profil ») ce qui, en terme de budget global, pourrait conduire à une réduction de l'impact et donnerait l'impression que le programme est plus cher qu'il ne l'est.
- S'approvisionner en biens locaux plus chers, employer de la main d'œuvre locale moins performante ou moins qualifiée (voir plus bas).
- Créer un kit de communication/d'information avec dépliants et documentation.

Il pourrait être utile d'identifier certains coûts dès le départ et d'étudier avec les donateurs comment les couvrir. Ceci est essentiel surtout parce qu'ils ne font pas nécessairement partie des coûts de sécurité traditionnellement définis, inclus dans le budget.

Poursuivre une approche d'acceptation pourrait nécessiter certains ajustements des règlementations administratives ou juridiques. Par exemple :

- Le règlement pourrait demander d'obtenir trois cotations et de choisir celle qui offre le meilleur rapport qualité-prix. Mais pour l'acceptation, il sera peut-être préférable de répartir les contrats sur différents secteurs de la population locale afin que celle-ci sente que les bénéfices sont partagés de manière équitable. De même, il pourrait être judicieux d'acheter localement, même si un fournisseur non local offre un meilleur rapport qualité-prix.
- L'organisation pourrait choisir d'avoir un équilibre de groupes ethniques ou d'utiliser du personnel de la région locale, même si initialement cela réduit globalement la qualité et l'efficacité. Cela demandera un ajustement des pratiques des ressources humaines.
- De nombreuses organisations ont pour politique de ne pas transporter des personnes qu'elles n'emploient pas. Cependant, ne pas emmener un enfant malade à l'hôpital dans un véhicule libre pourrait être difficile à justifier. Il pourrait être nécessaire d'inclure des exceptions dans une politique de non-transport, pour des raisons morales ou pour favoriser l'acceptation.

3.3 Protection

Une approche de protection s'efforce de réduire la vulnérabilité. Elle peut le faire de deux façons : soit en durcissant la cible soit en augmentant ou en réduisant la visibilité. Une approche de protection ne tente pas d'agir sur la menace (c'est-à-dire de la supprimer). Le risque est réduit uniquement en agissant sur la vulnérabilité de l'organisation.

3.3.1 Durcir la cible

Durcir la cible repose essentiellement sur des moyens physiques et sur des procédures qui réduisent la probabilité qu'une menace s'approche de la cible ou qui réduisent l'impact potentiel de la violence sur celle-ci.

Si des bureaux et des habitations (et leurs occupants) sont une cible potentielle, une protection physique peut être apportée, par exemple des murs d'enceinte, pouvant être surmontés de fil barbelé ; créer une zone interdite aux véhicules ; et installer des portails en fer et des barreaux en fer aux fenêtres. Les procédures de protection incluent contrôler l'accès des visiteurs et effectuer des contrôles aléatoires et des patrouilles. Si les attaques à main armée constituent une menace pendant les déplacements, des véhicules à carrosserie dure ou blindés pourraient être appropriés. Tout comme un gilet pare balles ou un film de sécurité, ils ne réduisent pas la probabilité qu'une menace atteigne la cible mais peuvent réduire l'impact des balles et des explosions. Il en est de même pour les abris anti bombes et les murs de protection contre les tireurs d'élite. Pour de plus amples renseignements sur les mesures spécifiques de gestion et d'atténuation des menaces, voir Partie V.

Une tactique courante est « le nombre fait la force » : rouler en convoi, par exemple, ou loger le personnel dans des lotissements où les maisons sont proches les unes des autres. « Le nombre fait la force » peut être une tactique très efficace dans un grand nombre de contextes dangereux, mais elle n'arrêtera pas un attaquant bien déterminé, et pourrait être contre-productif. Rouler en convoi ou regrouper les bureaux pourrait représenter une cible plus importante pour un agresseur éventuel voulant maximiser l'impact avec une seule attaque. De même, bien que l'équipement de communication comme les radios et téléphones puissent être très efficaces, cet équipement coûteux pourrait aussi attirer l'attention. L'utilité d'un bon système de communication sera également limitée à moins qu'une force d'intervention rapide ne soit disponible à l'autre bout de la ligne. Un avertissement par la lumière et le son (p. ex. des projecteurs allumés par des détecteurs de mouvement ou des sonneries d'alarme à l'extérieur d'un bâtiment) avant une attaque peut permettre au personnel de prendre des mesures d'évitement (aller dans une pièce sûre, sortir discrètement) ou de demander une assistance immédiate. Mais, ici aussi, ces dispositifs n'empêcheront pas nécessairement un incident de se produire.

3.3.2 Programmes discrets/à faible visibilité

Diriger des programmes discrets est une tactique de protection de plus en plus courante dans les organisations d'aide. Cette tactique implique le retrait du nom et du logo des bâtiments qui abritent les bureaux, des véhicules, des lieux de résidence et des membres individuels du personnel. Elle peut aussi nécessiter d'utiliser des voitures ou des taxis privés, en particulier des véhicules qui ne se distinguent pas du contexte local, de limiter les déplacements et de retirer les équipements révélateurs, tels que les radios VHF ou les téléphones satellites et les antennes HF. Dans certains contextes à très haut risque, tout ce qui peut associer le personnel à une organisation – clés USB, documents d'identité de l'organisation, téléphones mobiles, ordinateurs – peut être « aseptisé ». Le personnel susceptible de se distinguer parmi la population locale, peut être redéployé. En Irak, des mesures plus radicales ont été prises, entre autres l'utilisation de fausses identités par le personnel, travailler sans adresse opérationnelle fixe et ne pas être informé de l'identité de ses collègues. On cachait intentionnellement aux bénéficiaires la source de leur assistance.

Une autre option pour être discret consiste à utiliser des logos amovibles (c.à.d. magnétiques) pour les véhicules, pouvant être retirés dans les zones où la visibilité est déconseillée. Savoir quand montrer un logo et quand le retirer demande une très bonne évaluation dynamique des risques locaux. Une ONG travaillant dans les Territoires palestiniens occupés et en Israël, par exemple, a donné instruction à son personnel de retirer les logos lorsqu'il travaillait dans les camps de réfugiés, où il est connu que le risque d'être victime d'un rapt est très élevé, mais de mettre le drapeau de l'organisation

en évidence pour passer aux postes de contrôles ou dans les zones où il y a un risque d'incursion militaire israélienne. N'oubliez pas qu'il est facile de voler les logos magnétiques et de les utiliser pour se faire passer pour des membres de l'organisation.

Une approche discrète/de faible visibilité pose de grandes difficultés. Elle peut compliquer la programmation, en particulier dans les cas extrêmes, et peut éloigner l'organisation de sources d'information qui pourraient autrement renforcer sa sécurité. Elle pourrait aussi donner lieu à des suspicions et à des perceptions erronées de ce que l'organisation fait, ce qui nuirait à son acceptation. C'est aussi une approche difficile à maintenir si l'organisation recherche une plus grande reconnaissance de son travail de la part du public ou des bailleurs de fonds. En général, les organisations ne considèrent pas une approche discrète comme un moyen permanent d'opérer, mais plutôt comme un moyen exceptionnel et limité dans le temps. Elle peut aussi être adoptée dès le début d'un programme, puis peu à peu atténuée au fur et à mesure que les opérations s'intensifient. Cette approche a été par exemple utilisée dans des zones tribales du Pakistan.

3.4 Dissuasion et protection armée

La dissuasion signifie utiliser une contre-menace : essentiellement, décourager des agresseurs éventuels en faisant naître la crainte des conséquences qu'ils pourraient subir. Dans le secteur humanitaire, le terme sécurité opérationnelle humanitaire est devenu, pour beaucoup, synonyme d'utilisation de protection armée - la forme de dissuasion la plus forte utilisée par les organisations. Il existe, pourtant, d'autres moyens de dissuasion, que cette section aborde brièvement avant d'entamer un examen en profondeur de la protection armée au cours des opérations humanitaires. La décision d'adopter une protection armée demande une mûre réflexion. Même lorsqu'une force est de petite taille, faiblement armée et a reçu l'ordre d'utiliser ses armes uniquement pour l'autoprotection, l'utilisation potentielle de puissance de feu introduit une différence qualitative dans la stratégie de sécurité. Elle a également une profonde influence sur l'image et la perception des organisations humanitaires en général.

3.4.1 Formes de dissuasion autres que la force armée

Moyen de pression juridique et diplomatique

Le droit national et, dans une certaine mesure, le droit international prévoient certaines protections juridiques pour les travailleurs humanitaires. Malheureusement, dans la plupart des circonstances, essayer d'influencer avec des arguments juridiques n'est pas toujours très efficace. Les organisations d'aide internationales pourraient obtenir un soutien de gouvernements donateurs étrangers, en particulier pour résoudre des problèmes administratifs

avec les gouvernements hôtes ou pour en négocier l'accès, mais des relations étroites avec les gouvernements donateurs peuvent compromettre l'apparence d'indépendance et de neutralité. Il est important, lorsque l'on contacte ou sollicite les gouvernements donateurs ou étrangers de renforcer les principes humanitaires de neutralité, d'indépendance et d'impartialité.

Suspension des opérations ou retrait

Face à certaines menaces ou après des incidents de sécurité, les organisations ont parfois suspendu temporairement leurs programmes d'aide, ou menacé de le faire. La continuation ou la reprise du programme s'effectue ensuite à condition que le problème soit résolu ou que la situation ait été améliorée. Selon des observations empiriques, cette tactique n'obtient pas toujours de très bons résultats et les organisations reprennent souvent leurs programmes sans aucune amélioration manifeste, ce qui compromet leur crédibilité et rend moins plausible toute menace similaire faite par la suite.

Une suspension ou la menace d'une suspension pourrait être efficace dans les circonstances suivantes :

- Elle n'est pas essentiellement perçue comme une punition pour la population civile qui n'est pas liée aux causes d'insécurité et qui n'est pas en position d'améliorer la sécurité.
- Un segment influent de la population ou le pouvoir local peut être mobilisé au nom de l'organisation.
- Les organisations sont prêtes à maintenir la suspension jusqu'à ce que la situation soit résolue de manière satisfaisante et n'annuleront pas la décision trop rapidement en raison de pressions internes ou externes à l'organisation.
- D'autres organisations ne réduisent pas l'efficacité de l'action en intervenant pour combler le vide. Un front commun doit être établi avant la suspension des opérations.

Sauf si l'incident est très grave, une suspension sélective (p. ex. dans un lieu donné ou pour une période donnée) ou la réintroduction progressive des services pourrait fournir une plus grande marge de manœuvre. Une suspension totale a tendance à créer une situation difficile de « tout ou rien ».

Une autre option de dissuasion est de forger une alliance avec des hommes forts de la région. Dans le Nord-Caucase, par exemple, une organisation louait des bureaux et des logements appartenant à un puissant homme d'affaires de la région. Il était manifeste, sans déclaration explicite, qu'une attaque contre l'organisation serait une attaque contre lui et son clan, ce qui constituait une sorte de stratégie de dissuasion implicite. Cette option doit être adoptée

avec précaution car vous pouvez aussi devenir le jouet de la protection d'une éminence grise.

3.4.2 Protection armée : la question fondamentale

La protection armée et l'action humanitaire ne font pas très bon ménage. Bien qu'en réalité quasiment toutes les organisations d'aide aient utilisé, à un moment ou à un autre, une forme de protection armée, les discussions à ce sujet sont extrêmement délicates. Cette section fournit un cadre plus systématique pour aborder le sujet. Ceci n'est pas censé être un argument en faveur de l'utilisation de protection armée. Il est possible, à chaque étape du raisonnement, de conclure que la protection armée pourrait ne pas être une option valable. Toutefois, avant de procéder, tenez compte du fait qu'envisager une protection armée pourrait indiquer que le seuil de risque acceptable a déjà été franchi et que la réelle décision devrait être de se retirer ou de ne pas entrer dans la région en question. Si ce seuil n'a pas encore été atteint, ou si la protection armée peut potentiellement réduire le risque à un niveau plus acceptable, trois grands domaines entrent en jeu pour examiner la situation : les principes, le contexte et la gestion.

Questions de principe et autres considérations

Les questions suivantes doivent être étudiées :

- L'organisation a-t-elle une objection de principe à l'utilisation de la force, quelles que soient les circonstances ?
- Les avantages d'utiliser une protection armée dans ce contexte l'emportent-ils sur les risques ?
- Y a-t-il de sérieuses inquiétudes quant à la gestion d'une protection armée, et ces inquiétudes peuvent-elles être surmontées ?

Certaines personnes affirment que la protection armée va à l'encontre des principes fondamentaux de l'action humanitaire. Cette position est en général fondée sur des considérations éthiques ou opérationnelles à long terme. L'argument éthique soutient que l'action humanitaire n'est jamais compatible avec l'utilisation de la force. Dans une perspective idéologique, une organisation peut refuser une protection armée parce que son utilisation, par principe, contribue à la production et à la distribution continues d'armes. Une perspective plus conditionnelle pourrait porter moins sur la production d'armes proprement dite que sur leur prolifération incontrôlée, autrement dit la perte d'un monopole de la répression de la violence par les autorités responsables de la sécurité et de l'ordre public.

La considération opérationnelle à long terme est que si, dans un contexte spécifique, une protection armée peut être justifiable, elle fragilise l'image

globale de l'action humanitaire dans le monde et pourrait donc donner lieu à une plus grande insécurité ailleurs ou plus tard. Selon ce raisonnement, avoir recours à une protection armée trop rapidement ou trop souvent compromet les efforts globaux visant à rétablir le respect du droit humanitaire international et de l'action humanitaire indépendante.

Il y a également des considérations pratiques. Avec une escorte armée, le travail humanitaire est beaucoup moins flexible sur le plan des mouvements, car les autorisations et les escortes doivent souvent être organisées à l'avance. Cela doit être pris en compte dans la conception du programme. Une plus grande prévisibilité des mouvements peut rendre une organisation plus vulnérable aux attaques, surtout si les escortes ne sont pas totalement dignes de confiance.

Bien qu'il soit incontestable que l'autorisation et l'acceptation soient les meilleurs moyens d'obtenir une sécurité de base, les arguments moraux pourraient ne pas suffire ; même les États démocratiques et pacifiques ont besoin d'une force de police et de sécurité pour assurer le respect de la loi et des droits fondamentaux de leurs citoyens. Dans certains contextes, l'utilisation d'une protection armée pour faciliter la prestation d'aide pourrait être une fonction de l'État assumant ses obligations conformément au droit humanitaire international. Les arguments en faveur de l'utilisation d'une protection armée sont que celle-ci peut être acceptable en dernier recours, dans le cas où la vie de personnes serait mise en danger si l'assistance était écourtée (voir, par exemple, le Comité permanent inter agences et les directives des Nations Unies).[4]

Un autre aspect important est de savoir qui bénéficie de la protection armée : s'agit-il uniquement de l'organisation d'aide et de son personnel, ou la protection peut-elle bénéficier à un plus grand public et donc renforcer la sécurité publique ? L'utilisation d'armes et de gardes armés, peut-être recrutés localement, aura-t-elle un effet apaisant sur la situation locale ou bien augmentera-t-elle les tensions ? Contribue-t-elle à la « privatisation » de la sécurité, selon laquelle ceux qui en ont les moyens peuvent acheter la sécurité tandis que d'autres doivent vivre dans la peur? Met-elle indirectement d'autres personnes en danger en faisant d'elles des cibles plus faciles ? Dans des environnements où le taux de criminalité est extrêmement élevé, les escortes et les gardes armés peuvent être largement utilisés. Par exemple,

4 IASC, Civil–Military Guidelines and Reference for Complex Emergencies (Directives et références civiles-militaires pour les contextes d'urgence), 7 mars 2008 ; Directives sur l'utilisation des ressources militaires et de la protection civile étrangères dans le cadre des opérations de secours en cas de catastrophe, Nations Unies, novembre 2006 (révision novembre 2007) ; Directives sur l'utilisation des ressources militaires et de la protection civile dans le cadre des situations d'urgence complexes (Directives MCDA), mars 2003 (révision janvier 2006).

entre l'aéroport et la ville de Lei en Papouasie-Nouvelle-Guinée (une distance de 10 à 15 km), les travailleurs humanitaires voyagent dans des véhicules adaptés appartenant à une société de sécurité, escortés par des gardes armés. Bien que cela soit inévitable, il est important d'envisager quel effet ce moyen a, le cas échéant, sur l'environnement de sécurité au sens large.

Même si l'utilisation de protection armée est jugée nécessaire et légitime, il pourrait ne pas être éthiquement correct ou pratique de payer les services de prestataires, de groupes ou de personnes privés (plutôt que d'utiliser la protection de forces de police ou militaires mandatées par l'État ou par la communauté internationale, qui pourrait être fournie gratuitement). Suite aux cas d'escroquerie en matière de protection chez les gardes de la milice somalienne dans les années 1990, certains travailleurs humanitaires ont affirmé que les organisations humanitaires ne devraient jamais payer pour une protection armée. La réalité est que la plupart l'ont fait.[5] Dans certains pays, la force de sécurité étatique est inefficace et les organisations humanitaires ont fourni un soutien matériel à l'État, par exemple des véhicules ou en payant un service d'escorte. Dans le nord du Kenya, par exemple, les organisations d'aide couvrent les frais de véhicules et de carburant des escortes de police armées.

Questions de contexte

Si le seuil de risque acceptable n'a pas été franchi et qu'une protection armée n'est pas exclue par principe, une autre série de questions spécifiques au contexte doit être posée. Quelles sont les menaces et d'où proviennent-elles ? La protection armée est-elle la seule et la meilleure réponse possible ? La protection armée réduit-elle ou augmente-t-elle le risque ?

Il faut noter qu'à certains endroits, par exemple en Amérique Latine, l'utilisation de protection armée est dictée par les pratiques de sécurité en vigueur localement. Les ONG utilisent des gardes armés simplement parce que « tout le monde le fait ». Dans ces cas-là, ne pas adopter cette pratique pourrait nécessiter un dialogue inter organisations plus large et une action commune.

Nature et origine des menaces

De quoi ou de qui la protection armée est-elle supposée vous protéger ? D'où proviennent les menaces et pourquoi ? La question de protection armée se pose souvent lorsqu'il y a un risque d'assassinat envers le personnel humanitaire, de rapt, de vol à main armée ou d'embuscade et de vol ou de destruction de convois de l'aide. Des distinctions importantes peuvent être faites entre les menaces liées à la sécurité du lieu et celles liées à la sécurité

5 A. Stoddard, A. Harmer et V. DiDomenico, The use of Private Security Providers and Services in Humanitarian Operations (L'utilisation de prestataires et de services privés de sécurité dans les opérations humanitaires), GPH Rapport 27 (Londres : ODI, 2008). Voir Annexe 4 pour un exposé détaillé sur les prestataires de sécurité privés.

des déplacements ainsi qu'entre les menaces spécifiquement dirigées vers l'organisation (son personnel et ses biens) et celles dirigées plus généralement vers les populations dans le besoin. Une analyse plus approfondie permettra certainement de savoir ce qui constitue la menace et pourquoi.

Les menaces ou incidents pourraient survenir parce que les opérations de l'organisation ne sont pas perçues comme étant neutres. Une protection armée pourrait renforcer cette perception. Une approche pourrait être de viser un positionnement politique « neutre » et mieux équilibré. Une plus grande diffusion d'informations sur l'organisation et sur la façon dont elle opère ainsi que des efforts plus actifs aideront à obtenir le consentement et l'acceptation. Si cela est impossible, des options autres que la protection armée pourraient encore être envisageables. Si de nouveaux véhicules tout terrain sont la raison des ciblages, utilisez des véhicules ordinaires d'occasion. Au Darfour, certaines organisations ont utilisé des charrettes tirées par des ânes pour transporter des biens afin de minimiser le risque de détournement de voiture. Si les convois et entrepôts des organisations internationales sont une cible parce qu'ils sont en dehors du « système social », utilisez des commerçants et négociants locaux qui sont « dans le système ». Si les étrangers sont la seule cible de rapt, un personnel national pourrait diriger le programme, en supposant qu'il ne court pas un risque égal ou plus important, et que le risque est transféré de manière responsable.

Même dans les cas où une protection armée semble justifiée, elle pourrait ne pas constituer un moyen de dissuasion raisonnable, ou pourrait accroître le risque. Par exemple, si des cambrioleurs soupçonnent qu'un résident possède une arme à feu, ils pourraient devenir violents s'ils sont surpris en flagrant délit. Si des bandits sur la route voient un convoi armé, ils pourraient tirer avant de le piller. Si une protection armée est fournie par les forces du gouvernement ou par une faction particulière, l'organisation pourrait devenir une cible légitime aux yeux de l'opposition armée. Il y a également le risque d'accidents avec des « tirs amis » ou des armes maniées sans précaution ou ne fonctionnant pas correctement.

Bien que la protection soit la décision individuelle d'une organisation, son utilisation possède également des implications pour d'autres ; bien entendu, un bon principe opérationnel est que la population ne fasse pas la différence entre différentes organisations d'aide ou même entre les ONG et les NU. Une organisation ayant une protection armée aura une influence sur l'image et la perception de toutes les organisations humanitaires. Cela sera une influence potentielle sur l'acceptation et les relations de toutes ces organisations. C'est un sujet qui mérite une réflexion et une discussion structurées entre organisations. Adopter une politique commune est, de loin, préférable à la discorde.

Maintenir la distinction entre l'organisation et sa protection armée

Une règle élémentaire pour maintenir une distinction dans la perception entre l'organisation et les forces armées qui la protègent est que les hommes armés qui protègent les convois voyagent dans des véhicules séparés. Les armes ne doivent pas être introduites dans les locaux ou les véhicules de l'organisation d'aide et les travailleurs humanitaires ne doivent pas porter de vêtements qui ressemblent à ceux des forces armées. Les organisations d'aide n'utiliseront pas les ressources des forces de sécurité (les camions, les véhicules blindés, les hélicoptères) et les forces de sécurité n'utiliseront pas les ressources de l'organisation. Si cela est absolument inévitable, le bien en question doit être repeint et une nouvelle inscription doit y être apportée de manière à ne représenter que son propriétaire actuel. Les gardes armés peuvent également être exclus de l'enceinte de l'organisation, mais cela pourrait réduire leur efficacité en cas d'attaque. Si la menace porte sur le rapt ou l'assassinat, des gardes du corps armés devront exercer une « protection rapprochée ». Selon le contexte spécifique, ces mesures aideront ou pas à maintenir une distinction dans la perception et permettront à l'organisation de préserver en partie son image civile et de non-combattant.

Dans les contextes dangereux, les organisations ont tendance à penser à des mesures qui renforceront leur propre sécurité. Il pourrait être utile de se demander si la sécurité pourrait être améliorée de façon plus générale et comment. Par exemple, des gardes armés dans un camp de réfugiés pourraient être déployés de façon à protéger non seulement le personnel de l'organisation mais aussi les femmes refugiées risquant d'être agressées sexuellement lorsqu'elles vont chercher de l'eau et du bois de chauffage. Un système pourrait être instauré selon lequel les gardes armés de plusieurs organisations individuelles patrouilleraient dans le quartier et renforceraient donc la sécurité pour tous. En cas de présence d'une opération de maintien de la paix par les NU dont le mandat est de protéger les civils, des troupes peuvent être déployées dans des zones dangereuses pour protéger aussi bien les travailleurs humanitaires que la population locale. Pendant l'intervention suite au tremblement de terre d'Haïti en janvier 2010 par exemple, les USA et les NU ont fourni une protection armée au cours de la phase initiale de distribution alimentaire.

Il est également important de se demander qui fournit la protection armée. Les sources incluent l'armée nationale, la police nationale, un groupe de résistance armé, les Casques bleus et la police des NU, la milice locale, des sociétés de sécurité privées et des gardes armés employés par l'organisation.

Dans certaines circonstances, une organisation non opposée, par principe, à l'utilisation de la force, pourrait constater qu'aucun des prestataires potentiels n'est acceptable ni efficace, et devoir choisir entre opérer sans protection ou se retirer. Les questions à se poser lorsque l'on envisage un prestataire sont, entre autres :

- Quelle est la position politique du prestataire dans un conflit donné - autrement dit, pensera-t-on que l'organisation prend parti si elle a des relations avec un acteur particulier ?
- Quelles sont l'image publique et la réputation du prestataire ? Par exemple, si l'armée ou la police nationale est généralement perçue comme un instrument de répression et d'exploitation, ou si une faction armée a une réputation de brutalité envers les civils, utiliser leur « protection » pourrait endommager l'image publique de l'organisation.
- Est-il important, pour le prestataire, de fournir une protection à une organisation d'aide par rapport à ses autres objectifs ? Le prestataire pourrait avoir un autre programme (par exemple nouer le dialogue avec l'ennemi ou appréhender un criminel) qui, à des moments cruciaux, pourrait primer sur l'attention portée à la sécurité de l'organisation ou même la compromettre.
- Le prestataire est-il professionnel ? Les gardes sont-ils bien formés, raisonnablement rémunérés, ont-ils un équipement en bon état de fonctionnement, leurs ordres sont-ils clairs, sont-ils bien supervisés et disciplinés ? Un personnel mal payé et mal formé peut faire plus de tort que de bien.
- Quel degré de contrôle et de gestion l'organisation souhaite-t-elle ou doit-elle avoir ? Les forces de sécurité nationales, les groupes rebelles ainsi que les Casques bleus et la police des NU, par exemple, conserveront leur propre chaine de commandement. Une milice recrutée, des sociétés de sécurité privées ou des gardes employés par l'organisation pourraient être plus étroitement gérés par l'organisation. Avoir une autorité plus directe sur les prestataires de protection armée permet un meilleur contrôle mais rend également l'organisation directement responsable de leur comportement et de leurs actions.

Questions de gestion

Questions essentielles à se poser sur la gestion :

- Les politiques, procédures et compétences de gestion internes nécessaires pour gérer cette relation sont-elles disponibles ?
- Quelles sont les mentions contractuelles nécessaires ?
- Qui maintient le commandement et le contrôle et qui détient l'autorité et la responsabilité, et de quoi ?

Les questions de gestion interne pourraient inclure :

- Qui, au sein de l'organisation humanitaire, prend les décisions/approuve l'utilisation d'une protection armée ?
- Quelles connaissances et quelle expérience les responsables devront-ils avoir ?
- Comment les offres sont-elles rédigées et comment les offres des prestataires privés de sécurité locaux sont-elles évaluées ? (voir Annexe 4)
- Quelles demandes de renseignements peuvent être faites concernant le professionnalisme et l'intégrité d'un prestataire de services potentiel ?
- Les critères de sélection des gardes peuvent-ils être vérifiés ?
- Qui, dans le bureau national, a la responsabilité quotidienne de gérer les gardes, et cette personne a-t-elle les compétences et l'assurance nécessaires pour le faire ?

Les mentions contractuelles comprennent :

- Les critères de sélection des gardes, comme l'âge, l'état de santé, l'alphabétisme, l'interdiction de consommer de l'alcool ou de la drogue et l'interdiction d'avoir un autre emploi (tout au moins si cela entraîne une perte de sommeil).
- Les exigences essentielles des chefs et niveaux minimums de supervision.
- Les normes minimales de recrutement et de formation supplémentaire en cours d'emploi sur, entre autres, des sujets de base tels que le droit local et le pouvoir d'arrestation, les incendies et les menaces liées aux explosifs, la tenue de registres, l'évacuation des bureaux, les procédures de fouille des véhicules et de fouille corporelle, la fouille des colis et du courrier et les soins de premier secours.
- Si le service fourni inclut une unité d'intervention rapide pour appuyer les escortes ou les gardes en cas de menace ou d'incident grave, tous les autres accords devront alors être applicables à ce personnel et à ses actions. Vérifiez qui fait partie de la force et si les instructions adoptées sont transmises clairement à tous.
- Le besoin de protection armée n'est pas constant et les contrats peuvent être annulés de manière soudaine. Énoncez clairement les critères et procédures relatifs à la résiliation précoce des contrats ou des accords. Des contrats à court terme et renouvelables donnent une plus grande flexibilité mais pourraient être plus onéreux.
- Il existe des règles juridiques qui régissent la responsabilité et la compensation en cas d'échange de tirs provoquant des blessés ou des morts, mais dans certaines situations le droit coutumier sera appliqué. Qui est responsable si un garde, un assaillant ou un tiers est blessé ou tué dans un échange de tirs ? La responsabilité de l'organisation peut-elle

se limiter aux actions qui sont strictement couvertes par les termes de l'accord ou qui sont effectuées sous ordres ?
- Les rémunérations doivent être étudiées avec soin. Les gardes travaillent souvent pendant de longues heures, ont des horaires contraignants et font un travail pouvant être dangereux. Un salaire trop bas pourrait engendrer un mauvais niveau de performance.

Une autre question essentielle concerne le commandement et le contrôle : sous quelle autorité les gardes sont-ils placés, qui a le pouvoir de commandement, qui est chargé de leur discipline ? Si les forces de sécurité externes fournissent une protection armée, quelle est l'autorité relative de leur commandant par rapport à celle du responsable de l'organisation ? Qui, par exemple, détermine les règles qui régissent l'utilisation de la force mortelle et qui s'assure que les gardes les ont entièrement comprises ? La règle de base sera probablement que la force ne peut être utilisée que pour protéger la vie en cas de menace évidente et pendant la durée de la menace. Autrement dit, la force mortelle peut être utilisée uniquement comme moyen de défense et non pas, par exemple, pour tirer sur un cambrioleur, même s'il est armé, qui s'enfuit et qui ne constitue plus une menace immédiate. Ce qui constitue une menace immédiate de mort et une menace au bien-être devra être évoqué concrètement, en imaginant différents scénarios.

Les règles d'engagement pour la protection des biens devront aussi être clarifiées. Une organisation pourrait instinctivement préférer que la force soit utilisée uniquement lorsque seuls des biens sont en danger, mais est-il acceptable de ne pas réagir lorsqu'un entrepôt est vidé ou lorsque tous les aliments d'un convoi sont volés par des hommes armés, surtout si des personnes ont réellement besoin de ces approvisionnements et en sont vraiment tributaires ? L'utilisation d'armes à feu ne serait pas autorisée pour éviter le vol d'un portefeuille ou d'un téléphone portable, mais qu'en est-il de biens de plus grosse valeur, comme les véhicules et les ordinateurs ? Fixez une limite et expliquez clairement où elle est. Un autre point important est de convenir des procédures et des approches. Il est conseillé d'étudier, puis de clarifier et de se mettre d'accord sur les procédures à adopter dans un certain nombre de scénarios possibles, par exemple que faire si un visiteur refuse d'être fouillé ou insiste pour faire entrer ses propres gardes armés, et jusqu'où aller dans la poursuite de voleurs ou d'agresseurs en fuite. N'oubliez pas non plus que le commandement et le contrôle vont dans les deux sens : si une organisation se place sous la protection d'un acteur armé, elle sera tenue de respecter ses règles. Quitter brusquement un convoi, s'élancer en tête ou s'éloigner au volant d'un véhicule ne sera pas accepté par le prestataire de l'escorte.

Dans une force multinationale de maintien de la paix, des armées de diverses nationalités ont en général différentes traditions et cultures, entre autres sur le plan du commandement et du contrôle, des règles d'engagement et de ce qui est jugé être une utilisation de la force appropriée ou excessive. Des entretiens approfondis avec les commandants sur le terrain pourraient être nécessaires pour s'assurer d'une compréhension commune. De même, l'armée nationale pourrait déployer différents contingents de troupes pour assurer la protection. Divers commandants auront des vues différentes, ce qui nécessitera un accord détaillé et écrit, rédigé en collaboration avec un haut responsable. Contrôlez cela pour vous assurer que les remplaçants sont pleinement informés.

En ce qui concerne les armements et autres équipements, il faudra parvenir à un accord sur :

- Qui fournit les armes (normalement, le fournisseur de personnel)
- Le type d'armement utilisé par les gardes (p. ex. pistolets, fusils ou pistolets mitrailleurs).
- Qui est responsable de fournir les munitions et de vérifier que les armes sont bien entretenues et correctement enregistrées.
- Qui est responsable de la fourniture d'équipement supplémentaire, comme les vêtements imperméables, torches et bottes adéquates.
- En général, les gardes armés ne viennent pas avec des véhicules. Il faudra donc décider si et quand ils peuvent utiliser les véhicules de l'organisation.

Orientations de politique

Les organisations doivent avoir une politique sur l'utilisation de protection armée. Les points importants à y inclure sont :

- Une clarification de la position de principe de l'organisation concernant l'utilisation de forces armées.
- Les conditions qui pourraient justifier l'utilisation d'une protection armée, par exemple pendant l'évacuation ou la relocalisation du personnel en période d'extrême insécurité. Ce point doit inclure des références au niveau du besoin humanitaire auquel l'organisation tente de répondre et le risque posé à son personnel et à ses biens. Précisez qu'il s'agit d'une option de dernier recours : toutes les autres options ont été étudiées et aucune autre solution appropriée ou adéquate n'a été trouvée pour ces circonstances.
- Les considérations et risques clés (juridiques, physiques et de réputation), à la fois pour l'organisation concernée et pour d'autres acteurs, au moment de choisir entre plusieurs prestataires potentiels et comment ils peuvent être évalués.

- Les termes devant être adoptés entre l'organisation et le prestataire.
- La procédure de l'organisation pour la prise de décisions et le bilan périodique.
- L'obligation d'accompagner l'utilisation de protection armée de plus grandes mesures de communication pour la justifier.

Ne confondez pas la politique sur la protection armée et la politique sur les sociétés de sécurité privées, même si ces dernières sont souvent les prestataires de protection armée. Une organisation pourrait utiliser des sociétés de sécurité privées à d'autres fins (p. ex. l'évaluation des risques et les audits de sécurité) et, dans toutes les opérations du monde entier, la protection armée n'est en aucun cas fournie uniquement par des sociétés privées.

Une politique possible

Selon la politique d'une organisation, la protection armée peut être envisagée quand :

- un grand nombre de vies sont en danger ;
- la menace n'est pas politique mais liée à la criminalité;
- le prestataire est acceptable ; et
- la dissuasion peut être efficace.

Chapitre 4
Évacuation, hibernation, gestion d'un programme à distance et retour

Bien que cela ne soit jamais un scénario plaisant, les circonstances exigeront parfois qu'une organisation se retire d'une région où il existe un haut niveau d'insécurité ou qu'elle limite la présence de ses programmes dans cette région. Ce chapitre aborde les principales réponses et modalités opérationnelles dans ces situations dites d'accès limité. Quatre scénarios de base sont à considérer : l'évacuation ou la relocalisation, l'hibernation, la gestion de programmes à distance et le retour.

L'évacuation et la relocalisation font référence au retrait physique du personnel (et/ou de leurs familles) et des biens d'un contexte dangereux. L'évacuation indique généralement la traversée d'une frontière internationale, tandis que la relocalisation fait référence aux mouvements à l'intérieur d'un pays.[1] Ces déplacements peuvent être accélérés par une nouvelle éruption du conflit, une recrudescence de l'agitation, une attaque envers les organisations humanitaires par des groupes armés ou une catastrophe naturelle. Une évacuation peut également être forcée si l'organisation est expulsée par le gouvernement. L'hibernation implique l'arrêt des mouvements du personnel et des programmes sur le terrain ou de rester dans un ou plusieurs des sites de rassemblement, soit parce que l'évacuation est impossible ou trop dangereuse, soit parce qu'il est jugé que la situation est susceptible de s'améliorer prochainement. La gestion à distance concerne les programmes pour lesquels une organisation internationale a dû modifier de manière significative des modes opérationnels habituels en raison de l'insécurité. La gestion à distance fait parfois référence à tout type d'opération réalisée à distance (même si c'est un choix), mais cette RBP utilise le terme pour indiquer exclusivement une position réactive, imprévue, due à des conditions de sécurité qui se détériorent. Le retour désigne le processus selon lequel une organisation (ou une certaine catégorie de personnel, comme le personnel international) retourne dans une région de laquelle il avait été évacué ou relocalisé et reprend son travail habituel.

4.1 L'évacuation et la relocalisation

4.1.1 Quelques hypothèses courantes

Il est important de savoir qu'il existe quatre hypothèses sur l'évacuation et la relocalisation, mais qu'elles peuvent souvent induire en erreur.

1 Selon la situation géographique, un petit nombre de membres du personnel peut temporairement être placé de l'autre côté d'une frontière nationale, et il ne faut donc pas présumer que l'évacuation est nécessairement plus grave ou plus permanente que la relocalisation ; dans de nombreux cas, les termes sont utilisés de manière interchangeable.

1. La détérioration sera progressive

L'évacuation est envisagée en dernière mesure de réduction progressive à l'exposition, allant de la suspension des déplacements d'une certaine catégorie de personnel, à la suspension des opérations, au retrait partiel du personnel d'un lieu, et enfin au retrait total et à la cessation des activités. N'oubliez pas, cependant, que les événements peuvent dépasser les plans. Planifier les phases de la sécurité, bien qu'utile, peut donner l'impression de progression linéaire même si ce n'est pas toujours le cas (voir Chapitre 2 : « Évaluation des risques »).

2. L'évacuation s'effectuera comme prévu

Il est toujours utile de planifier, mais il est important de ne pas oublier que :

- les membres du personnel ne se réfèrent pas aux plans en cas de crise soudaine et grave ;
- des éléments importants peuvent avoir été oubliés dans la planification ;
- les choses ne se déroulent pas toujours comme prévu en raison d'acteurs et de facteurs externes ; et
- l'évacuation peut être forcée, par exemple lorsqu'une organisation est expulsée par les autorités du gouvernement. Cette situation nécessite un type différent de planification (voir Section 4.1.5 ci-dessous).

3. L'évacuation sera possible

Dans de nombreuses situations, les voies d'évacuation sont bloquées, la capacité logistique d'évacuer est insuffisante ou il devient tout simplement trop dangereux de tenter une évacuation et le personnel doit donc ne pas bouger et faire face à la crise. Un trop grand nombre de plans de sécurité considèrent uniquement l'évacuation, négligent l'option de relocalisation et n'envisagent pas l'hibernation.

4. Le retour sera possible

Le personnel évacué ne pourra peut-être pas retourner rapidement sur le lieu de travail et l'organisation pourrait se retirer du contexte ou effectuer une gestion des programmes à distance pendant des semaines, des mois ou même des annnées.

4.1.2 La décision de se retirer

Décider de rester ou de partir

La relocalisation et surtout l'évacuation sont des décisions difficiles - pas seulement d'un point de vue programmatique mais aussi d'un point de vue éthique. Il est difficile d'allier l'impératif humanitaire et le besoin d'assurer la sécurité du personnel. Si la mission exige la prestation de services, il peut être tentant de rester si cela peut être fait utilement et si les normes peuvent être maintenues. Rester peut aussi démontrer la solidarité envers une

population en danger et peut maintenir une présence pour la surveillance et le témoignage.

D'autres facteurs peuvent influencer la décision de rester ou de partir :

- Les procédures internes de l'organisation exigent que le retour sur le lieu d'opération soit autorisé par le siège, ce qui peut limiter l'attrait d'un retrait rapide ou temporaire.
- Les pressions pour mettre en œuvre un projet, de crainte de perdre le financement futur d'un bailleur de fonds.
- Des membres du personnel sur le terrain ne perçoivent pas l'augmentation des risques ou pensent que leur présence est justifiée pour l'impact du programme ou même pour la sécurité de leur propre emploi.
- Une inquiétude que des retraits répétés ou trop rapides puissent compromettre l'acceptation.

La tentation sera de différer la décision jusqu'au dernier moment, lorsque la situation sera si claire que l'hésitation ne sera plus permise. Cette stratégie comporte de grands risques, car les événements pourraient changer rapidement et le retrait pourrait devenir impossible. Partir avant que quelque chose ne se produise rend généralement le retour plus facile que lorsque l'évacuation a été forcée suite à un grave incident de sécurité. Les bonnes pratiques impliquent l'installation d'éléments déclencheurs ou d'indicateurs du retrait avant que la situation devienne critique (voir Chapitre 2 pour plus de recommandations sur la décision de rester ou de partir). Veillez également à étudier la possibilité d'un retrait temporaire, préventif, par exemple extraire le personnel de certains lieux avant des événements politiques qui pourraient avoir un dénouement explosif, comme une élection controversée ou l'annonce de résultats électoraux.

Le pouvoir décisionnel

Il faut bien préciser non seulement dans quelles conditions une organisation évacuera les lieux ou se relocalisera, mais aussi qui a l'autorité finale de cette décision.

- Cette décision appartient-elle au siège international ou au directeur national ? Que doit-on faire si les opinions divergent ?
- Un responsable de programme ou de bureau dans une base provinciale peut-il prendre la décision de relocaliser son personnel sans l'autorisation préalable du représentant de l'organisation dans la capitale ?
- Si le plus haut responsable sur le terrain s'est déjà retiré, qui a l'autorité d'ordonner le retrait d'un plus grand nombre de personnes ou de tout le personnel restant ?

- Est-il bien précisé à tout le personnel que les décisions prises par la direction sont impératives ?

Des recommandations pour mettre en place une équipe chargée de la gestion d'une évacuation ou d'une relocalisation, sont données au Chapitre 5 : « Signaler un incident et gérer un incident critique ».

Considérations inter organisationnelles

Les évacuations en temps de crise grave nécessitent en principe une collaboration entre organisations, pouvant être compliquée par des appréciations différentes du risque (voir Chapitre 2 : « Évaluation des risques »). Le fait que certaines organisations évacuent les lieux et d'autres pas, pourrait réellement changer le risque et augmenter la vulnérabilité de ceux qui restent. Il peut ne plus y avoir suffisamment d'organisations présentes, ce qui pourrait encourager le pillage, le vol et les attaques. Si une organisation compte sur le soutien des NU ou d'un gouvernement étranger, par exemple pour mobiliser des hélicoptères, des avions, un convoi ou un navire, qu'advient-il de son pouvoir décisionnel ?

Les politiques d'évacuation et de relocalisation

La présence des NU, d'ONG et de missions diplomatiques peut impliquer que la situation est tolérable en matière de sécurité et que les autorités locales et nationales ont un contrôle suffisant pour maintenir la sécurité des acteurs internationaux. Une évacuation donnera évidemment un message opposé, que les acteurs politiques – les autorités nationales ou locales, un gouvernement étranger ou un groupe de rebelles armés – pourraient vouloir éviter à tout prix. Gardez cela à l'esprit lorsque vous considèrerez les conseils d'acteurs politiques. La question est de savoir si les autorités locales (ou les groupes armés qui contrôlent la région) doivent être informées avant de décider de la sortie de l'équipe. Ne pas les avertir pourrait les indigner et compliquer les relations au retour de l'organisation ; en même temps, si les autorités sont informées, elles pourront tenter d'exercer une pression sur l'organisation pour la dissuader de partir.

4.1.3 Planifier et gérer le retrait du personnel

Établir une politique

En termes de relocalisation et/ou d'évacuation, la politique concernant le personnel doit être documentée et communiquée clairement au préalable. Dans la mesure du possible, les droits et responsabilités des employeurs et des employés doivent être énoncés dans les contrats d'emploi ou dans la politique de sécurité. Des recommandations explicites doivent être en place stipulant qu'en périodes de risque élevé, le personnel non essentiel sera relocalisé ou évacué de la région. Il faut indiquer clairement qui, parmi

les personnels, est considéré comme personnel essentiel et non essentiel et comment cette distinction sera faite au moment voulu (voir ci-dessous).

En ce qui concerne le personnel international, il faut énoncer clairement que le refus de quitter la zone sera considéré comme une démission et entraînera l'annulation immédiate du contrat d'emploi. De même, il est nécessaire de préciser qu'une personne a le droit de demander de quitter une zone dangereuse si elle a un sentiment profond d'insécurité. Notez que cela pourra entraîner des dépenses financières importantes, et devra donc être autorisé par la haute direction. En cas d'évacuation facilitée par une ambassade (p. ex. d'un pays européen ou nord-américain), sachez à l'avance quels membres du personnel rempliraient les conditions requises et s'ils choisiraient cette option plutôt qu'une évacuation agencée par l'organisation. En ce qui concerne les membres du personnel national, il faut préciser quels sont leurs droits et ceux des personnes à charge en matière de relocalisation (à l'intérieur du pays) et d'évacuation (à l'étranger). Ces droits seront fonction de la base d'opération stipulée dans leur contrat et de la probabilité que ces personnes soient directement ciblées (voir plus bas).

Retraits partiels : réduction de personnel non essentiel ou à haut risque

Envisagez un retrait partiel du personnel. Déplacer seulement une partie de l'équipe diminuera le risque et la responsabilité en termes de sécurité. En période de tension croissante, et dans le cadre de la procédure associée à une phase de sécurité spécifique, le personnel non essentiel doit être relocalisé. Le but de cette mesure préventive est de réduire la vulnérabilité globale en diminuant le nombre de personnes en danger, et de rendre ainsi une opération de relocalisation ou d'évacuation en temps de crise plus gérable.

Le personnel non essentiel comprend généralement toutes personnes non indispensables à la continuation du programme. Évaluez la probabilité que certains éléments du programme ou qu'un programme dans sa totalité puissent être maintenus. Pensez au personnel pouvant être à un échelon moins élevé mais ayant une fonction critique dans les situations d'urgence (p. ex. les spécialistes en logistique ou en communication). Envisagez aussi d'extraire le personnel exposé à des risques particulièrement élevés, qu'il soit « essentiel » ou pas. Certaines nationalités ou groupes ethniques ou religieux peuvent constituer une cible de choix potentielle. De même, dans certaines situations les femmes pourraient être exposées à un plus haut risque.

Un membre du personnel pourrait trouver difficile psychologiquement de réagir face à une insécurité croissante, ou pourrait se sentir en grand danger. Il pourrait s'agir d'un membre du personnel ayant un poste opérationnel clé. Cette personne devra probablement être déplacée, car maintenir des

personnes dans une situation qui se détériore peut, au bout du compte, causer plus de problèmes que leur départ prématuré.

Considérations relatives au personnel recruté à l'échelle nationale

L'évacuation ou la relocalisation soudaine d'homologues internationaux peut contrarier et irriter le personnel national. Le fait que l'organisation semble traiter le personnel international avec un plus grand égard pourrait engendrer du ressentiment et contredire ses affirmations d'égalité de traitement de tout son personnel. Le personnel national pourrait aussi ne se rendre compte que très tard des limites exactes des responsabilités de l'organisation en ce qui les concerne. Tout cela n'est pas nécessaire : dans le cadre du processus de planification de la gestion de la sécurité, le personnel national doit savoir précisément ce qu'il peut attendre ou pas afin de pouvoir prendre ses propres dispositions pour sa sécurité et celle des personnes à charge.

La plupart des organisations croient que leur obligation de diligence envers les membres du personnel national n'inclut pas généralement leur évacuation à l'étranger, puisqu'ils restent d'abord et avant tout citoyens du pays frappé par la crise. De part les limites financières, légales et pratiques auxquelles l'organisation est soumise, même si elle voulait évacuer son personnel national, il n'existe pas de solution simple pour combler l'écart entre ce qu'elle veut faire et ce qu'elle peut faire dans la pratique. Ceci dit, il existe des instruments légaux internationaux et des procédures nationales pour donner asile aux personnes ayant de réelles craintes de persécution. Les NU, par exemple, sont prêtes à considérer l'évacuation des membres du personnel recrutés à l'échelle nationale si leur vie est mise en danger de par leur emploi. De même, un employé d'une ONG internationale pourrait être persécuté pour ses liens avec l'organisation. Ce problème devient plus complexe lorsqu'une catégorie plus large de personnes est menacée. En 1994, au cours du génocide au Rwanda, un grand nombre de Tutsis et de Hutus modérés faisant partie des personnels d'organisations internationales ont été tués ; le personnel international, bien qu'exposé à un risque beaucoup moindre, a été évacué. Après 2003, les chrétiens en Irak ont été ciblés, surtout ceux travaillant pour des ONG internationales.

Les membres du personnel national pourraient travailler dans une base opérationnelle située dans une partie du pays autre que leur région d'origine, sur un territoire physiquement et socialement inconnu. Ils se retrouveraient alors dépourvus de leurs mécanismes de soutien habituels. Le personnel national relocalisé peut donc être exposé à de plus hauts risques. Si la relocalisation est une conséquence de leur emploi, l'organisation doit assumer la responsabilité de transférer ces personnes et leurs familles dans le lieu où elles ont été recrutées ou, si ce lieu n'est pas sûr non plus, dans une autre région ne présentant aucun danger.

Il serait malavisé de présumer que tout le personnel national souhaite partir. Certaines personnes pourraient souhaiter rester afin de protéger leur famille et leurs biens, ce qui soulève la question suivante : quelle aide, le cas échéant, ces personnes devraient-elles recevoir ? Un soutien pourrait inclure la fourniture de téléphones portables, de cartes d'appel prépayées, l'accès aux locaux de l'organisation pour elles et leurs familles ou des lettres d'emploi ou de référence. Dans de nombreuses circonstances, l'aide la plus pratique sera financière. Évoquez préalablement avec le personnel national s'il préfère une somme en monnaie locale ou étrangère ou une combinaison des deux. Le calcul d'un montant forfaitaire pour le personnel qui n'est pas officiellement licencié mais qui arrêtera de travailler en raison des risques de sécurité, peut être exprimé en termes de paiement continu pour vacances annuelles ou vacances exceptionnelles, d'indemnité de licenciement ou d'indemnité compensatrice de préavis non effectué. En fonction des moyens, des échelles de salaires et du coût de la vie, environ deux à trois mois de salaire permettront au personnel et aux personnes à charge d'avoir quelques réserves financières. Une autre option est de donner à tous la même somme forfaitaire quel que soit leur salaire. Afin d'effectuer ces paiements il pourrait être nécessaire de se procurer d'importantes sommes d'argent liquide, ce qui constitue en soi un risque (voir le chapitre 11 sur la sécurité de l'argent liquide). Dans les contextes à haut risque, cet argent peut être gardé en réserve dans un coffre-fort.

Personnel d'entretien, prestataires et consultants

Le personnel d'entretien employé par l'organisation est-il inscrit au registre du personnel ou est-il engagé en sous-traitance par des personnes individuelles (principalement des membres du personnel international) ? Quelle responsabilité l'organisation peut-elle assumer et assumera-t-elle ? D'autres personnes peuvent être embauchées en tant que prestataires ou consultants, par exemple les chauffeurs, les entrepreneurs ou les analystes locaux. En général ces personnes s'attendront à ce que l'organisation assume la responsabilité de leur sécurité, précisez donc bien, à la signature du contrat, ce qu'elles peuvent attendre de votre part et ce que vous ne pourrez pas fournir.

Organisations partenaires locales

Les organisations qui travaillent en étroite collaboration, sous contrat ou en partenariat, avec une organisation locale devront clarifier, à la signature du contrat ou du protocole d'accord, ce qu'elles jugent être leurs responsabilités et ce que les organisations locales peuvent attendre de leur part de façon réaliste. Cela pourrait être une formation sur la gestion de la sécurité et la participation de partenaires dans l'élaboration des consignes de sécurité communes.

4.1.4 Se préparer à être expulsé par le gouvernement : un cas particulier

Dans certains contextes, il pourrait être justifié de se préparer à un potentiel

retrait forcé, tel que l'expulsion ordonnée par le gouvernement. Cela pourrait être le cas lorsque des organisations de profile similaire ont récemment été expulsées, ou lorsqu'il y a lieu de penser que l'organisation pourrait être ciblée par un gouvernement hôte hostile. Les préparations seront en grande partie similaires à celles d'une évacuation provoquée par des risques de sécurité. Toutefois, posez-vous les questions suivantes :

- L'organisation tentera-t-elle d'intenter un recours contre la décision et si oui, par quel moyen (judiciaire, discussions directes avec les autorités, plaidoyer ou pressions dans le cadre d'un consortium, campagnes médiatiques, discussions avec les bailleurs de fonds ou les ambassades ?)
- Quelles mesures ont été prises pour empêcher que des informations potentiellement délicates, confidentielles ou personnelles ne soient divulguées par inadvertance (voir plus bas) ?
- L'expulsion exposera-t-elle le personnel national (ou autre personnel restant) à un danger spécifique ?
- Des mesures peuvent-elles être prises pour éviter que le personnel (en particulier le personnel national restant) ne soit harcelé ou menacé par les autorités gouvernementales ?
- Le personnel national recevra-t-il des salaires ou des indemnités de licenciement, cela devra-t-il être exigé par le gouvernement, et pendant combien de temps ?
- Le risque que les biens soient saisis définitivement peut-il être minimisé ?
- Quel pourrait être le rôle des gouvernements appuyant financièrement les programmes pour annuler la décision ou pour exhorter le gouvernement hôte à faire preuve d'une plus grande indulgence ?
- Quelle sera la réaction des médias (locaux et internationaux) et comment sera-t-elle reçue ?

4.1.5 Planifier et effectuer une évacuation ou une relocalisation

S'exercer pour une évacuation ou une relocalisation

Le plan d'évacuation/de relocalisation doit être régulièrement revu et examiné avec le personnel, surtout s'il est de plus en plus probable qu'un retrait sera nécessaire. Pour cela, des exercices de simulation[2] peuvent être effectués ou une simple réunion d'équipe peut être organisée pour revoir les politiques, procédures et plans. Au plus fort d'une crise, des membres individuels du personnel pourraient être tentés de prendre toutes sortes de mesures non prévues et d'aller à des endroits autres que les lieux de rassemblement prévus. La conséquence sera probablement une plus grande confusion, un retard dans l'évacuation et un risque plus important pour tout le monde. Aucune initiative individuelle qui s'écarte du plan ne doit être prise sans l'autorisation préalable du chef de l'équipe de gestion de la crise.

2 Tout exercice de ce type doit être effectué avec discrétion, de sorte à ne pas inquiéter d'autres personnes au sujet d'une évacuation imminente ou de l'existence d'une menace qu'elles ignorent.

Logistique et planification de l'itinéraire

Les questions clés sont :

- Quels routes et moyens de transport sont les plus utilisables dans différents scénarios ?
- Quel type de déplacement est le plus susceptible de réduire le risque : avec logos, drapeaux et antennes de radio mobile HF mis en évidence, ou discret sans aucun de ces signes apparents ?
- Combien de moyens de transport sont disponibles, pour combien de personnes ? Quels types de biens ou d'effets personnels peuvent être pris ?
- Qui fournit le transport (si ce n'est pas l'organisation elle-même, des dispositions devront être prises avec une autre organisation). Évoquez au préalable la capacité, les exigences des procédures et les limites de la responsabilité et des obligations de l'organisation. Cela nécessite une connaissance approfondie des politiques de l'organisation ou de l'auxiliaire de transport. Demandez dans quelles circonstances un avion charter privé (ou un vol EVASAN) ne prendra pas le personnel, malgré les accords préalables.

Beaucoup d'évacuations et de relocalisations dépendent de la collaboration entre différentes organisations. N'élaborez pas un plan seul. Bien qu'il soit généralement plus sûr de rouler en convoi avec d'autres ONG, cela implique aussi un moins grand contrôle de la façon dont l'évacuation est effectuée. Évoquez préalablement avec d'autres organisations si possible comment ces problèmes seront abordés.

Dans certains scénarios de relocalisation ou d'évacuation, le personnel devra peut-être conduire ou même marcher sur une longue distance. Dans d'autres, il devra aller du lieu de rassemblement, au port ou à l'aéroport par ses propres moyens. Veillez à prévoir la route au préalable à l'aide de cartes routières ou de schémas que vous aurez préparés. Vous devrez probablement explorer la possibilité d'utiliser des routes secondaires si celle qui avait été choisie est bloquée ou jugée trop dangereuse. Pensez également aux impératifs des différentes routes et à l'impact potentiel de diverses conditions climatiques. Il pourrait, par exemple, ne pas être possible de rouler jusqu'à la frontière et le personnel pourrait devoir marcher sur une longue distance, pendant même plusieurs jours. Soyez prêts, prévoyez des provisions et un équipement de marche.

Pour se préparer à une évacuation par voie aérienne, les coordonnées GPS, les images satellites du terrain (p. ex. Google Earth) et les renseignements sur la condition physique des pistes d'atterrissage doivent être obtenus au préalable, par informatique au siège ou par les sociétés de charter privées pour accélérer les options possibles de transport par avion.

Dans les lieux à haut risque où l'évacuation est probable ou a déjà été effectuée, des préparations plus avancées peuvent être faites. Par exemple, avant leur évacuation vers la Jordanie et le Koweït en 2003, un grand nombre d'organisations internationales travaillant en Irak avaient déjà ouvert un bureau dans ces pays.

Préparation des points de rassemblement

Identifier les lieux où les personnes qui seront relocalisées ou évacuées devront se rassembler avant l'évacuation. Ces lieux doivent être accessibles, sûrs, suffisamment grands pour loger de nombreuses personnes et plusieurs véhicules, et doivent être équipés de moyens de communication fiables et de stocks d'urgence (notamment des fournitures en médicaments et en carburant) pouvant être emportés lors de l'évacuation ou pouvant permettre au lieu de rassemblement de servir de lieu d'hibernation si l'évacuation se révélait impossible. Dans certains cas, les coordonnées GPS ainsi que les cartes indiquant les points de rassemblement pourront préalablement être partagées (ou même établies d'un commun accord) avec d'autres organisations ou avec les autorités nationales.

Préparations individuelles

Le siège de l'organisation et le responsable logistique doivent avoir des informations exactes et régulièrement mises à jour sur le nombre d'employés (et membres de leurs familles) qui remplissent les conditions requises pour une évacuation internationale. Les exigences spécifiques par exemple médicales, ou la présence de très jeunes enfants, doivent être indiquées. S'il est probable que l'évacuation internationale se fera vers un pays voisin, contactez les autorités de ce pays ou l'ambassade concernée et explorez la possibilité de maintenir des visas valides pour ce pays pour toutes les personnes pouvant être évacuées. Toutes les personnes concernées devront idéalement recevoir des avances en liquide ou une ou plusieurs cartes de crédit pour couvrir les frais initiaux jusqu'à ce que le flux de trésorerie de l'organisation soit rétabli.

Au cours d'une relocalisation ou d'une évacuation, les personnes entrant en ligne de compte n'ont généralement droit qu'à un ou plusieurs bagages n'excédant pas un poids maximum (en principe 5 à 10 kg). En périodes de haute tension, les membres du personnel devront toujours avoir un « sac d'évacuation » et les documents indispensables prêts. Les personnes devront prendre soin de leurs propres passeports ; ceux-ci ne devront pas être gardés dans le coffre-fort du bureau.

Dossiers et informations organisationnels clés

Certaines informations essentielles sont nécessaires pour faire un rapport aux bailleurs de fonds après l'évacuation et pour permettre un retour

à la base opérationnelle avec les informations adéquates une fois la période dangereuse passée. Ces informations comprendront les inventaires des biens, les documents comptables, les factures payées depuis le dernier rapport financier, les détails du registre du personnel, les contrats et les dettes non réglées, les protocoles d'accord, l'enregistrement et la correspondance fiscale avec les autorités nationales. Pour plus de renseignements sur la protection d'informations délicates, voir Chapitre 7 : « Gérer la sécurité des communications ».

Stocks, ressources et obligations financières

Clarifiez à l'avance quelles ressources doivent être emportées, lesquelles doivent être laissées, et ce qu'il adviendra du stock restant. Gardez une trace des obligations financières, par exemple envers les bailleurs, fournisseurs, prestataires, personnel et propriétaires de véhicules loués, et envisagez de les régler avant de partir. Si cela n'est pas possible, emmenez les documents à jour en vue d'une utilisation ultérieure.

4.1.6 Après l'évacuation ou la relocalisation

Un certain nombre de mesures immédiates et pratiques doivent être prises après une relocalisation ou une évacuation :

- Dès la première opportunité, contactez le siège et communiquez-lui les dernières nouvelles détaillées concernant le personnel, la sécurité, les finances et les déplacements imminents prévus.
- Si l'évacuation a été faite dans un pays étranger, contactez à l'arrivée les représentants de ce pays (si cela n'a pas déjà été fait par le siège ou avant votre arrivée), ainsi que les ambassades concernées et les autorités locales si le séjour est susceptible d'être prolongé.
- Établissez ou rétablissez le contact et la communication avec le personnel qui est resté sur place (voir plus bas).
- Dans le cas d'une évacuation internationale, envisagez qui peut utilement rester dans la région (s'il s'agit d'un pays voisin) et qui devrait rentrer chez soi (en vacances annuelles ou en fin de contrat).
- Organisez des locaux à moyen terme (pour les bureaux et lieu de résidence) et l'accès aux ressources financières.
- Préparez un rapport destiné au siège et aux bailleurs de fonds, contenant les dernières nouvelles détaillées concernant le personnel, les ressources, les stocks et les finances ainsi que les dettes non réglées au moment de l'évacuation.
- Interrogez le personnel évacué et fournissez-lui un soutien psychologique, car l'évacuation engendrera probablement diverses émotions pénibles. Cela peut inclure un épuisement émotionnel et un sentiment d'échec, de colère et de culpabilité envers ceux qui sont restés sur place.

Planifier la continuation du programme

Il est possible de demander au personnel national de poursuivre le programme. Il est impératif que cette situation soit planifiée et communiquée en détail au préalable. Soyez attentifs aux points suivants :

- L'attribution des tâches et des responsabilités. Les domaines clés comprennent la gestion financière, l'administration, la sécurité, les communications internes et externes, la gestion du personnel, la logistiques, les activités du programmes et l'écriture de rapports.
- Les limites de la responsabilité. Il faut préciser très clairement que le bien-être du personnel prime et que les employés ne doivent pas s'exposer au risque en tentant de sauver les ressources d'une organisation.
- Les limites de l'autorité. Les employés peuvent-ils acheter ou vendre des biens, recruter et licencier du personnel ou prendre des mesures disciplinaires, signer de nouveaux contrats, communiquer avec les autorités ou décider d'apporter des modifications au programme, par exemple ? Quels aspects nécessitent une autorisation préalable et que doit faire le personnel si la communication est interrompue pendant une période prolongée ?
- Les nouvelles dispositions pourraient aussi influer sur d'autres acteurs, y compris d'autres organisations, les ambassades concernées, les autorités locales et la banque. Le contexte, la taille et la visibilité du programme en cours dicteront si les nouvelles dispositions doivent être communiquées sur une large distance et à un grand public. Le personnel national pourrait être plus vulnérable aux pressions, à l'intimidation et aux menaces, auquel cas la discrétion serait sans doute conseillée.
- Un protocole de communication avec les représentants de l'organisation.
- Un calendrier de l'examen et de la révision de ces dispositions.

N'oubliez pas que la relocalisation ou l'évacuation pourraient durer beaucoup plus longtemps que prévu et pourraient entraîner une programmation à distance ; voir plus bas pour des orientations supplémentaires.

4.2 L'hibernation

4.2.1 Les scénarios de l'hibernation

L'hibernation dans une zone dangereuse peut être volontaire ou forcée. L'hibernation volontaire peut être une bonne option lorsque rester sur place est plus sûr que de partir, ou lorsque l'on a besoin de temps pour évaluer la capacité de partir (mais n'oubliez pas que l'hibernation peut aussi exposer le personnel au risque : le fait qu'une organisation et ses ressources n'ont pas été ciblées lors de crises précédentes ne signifie pas qu'elles ne risqueront

jamais rien). L'hibernation forcée peut résulter d'un déroulement rapide d'événements qui ne pouvait pas être anticipé ou peut être imposée si le retrait devient impossible (p. ex. l'avion prévu n'arrive pas). L'hibernation forcée pourrait signifier que le personnel est confiné dans le même bâtiment pendant des heures, des jours ou même des semaines d'affilée.

4.2.2 Se préparer pour l'hibernation

Si possible, identifiez et équipez plus qu'un local pour une retraite ou une hibernation. Les besoins physiques à long terme incluent :

- de la nourriture, de l'eau et des médicaments essentiels (notamment un kit de traitement prophylaxie post-exposition ou PPE (voir le chapitre 12 sur l'agression sexuelle) ;
- des installations pour le repos, les besoins sanitaires et la ventilation ;
- du carburant et un équipement pour faire la cuisine ; et
- un éclairage, comme des bougies, des lampes de poche et des lampes tempêtes.

Il faut aussi tenir compte des besoins psychologiques à long terme ; dans la mesure du possible, essayez de fournir des livres et des jeux, des moyens supplémentaires pour être en contact avec le monde extérieur (radio, télévision, téléphones) et un espace pour faire de l'exercice tous les jours.

Il est essentiel d'avoir des moyens de communication avec le monde extérieur, par une combinaison de radio, téléphones mobiles / satellites et Internet. Cela nécessitera une alimentation électrique permanente, comme par exemple des piles rechargeables. Gardez à l'esprit le fait que les générateurs peuvent être bruyants et attirer les pilleurs. En cas de pillage, l'une des choses les plus précieuses à préserver sont les moyens de communication. Essayez de bien cacher une radio et une antenne ou un téléphone satellite dans un endroit où on ne pourra pas les trouver même si le local est complètement dévalisé.

Considérez la possibilité d'avoir des pièces de sécurité ou des abris anti-bombes si les bombardements sont un risque possible. Une pièce de sécurité n'a ni porte donnant sur l'extérieur du bâtiment ni fenêtres. Demandez conseil à des experts techniques qualifiés car les pièces de sécurité et les abris anti-bombes peuvent être dangereux s'ils ne sont pas construits selon les normes adéquates. Ces recommandations doivent couvrir toutes les considérations pratiques telles que la communication (n'oubliez pas que les téléphones satellites doivent être connectés par câble à une antenne externe), l'accès à l'électricité ou aux générateurs et les sanitaires.

4.3 Gestion de programmes à distance

4.3.1 Qu'est-ce que la gestion de programmes à distance ?

La gestion de programmes à distance, pratiquée par la plupart des organisations, est en principe une situation réactive plutôt que planifiée, en raison de mauvaises conditions, de détérioration ou d'autres restrictions existant dans le contexte opérationnel. Elle peut inclure :

- Le retrait du personnel international ou d'autres catégories de personnel, en particulier les personnes jugées être exposées à un risque particulièrement élevé sur le lieu du programme.
- La modification des structures de gestion afin de donner une plus grande responsabilité au personnel national et/ou local qui reste sur place.
- La création de nouvelles mesures opérationnelles avec les partenaires locaux, notamment les ONG, les organisations communautaires et les autorités locales.

Différents termes sont utilisés pour décrire divers types de gestion de programmes à distance. Le « contrôle à distance », la « gestion par contrôle à distance » ou « la gestion à distance » peuvent faire référence à des situations où la même structure de gestion reste en place, autrement dit le personnel international maintient sa pleine autorité décisionnelle. Dans cette RBP, la gestion de programmes à distance est utilisée comme terme générique et fait référence à tous les systèmes décrits plus haut. Le terme « programmes à accès limité » est également utilisé, mais cela fait référence à une gamme de problèmes beaucoup plus large que la sécurité, notamment les restrictions imposées par le gouvernement et l'isolement physique. La gestion de programmes à distance indique l'adaptation opérationnelle causée *spécifiquement* par l'insécurité.

La gestion des programmes à distance n'est pas un phénomène nouveau. Pendant la Guerre froide, les organisations de solidarité ont fourni une aide directement aux mouvements de résistance (en Érythrée, en Éthiopie et en Afghanistan dans les années 1980), sans grande surveillance de la part du personnel international. À la fin des années 1990, une grave détérioration dans la situation de sécurité a forcé les organisations humanitaires à relocaliser leurs bases opérationnelles et leur personnel international de Tchétchénie en Ingouchie puis en Ossétie du Nord. À la fin 2003 et en 2004, un grand nombre d'organisations ont relocalisé leur personnel international de certaines parties d'Irak vers Amman en Jordanie. Plus tard, la détérioration des conditions de sécurité en Afghanistan et au Pakistan a nécessité la mise en place d'une gestion à distance. La gestion des programmes à distance est également utilisée depuis plusieurs années en Somalie, au nord de l'Ouganda, à Gaza, au Sri Lanka, en Colombie et au nord du Soudan.

Cette approche est de plus en plus courante non seulement en raison de l'augmentation des risques auxquels sont exposés les travailleurs humanitaires (y compris le personnel international), mais aussi en raison des progrès rapides dans le domaine des transports et surtout de la technologie de la communication. Il est plus facile que jamais, grâce aux téléphones cellulaires, aux téléphones satellites et à l'Internet de maintenir des contacts réguliers avec le personnel national ou avec des partenaires basés sur le terrain ainsi que de contrôler les programmes. Une ONG internationale travaillant par le biais d'organisations partenaires en Irak a récemment fermé ses bureaux à Amman et gère aujourd'hui ces partenaires depuis le Liban et le Royaume-Uni.

4.3.2 Les défis de la gestion de programmes à distance

La gestion de programmes à distance est souvent une adaptation de dernier recours et ponctuelle. De ce fait, elle présente en général de grandes difficultés. Celles-ci peuvent inclure :

- Des problèmes éthiques concernant le transfert des risques, en particulier si l'on demande aux membres du personnel ou aux partenaires locaux qui assurent les responsabilités d'un programme, de prendre des risques plus élevés. L'argent qu'ils peuvent gagner rend pratiquement impossible de refuser cette opportunité.
- Des difficultés pour évaluer l'évolution des risques de sécurité, et le contexte en général, car le personnel et les partenaires sur place pourraient devenir moins sensibles à des changements subtils.
- Des difficultés de communication et de logistique relatives au soutien du personnel sur place.
- Des problèmes de sécurité pour faire parvenir de l'argent ou des fournitures au personnel et aux partenaires.
- Une dépendance physique excessive de quelques membres du personnel dans des contextes à grand stress, entraînant un épuisement professionnel.
- Des difficultés pour assurer un bon suivi du programme, affectant la qualité et la responsabilité.
- Des difficultés pour maintenir la coordination entre organisations sur place, car le personnel et les partenaires qui prennent en charge les responsabilités du programme n'étaient au préalable généralement pas impliqués dans les activités de coordination.
- La gestion à distance peut compromettre les perceptions de neutralité et d'indépendance si l'organisation partenaire ne peut pas maintenir les principes humanitaires. Elle peut également nuire à l'acceptation en raison de la détérioration de la qualité du programme ou d'une plus grande corruption (bien qu'une plus grande adhésion locale puisse renforcer l'acceptation).

- Des difficultés pour répondre aux exigences des bailleurs de fonds en ce qui concerne le suivi et l'établissement de rapports.
- Un plus grand accent sur la gestion de la sécurité, de sorte qu'elle ne devienne plus un moyen pour arriver à une fin, mais une fin soi.

La possibilité que la gestion d'un programme à distance soit simplement un transfert des risques au personnel national ou aux organisations partenaires locales mérite une mention particulière. Les risques de sécurité peuvent être jugés trop élevés pour le personnel international mais cela ne signifie pas nécessairement que le personnel national ou local sera exposé à un risque moins élevé. En Tchétchénie à la fin des années 1990, en Irak depuis 2003, en Afghanistan depuis environ 2004, au centre-sud de la Somalie et au Puntland, les personnels internationaux et nationaux étaient exposés au risque de rapt et d'assassinat ciblé, à des degrés différents. Il est important d'évaluer les risques pour le personnel restant, basé dans les conditions spécifiques de la région, plutôt que de présumer que le personnel local sera automatiquement exposé à des risques moins importants. Dans certains cas, l'absence de personnel international pourrait exposer le personnel national à un risque plus élevé.

Dans toute la communauté des organisations humanitaires, l'absence générale de plans d'urgence et de préparation stratégique à des scénarios de gestion à distance aggrave considérablement les difficultés qui se présentent. De plus, le manque d'orientations et de procédures organisationnelles sur le sujet semble particulièrement problématique étant donné l'ampleur de la pratique dans les situations dangereuses.

4.3.3 Gestion de la sécurité lors de l'exécution d'un programme à distance

L'exécution d'un programme à distance soulève également de nouvelles considérations financières, de sûreté et contractuelles, et nécessite une nouvelle analyse des avantages et des risques. N'oubliez pas que poursuivre les programmes avec une gestion à distance pourrait être plus risqué que de cesser complètement les opérations, et que la fermeture d'un programme géré à distance pourrait entraîner des risques si elle suscite l'animosité du personnel affecté.

S'il est possible de continuer à opérer dans le cadre d'une approche de suivi à distance, des changements seront nécessaires dans la structure, le style et l'approche de gestion. Les procédures de gestion pourraient devenir plus complexes et onéreuses et comporter de fréquents contrôles ou rapports verbaux sur des aspects financiers, programmatiques ou de ressources humaines. Il pourrait être nécessaire de créer de nouveaux moyens de surveillance des programmes, par exemple prendre des photos des résultats du projet (des sources d'eau ou des écoles nouvellement construites), avec les coordonnées

GPS. Certaines techniques pourraient accroître la sécurité du personnel. Parmi celles-ci, on peut noter le fait d'utiliser des tiers pour contrôler les résultats ou la radio locale pour informer le public des droits des bénéficiaires. L'objectif ou l'approche même du programme pourrait devoir être adapté pour donner explicitement une plus grande responsabilité au personnel national.

Faire la transition

La gestion des programmes à distance a parfois tendance à apparaitre plus ou moins subrepticement. Au fur et à mesure que les conditions de sécurité se détériorent, une organisation peut ne pas réaliser qu'elle passe progressivement à une approche d'exécution de programme à distance. Les visites du personnel sur le terrain se font de plus en plus rares, mais on s'attend à ce que cette situation ne soit que temporaire. La gestion d'un programme à distance ayant de larges implications dans la gestion de la sécurité (et dans d'autres domaines), il est important que les hauts responsables fassent leur possible pour planifier et déterminer le nouveau mode d'exécution avant qu'une situation de gestion à distance ne s'installe de facto.

Il pourrait être utile d'établir au préalable des critères, en prévision de la nécessité d'un changement de mode de travail, et de considérer ce que cela signifierait pour l'équipe, les partenaires et les autorités locales. Les déclencheurs pourraient inclure le nombre de visites de la direction qui ont été reportées, le nombre d'incidents d'un certain type ou le nombre de déplacements reprogrammés en raison de risques de sécurité. À certains moments, l'incertitude d'une situation ambiguë pourrait être si perturbante qu'il serait justifié d'adopter une approche différente. L'une des responsabilités les plus importantes est, bien entendu, la sécurité du personnel : qui en est chargé et à quel niveau d'autorité ? Passer formellement à une gestion à distance et définir clairement ce que cela signifie et pour quelles personnes, clarifie les attentes et les responsabilités, notamment en ce qui concerne la gestion de la sécurité.

L'insécurité et les limites de plus en plus importantes imposées sur la façon dont les programmes sont exécutés peuvent parfois être identifiées à l'avance. Par exemple, une ONG internationale travaillant en Éthiopie a conçu un partenariat avec une organisation basée dans la région, et ceci dès le début d'un programme nutritionnel. En effet, cette organisation savait que le personnel international ne serait pas le bienvenu dans la zone d'opération. Les approvisionnements étaient pré-positionnés en prévision d'une intervention d'urgence et le personnel de l'organisation locale a été formé pour ce type d'intervention.

Évaluations des risques

Même si le personnel national (ou celui des organisations partenaires locales) est réellement exposé à un moindre risque que le personnel international, les

conditions de sécurité peuvent changer rapidement. Il est donc important de trouver un moyen de suivre l'évolution de la situation et d'arrêter le programme si les risques pour le personnel national restant deviennent inacceptables. Il est bon de garder en mémoire que le personnel national pourrait être moins susceptible que le personnel international de rapporter que le niveau global de risque est devenu intolérable. Le personnel international doit être en mesure de remettre en question et de recouper les informations obtenues sur le terrain. Cela peut être fait par le biais d'un réseau de contacts locaux (commerçants, autorités locales) qui peuvent être joints par téléphone, ou en partageant l'information et l'analyse avec d'autres organisations opérant dans la région.

Formation et ressources

Il pourrait être possible d'apporter au personnel national les connaissances et les compétences nécessaires, notamment en gestion de la sécurité. Le personnel national opérant en Iraq s'est rendu à Amman, les somaliens se sont rendus au Somaliland et à Nairobi, pour participer à une formation sur le mandat et la mission de leur organisation, les principes humanitaires et la gestion de la sécurité. En Somalie, une ONG internationale travaillant exclusivement avec des employés nationaux a fait venir plusieurs douzaines de membres du personnel et de partenaires à Hargeisa pour revoir son plan de sécurité.

Lorsque vous travaillez avec des organisations partenaires nationales, il faut vous demander si elles pourraient avoir besoin de ressources supplémentaires ou d'une formation en gestion de la sécurité. Bien qu'en général la même obligation de diligence ne soit pas applicable, une organisation internationale pourrait souhaiter financer du matériel (radios, véhicules, protection du site) ou une formation pour une organisation locale si elle le demande. Il ne faut pas présumer que toutes les ONG nationales sont en mesure d'assurer leur propre sécurité uniquement par le biais de l'acceptation.

Selon de récentes études, les pratiques identifiées comme contribuant à une gestion de programmes à distance efficace sont entre autres :[3]

- Inclure un scénario de gestion à distance lors des exercices de planification d'urgence ; envisager au préalable des partenaires locaux potentiels, des structures de gestion et de suivi et des stratégies de sortie et de transition.
- Établir des procédures et des instructions claires pour le personnel et les partenaires concernant la communication et l'établissement de rapports d'activités et de progrès.
- Organiser des réunions et des discussions régulières hors de la région

3 Abby Stoddard, Adele Harmer et Jean S. Renouf, Once Removed : Lessons and Challenges in Remote Management of Humanitarian Operations for Insecure Areas (Retrait : Leçons et difficultés de la gestion à distance des opérations humanitaires dans les régions dangereuses) (New York : Humanitarian Outcomes, 2010).

avec le personnel local ou les représentants des partenaires locaux sur la gestion et la coordination.
- Effectuer des contrôles impromptus et des visites et audits à l'improviste, si possible.
- Recouper et vérifier les informations de suivi avec celles d'autres organisations et celles provenant de différents contacts sur le terrain. Établir et maintenir un réseau local de sources d'informations, d'intermédiaires et de facilitateurs dans la communauté locale.

4.4 Retour

4.4.1 Décider de retourner sur les lieux

La question clé est ici d'établir si la situation est suffisamment sûre pour permettre le retour du personnel ou d'intensifier sa présence, et de savoir qui, dans l'organisation, assumera la responsabilité de la décision de conduire une mission exploratoire, puis ultérieurement d'autoriser le retour du personnel évacué et relocalisé. En l'absence d'un changement relativement radical sur le terrain (p. ex. le dirigeant d'un groupe rebelle est vaincu et le mouvement armé s'effondre rapidement, permettant au gouvernement de rétablir son contrôle sur la totalité du territoire), le retour pourrait également être progressif et échelonné. Tout d'abord, quelques brèves missions exploratoires pourraient être organisées pour réévaluer la situation, puis une présence plus permanente du personnel essentiel pourrait être établie dans une base opérationnelle, suivie du retour progressif d'un plus grand nombre de membres du personnel de l'organisation et enfin du personnel associé dans de plus nombreuses bases opérationnelles. Cela a été le cas de plusieurs grandes organisations retournant en Irak et en Afghanistan.

Les informations essentielles pour évaluer la situation de la sécurité lors d'une mission exploratoire comprennent :

- La situation réelle sur le terrain (sécurité, militaire, politique).
- Les changements possibles dans les prochains 3 à 6 mois et leurs implications en matière de sécurité.
- La situation logistique (aéroports, routes), des communications et des services (banques) suite à la crise.
- Le lieu et le statut du personnel non évacué.
- Le statut des biens, des ressources et des stocks laissés sur place.
- Les mouvements de la population locale.
- La disponibilité de provisions essentielles, surtout la nourriture, l'eau et le carburant.
- L'image de l'organisation sur le terrain, la possibilité de gérer les perceptions et la manière de le faire.

- Le niveau de ciblage direct des éléments étrangers, notamment des travailleurs humanitaires.
- La capacité organisationnelle de gérer la sécurité dans le contexte actuel.
- Une analyse des risques et avantages globaux.

4.4.2 Gérer un retour

Le retour du personnel international ou d'autres membres ayant préalablement quitté les lieux, est susceptible de créer une situation délicate, surtout pour les membres du personnel local et national ainsi que leurs homologues, qui se seront probablement accoutumés à une plus grande autonomie et qui retirent de la fierté et de l'assurance d'avoir fait face seuls. Il sera important de préciser que les employés ne retournent pas sur les lieux parce que l'organisation s'inquiète de la façon dont les programmes ont été gérés en leur absence. Des réunions entre les employés sur le terrain (souvent nationaux) et les cadres (souvent internationaux) dans des lieux où les deux parties seraient en sécurité (p. ex. en Somaliland pour les programmes du centre-sud de la Somalie ayant leur siège à Nairobi) sont également un moyen de maintenir la coordination et les relations entre les membres du personnel des deux endroits. En général, donner au personnel restant une plus grande initiative doit être considéré comme une conséquence indirecte positive de la gestion de programmes à distance. Les plus hauts niveaux de prise de décisions sur le terrain ne doivent pas nécessairement être changés après le retour physique de cadres ou d'autres employés internationaux.

Chapitre 5
Rapport d'incident et gestion d'un incident critique

5.1 L'importance du rapport et du suivi d'un incident

Il est vital de rapporter les incidents de sécurité, notamment les menaces et les incidents évités de justesse, pour trois raisons principales :

- Pour alerter le bureau sur le terrain et le siège afin de les informer et, si nécessaire, afin qu'ils fournissent de l'aide.
- Pour alerter les personnes travaillant dans d'autres organisations, et le cas échéant, les autorités et la population locales, afin qu'elles prennent des mesures de précaution.
- Pour permettre la surveillance et l'analyse des tendances des incidents, qui guideront les évaluations des risques de sécurité et la prise de décisions.

Rapporter un incident peut considérablement aider les responsables de la sécurité à comprendre le contexte opérationnel et à prévoir le type d'incidents susceptibles de se produire à l'avenir. Saisir, dans une base de données, la description générale fiable des incidents survenus dans le monde, permet une meilleure analyse de la sécurité aux niveaux national, régional et mondial. Plusieurs grandes organisations humanitaires disposent aujourd'hui d'un système interne de rapport et d'enregistrement d'incidents, certains accessibles en ligne. Ce système peut éviter la confusion sur la nature et les classifications d'incidents et permettre au personnel de fournir les informations cruciales et nécessaires. Ces détails peuvent révéler des concentrations géographiques d'incidents, permettre de comprendre les types d'incidents qui ont lieu et indiquer si le nombre global d'incidents est en augmentation ou en baisse. Ce type de renseignements peut ensuite permettre de prendre des décisions où d'allouer des ressources de sécurité limitées (humaines et financières), par exemple sur quel type de formation en matière de sûreté et de sécurité se concentrer.

La centralisation des rapports d'incidents de toutes les organisations opérant dans le même contexte, par exemple par le biais d'une structure de coopération sécuritaire telle qu'ANSO en Afghanistan, peut également présenter un grand avantage. Elle peut permettre une analyse plus objective des caractéristiques des incidents et de déterminer les tendances si les données sont analysées à temps. C'est l'une des fonctions pour lesquelles une structure de sécurité

inter organisationnelle (voir Chapitre 1) peut être extrêmement utile. Une orientation de la part des cadres est nécessaire pour que les personnes comprennent bien ce qu'elles sont censées rapporter et comment - et quelle pourra être l'utilité de ces informations.

5.1.1 Qu'est-ce qui est classé comme « incident à rapporter » ?

Un incident de sécurité se définit par tout ce qui porte atteinte au personnel ou aux personnes associées, ou tout ce qui occasionne une perte de ressources ou un dommage. Un « incident évité de justesse » est quelque chose qui a failli causer ce type d'atteinte, de dommage ou de perte. Une menace peut être écrite ou verbale ou peut être un geste physique, à condition qu'elle signifie, de façon crédible, l'intention de porter atteinte. Il est important d'inclure les incidents même mineurs, et de déclarer les incidents évités de justesse. Si vous avez un doute, déclarez-le malgré tout. Il faut également mentionner les incidents ou les incidents évités de justesse touchant d'autres acteurs impliquées dans le programme, y compris les organisations partenaires et les prestataires. Il pourrait également être utile d'inclure, dans les termes du rapport, tout incident dans lequel un membre du personnel a porté atteinte à un tiers, ou a perdu ou endommagé les biens ou ressources d'un tiers.

5.1.2 Le rapport d'incident

Il est important d'alerter ses collègues et collaborateurs dès qu'un incident s'est produit, même si toutes les informations n'ont pas encore été obtenues. Cependant, un rapport plus complet est généralement rédigé après l'incident et après la réponse à l'incident bien que, dans le cas d'incidents prolongés (p. ex. un rapt) un rapport puisse être produit avant la fin de celui-ci. . Les rapports d'incidents sont classées au niveau du terrain et communiqués au siège ; ils pourraient également être communiqués à une structure inter organisationnelle sur le terrain, si une telle structure existe.

Il est possible qu'une organisation ait un formulaire standard de rapport d'incident, et que ce document soit même disponible en ligne pour en faciliter l'accès. Quel que soit le format utilisé, ce qui est important c'est que les informations clés soient fournies. Le rapport d'incident portera essentiellement sur les questions fondamentales suivantes : que s'est-il produit, qui en est l'auteur, qui a été victime, quand et où l'incident s'est-il produit. Il est important de vérifier toutes ces informations. Il pourrait être pertinent d'ajouter un commentaire sur le « pourquoi » et « pourquoi cette organisation » (ce commentaire peut être éliminé si le rapport d'incident est partagé avec d'autres organisations). L'organisation était-elle spécifiquement ciblée, et si oui, pourquoi ? Assurez-vous d'indiquer le degré de confiance de la réponse à ces questions. Parfois, la réponse est évidente parce que les auteurs de l'incident l'ont donnée, mais dans d'autres cas il pourrait ne s'agir que d'une supposition.

Les problèmes courants concernant le rapport d'incident comprennent :

- Ne connaître l'identité des auteurs ou leurs intentions que beaucoup plus tard, ou dans certains cas, ne jamais les connaître. Il est important d'indiquer le degré de confiance dans les rapports et de changer les traces écrites internes à l'organisation si de nouveaux détails émergent.
- Il y a une réticence naturelle à reconnaître que des actions ou omissions de l'organisation ou de certains membres de son personnel ont contribué à ce qu'un incident se produise.
- Des difficultés de classification, par exemple, pour faire la distinction entre un vol, un cambriolage et un vol à main armé, et entre un enlèvement et un rapt. La définition de chacune de ces différentes catégories doit être claire pour toutes les personnes utilisant le système de rapport.

Informations clés du rapport d'incident

- Type d'incident, p. ex. rapt, mort, attaque grave, vol.
- Qui était impliqué ?
- Quand l'incident s'est-il produit ?
- Où l'incident s'est-il produit ? (avec le plus de précision possible)
- Combien de blessés y a-t-il eu et quelle est la gravité des blessures ?
- Quelle action d'urgence a été prise jusqu'à présent ? Une réponse supplémentaire est-elle nécessaire ? Si oui, laquelle ?
- Combien d'agresseurs y avait-il, qu'ont-ils fait et où sont-ils à présent ?
- La situation est-elle toujours en cours ?

Il est important de s'assurer que la confusion ou le désaccord sur la classification et la terminologie ne gênent pas l'institution d'un système de rapport d'incident. Si les membres du personnel ne peuvent pas systématiquement appliquer la classification, s'il y a des barrières de langue ou si le personnel trouve la procédure intimidante et décourageante, faites tout le nécessaire pour que l'information soit enregistrée. Certaines organisations et structures de sécurité centralisent la classification des incidents, si bien que le personnel peut tout simplement transmettre les informations qu'il possède aussi rapidement que possible, puis les coordinateurs de sécurité interviennent auprès des personnes concernées pour répondre aux questions le cas échéant et effectuer la classification et l'enregistrement formel au centre.

5.2 Gestion d'un incident critique

Un incident critique est un incident de sécurité suffisamment grave pour

entraîner une situation ayant le potentiel de causer des perturbations importantes dans les opérations ou même d'y mettre fin.[1]

5.2.1 Préparation : établir des structures de gestion d'incident critique

Afin de répondre à un incident critique, une organisation doit développer à la fois une procédure et une équipe de gestion d'incident critique (EGIC). L'équipe de gestion d'incident critique doit définir les responsabilités hiérarchiques et faire une distinction claire entre les rôles assumés au niveau du bureau pays et ceux assumés au bureau régional et au siège. Chacun doit comprendre sa position. Pour certains incidents, une EGIC pourrait n'opérer qu'au niveau du terrain, mais il faut que tout le monde sache bien quand faire intervenir le bureau régional et le siège si nécessaire. Les incidents graves ou prolongés (un assassinat, un attentat à la bombe, un rapt, une situation d'otage ou une hibernation forcée) ou les changements majeurs tels qu'une relocalisation ou une évacuation demanderont généralement une EGIC spécialisée.

La gestion d'un incident critique est difficile et demande des compétences particulières. Une gamme de compétences et d'expertises seront nécessaires et certaines pourraient devoir être obtenues en dehors de l'organisation. Il est judicieux d'identifier les importants besoins humains potentiels au préalable, par exemple des psychologues ou des spécialistes en négociation. Certaines organisations ont recours à d'anciens membres du personnel dignes de confiance, qui connaissent l'organisation et dont les compétences et l'expérience sont reconnues. Assurez-vous que des ressources financières sont disponibles et investissez, au préalable, dans une formation sur la préparation comprenant des exercices de simulation.

Les membres de l'EGIC (et leurs suppléants en cas d'absence) doivent être identifiés à l'avance (un organigramme précis devra être créé indiquant les responsabilités qui ont été définies et une liste de contacts). Une EGIC doit être de petite taille et inclure des personnes occupant diverses positions fondamentales comme le directeur de pays, la personne de référence en matière de sécurité, des membres des services logistique, RH, communication et conseils juridiques. Un responsable d'incidents critiques (RIC) pourra être nommé soit à la place de l'EGIC soit en supplément. Le RIC devra avoir le pouvoir d'allouer le personnel, l'équipement, les finances et autres ressources appropriées pour obtenir une réponse efficace, en temps voulu.

La première étape pour réagir face à un incident critique doit toujours être de décider si une action immédiate est requise pour préserver la vie

1 Définition tirée de la FISCR, Stay Safe: The International Federation's Guide for Security Managers (Rester en sécurité : Guide de la Fédération internationale destiné aux responsables de la sécurité) (Genève : FISCR, 2007).

ou assurer la sécurité. Des informations vérifiables contenant les détails de l'incident doivent être obtenues. Cela fera partie de la déclaration initiale. Des informations supplémentaires ou des modifications doivent être communiquées au fur et à mesure qu'elles surviennent. Ayez toujours en place un système de rapport d'incident qui permette à la fois l'enregistrement et l'analyse des incidents. L'enregistrement des incidents critiques doit être effectué immédiatement après le rapport d'incident. Il s'agit d'enregistrer la chronologie des événements, les appels téléphoniques, les notes sur les réunions et de s'assurer que tous les documents sont classés.

5.2.2 Le rôle de l'équipe de gestion d'incident critique

Dès réception d'un rapport d'incident, l'EGIC doit décider :

- Si les activités du programme doivent être suspendues ou si le personnel doit être déplacé dans un lieu plus sûr.
- Si un personnel de soutien supplémentaire doit être déployé pour apporter une aide.
- Quelles informations doivent être communiquées à l'intérieur et à l'extérieur de l'organisation et quelles sont les limites ou les questions de confidentialité.
- Quel est l'objectif final (évacuation des blessés, rapatriement des corps, remise en liberté d'un membre du personnel victime d'un rapt).

L'EGIC devra également envisager les problèmes médicaux et de sécurité, le soutien logistique et la capacité de mobilisation instantanée, les questions juridiques et les questions de communication et médiatiques. Des personnes blessées pourraient avoir besoin de soins immédiats ou à long terme. S'il y a eu des décès, les membres de la famille devront être informés et des mesures devront être prises pour les obsèques, les frais d'enterrement et autres. La sécurité pourrait être toujours un problème si les personnes non affectées par l'incident sont malgré tout en danger. De plus, un soutien logistique pourrait être nécessaire pour organiser des missions de recherche et de sauvetage ou de relèvement, des évacuations médicales, le rapatriement ou le retour des corps aux familles. En fonction de la situation, un personnel spécialisé pourrait être envoyé au bureau concerné sur le terrain, par exemple pour fournir une capacité de recherche et sauvetage, une aide médicale ou médico-légale, un soutien et un accompagnement psychologiques. Le bureau régional et le siège pourraient également avoir besoin de cette expertise.

5.2.3 Évacuation et relocalisation

Si la situation nécessite la relocalisation ou l'évacuation du personnel, l'EGIC devra gérer et surveiller :

- Les développements de la situation par l'intermédiaire d'un réseau de contacts, le système de télécommunication et les médias locaux et internationaux.
- Les structures logistiques et la sécurité.
- Le rassemblement et le déplacement organisé de tout le personnel devant être déplacé.
- Les ressources devant être emmenées.
- Les questions financières et administratives.
- La mise en sécurité de la documentation essentielle, confidentielle et délicate.
- Les communications internes avec le siège et le personnel sur le terrain.
- Les communications externes avec d'autres organisations, les autorités nationales et les ambassades concernées.
- Les relations publiques (communications avec la population locale, la presse locale et internationale) y compris les messages aux médias (voir Chapitre 7 : « Gérer la sécurité des communications » pour plus de renseignements sur les relations avec les médias).
- La tentative de continuer le programme.
- La coordination et le suivi internes des diverses actions mises en œuvre.

Dans le cas d'une opération de sortie de plusieurs organisations, établissez un point de coordination central. Pour de plus amples renseignements sur la planification et l'exécution d'une évacuation, voir le chapitre 4.

5.2.4 Communications

Au niveau du pays

En temps de crise, de nombreuses personnes et organisations devront sans doute être informées très rapidement. Au lieu de charger une personne de cette tâche, établissez un réseau de communications fiable dans lequel chaque « nœud » a la responsabilité de transmettre l'information à trois ou quatre autres nœuds. Un moyen facile de réaliser cela est d'utiliser l'organigramme de la mission. Celui-ci doit être actualisé régulièrement à intervalles prédéterminés afin que les noms et numéros de téléphone soient exacts. Il faudra également préciser à l'avance si le contact se fera par téléphone, SMS ou radio. Les points focaux, s'ils sont en place, peuvent être intégrés dans le system. Pendant une urgence, les réseaux de communications nationaux sont susceptibles d'être en panne ou surchargés : si possible, assurez-vous que l'organisation dispose d'autres moyens de communication indépendants de ceux de l'infrastructure nationale.

Si l'incident remet en question la continuation des activités du programme et peut-être la présence même de l'organisation dans un contexte donné, il sera nécessaire de communiquer avec les communautés affectées, le public et les donateurs clés.

Entre le bureau du pays et les bureaux de la région et du siège

Des communications fiables, spécialisées, 24 heures sur 24 et éventuellement sécurisées seront nécessaires entre le bureau du terrain affecté et l'EGIC du bureau régional et du siège. Attendez-vous à une interruption temporaire des communications et préparez-vous en conséquence. Prévoyez également le besoin de traduction si l'équipe régionale ou le siège ne parle pas la langue locale. Communiquez avec d'autres personnes dans les bureaux les plus directement affectés, ainsi qu'avec le reste de l'organisation. Pour un incident grave, le Conseil d'administration devra être tenu informé et pourra être consulté concernant des décisions critiques.

Il pourrait être nécessaire de communiquer avec les médias locaux, nationaux et internationaux. Préparez-vous à ce qu'ils vous contactent. Envisagez de diffuser la déclaration sur les sites Internet et intranet de l'organisation. Songez à l'information qu'elle contiendra. Précisez bien quelles informations doivent rester confidentielles, qui est inclus dans le cercle de communication et comment la confidentialité sera protégée.

Familles, voisins et autres organisations

Vous devrez communiquer avec les familles du personnel affecté par l'incident. Attendez-vous à ce que les familles prennent elles-mêmes l'initiative de vous contacter, surtout si l'incident dure longtemps. Vous devrez également communiquer avec les familles des personnes non-employées mais concernées par l'incident. Si le bureau de l'organisation s'est fait attaquer, par exemple, parlez aux voisins, dont le sentiment d'insécurité s'est probablement intensifié. L'objectif principal doit être de s'occuper du personnel de l'organisation mais il sera normalement toujours nécessaire d'alerter d'autres organisations d'aide au sujet d'un incident de sécurité majeur, afin qu'elles puissent prendre des mesures de précaution.

5.2.5 Relations avec les autorités

L'accord et la collaboration avec le gouvernement hôte pourraient être nécessaires pour le traitement rapide des demandes de visas pour le personnel de soutien en cas de crise ou autre personnel à mobiliser instantanément. Selon la nature de l'incident, aussi bien le gouvernement hôte que les gouvernements des membres du personnel concernés pourraient mobiliser leurs propres experts en réponse à l'incident. Cela peut créer une situation difficile sur le plan de la responsabilité et de l'obligation de diligence. Si une autre entité prend les devants, défendez ce que vous jugez être l'intérêt supérieur de la victime – de préférence en coordination et accord avec la famille de la victime. Il pourrait être possible de devancer cela en demandant aux représentants du gouvernement concerné quelles actions ils souhaiteraient prendre dans l'éventualité d'un incident particulier.

5.2.6 Considérations administratives, juridiques et financières

Certaines situations nécessiteront des conseils juridiques. Ceux-ci pourraient porter sur les termes des contrats, les avantages des employés, les questions d'assurance, les droits légaux selon le droit du travail applicable, la représentation juridique auprès d'un gouvernement hôte ou de son propre pays, ou encore comment aborder les problèmes juridiques et les réclamations en dommages et intérêts.

Gérer un incident critique, surtout un incident prolongé, demande également un soutien administratif et des ressources humaines spécialisées. Il pourrait y avoir d'autres dépenses urgentes pour le transport, l'équipement ou les services externes. De plus, le personnel victime pourrait être dans l'incapacité temporaire de travailler en raison de blessures physiques ou de stress psychologique. Pour veiller à la continuité des opérations, il pourrait être nécessaire de faire intervenir des remplaçants temporaires. Attendez-vous donc à avoir besoin d'argent supplémentaire pour couvrir des dépenses imprévues et non inscrites au budget. Certaines de ces dépenses, mais pas toutes, seront couvertes par l'assurance de l'organisation (voir Annexe 5).

Les personnes directement affectées par un incident (y compris les témoins) auront besoin d'un soutien et d'un accompagnement psychologique. Il en va de même pour les personnes frappées par un deuil ou traumatisées. Ce soutien pourrait aussi être offert à d'autres membres du personnel et aux familles des victimes.

5.3 Gestion post-incident

5.3.1 Compte-rendu et bilan après action

Toute personne, membre du personnel ou pas, ayant été directement impliquée dans la gestion de l'incident doit avoir l'opportunité de recevoir un compte-rendu. Cela peut aussi inclure le personnel qui se trouvait près du lieu de l'incident mais qui n'était pas directement impliqué dans sa gestion. Tout incident ou incident évité de justesse ayant un impact sur l'organisation, ses programmes, ses partenaires ou ses prestataires mérite une analyse. Le bilan après action doit être une pratique standard. Pour les incidents graves, envisagez une évaluation plus approfondie et idéalement indépendante qui permettra d'établir pourquoi l'incident s'est produit, comment il a été géré et pourquoi il a eu cet impact. Les questions clés incluent :

- Les mesures de sécurité étaient-elles en place ?
- Les mesures de sécurité étaient-elles en place mais ont-elles été correctement communiquées au personnel ?

- Les mesures de sécurité étaient-elles en place et ont-elles été communiquées mais n'ont-elles pas été comprises ?
- Les mesures de sécurité étaient-elles en place mais n'ont-elles pas été suivies ?
- Les mesures de sécurité étaient-elles en place et ont-elles été suivies mais ne convenaient-elles pas à la menace ?
- Les signes d'alerte d'une menace spécifique imminente ont-ils été notés et pris en compte, ou ont-ils été notés mais ignorés ?
- Le risque d'une menace spécifique a-t-il été correctement évalué comme faible, et les mesures de sécurité appropriées étaient-elles en place mais l'incident s'est-il produit malgré tout ?
- Une EGIC n'était-elle pas pré-identifiée, ou était-elle pré-identifiée mais non préparée ?

Tout incident grave affectant une autre organisation mérite également une attention et une analyse. Cette analyse pourrait ne pas nécessairement conclure que l'organisation est en plus grand danger. Il pourrait y avoir diverses raisons pour lesquelles ce qui s'est produit dans une autre organisation n'est pas susceptible de se produire dans la vôtre. La capacité d'effectuer une analyse raisonnable d'un incident affectant une autre organisation dépendra bien entendu de la quantité d'informations fiables qui peut être obtenue.

5.3.2 Revue du seuil acceptable de risque

Tout incident grave, qu'il affecte ou pas votre organisation, doit déclencher une revue du seuil acceptable de risque de votre organisation. Cet incident ou incident évité de justesse signale-t-il que l'analyse initiale était déficiente ? Indique-t-il que l'organisation a franchi le seuil de risque acceptable ? Quelles sont les conséquences pratiques ? Les mesures de sécurité peuvent-elles être renforcées pour réduire le risque ? Des modifications devraient-elles être apportées à la stratégie de sécurité opérationnelle, et ces changements seront-ils efficaces ? Le personnel devrait-il être retiré de zones à haut risque ? Si des ajustements ou des changements sont nécessaires, le personnel adéquat devra être mis en charge de la mise en œuvre de ces changements et un calendrier devra être établi. Cela pourrait nécessiter une formation nouvelle ou supplémentaire.

5.3.3 Renouvellement du consentement averti

C'est aussi un moment approprié pour communiquer à tout le personnel la nouvelle évaluation de la situation de sécurité et de la nature et du niveau du risque, ainsi que l'efficacité probable des mesures de sécurité de l'organisation. Le personnel devra avoir l'opportunité de décider s'il est prêt, dans ces circonstances, à continuer à travailler pour l'organisation.

Partie 3
Le personnel en charge de la gestion de la sécurité

Chapitre 6
Le personnel en charge de la gestion de la sécurité

Ce chapitre porte sur le rôle des personnes dans la gestion de la sécurité : individus et équipes qui constituent le personnel d'une organisation. Il débute avec la description du rôle du responsable de la sécurité sur le terrain, ou point focal de sécurité, et mentionne des éléments du descriptif du poste ainsi que les avantages d'employer du personnel international ou national pour ce rôle. Le chapitre aborde ensuite les types de compétences personnelles et d'équipes nécessaires à une bonne gestion de la sécurité.

La troisième section examine les différents types de menace auxquels sont exposées différentes catégories de personnel : international, national et local, ainsi que les paramètres de la gestion de la sécurité qui concernent le genre. Cette section étudie également le personnel qui, dans certains cas, peut constituer une potentielle source de problèmes de sécurité, et comment atténuer ces derniers. La quatrième section aborde les problèmes de sécurité qui sont généralement traités par une cellule des ressources humaines de l'organisation : la composition, le recrutement et l'assurance du personnel ainsi que son accès à une formation spécifiquement axée sur la sécurité. La section finale aborde la gestion du stress.

6.1 Les responsables de la sécurité sur le terrain

Dans les contextes à haut risque, la gestion de la sécurité justifie généralement au moins un membre du personnel spécialisé à plein temps. Cette personne gère les tâches liées à la sécurité au quotidien, tandis que le directeur de pays a généralement la responsabilité première en matière de sécurité. Les Nations Unies utilisent depuis un certain temps des agents de sécurité sur le terrain et, au cours des dernières années, des ONG internationales ont également commencé à créer ces postes. Il est utile d'établir des indicateurs de changement, dans le contexte de la sécurité, qui créent ou suppriment le besoin d'avoir un agent de sécurité à plein temps. Les agents peuvent n'être responsables que d'une zone à haut risque particulière dans un contexte opérationnel plus large. Dans les environnements à faible risque, certaines tâches liées à la sécurité peuvent être déléguées à la personne en charge de la logistique ou à un chef de bureau.

Trois domaines sont à considérer lorsque vous nommez un responsable de la sécurité ou chargé de liaison :

- Quel sera son descriptif de poste ?
- Quelles compétences sont nécessaires et donc quel profil de carrière et quelle expérience sont souhaitables ?
- Faut-il employer une personne internationale ou nationale ?

6.1.1 Le descriptif de poste

Le descriptif de poste pour un responsable de la sécurité sur le terrain pourrait inclure les éléments suivants :

- Effectuer une analyse continue des risques dans le contexte opérationnel, notamment envoyer des alertes de sécurité au personnel et au personnel associé.
- Aider à élaborer des stratégies d'atténuation des risques, y compris des procédures opérationnelles standard, des consignes et des plans d'urgence (notamment la réponse à une crise, la relocalisation et l'évacuation).
- Informer le personnel nouvellement arrivé et veiller à ce que tout le personnel soit tenu à jour des changements survenus dans les conditions de sécurité.
- Maintenir un système de rapport d'incident.
- Conseiller en matière de protection technique et de communication, par exemple sur le choix et la sécurisation d'un lieu, ainsi que sur le fonctionnement et la bonne utilisation de l'équipement de communication.
- Surveiller le respect des procédures et des plans.
- Encadrer le personnel lié à la sécurité, tel que les gardes, les opérateurs radio et les chargés de liaison en matière de sécurité nationale.
- Fournir une formation et un accompagnement à ses collègues pour leur permettre de développer des compétences en matière de sécurité.
- Fournir des conseils sur la budgétisation des dépenses en matière de sécurité opérationnelle.
- S'impliquer dans la réponse à un incident et dans la gestion d'une crise ainsi que dans les bilans et évaluations ultérieurs.
- Communiquer et échanger des informations avec d'autres organisations humanitaires et avec les autorités.

Effectuer toutes ces tâches serait difficile, à plus forte raison si les responsables de la sécurité sont censés assurer une permanence 24 heures sur 24, sept jours sur sept. Les points focaux de sécurité sur le terrain sont souvent surmenés et extrêmement stressés. Des mesures d'atténuation doivent être envisagées, par exemple établir un tableau de service pour éviter d'appeler toujours la même personne et pour que des problèmes mineurs puissent être réglés par quelqu'un d'autre. Le responsable de la sécurité ne peut non plus assumer seul la responsabilité de la gestion de la sécurité : une approche d'équipe est essentielle. La sécurité doit être un sujet de discussion, de

préférence le premier, sur l'ordre du jour de toutes les réunions de la direction. Les questions de sécurité doivent également être examinées au sein des équipes. L'accent doit être mis sur l'intégration de la sécurité dans le processus global de gestion.

6.1.2 Connaissances et compétences

Les compétences en matière de sécurité peuvent être largement classées comme « douces » et « dures ». Les compétences dures sont plus d'ordre technique et font référence à la nature et au fonctionnement de ressources spéciales, telles que l'équipement radio, les systèmes d'alarme, les films de sécurité, les gilets pare balles et les murs anti-souffle. Ces compétences sont souvent associées avec une expérience dans les forces de sécurité, comme les services militaires, de police ou des renseignements, où les individus peuvent avoir développé une connaissance des armes, des tactiques militaires, des opérations de police ou du contre-terrorisme. Les compétences dures peuvent également inclure des compétences d'investigation, c'est-à-dire la capacité d'enquêter avec impartialité sur un incident et de faire ensuite des recommandations solides et une analyse des menaces et des risques.

Les compétences douces font référence à l'aptitude à travailler avec une équipe multiculturelle, à la possession de compétences d'accompagnement et d'enseignement, à l'aptitude à créer des relations et de bonnes communications et à une expérience de planification et de budgétisation. Elles incluent également la capacité de développer et de maintenir des réseaux dans la communauté (surtout pour obtenir des informations sur des menaces possibles), ainsi que la capacité de comprendre et d'analyser des contextes souvent très différents du point de vue culturel, social et politique (et les violents conflits qui existent dans ces contextes).

Les compétences nécessaires peuvent dépendre des compétences déjà présentes au sein de l'équipe : le logisticien et l'ingénieur de travaux publics peuvent peut-être apporter quelques compétences dures, permettant au responsable de la sécurité de mieux se concentrer sur le côté plus doux du poste. Elles peuvent aussi dépendre du contexte dans lequel l'organisation opère : dans un environnement où se déroulent des combats et où opèrent des unités militaires (pouvant être irrégulières et insurgées), comme au nord du Sri Lanka en 2008, des compétences plus dures et des connaissances militaires pourraient être requises. Dans un environnement caractérisé par des milices tribales et locales, où tout le monde est en fait irrégulier, comme dans certaines parties des régions de Somalie et de la RDC, une personne possédant des compétences plus douces pourrait être nécessaire. Les contextes à haut taux de crime pourraient demander un éventail complet de compétences, qui ne pourront probablement pas être offertes par une seule personne.

6.1.3 Chargés de liaison internationaux ou nationaux pour la sécurité ?

Une décision fondamentale concerne le choix d'un point focal de sécurité parmi le personnel international ou national. Bien qu'il faille être prudent et ne pas trop généraliser, chaque personne a tendance à apporter différentes compétences et expériences au poste. Certaines sont résumées dans le tableau qui suit. Il est généralement préférable d'avoir une équipe de sécurité comprenant à la fois des membres internationaux et nationaux, peut-être en démarrant une opération avec un cadre supérieur international en tant que point focal de sécurité, et un membre du personnel national prenant la succession ultérieurement.

Le taux de renouvellement du personnel international peut être élevé, et celui-ci ne connaît pas toujours bien le contexte. Souvent, les travailleurs nationaux ont pris part à des opérations d'aide humanitaire dans leur propre société pendant de nombreuses années et certaines personnes auront peut-être aussi travaillé pour la même organisation pendant quelque temps. Pour le personnel national, la préoccupation est cependant le risque d'accoutumance : parce qu'il vit et travaille dans un contexte à haut risque, sa perception des menaces et des risques pourrait être différente. Un comportement qu'il considère comme sûr pourrait ne pas être considéré comme tel par le personnel international. À Nairobi, par exemple, le personnel national pourrait sans problème voyager dans des taxis collectifs (*matatus*), alors que le personnel international pourrait avoir l'interdiction de les utiliser.

Le personnel international pourrait être plus apte que le personnel national à aborder les questions de sécurité de manière impartiale, ou tout au moins jugée impartiale. Cela peut être le cas des conflits ethno-politiques où l'animosité entre les membres du personnel issus de divers milieux (par exemple au Sri Lanka, entre les Tamils et les Cinghalais) est manifeste. Dans ce cas, un membre du personnel international pourrait aborder les questions de gestion de la sécurité proportionnellement au risque et non pas en fonction de la méfiance éprouvée envers un groupe ethnique. Dans d'autres contextes, un membre du personnel international pourrait être jugé plus impartial par une force militaire qui est partie à un conflit (par exemple dans les discussions avec le gouvernement soudanais au Darfour ou avec les militaires israéliens dans les Territoires occupés palestiniens).

6.2 Compétences personnelles

6.2.1 Consignes d'autodiscipline dans le comportement

Les consignes de comportement suivantes, pour les membres du personnel, font partie des bonnes pratiques de sécurité.

Tableau 10: Forces/faiblesses des personnels internationaux et nationaux désignés comme points focaux de sécurité

Personnel international	Personnel national
• Peut avoir une compréhension plus large de l'organisation, de ses valeurs, sa culture, ses politiques et ses procédures. • Meilleure compréhension de la gestion des donateurs et du projet ainsi que des exigences concernant l'établissement de rapports. • Susceptible d'être plus objectif dans l'analyse du contexte du risque. • Susceptible d'être perçu comme plus impartial par les parties à un conflit. • Moins susceptible d'être soumis à des pressions par des acteurs locaux. • Est dans une meilleure position pour imposer la discipline au personnel national et international. • Est dans une meilleure position pour communiquer avec le personnel international d'autres organisations. • Pourrait avoir une plus grande expérience de la rédaction de rapports.	• A une meilleure connaissance du contexte social, culturel et politique. • Connaît l'histoire qui définit les perceptions et les attitudes de la population locale. • Parle les langues locales. • A un réseau local pouvant fournir des informations et faciliter l'accès. • Est en meilleure position pour communiquer avec le personnel national d'autres organisations.
• N'a pas la même compréhension du contexte social, culturel et politique. • Ne connaît pas l'histoire qui détermine les perceptions et les attitudes de la population locale. • N'a généralement pas accès aux médias locaux ou aux réseaux locaux d'information et d'accès. • Est plus susceptible d'avoir un comportement inapproprié et indélicat.	• Est accoutumé à vivre dans un environnement à haut risque, est moins conscient des risques et pourrait ne pas identifier les risques encourus par le personnel international. • Appartient à un secteur de la société et pourrait donc ne pas être objectif, ou pourrait ne pas être perçu comme étant objectif. • Pourrait ne pas pouvoir résister aux pressions exercées par d'autres acteurs de la société. • Pourrait ne pas avoir eu l'opportunité de développer des compétences en gestion de projets. • Pourrait ne pas être en mesure d'imposer la discipline au personnel international. • Pourrait être plus motivé par l'opportunité économique offerte par l'emploi (bien que la même hypothèse puisse être vraie pour un membre du personnel international).

Maintenir une connaissance constante de la situation

Soyez conscient du contexte plus large dans lequel vous travaillez, et de la façon dont vous pourriez être perçu. Gardez les yeux et les oreilles ouverts, écoutez les opinions de la population et informez-vous des perceptions locales par la presse locale, en écoutant vos collègues et la population locale et en parlant avec eux. Dans votre lieu de travail, maintenez vos connaissances du terrain : sachez où vous vous trouvez, observez l'environnement pour y détecter des menaces potentielles et pour repérer où vous pourriez trouver de l'aide ou un abri, ou dans quelle direction une manœuvre évasive pourrait être faite. Privilégiez la prudence : si vous avez un doute, restez à l'extérieur ou sortez, selon le cas. Fiez-vous à votre instinct et ne vous laissez pas influencer par les autres.

Restez conscient de la sécurité

Observez les consignes et procédures de sécurité de l'organisation et admettez que, dans des contextes de violence, l'insécurité et le danger imposeront des contraintes sur la liberté individuelle. Comprenez que prendre des risques peut mettre vos collègues en danger et influer l'image de l'organisation. Sentez-vous responsable de la sécurité et agissez lorsque des mesures de sécurité sont négligées sur la route, dans le bureau ou pendant et après les heures de travail. Si vous voyez ou entendez quelque chose pouvant avoir des implications de sécurité, signalez-le même si vous n'êtes pas certain que ce soit important. Rappelez-vous que personne ne sera aidé si vous êtes blessé ou tué.

Observez la discrétion

Ne mettez pas en évidence des signes de richesse ou de statut d'étranger et gardez vos opinions personnelles sur les questions sociales et culturelles pour vous-même. Une personne tranquille et discrète est moins susceptible d'attirer une attention non souhaitée.

Maintenez le contact et la communication

Informez toujours quelqu'un de l'endroit où vous allez et quand vous comptez être de retour. Déplacez-vous toujours avec un moyen de communication et une liste de contacts à portée de main.

Déplacez-vous avec assurance et détermination

N'ayez pas un comportement arrogant, mais ne semblez pas non plus incertain ou perdu, ce qui pourrait être perçu comme un signe de faiblesse ou de vulnérabilité. Marchez en montrant que vous savez où vous êtes et où vous allez, même si vous êtes perdu, faites preuve d'assurance et de sang froid dans votre posture, votre expression faciale et le mouvement de vos yeux.

Faites preuve de tact et de diplomatie

Évitez d'entrer en conflit avec la population locale et de montrer de la colère

ou de l'arrogance. Évitez les querelles au sujet de questions culturelles ou politiques avec des personnes que vous connaissez peu. Abstenez-vous de commentaires désapprobateurs ou désobligeants sur les coutumes et habitudes locales. Soyez toujours respectueux. En ce qui concerne les programmes, prenez le temps d'écouter les inquiétudes des personnes, leurs priorités et leurs plaintes. Ne faites pas de promesses que vous ne pourrez pas tenir et résolvez toujours les conflits.

6.2.2 Calmez la colère et l'hostilité

Les codes relatifs aux signes de colère et d'hostilité sont différents selon les cultures sociales. Les membres du personnel international viennent généralement avec le code de leur pays d'origine. Il est conseillé d'évoquer cela de manière informelle avec vos collègues et d'en considérer les implications potentielles. En Indonésie par exemple, comme dans de nombreuses autres cultures de l'Asie du Sud-Est, un fort accent est mis sur la politesse formelle, le respect des personnes âgées et des supérieurs, la maîtrise de soi, et exprimer l'irritation ou la colère est désapprouvé. Un personnel international ne connaissant pas cette culture pourrait ne pas réaliser qu'il provoque la colère ou l'hostilité s'il ne remarque pas les signes et expressions culturels. Le personnel national, en revanche, pourrait avoir des difficultés à répondre de manière appropriée s'il est soudain confronté à une expression de colère. Tous deux devront apprendre à adapter leurs habitudes.

Du point de vue de la sécurité, il est utile d'apprendre à calmer votre colère et votre hostilité de même que celles des personnes en face de vous. Parfois, le comportement d'une personne peut en partie influencer une situation tendue et potentiellement menaçante ; la capacité à garder la maîtrise de soi et l'esprit clair est donc importante pour sa propre protection. Il y a deux défis simultanés : contrôler ses propres réactions et apaiser l'hostilité d'une autre personne. Les recommandations pour calmer des situations hostiles sont entre autres :

- Soyez conscient de votre expression faciale et de votre langage corporel : 90 % de la communication est non verbale. Tenez-vous légèrement sur le côté de la personne en colère plutôt que directement en face d'elle.
- Gardez une voix calme.
- Écoutez sans interrompre, car les interruptions ne feront qu'exacerber la colère (si la personne en colère se répète, sachez comment paraphraser ce qu'elle dit de sorte à lui montrer que vous écoutez et que vous avez compris).
- Montrez de la curiosité et demandez à la personne de clarifier et de préciser ce qu'elle dit afin de comprendre ce qui l'indigne et ce qui a provoqué son hostilité. Ne contredisez et ne corrigez pas une personne en colère avant qu'elle ait fini d'extérioriser sa colère.

- Concentrez-vous sur le problème et non pas sur la personne : ne la confrontez pas personnellement et évitez de la juger ouvertement ; ne répondez pas à des jugements provocateurs sur vous-mêmes ou sur votre organisation.
- Gardez votre dignité, mais permettez à la personne en colère de garder aussi la face.

Choisir de contrôler la colère et de calmer l'hostilité ou pas est un jugement situationnel. Le faire sera probablement le plus efficace si la personne est hostile et indignée mais pas sur le point de faire du mal. Si quelqu'un devient très menaçant, retirez-vous ou obtempérez sans délai et sans résistance verbale. Si le principal message de la personne en colère exprime une objection à votre présence, dites que vous l'avez comprise et partez.

6.2.3 Techniques pour survivre à un incident et à une crise

Les confrontations et le danger grave provoquent le choc, la crainte et la terreur. Ces sentiments peuvent dominer la personne et conduire à un comportement qui augmente le risque au lieu de le réduire. Avec préparation, cependant, il est possible d'apprendre à accroître sa capacité de survie dans des situations dangereuses. Le but de l'exposition préalable à des situations menaçantes par le biais d'une formation comportant des simulations et jeux de rôles, est de réduire l'élément de surprise, d'aider les membres du personnel à garder le contrôle d'eux-mêmes et de leur permettre ainsi de réagir de manière à ne pas aggraver le danger pour eux-mêmes. Les principaux éléments du contrôle mental sont :

- ne paniquez pas ;
- agissez ou réagissez rapidement, mais en ayant conscience de la situation ;
- ne montrez aucune colère ou crainte à vos agresseurs ;
- gardez votre dignité ; et
- préservez votre vie

Il pourrait être impossible d'éviter ou de contenir l'agression dirigée contre vous, et vous pourriez être accablé par la force. Cela peut arriver, par exemple, en cas d'agression sexuelle, de détention ou de rapt. Dans ces circonstances, l'accent ne sera plus sur les techniques de comportement mais sur les techniques de survie mentale. Celles-ci sont évoquées dans les chapitres concernés.

6.3 Compétence des équipes

6.3.1 Pourquoi des équipes ?

Des équipes efficaces sont un facteur important dans la réduction du risque et dans la survie en cas d'incident et de crise. Un bon travail d'équipe signifie que :

- Chacun est conscient des risques de sécurité et partage des informations.
- Chacun aide à maintenir un haut niveau de sensibilisation à la sécurité.
- Les membres de l'équipe se soutiennent mutuellement pour surmonter le stress et la crainte.
- Au moment d'un incident, les personnes affectées peuvent se concentrer sur les agresseurs et sur les consignes indiquant quoi faire et ne pas faire, sachant que les autres membres présents réagiront également avec habilité.
- La gestion de la crise sera souple, efficace et compétente parce que les membres de l'équipe connaissent leurs rôles et leurs tâches.
- Les membres de l'équipe connaissent la hiérarchie ainsi que les forces et faiblesses de chacun, et ils peuvent changer de rôle si la situation le demande.

6.3.2 Qu'est-ce qui fait qu'une équipe est efficace ?

Les éléments nécessaires pour avoir une équipe efficace dans le domaine de l'aide humanitaire sont les mêmes que partout ailleurs, c'est-à-dire :

- Une identité claire, une mission et une intention communes.
- Des rôles précis.

Principes du style de commandement et de gestion

- L'autorité est attribuée, le commandement est acquis.
- Un chef d'équipe est respectueux et respecté.
- Le respect des membres de l'équipe découle de la perception que l'on a du chef d'équipe, qui doit être :
  - responsable, compétent et qualifié ;
  - capable d'exposer sa position en se basant sur des arguments plutôt que sur l'autorité ;
  - conscient de ses propres faiblesses et prêt à demander conseil et à écouter ;
  - équitable, juste et impartial, et prêt à changer une décision si de plus amples informations ou de meilleurs arguments sont présentés ;
  - prêt à donner à chacun une place appréciée au sein de l'équipe ;
  - en mesure d'aborder le problème professionnel au lieu de porter un jugement sur la personne ;
  - consultatif lorsque c'est possible, capable de trancher lorsque c'est important ; et
  - responsable de ses décisions.
- Les différents membres d'une équipe peuvent faire preuve de commandement dans leur propre domaine de compétence.

- Une responsabilité et une autorité se confondant partiellement (pas d'autorité sans responsabilité ; pas de responsabilité sans autorité).
- De la clarté sur la façon dont les décisions sont prises et quels processus décisionnels sont applicables et à quels moments (processus consensuel lorsque les circonstances et les problèmes le permettent ; consultatif, mais pas nécessairement, lorsque des décisions doivent être prises ; centralisé en ce qui concerne les règles et les ordres impératifs et en temps de gestion de crise).
- Un bon partage de l'information.
- Une grande appréciation de la valeur et de l'importance du travail d'équipe.
- Des approches et relations personnelles constructives.
- Des approches de gestion de conflit efficaces.

Une équipe a une culture horizontale : tous les membres ont une valeur égale, tout en ayant des rôles et responsabilités différents. Les équipes opèrent également dans des organisations qui ont une structure de gestion verticale, et toutes les personnes n'ont pas la même voix au chapitre à l'intérieur de l'équipe. En général, les organisations humanitaires insistent toutes sur des aspects différents, mais dans la pratique toutes doivent combiner ces deux aspects du travail d'équipe.

6.3.3 Les équipes et le commandement

Les éléments clés qui aident à unir les membres sont le style de commandement et de gestion. Il est important non seulement de connaître ces concepts mais aussi de comprendre ce qu'ils signifient dans la pratique. L'encadré qui suit énonce les principes qui peuvent guider un style de gestion.

Les chefs d'équipe encouragent le travail d'équipe, mais pas au point que la hiérarchie, l'attribution des responsabilités et de l'autorité deviennent difficiles à déterminer. En définitive, les organisations existent pour remplir certaines fonctions et des objectifs spécifiques. Bien que les équipes soient un moyen important et vital pour arriver à ces fins, elles ne sont malgré tout qu'un moyen. Les responsables doivent encourager et entretenir de bonnes relations avec chacun, mais pas au point de se soustraire aux problèmes mettant en jeu la responsabilité, la performance et la discipline professionnelles. Le travail d'équipe efficace et le bon moral du personnel peuvent être considérablement compromis si le chef d'équipe permet trop longtemps aux membres qui ne remplissent pas leurs fonctions de ne pas être sanctionnés.

Les responsables sont chargés de stimuler l'efficacité du travail d'équipe en faisant preuve de commandement, mais cette responsabilité ne peut être uniquement la leur ; chaque membre de l'équipe la partage - à plus

forte raison dans des situations instables et dangereuses. C'est le cas, en particulier, lorsque le roulement du personnel et d'autres obligations pressantes empêchent un responsable sur le terrain d'assumer entièrement cette responsabilité seul.

6.4 Différencier les menaces et les risques pour différentes catégories de personnel

Cette section examine les diverses circonstances de sécurité auxquelles sont exposées différentes catégories de personnel d'une organisation humanitaire. Les membres du personnel national, local et international, les hommes et les femmes, feront face à différentes menaces, n'auront pas la même vulnérabilité et pourraient percevoir des menaces similaires de manières sensiblement différentes. Les diverses menaces envers différentes catégories de personnel et le risque qui en résulte dépendront du contexte, et seront définis par une évaluation détaillée des risques de sécurité (voir Chapitre 2). Les membres du personnel peuvent eux-mêmes être à l'origine de menaces de sécurité ; ceci est également étudié plus loin.

6.4.1 Personnel international, national et local

Le recrutement des organisations d'aide a considérablement évolué au cours des 15 à 20 dernières années. Dans de nombreuses organisations d'aide internationales, les travailleurs nationaux représentent 85 à 95 % de leurs effectifs totaux. Pour beaucoup, une grande proportion du personnel national travaille pour l'organisation depuis cinq ans ou plus, et constitue une base importante d'expérience et de mémoire institutionnelle sur le terrain.

Le personnel international comprend souvent des employés qui ont commencé en temps que personnel national dans une organisation et qui, plus tard, ont pris pour la même organisation des postes dans d'autres pays, ainsi que des membres d'une diaspora qui rentrent travailler dans leur pays d'origine. Certaines organisations disposent également d'une catégorie intermédiaire de personnel recruté à l'échelon régional, c'est-à-dire des personnes venant de pays voisins, comme les Kenyans qui travaillent au Soudan ou les Sierra Léonais qui travaillent au Liberia. Bien qu'ils ne donnent pas toujours lieu à des différences contractuelles, les travailleurs nationaux pourraient aussi être classifiés comme locaux (c.à.d. travaillant dans leur milieu de vie) ou relocalisés (c.à.d. travaillant dans une partie différente de leur propre pays). Enfin, les ressortissants d'un pays tiers sont des étrangers recrutés localement qui, à des fins légales et contractuelles, sont traités comme personnel local.

La plupart des organisations affirment qu'elles considèrent le personnel national comme équivalent au personnel international sur le plan de leur

obligation de protection. Dans la pratique, toutefois, il y a des différences entre ce qu'une organisation peut et sera prêtre à faire pour le personnel international et le personnel national en temps de crise. De nombreuses organisations donnent encore la majorité des ressources organisationnelles liées à la sécurité aux membres du personnel international, qu'il s'agisse de formations, de logements plus sûrs, de moyens de transport ou d'équipements de communication. Ceci, avec la pratique de longue date d'évacuer le personnel international en temps de risque de sécurité très élevé et l'élargissement de la gestion de programmes à distance, pourrait donner lieu à une supposition implicite ou explicite que les membres du personnel national courent un moins grand risque que leurs collègues internationaux. Les faits ne confirment pas cette supposition. Selon les statistiques disponibles, la tendance à long terme des attaques envers les membres du personnel national par rapport à leur nombre sur le terrain est en hausse, et des suppositions injustifiées concernant la sécurité de ces personnes pourraient être en partie responsables.[1]

Être simplement « de la région » n'implique pas automatiquement été exposé à un moindre risque. En fait, les travailleurs nationaux peuvent faire face à un éventail de menaces qui ne peuvent atteindre le personnel international :

- Parce qu'ils font partie de la population plus large et ont la même vulnérabilité qu'elle.
- En raison de leur identité sociale ou politique perçue dans leur société lorsque celle-ci est profondément divisée ou est en guerre contre elle-même.
- Parce que leur travail pour une organisation internationale leur donne un meilleur statut et une plus grande visibilité, et qu'il les fait paraître plus riches que la population locale.
- Parce qu'ils peuvent gérer des biens ou de l'argent ou qu'ils ont une influence sur le recrutement ou l'attribution de contrats locaux.
- Parce que leur poste les place dans des situations et des lieux dangereux dans lesquels ils ne se trouveraient pas s'ils n'étaient pas employés à ce poste.
- Parce que leur emploi dans une organisation internationale fait d'eux une cible pour ceux qui veulent spécifiquement atteindre cette organisation ou une organisation internationale en général.

Cela peut engendrer toutes sortes de pressions et de menaces, par exemple :

- Le mécontentement et les accusations des cercles de la société parce qu'ils ne respectent pas les coutumes et normes traditionnelles et font

1 Pour obtenir une analyse des menaces auxquelles sont exposés les travailleurs humanitaires nationaux, voir *Providing Aid in Insecure Environments* (L'aide humanitaire dans les contextes dangereux), rapports de 2006 et 2009 (Overseas Development Institute)

partie d'une organisation qui démontre des valeurs différentes, sans doute plus libérales.
- Des pressions pour procurer du travail ou d'autres avantages.
- Des pressions pour fournir des informations confidentielles concernant les objets de valeur, comment et quand y avoir accès.
- Le risque d'être enrôlés de force dans les groupes armés ou d'être arrêtés par les autorités pour être soupçonnés de soutenir un groupe de l'opposition.
- La contrainte du gouvernement ou d'autres groupes de fournir des informations et des renseignements confidentiels concernant l'organisation.
- L'accusation d'aider un « occupant étranger » en tant que « collaborateurs » ou « espions ».

6.4.2 Les rôles des genres et les risques de sécurité

Le sexe d'une personne est un fait biologique, mais le genre est un concept social et culturel qui est exprimé par le comportement et les relations, ce qui peut compliquer la gestion de la sécurité. Par exemple, pour paraître fort, un homme pourrait refuser d'admettre qu'il ne possède pas certaines compétences (conduire un véhicule tout terrain, par exemple) ou pourrait adopter une attitude ou une apparence macho pouvant provoquer l'indignation et contribuer à l'intensification d'une situation déjà tendue. Dans une situation dangereuse, les hommes pourraient vouloir prendre le contrôle et se dépeindre comme protecteurs des femmes. Cela pourrait provoquer des tensions dans l'équipe et, dans une situation délicate ou dangereuse, accroître le risque. Cela pourrait également engendrer des sentiments de culpabilité et d'humiliation après des incidents de sécurité touchant des collègues féminins. Les situations peuvent s'intensifier plus rapidement lorsqu'elles mettent en jeu des hommes, tout simplement parce que l'agresseur s'attend à ce qu'un homme constitue une menace potentiellement plus grande ou à ce qu'un homme oppose une vive résistance. C'est pourquoi de nombreuses compagnies aériennes par exemple, enseignent à leur personnel de cabine féminin comment réagir face à des passagers difficiles et même face à des pirates de l'air.

Les femmes sont en général plus conscientes de leurs vulnérabilités particulières, surtout à l'agression sexuelle. Aujourd'hui, de nombreuses organisations considèrent avec sérieux les menaces particulières envers le personnel féminin sur le terrain et incorporent cet élément dans leur procédure de gestion du risque. Cependant. il est important de ne pas oublier que les hommes peuvent aussi être victimes d'agression sexuelle, et que les hommes et les femmes peuvent percevoir le niveau de risque différemment. De plus, selon le contexte et l'attitude de leurs collègues masculins, il se peut que les femmes aient à fournir un travail considérable pour être prises au sérieux et affirmer leur indépendance et leur liberté de choix par des moyens différents de ceux de

Étude de cas : remise en question de l'évaluation du risque effectuée par une responsable

La représentante d'un pays dans un contexte à haut risque a finalement donné sa démission parce que le siège de l'organisation ne lui avait pas offert un soutien tangible lorsque des collègues hommes ont refusé d'accepter ses consignes de sécurité, qu'ils considéraient comme surprotectrices et excessives. Le siège lui a confirmé que la gestion de la sécurité était sa responsabilité mais n'a pas soutenu son autorité. Elle a jugé que, puisque son autorité avait été remise en question et affaiblie, elle ne voulait pas prendre la responsabilité d'un incident éventuel, et a donc démissionné.

leurs collègues hommes, ce qui pourrait ultérieurement compliquer l'harmonie de l'équipe ou même encourager un comportement à prendre des risques.

Le genre et l'autorité

La majorité des conseillers internationaux et surtout nationaux en gestion de la sécurité ou du risque (ainsi que les formateurs en sécurité) sont des hommes, bien que le nombre de femmes dans ce secteur augmente progressivement. Les femmes émettront certainement des réserves pour rapporter des incidents concernant des avances sexuelles non souhaitées, un harcèlement sexuel ou une agression sexuelle à un collègue homme, qui pourrait être tout aussi gêné de prendre la déclaration. Lorsque les rôles sont inversés, le personnel masculin, selon son attitude, pourrait accuser les responsables féminins d'être trop peu enclines à prendre des risques et pourraient, en conséquence, hésiter à accepter leurs évaluations des risques et procédures de sécurité qui en découlent. Inversement, le personnel féminin pourrait contester les mesures de sécurité prises par un responsable homme parce qu'elles les jugent condescendantes ou sexistes, surtout si elles imposent des restrictions sur ce qui est jugé être la liberté individuelle. Des restrictions pourraient être placées sur le choix de résidence des femmes par exemple, ou elles pourraient être obligées, la nuit, de se déplacer accompagnées, alors que les hommes ne le sont pas. Dans certains contextes, les codes d'habillement pourraient être moins tolérants pour les femmes que pour les hommes, et l'on pourrait conseiller aux femmes de ne pas fréquenter publiquement des hommes qui ne sont pas des membres de leur famille. Limiter ce qui est perçu comme des libertés individuelles, surtout après les heures de travail, le week-end et pendant les vacances, donne toujours lieu à des contestations. Parler de ces questions ouvertement et développer un code de conduite interne pour le personnel peut grandement contribuer à maintenir la clarté concernant les responsabilités et libertés individuelles.

Genre et négociation

Les garanties de sécurité doivent être négociées avec des acteurs gouvernementaux et non gouvernementaux. La résolution des problèmes de sécurité pourrait nécessiter une négociation. Il est probable que les interlocuteurs réagiront différemment lorsque des négociations au nom d'une organisation sont conduites par une femme plutôt que par un homme. Dans certaines sociétés traditionnelles, les interlocuteurs pourraient être offensés de devoir discuter de problèmes avec une femme. Dans certains contextes, cependant, à l'inverse des hommes, les femmes pourraient être considérées comme moins menaçantes envers les hommes. Nommer une femme en tant que porte-parole pourrait donc être un choix délibéré. Pour des raisons similaires, une organisation pourrait choisir des interprètes féminins, bien qu'elles puissent constituer une cible plus facile pour les agresseurs qui veulent exhiber leur pouvoir ou qui se sentent insultés de devoir parler à une femme.

6.4.3 Le personnel, source de problèmes de sécurité

Les membres du personnel peuvent eux-mêmes être une source de problèmes de sécurité.

Personnel irresponsable

Les membres du personnel qui se comportent de manière irresponsable, avec incompétence ou arrogance peuvent être une menace envers eux-mêmes. Le comportement irresponsable peut comprendre l'abus d'alcool ou de drogues (pendant ou en dehors des heures de travail) ; exprimer publiquement des opinions politiques personnelles pendant les heures de travail ; dédaigner les procédures de sécurité ; être trop sûrs d'eux et penser qu'ils peuvent faire face à toute situation de danger parce qu'ils le font depuis de nombreuses années ; ou adopter une approche fataliste concernant leur bien-être. Les conséquences d'un tel comportement affectent plus que la personne, elles mettent en danger la réputation de l'organisation et la sûreté et la sécurité d'autres membres du personnel et d'autres organisations.

Personnel mécontent

Des travailleurs mécontents, qui ont le sentiment d'avoir été mal traités par leur employeur, pourraient ressentir une moins grande loyauté et créer des problèmes de sécurité. Pour minimiser ces risques, des politiques d'emploi et de ressources humaines claires, cohérentes et transparentes sont nécessaires. Il en va de même avec des procédures précises pour prendre une action disciplinaire et pour les licenciements, économiques ou autres. Être perçu comme un employeur équitable et juste renforcera la loyauté du personnel. Dans des situations délicates, ou en ce qui concerne des individus particuliers, il pourrait être utile de demander conseil à des collègues nationaux dignes de confiance sur le meilleur moyen de sanctionner ou de licencier le personnel

national. Le meilleur plan d'action du point de vue de la sécurité pourrait ne pas toujours être strictement conforme aux procédures formelles.

Personnel déloyal

Le personnel national pourrait fournir aux criminels des informations confidentielles moyennant une part des biens ou ressources qui auront été volés grâce à ces informations ; ou il pourrait transmettre des « informations sensibles » réelles ou fausses aux autorités ou à des acteurs non gouvernementaux afin de compromettre l'image et les procédures de sécurité de l'organisation. De la prudence au moment du recrutement, de la transparence sur l'organisation et sa mission, une supervision du personnel, des vérifications et bilans internes et une vigilance en matière de sécurité réduiront le risque.

Personnel corrompu ou malhonnête

Des vérifications financières, le contrôle des stocks ou une analyse d'incident peuvent suggérer qu'un membre du personnel international ou national a été corrompu ou est malhonnête. Par exemple, il pourrait voler de l'argent à l'organisation ou recruter des membres de sa famille ou des amis en dérogation aux politiques des RH et nuire ainsi à l'image de l'organisation. Cette situation est difficile et nécessite une action prudente mais aussi déterminée. La prudence est nécessaire pour éviter de porter de fausses accusations et pour devancer une réaction violente si un membre du personnel malhonnête s'apercevait que l'on mène une enquête à son sujet et se sentait menacé. Une action est néanmoins nécessaire pour éviter une atmosphère générale de méfiance omniprésente. L'investigation devra être discrète aussi longtemps qu'il y a suspicion mais sans évidence de méfaits. Le personnel international doit prendre la direction de ces investigations, car le personnel national pourrait être plus vulnérable aux représailles. Si l'évidence est suffisante pour justifier un licenciement, réfléchissez à la meilleure façon de procéder.

Discipline

Toute stratégie de sécurité sera affaiblie si le personnel n'a pas la discipline nécessaire pour la suivre. Le défi, pour le responsable, sera de faire preuve de compétence dans la gestion de la sécurité et de démontrer la solidité de l'analyse du risque, et il devra faire intervenir l'équipe dans la planification et les revues de la sécurité, afin que le personnel comprenne la logique au lieu de réagir à ce qu'il perçoit être un décret administratif insensé. Dans des contextes à plus haut risque, les procédures de sécurité devront peut-être être impératives, et les infractions devront être déclarées comme des fautes passibles de mesures disciplinaires.

6.4.4 La sphère privée

Un autre domaine difficile est celui de la sphère privée. Pendant une phase

d'alerte à la sécurité, il pourrait être facile de donner instruction au personnel international de se comporter avec prudence pendant leur temps libre. À d'autres moments, cependant il pourrait être difficile d'expliquer par exemple, que l'abus d'alcool en public, avoir un trop grand nombre de liaisons et d'aventures indiscrètes ou se comporter avec arrogance et porter des vêtements incorrects n'est pas un moyen acceptable de se décontracter et n'est pas uniquement le problème de la personne concernée mais nuit à l'image de l'organisation et des travailleurs humanitaires internationaux en général. Faire un travail humanitaire ne demande pas d'avoir une vie de saint, mais cela demande une certaine sensibilité sociale et culturelle et n'autorise pas à avoir une totale liberté personnelle. C'est une question difficile et délicate, qui doit être abordée à l'échelon de l'organisation. Les responsables doivent montrer l'exemple et convaincre en présentant de bons arguments ; ils ne doivent pas éviter de confronter le personnel dont le comportement est jugé offensant et dangereux. Un grand nombre d'organisations internationales ont un code interne de bonne conduite qui régit le comportement et l'attitude des employés et que les nouvelles recrues doivent signer. Ce code doit ensuite être mis en application.

Pour les membres du personnel national, la question est légèrement différente ; en tant que citoyens, ils ont le droit, après tout, de se comporter comme ils le souhaitent dans les limites des lois de leur pays. Le droit du travail national prévoira également des restrictions sur ce que les employeurs peuvent demander à leur personnel national en dehors des heures de travail. Il s'agit manifestement d'un domaine que les travailleurs nationaux doivent évoquer entre eux et que les employeurs doivent aborder avec le personnel national

6.5 Ressources humaines

6.5.1 Composition du personnel

En règle générale, la composition du personnel doit être élargie et équilibrée, autrement dit elle doit refléter la composition de la société hôte, soit de tout le pays soit tout au moins de la région ou du bureau individuel, sur le plan de l'appartenance ethnique et religieuse, par exemple, et de tous les échelons de la société. Cela ne signifie pas que les critères techniques et professionnels ne doivent pas être les éléments moteurs du recrutement d'un individu, mais que d'autres facteurs doivent également être considérés, tout au moins à l'échelon de l'organisation. La composition du personnel est un facteur très important dans la façon dont une organisation est perçue, ce qui est aussi critique pour la stratégie d'acceptation de l'organisation. La diversité du personnel dans un contexte socialement hétérogène et politiquement fragmenté est généralement un actif. Elle soutient les affirmations de neutralité et d'impartialité de l'organisation, peut contribuer à développer des relations élargies et peut donner accès à des informations et des perspectives provenant de diverses

sources. L'inconvénient est que cela pourrait amener des tensions et des conflits externes dans l'organisation. La diversité crée ses propres difficultés, mais elles sont généralement compensées par les avantages. De plus, si l'organisation est impliquée dans des projets de consolidation de la paix ou de résolution du conflit dans la communauté au sens large, il est essentiel de pouvoir promouvoir cette conception en premier lieu parmi son propre personnel.

Dans certaines situations, un profil équilibré de personnel pourrait ne pas être possible ou désirable, tout au moins pas à un échelon plus haut (c.à.d. national). Lorsqu'il y a un fort antagonisme entre des groupes, certains employés pourraient ne pas être jugés dignes de confiance ou pourraient ne pas se sentir en sécurité dans les zones contrôlées par des personnes ayant la même identité que celle de l'adversaire. Il ne faut pas supposer cela automatiquement, et parfois une personne peut être acceptée même lorsque son groupe n'est en général pas bien considéré. Pour des raisons similaires, les organisations doivent être prudentes lorsqu'elles relocalisent leur personnel, qui pourrait susciter de la jalousie ou de la suspicion dans sa nouvelle communauté hôte. Dans ce contexte, il est généralement utile de « répartir la richesse » en offrant de l'emploi à des personnes qualifiées aussi proches de la communauté hôte que possible.

On pourrait aussi appliquer des considérations similaires pour recruter du personnel international. Lorsqu'un conflit a une dimension régionale ou internationale, il pourrait être difficile pour un membre du personnel international d'un certain pays de surmonter une suspicion et une hostilité automatiques et généralisées. Par exemple un Éthiopien pourrait avoir des difficultés pour travailler en Somalie et un Indien pourrait ne pas être le choix le plus approprié pour travailler dans certaines parties du Pakistan. Le même principe pourrait également être applicable en ce qui concerne la religion : Il pourrait être plus prudent de recruter des musulmans pour travailler dans des sociétés à prédominance musulmane, ou des hindous dans les zones touchées par le mouvement intégriste. Pendant longtemps, seul le personnel tamoul pouvait travailler en sécurité dans la région du Vanni dans le nord du Sri Lanka. Après l'invasion de l'Irak par les Etats-Unis en 2003, les organisations internationales qui avaient gardé leur personnel à prédominance sunnite, ont eu des difficultés relationnelles avec le nouveau gouvernement essentiellement chiite. Bien entendu, le gouvernement n'a pas apprécié le fait que tous les agents de programme ou traducteurs étaient issus de l'autre groupe religieux.

6.5.2 Recrutement

Ne pas investir du temps dans un recrutement prudent et dans le contrôle ultérieur du personnel peut être coûteux, aussi bien sur le plan de la performance professionnelle que sur celui de la sécurité.

Personnel international

Les critères de recrutement du personnel international doivent concerner des compétences autres que des compétences techniques. Le tact et les compétences interpersonnelles, la sensibilité culturelle et un sens bien développé des responsabilités et de l'autodiscipline sont des facteurs importants qui contribuent à la sécurité et à la gestion (des programmes). L'expérience sur le terrain n'est pas une garantie de maturité : la quantité n'est pas une garantie de qualité. De plus, bien que l'expérience soit désirable, prendre une personne ayant tenu un poste très exigeant et souffrant encore d'épuisement professionnel, n'est bien entendu pas prudent.

Dans certaines organisations, les RH assument certaines tâches concernant la préparation et les orientations de la mission, mais inévitablement, le meilleur apprentissage se fait sur le terrain. Étant donné que dans certains endroits les statistiques indiquent un risque accru dans les trois premiers mois d'une mission, il est impératif d'organiser des séances intensives d'information pour le nouveau personnel dès son arrivée. Ces informations devront inclure des orientations contextuelles détaillées et une explication de la logique des mesures de sécurité qui sont en place.

Personnel national

Recruter le personnel national adéquat est crucial mais aussi difficile, surtout lorsqu'une organisation est nouvelle dans un contexte et doit répondre avec urgence à une crise. Les premières recrues nationales auront de l'influence car, tout au moins les premiers temps, elles seront fortement impliquées dans la gestion de l'organisation et dans le recrutement de personnel supplémentaire. Les points suivants sont des principes de bonne pratique dans le recrutement de personnel national et dans l'externalisation de services nationaux.

Tout d'abord, obtenez des références aussi bien professionnelles que sociales et vérifiez-les avec diligence. Des qualifications techniques ayant trait au poste sont nécessaires mais ne sont pas un critère suffisant de recrutement. Les références professionnelles doivent toujours être consultées. L'obtention de références dites « sociales » fait également partie des bonnes pratiques : cela consiste à identifier d'autres personnes de la communauté, de préférence ayant un certain standing et une certaine autorité, prêtes à garantir l'intégrité du candidat. Dans des contextes sociaux plus traditionnels, ces personnes peuvent servir de garant à un membre du personnel. Obtenir des références sociales demande du temps et des efforts, mais cela peut éviter de recruter des personnes qui ont une mauvaise réputation ou même des liens criminels. Cela peut aussi créer des liens plus forts avec le milieu social environnant. Ce que nous devons empêcher, c'est la pratique selon laquelle un candidat national est recruté suite à la recommandation d'une autre personne locale, mais ensuite est

obligé de payer un pourcentage de son salaire au garant. Soyez conscients que les garants peuvent mettre en doute ce qu'il considèrent comme de mauvaises politiques et pratiques de personnel de l'organisation humanitaire.

Ensuite, commencez avec des contrats à court terme. Si vous recrutez dans un contexte entièrement nouveau, ou si vous êtes pressé, il serait peut-être judicieux de donner des contrats à court termes sans garantie de renouvellement. En même temps, prenez connaissance de la législation du travail et respectez-la en ce qui concerne les renouvellements répétés de contrats à court terme.

6.5.3 Assurance

Une assurance médicale, comprenant l'évacuation, n'empêchera pas la maladie ou les blessures, mais permettra d'avoir accès physiquement et financièrement aux soins médicaux, ce qui pourrait éviter de pires conséquences. Une assurance vie et une assurance invalidité permettent de limiter les conséquences financières d'un incident. De nombreux membres du personnel national ne possèdent pas ces assurances parce qu'elles ne sont pas disponibles ou parce qu'elles sont trop onéreuses. S'ils ont une assurance, celle-ci ne couvrira souvent que quelques risques et les remboursements pourraient être si bas qu'elle sera inadéquate en cas de maladie ou de blessure grave. Si le personnel national constitue la majeure partie des effectifs, ses besoins en assurance devront être abordés (voir Annexe 5).

6.5.4 Accéder à une formation en sûreté et sécurité

Faites des efforts particuliers pour que tout le personnel ait accès à une formation en matière de sécurité et à des opportunités d'apprentissage. Bien qu'au cours des dix dernières années la fourniture de formations en sûreté et sécurité ait augmenté, c'est en grande partie le personnel international qui en a bénéficié. Étant donné que les travailleurs nationaux constituent la majeure partie des effectifs, et qu'ils représentent généralement la plus grande continuité dans un contexte opérationnel donné, il est critique de leur fournir une formation. La traduction de supports de formation dans les langues locales et la formation des animateurs locaux, pourraient être trop difficiles et trop coûteuses pour une organisation unique, et pourraient donc constituer un autre domaine de collaboration entre plusieurs organisations et d'investissement commun.

Les cours de formation restent en principe une expérience isolée : sans pratique régulière, une grande partie des informations communiquées est rapidement oubliée. Des références continues aux questions de sûreté et de sécurité dans le travail quotidien, et bien entendu surtout en périodes de risque accru, sont essentielles, de même que les exercices périodiques.

La participation active de tout le personnel dans la gestion de la sûreté et la sécurité est un autre élément critique pour développer les compétences.

6.6 Le stress et sa gestion

Le stress et la sécurité sont liés de diverses manières :

- Vivre dans un contexte dangereux contribue au stress.
- Lorsque des personnes sont stressées, leur performance professionnelle et leur jugement situationnel sont affectés et elles pourraient se mettre à agir de telle sorte qu'elles augmentent le risque pour elles-mêmes et pour autrui.
- Lorsque des personnes sont directement victimes d'un incident, ou lorsqu'elles sont témoins d'un incident dans lequel leur propre intégrité physique ou celle des personnes qui les entourent est menacée ou violée, elles peuvent ressentir des troubles de stress aigu.

La gestion du stress est donc l'une des dimensions de la gestion de la sécurité. Tout comme la sécurité, gérer le stress est à la fois une responsabilité individuelle et organisationnelle.

6.6.1 Qu'est-ce que le stress?

Le stress est une réaction naturelle, qui peut être positive et stimulante. Le stress n'est pas toujours débilitant. Il existe différents types de stress : sain et malsain. Le stress sain aide à se concentrer sur la tâche ou la situation immédiate, il mobilise l'énergie et prépare à l'action. Par exemple, avoir une date butoir peut créer du stress chez une personne mais peut aussi l'aider à accomplir le travail. Dans des situations de tension ou de risque, les personnes peuvent aussi ressentir une crainte rationnelle. Ceci est une réaction fonctionnelle justifiée face à une alarme et qui peut permettre d'avoir la concentration dont nous avons besoin pour survivre.

Cependant, lorsqu'on est stressé trop souvent, ou lorsque le stress est trop intense ou dure trop longtemps, il n'a plus un effet positif mais négatif. Tous les types de stress utilisent de l'énergie. Une série continuelle de dates butoir trop courtes ou une exposition constante à des situations à haut risque peut réduire les réserves d'énergie. Un stress malsain ou dysfonctionnel se présente de deux manières : stress *cumulatif* et stress *traumatique*. Le stress cumulatif est moins facilement reconnaissable ou admis et pourtant est très présent chez de nombreux travailleurs, y compris les acteurs humanitaires. Ce stress prolongé conduit ultérieurement à l'épuisement physique et émotionnel ou épuisement professionnel. Le stress traumatique résulte d'une exposition directe ou proche à des événements ou à des incidents traumatiques qui peuvent causer la mort

et qui occasionnent une perte physique ou émotionnelle. Les experts en santé mentale font une distinction supplémentaire entre *troubles de stress aigu*, qui peuvent se manifester quelques heures ou quelques jours après un événement, et *troubles de stress post-traumatique*, qui peuvent se manifester plusieurs mois ou même plusieurs années après un événement.

6.6.2 Qui est affecté par le stress ?

Tout le monde est susceptible d'être affecté par le stress, mais tout le monde ne sera pas nécessairement stressé par les mêmes choses ou de la même manière dans le même environnement. Le stress est le résultat d'une combinaison de demandes externes (stresseurs) et de ressources individuelles. Le stress se manifeste également différemment selon les personnes.

Tout le personnel du terrain

Tout le personnel, recruté à l'échelon international comme national, est vulnérable au stress. Les travailleurs nationaux pourraient avoir l'avantage d'être dans un contexte qu'ils connaissent très bien et conserver leurs réseaux de soutien social. Cependant, souvent ils ne sont pas externes au conflit, à l'inverse des expatriés, et ils pourraient avoir été exposés au danger depuis des mois, si ce n'est des années. Ils pourraient juger que les différences culturelles dans le style de travail sont stressantes et pourraient s'inquiéter au sujet de la sécurité de leur emploi et de leurs responsabilités financières et émotionnelles envers leur famille au sens large

Les responsables sur le terrain

Un grand problème non reconnu sur le terrain concerne le soutien du responsable. La gestion du personnel fait partie de la responsabilité du responsable sur le terrain, qui est donc censé être un pilier de stabilité, de soutien et de bon jugement à tout moment. Manifestement, ce n'est pas réaliste mais, surtout dans des organisations plus hiérarchiques, on ne sait pas exactement comment le responsable gère son propre niveau de stress. Un responsable qui prend la sûreté et la sécurité de son personnel au sérieux percevra certainement cette responsabilité comme stressante, surtout dans des contextes instables et dangereux. Les conseillers professionnels et les experts en santé mentale peuvent aussi être affectés par le stress causé par une exposition constante aux problèmes des personnes qu'ils essaient d'aider.

Les responsables de la sécurité

Les responsables de la sécurité sont vulnérables à de très hauts niveaux de stress pour diverses raisons : ils sentent, eux aussi, qu'ils sont personnellement responsables de la sûreté et de la sécurité de leurs collègues, et ils pourraient se sentir obligés d'être constamment prêts à intervenir. Ils pourraient se culpabiliser, de manière explicite ou pas, si quelqu'un a suivi ses consignes

et conseils mais a malgré tout été affecté par un incident grave. Ils pourraient également être confrontés à l'impact quelquefois épouvantable d'un incident (p. ex. une forte explosion de bombe). Ils pourraient devoir faire face à une frustration prolongée due à un engagement insuffisant envers la gestion de la sécurité dans une organisation.

Les responsables au siège

Au siège, certains personnels ayant sans doute de nombreuses années d'expérience sur le terrain, pourraient apporter au poste qu'ils occupent une accumulation de stress et certaines habitudes de vie et de travail acquises sur le terrain. En période de tension et de risque sur le terrain, ils pourraient ne pas être en mesure de s'en détacher. De plus, une grande quantité de stress peut être générée par la charge de travail, des rivalités internes, des intrigues institutionnelles et des crises organisationnelles au siège.

La famille et les proches

La séparation et les communications moins fréquentes, différentes expériences, le sentiment que les proches n'étaient pas présents lorsqu'on avait besoin de soutien, la perception que l'autre n'est intéressé que par ses propres problèmes, un changement de comportement, l'abus de substances (par exemple une consommation accrue d'alcool) et peut-être un changement de caractère ou de perspective sur le monde et sur la vie suite à des expériences intenses, peuvent avoir un effet néfaste sur les relations familiales et sur les amitiés. La gestion proactive et rétroactive du stress doit donc faire intervenir la famille.

Les hommes et les femmes sont tout aussi vulnérables au stress

Les femmes peuvent ressentir un plus grand stress en raison de leurs craintes vis-à-vis de la violence basée sur le genre. L'incertitude et un manque de confiance dans ses compétences en gestion et dans sa position peuvent affecter les hommes tout autant que les femmes. Leurs réactions peuvent toutefois être différentes. Selon certaines études, les femmes ont tendance à répondre différemment au stress, elles recherchent un plus grand contact social et un plus grand soutien auprès d'autres personnes, et intensifient leur rôle protecteur et bienveillant, tandis que les hommes ont une plus grande difficulté à admettre qu'ils ont atteint la limite de ce qu'ils peuvent supporter et qu'ils ont besoin de faire une pause.

6.6.3 Symptômes de stress négatif

Les symptômes possibles de stress négatif sont nombreux et divers et sont différents selon les personnes :

- Les symptômes physiques courants incluent la lassitude et un sentiment d'épuisement, qui peuvent pourtant être accompagnés d'hyperactivité et

de surmenage ou de problèmes de sommeil. Un sommeil excessif, continu, souvent accompagné de symptômes de grippe, peut se manifester après des incidents critiques ou peut être un signe d'épuisement professionnel plus général ; d'autres symptômes incluent les maux de tête et de dos et des troubles gastro-intestinaux. Les sueurs froides, l'hypertension artérielle et une augmentation de la fréquence cardiaque, des tremblements généraux et la nausée pouvant conduire au vomissement peuvent se produire dans des situations de troubles de stress aigu.

- Les symptômes comportementaux comprennent l'évitement de contacts sociaux réels et de relations, l'abus de substances, notamment la caféine, l'alcool, les cigarettes et peut-être la drogue, une série de relations amoureuses brèves occasionnelles et de relations sexuelles non protégées, la conduite dangereuse et la prise de risques en général.
- Les problèmes liés au travail peuvent inclure l'alcoolisme pendant les heures de travail, le retard, l'absentéisme, le manque de concentration et une réduction de la productivité ou une mauvaise performance professionnelle.
- Les personnes affectées émotionnellement peuvent perdre le moral, être pessimistes ou cyniques, être anxieuses, se sentir coupables et être dépressives. Mais l'excitation et un sentiment de pouvoir et d'invulnérabilité peuvent également être des symptômes de stress excessif. Une autre émotion exprimée peut être une identification excessive aux bénéficiaires et une empathie excessive, conduisant à une perte d'objectivité. Les cauchemars, les retours en arrière ou les émotions intenses concernant tout ce qui évoque un incident critique et donc souvent une tendance à vouloir éviter et réprimer toutes pensées ou tous sentiments à ce sujet, font partie des symptômes des troubles de stress post-traumatique.
- Les symptômes relationnels du stress incluent : se distancer des bénéficiaires en les intellectualisant ou en les déshumanisant ou en faisant constamment des plaisanteries à leur sujet (on appelle cela l'usure de compassion, exprimée par des commentaires cyniques), une mauvaise communication avec ses collègues et sa famille, le repli sur soi, l'irritabilité ou une tendance constante à chercher querelle et à être agressif.
- Les répercussions spirituelles ou philosophiques incluent : douter de son système de valeurs ou de ses croyances religieuses, remettre en question les domaines importants de la vie (sa profession, son emploi, son style de vie), des sentiments de menace et de victimisation, la désillusion et l'égocentrisme.

6.6.4 Gérer le stress

Le stress doit être géré à de multiples niveaux dans l'organisation. Cette section évoque comment procéder, au niveau de l'organisation, au niveau du terrain et au niveau individuel. Enfin, elle évoque l'importance de comprendre les différences culturelles et comment le stress est géré.

Au niveau organisationnel

Même si un plus grand nombre d'organisations humanitaires commencent à se pencher sur la sûreté et la sécurité et fournissent un soutien psychologique interne et externe pour la gestion du stress, beaucoup ne reconnaissent toujours pas le stress du personnel en tant que problème organisationnel. Pourtant les employés sont beaucoup plus exposés au stress qu'aux autres menaces. Le stress affecte la performance, le moral et la motivation. A la longue, il influence la durée qu'un membre du personnel souhaite rester dans la mission. Cela affecte donc le renouvellement du personnel

Les organisations peuvent aider à gérer le stress en reconnaissant que c'est une responsabilité organisationnelle, en l'évoquant et en élaborant des politiques de repos et de récupération de manière générale et face à une situation spécifique. Les niveaux de stress et la résistance au stress doivent également être pris en compte de manière explicite dans le recrutement et dans les décisions de redéploiement. Les organisations doivent examiner ce qu'elles attentent des responsables sur le terrain dans des environnements complexes, instables et fortement contraignants, et le soutien pratique qui leur est offert. Avoir des attentes similaires à celles que l'on aurait dans un contexte stable n'est pas réaliste et prépare le responsable à l'échec.

Au niveau de l'encadrement sur le terrain

Le responsable sur le terrain peut faire un certain nombre de choses pour gérer le stress de son personnel.

Un haut responsable doit passer du temps avec une nouvelle recrue afin qu'il y ait un échange personnel. C'est l'opportunité de parler à la personne des problèmes de sécurité et de signaler que le stress fera partie de son expérience et que c'est un phénomène normal. C'est aussi l'opportunité d'établir un rapport personnel et de mentionner que les responsables sont accessibles en cas de problème. Après une période initiale d'environ trois semaines, il est de bonne règle d'organiser une autre réunion pour évoquer la façon dont la nouvelle recrue s'adapte, ce qui va bien et ce qui semble plus difficile, aussi bien personnellement que professionnellement.

Tous les responsables sur le terrain doivent recevoir une formation de base en gestion. Elle permettra de les préparer à leur rôle et leur en donnera des attentes réalistes, ce qui pourra réduire le stress. Cette formation devra couvrir les principes de base de la gestion des personnels et pourrait inclure une identification de leur type de personnalité et de leur style de travail. Pour les responsables sur le terrain, apprendre sur le tas peut aussi se faire en discutant des problèmes dans des réunions d'équipes de coordination et en rédigeant des principes de bonne pratique explicites, notamment en ce qui concerne la gestion du stress.

Une bonne gestion signifie également savoir intervenir de manière délicate et avec respect lorsqu'une personne affiche des symptômes de stress excessif. Préparez-vous soigneusement : ce ne sera pas facile car la personne niera probablement qu'elle a un problème et pourrait se mettre sur la défensive et s'énerver. Il pourrait être nécessaire de soustraire une personne souffrant de stress excessif à un contexte difficile. Cela vaut pour son bien-être et pour la sûreté et la sécurité de toute l'équipe. Les responsables doivent avoir suffisamment d'assurance pour prendre cette décision, après avoir consulté leurs supérieurs. L'approche doit être ferme mais coopérative et ne doit pas mettre la personne concernée à l'index.

Il pourrait aussi être utile de parler du stress dans les réunions du personnel et d'encourager le personnel à en reconnaître les signes. Dans certains contextes cette approche puisse ne pas être appropriée sur le plan culturel.

Le compagnonnage est une technique courante chez les secouristes de la protection civile, les pompiers et les ambulanciers. Dans ce système, deux collègues qui s'entendent relativement bien font un accord préalable selon lequel ils s'observeront mutuellement pour repérer les symptômes de stress et feront part de leurs réactions. Il n'est pas improbable que deux compagnons du personnel international et deux compagnons du personnel national s'organisent séparément. Les membres du personnel national et ceux du personnel international pourraient passer plus de temps hors des heures de travail avec leur propre groupe plutôt qu'entre eux car il pourrait y avoir des difficultés de langue. Pourtant, un système de compagnonnage qui rassemble un membre du personnel national et un membre du personnel international, s'ils s'ont suffisamment à l'aise l'un avec l'autre, pourrait être une expérience d'apprentissage utile pour les deux personnes concernées.

Des adaptations pratiques et de politiques pourraient également être nécessaires dans les situations très stressantes, par exemple en ce qui concerne le repos, la récupération et les contacts familiaux, aussi bien pour le personnel national qu'international. Ces adaptations pourraient avoir des implications à court terme sur le plan des ressources mais elles auront des avantages à long terme dans une mission ou dans l'organisation et le risque sera mieux géré par tous. Les adaptations pratiques pourraient inclure d'essayer d'améliorer les conditions de vie ou de réorganiser la configuration d'une équipe si une personne s'y est mal adaptée. Si les exigences de travail ne sont pas réalistes, parlez-en et fixez des priorités.

Avant d'entreprendre une action stressante ou éprouvante sur le terrain, comme rouler dans une zone dangereuse, extraire les morts des gravats de maisons détruites par un tremblement de terre, ou apporter les premiers

approvisionnements à un groupe de personnes souffrant de malnutrition aiguë, le chef d'équipe pourra organiser une brève séance d'information. Au cours de cette séance, il sera mentionné que l'action comprendra une exposition à des facteurs stressants. À son retour à la base, l'équipe pourra à nouveau se réunir pour un bref exercice de « désamorçage », c'est-à-dire une revue de l'expérience de la journée, des activités entreprises et des réactions émotionnelles de chaque membre de l'équipe.

Lorsqu'un membre du personnel affiche des symptômes de profonde atteinte après avoir subi un incident ou assisté à un incident critique, et qu'il est donc vulnérable aux troubles de stress post-traumatique, un premier secours émotionnel pourrait être indiqué. Il est essentiel, dans ce cas, d'écouter avec empathie les émotions du survivant. Soulignez que l'affliction qu'il ressent est une réaction parfaitement normale et saine, que la personne n'est pas en faute et qu'elle retrouvera son équilibre physique et psychologique avec du temps et du repos. Explorer des problèmes personnels et émotionnels plus profonds provoqués par l'incident devra probablement être laissé aux soins d'un psychothérapeute expérimenté.

La séance d'information avant une mission critique et le suivi demandent une formation et une préparation spéciales. Ils doivent être effectués par quelqu'un qui comprend le contexte mais qui n'en fait pas partie. Faites votre possible pour créer un environnement protecteur et coopératif pour la personne concernée en attendant l'arrivée du spécialiste : créez un endroit où elle se sentira en sécurité, où elle aura accès à des moyens de communication avec ses proches et où elle sera à l'aise physiquement. Soyez conscient que le survivant pourrait dénier la profondeur de son affliction et s'opposer à ce que vous fassiez appel à un spécialiste : précisez bien qu'en ce moment la personne pourrait ne pas être le meilleur juge de son propre état d'esprit et qu'il est préférable de demander les soins d'un spécialiste.

Aider un responsable souffrant de stress

Dans les contextes instables, les attentes envers les responsables sur le terrain ont tendance à être irréalistes, aussi bien sur le plan du volume de travail que sur celui du niveau de compétences nécessaires pour le réaliser. Le niveau de responsabilité peut être une source importante de stress, surtout lorsqu'elle n'est pas interrompue la nuit, pendant les week-ends ou pendant les vacances. Tout le personnel doit sentir que leurs responsables sont forts, solides, fiables et source de stabilité. Un haut responsable qui montre des signes de stress profond, ou qui continue dans son poste bien que souffrant d'épuisement professionnel, démoralisera probablement son équipe. Les tactiques suivantes peuvent aider les hauts responsables sur le terrain à surmonter le stress.

- Avouez vos propres limites, à vous-même et à votre équipe. Admettre que vous non plus n'êtes pas à l'abri du stress ne compromet pas votre autorité si votre gestion est conforme à des principes et des arguments défendables. Invitez chacun à accepter sa part de responsabilité.
- Développez de bonnes relations avec votre propre supérieur, que ce soit au niveau régional ou au siège. Demandez-lui de venir pour se rendre compte de près des réalités auxquelles vous faites face et demandez-lui de vous épargner les pressions inutiles venant du siège.
- Déléguez ou partagez les tâches avec un représentant adjoint, un chef de bureau, un haut administrateur de programme ou un agent de liaison en matière de sécurité. Cela vous sera très utile si ces personnes ont de l'expérience et des aptitudes et si elles ne sont pas elles-mêmes sur une courbe d'apprentissage raide. Insistez pour nommer une personne de grande qualité au poste.
- Essayez, tout en restant le décideur final, de créer autour de vous une équipe qui partage les responsabilités.
- Faites appel à une personne pour tester vos idées, ou peut-être à un compagnon parmi vos pairs dans une autre organisation.
- Gérez votre niveau de stress de la même manière que celle que vous recommandez à votre personnel

Au niveau individuel

Chaque membre du personnel a la responsabilité de gérer son propre niveau de stress. Les facteurs qui jouent un rôle dans ce domaine sont les caractéristiques personnelles, les attentes, le mode de vie et le fait de connaître ses propres limites.

Un certain nombre de caractéristiques personnelles permettent de résister à l'impact négatif du stress, parmi celles-ci : une image de soi positive ou de l'amour-propre ; une confiance en soi réaliste ; une vision d'un ordre moral ou une philosophie personnelle ; l'aptitude intellectuelle de voir les diverses dimensions d'une situation et non pas considérer une situation à travers ses propres émotions ; une bonne constitution physique ; la capacité d'être constructif et de voir les éléments positifs d'une situation ; et, par-dessus tout, un bon sens de l'humour. Tous ces attributs donnent une force émotionnelle et de la résilience. Acceptez le fait qu'il y a certaines choses pour lesquelles vous ne pouvez rien faire, et essayez de vous concentrer sur les domaines sur lesquels vous avez de l'influence.

Dormez bien, mangez sainement et contrôlez votre utilisation de substances telles que la caféine, les cigarettes et l'alcool, qui procurent un faux sentiment de relaxation mais qui aggravent le stress physique et nerveux. Créez-vous un « nid », un espace à vous dans lequel vous pourrez mieux vous isoler et vous

relaxer. Pratiquez régulièrement de l'exercice physique, surtout si vous êtes confiné dans une enceinte ou à un bureau pour raison de sécurité. Rester en contact avec ses amis proches et les membres de sa famille est important et est aujourd'hui plus facile et moins coûteux avec les téléphones mobiles et Internet. Allez voir vos collègues ou amis et essayez de parler d'autre chose que du travail. Utilisez votre temps libre pour vous relaxer. Le rire a un grand effet tonifiant et a des bienfaits non seulement mentaux mais aussi physiques.

Connaissez vos propres limites et celles de votre autosuffisance. Autrement dit, reconnaissez que vos réserves ne sont pas illimitées et que, quand vous atteignez la limite, il est prudent d'appeler à l'aide et de rechercher un soutien. L'affliction ne disparaîtra pas si vous la refoulez. C'est une réaction humaine parfaitement normale dont personne n'est à l'abri, alors parlez-en et demandez de l'aide lorsque vous en avez besoin. Vous ne saurez probablement pas quelles sont vos réactions au stress aigu face à un événement constituant un danger de mort avant de vous trouver dans cette situation, mais au quotidien vous pouvez être attentif à vous-même et apprendre à reconnaître les facteurs qui vous stressent et leurs symptômes. Le stress pourrait s'accumuler au fil des années. Informez l'organisation dès que vous aurez besoin d'une mission dans un contexte moins stressant ; mettez fin prématurément à un contrat à long terme si vous pensez que vous avez atteint votre limite, ou faites une pause plus longue entre deux missions stressantes. S'il n'y a aucune autre option, quittez votre emploi.

Expériences culturelles et situationnelles du stress et de la gestion du stress

Les notions de stress et de la gestion du stress ont tendance à refléter les idées occidentales concernant la santé mentale. Il ne faut pas présumer que ces idées seront valables ou facilement comprises dans toutes les cultures. Par exemple, dans certaines cultures, les responsables sont censés faire preuve d'autorité et ne pas se montrer coopératifs et attentifs à l'affliction personnelle. Dans d'autres cultures, il est rare de parler ouvertement de ses émotions et reconnaître que vous ne pouvez plus gérer votre niveau de stress serait un déshonneur. Dans de nombreuses sociétés, les personnes sont beaucoup plus susceptibles de surmonter le stress par le biais de rites sociaux que par des moyens individuels tels qu'un soutien psychologique.

Le personnel national pourrait avoir une réaction et une approche très différentes pour faire face à un événement que le personnel international pourrait considérer comme traumatisant. Il pourrait être très difficile de définir un événement critique pour les membres du personnel national qui vivent dans un contexte de violence depuis des années, ou même des décennies. Dans de telles situations, les comptes-rendus et la notion de stress post-traumatique pourraient leur sembler étranges. Étant donné que le personnel national

vit dans ce contexte, son expérience de la violence pourrait être exprimée en termes sociaux et politiques ainsi qu'en termes psychologiques. Son adaptation, efficace à long terme, pourrait avoir d'importantes dimensions de justice, de réconciliation et de compensation qui vont au-delà de ce qu'une organisation pourrait dans un premier lieu tenter de fournir sur le plan d'un soutien post-traumatique.

Il est conseillé d'essayer de comprendre comment le stress est perçu dans le contexte particulier. Demandez activement conseils et informations à vos collègues nationaux. Par exemple :

- Le concept de stress et de traumatisme existe-t-il dans cette culture ; comment est-il ressenti, identifié et décrit par la population ?
- Comment est-il géré traditionnellement et historiquement, et par qui ?
- Quelle est aujourd'hui la nature du stress et du traumatisme et comment a-t-elle changé par rapport au passé ?
- Quelles stratégies d'adaptation sont actuellement utilisées et pourquoi. Sont-elles efficaces ?
- Quelles ressources peuvent être utilisées pour aborder les besoins actuels ?

La nature de la réponse pourrait être plus importante que la rapidité avec laquelle elle est donnée.

Partie 4
Gérer la sécurité de la communication

Chapitre 7
Gérer la sécurité de la communication

7.1 Télécommunications[1]

7.1.1 Télécoms et sécurité

La technologie de la communication s'est considérablement développée au cours des dernières années, et a fourni aux organisations humanitaires des moyens de meilleure qualité et moins coûteux d'échanger et de gérer l'information. On trouve de plus en plus de réseaux de téléphonie mobile, même dans les régions isolées, ce qui réduit la dépendance traditionnelle des organisations vis-à-vis des radios. Les téléphones satellites, utilisés dans les zones sans couverture de téléphonie mobile ou dans lesquelles le service a été perturbé ou n'est pas fiable, sont de plus en plus légers et de moins en moins coûteux. L'Internet est également de plus en plus accessible même dans les régions isolées, grâce à la technologie satellite. La technologie de voix par le protocole de l'Internet (VOIP), comme Skype, a réduit le coût des appels longue distance et a facilité le contact avec le siège et les bureaux régionaux. Les récepteurs de Système de positionnement global (GPS), peuvent déterminer la position d'une personne dans des lieux isolés et permettre de communiquer avec d'autres acteurs sur l'endroit précis d'un village, d'un site de distribution ou d'un point de repère.

Ce chapitre étudie certains aspects fondamentaux de la gestion des télécoms du point de vue de la sûreté et surtout de la sécurité. En ce qui concerne la sécurité, le premier point sera non seulement d'établir des communications efficaces dans un contexte donné, mais aussi de définir comment maintenir la communication en situation de crise. C'est une question interne mais également inter organisationnelle. Il est important de ne pas présumer que la technologie des communications rendra, à elle seule, l'organisation plus sûre. Bien utilisée, elle peut être extrêmement utile. Si un membre du personnel venait à disparaître, ses collègues pourraient sans doute surveiller ses mouvements et déterminer le lieu où le contact a été établi pour la dernière fois, à l'aide d'un logiciel qui repère une personne par le biais de son téléphone mobile ou satellite. Les moyens de communication peuvent réduire l'exposition au danger en permettant à l'utilisateur de prendre les mesures de sécurité appropriées en fonction des alertes lancées par messages SMS

1 Cette RBP n'est pas un guide technique. Elle fournit toutefois des recommandations et indique où la compétence technique est essentielle. L'installation et l'entretien du matériel nécessaire à l'utilisation de la radio nécessitent une expertise technique. Des bonnes pratiques détaillées sur l'installation et l'entretien de l'équipement des télécommunications sont disponibles sur le site de l'ICT Humanitarian Emergency Platform, www.wfp.org/ict-emergency.

afin qu'une action préventive puisse être entreprise. Cependant, dans certains contextes, l'utilisation des ressources télécoms peut accroître le risque. Dans des contextes très dangereux, certains appareils de communication (comme les radios et les téléphones satellites) sont très chers et peuvent attirer les criminels et les groupes armés qui cherchent à les voler. La technologie des appareils GPS, des téléphones satellites ou des appareils photo numériques peut susciter la suspicion. En Somalie, par exemple, certaines ONG se sont aperçues que l'utilisation des appareils GPS ne valait pas les risques de sécurité qu'elle entraînait parce qu'on les accusait d'aider les acteurs militaires en leur donnant le positionnement des groupes rebelles. Dans les contextes où il y a une forte probabilité que la possession de ces appareils engendre le crime, le personnel doit recevoir instruction d'utiliser l'équipement avec discrétion.

7.1.2 Choisir un équipement de communication

Les systèmes de communication ont tous des avantages et des inconvénients, décrits ci-dessous. Des considérations générales sont tout d'abord développées.

Respect de la législation

Veillez à ce que l'équipement de communication respecte la loi et la législation nationales. Généralement, les réseaux de communication nécessitent une licence avec le gouvernement hôte. Dans certains pays, certains équipements de communication sont interdits.

Performance

Considérez la couverture locale/nationale/régionale/internationale. Quelles sont les distances couvertes par le système télécoms et avec quelle efficacité ? Les distances présentent un intérêt particulier dans le cas des radios (HF/VHF ; voir plus loin) et des téléphones mobiles. L'objectif standard est que la couverture soit disponible 90 % du temps sur 90 % de la zone. Les divers équipements ont également une différente durée de vie. La durée de vie moyenne d'une radio base peut être de plus de cinq ans, celle d'une radio mobile est de deux ans ou plus (en général la durée de vie du véhicule dans lequel elle se trouve), celle d'une batterie de radio portative est d'environ 18 mois si elle est utilisée tous les jours. L'équipement commercial, plus robuste et plus puissant, durera bien entendu plus longtemps qu'un kit « amateur » non commercial.

La compatibilité des réseaux est également une considération. Les télécoms sont-ils compatibles avec les installations publiques ou avec celles d'autres organisations ? Les réseaux inter organisationnels (p. ex. HF, VHF, UHF et les communications satellites) sont disponibles dans la plupart des urgences et peuvent offrir des avantages pratiques sur le plan des opérations et de la sécurité, mais les systèmes doivent être conformes aux normes établies. Dans les endroits où le Groupe des télécommunications d'urgence (GTU)

est établi, la principale organisation prestataire du service, le PAM, devrait pouvoir être en mesure de fournir des informations concernant l'équipement standard.

Les réseaux Internet ou de téléphonie mobile pourraient être occupés ou surchargés. Cela pourrait ralentir leur performance ou complètement bloquer les messages. En situation d'urgence, l'infrastructure locale a généralement été endommagée ou paralysée, et les services de téléphonie mobile et l'Internet pourraient ne pas être disponibles. De plus, certains types de téléphones mobiles, de radios et de téléphones satellites pourraient ne pas recevoir les appels de détresse ou les notices de sécurité quand le système est occupé à transmettre des données. Cela peut constituer un risque.

Coût

Les budgets des projets doivent inclure une estimation des coûts de l'équipement de télécommunication, qui peuvent grandement varier d'une région à une autre et selon les besoins du programme. Souvent, les besoins de sécurité justifient le coût de l'équipement de communication. N'oubliez pas d'inclure le coût de former le personnel sur l'utilisation de l'équipement, ainsi que les frais initiaux et de fonctionnement. Les téléphones satellite, par exemple, sont fiables mais entraînent des frais de fonctionnement élevés. Les communications radio HF sont moins fiables mais leur utilisation est gratuite une fois le premier investissement effectué.

Besoins opérationnels

Les besoins en communication seront fonction du type de programmes ou de projets que l'organisation mène. Les besoins d'une opération d'aide alimentaire à grande échelle, avec un parc de camions et plusieurs points de distribution, ne seront pas les mêmes que ceux d'un petit service d'accompagnement psychosocial dans une communauté ou d'un programme de recherche des familles. Tenez compte du nombre de zones couvertes par le projet, de la distance qui les sépare (y compris la topographie), du type d'activités prévues par le projet, du nombre de travailleurs envisagé dans chaque zone du projet et des installations déjà disponibles. Considérez également les changements de scénario et de nature des programmes : quels pourraient être les besoins futurs au fur et à mesure de l'expansion ou de l'adaptation des programmes ? Attendez-vous à des développements dans les programmes, avec des changements de personnel, différents scénarios de bureaux et de base et des besoins de déplacement variés.

Vulnérabilité

En temps de crise, certains équipements de communication pourraient être surchargés et ne plus fonctionner de manière efficace, ou pourraient

être délibérément arrêtés. Lorsqu'un incident de sécurité majeur ou une catastrophe naturelle (par exemple un tremblement de terre) s'est produit, les réseaux peuvent très vite être engorgés. Dans d'autres situations, les autorités pourraient interrompre l'utilisation des réseaux pour les appels privés afin de les laisser libres pour les services d'urgence. Les réseaux de téléphonie mobile peuvent également être fermés pour raisons de sécurité, par exemple en cas de coup d'État. Dans certains contextes, les téléphones mobiles, les téléphones satellites et les radios portatives ont été modifiés pour en faire des déclencheurs d'engins explosifs improvisés (IEI). Dans ces contextes, le réseau pourrait être interrompu suite à une explosion.

Les systèmes les plus fiables sont probablement les radios HF et VHF, les téléphones satellite et les communications sur Internet. Cependant, n'oubliez pas qu'il est possible de brouiller les ondes radio et d'interrompre l'accès à l'Internet. Une combinaison de plusieurs moyens de communication sera probablement l'option la plus sûre et la plus fiable, surtout en déplacement. L'avantage des systèmes tels que la radio HF/VHF et, dans une large mesure, les téléphones satellites, c'est qu'ils sont contrôlés par l'organisation et ne dépendent pas des installations publiques, qui peuvent subir des pannes techniques ou être placées sous un contrôle politique. Compter uniquement sur les installations publiques pour les communications internationales peut donner lieu à des coupures en temps de crise. De même, les téléphones mobiles et les réseaux VHF dont la couverture/portée est fonction des relais, sont très vulnérables. En temps de crise, les relais peuvent facilement être mis hors d'usage. Les téléphones fixes peuvent ne plus fonctionner si la centrale téléphonique est endommagée ou détruite. Est-il possible d'obtenir des pièces de rechange et l'expertise requises si des réparations étaient nécessaires ? L'organisation peut-elle obtenir des ressources externes ? Y a-t-il une bonne alimentation en électricité ?

Coordination inter organisationnelle

Dans de nombreuses régions opérationnelles à haut risque, le Groupe des télécommunications d'urgence (GTU) fournit des services télécoms à toute la communauté humanitaire, y compris aux ONG. Envisagez de contacter le groupe de travail local du GTU, ou le PAM, prestataire du service GTU, pour savoir quels services sont disponibles dans votre région d'opération. Les Nations Unies ont établi une politique sur les Normes minimales de sécurité opérationnelle (MOSS) qui, dans certaines situations à haut risque, exigent la mise en œuvre d'un système de communication indépendant de l'infrastructure locale. Dans les régions où l'approche *Saving Lives Together* (Sauver des vies ensemble) est utilisée (voir Annexe 3), des ONG pourraient avoir l'opportunité de participer au système de radio des NU. Dans certaines régions, des fréquences radio ont été spécifiquement mises en place pour les ONG.

Autorisations administratives, permis et propriété

Chaque pays est souverain en matière de communication interne et en exercera le contrôle dans une plus ou moins grande mesure, en premier lieu par la fourniture d'un permis. En temps normal, l'autorisation d'utiliser un équipement radio est donnée par le bureau national des postes et télécommunications. Toutefois, en temps de conflit, d'autres autorités gouvernementales, telles que le ministère de la Défense, peuvent avoir l'autorité suprême. Dans les pays où le gouvernement ne fonctionne pas, une organisation chef de file, généralement des NU, peut assumer le contrôle. Avant d'acheter et d'importer l'équipement, vérifiez bien : l'autorisation d'utilisation (licence d'exploitation) ; la fréquence allouée ; l'indicatif d'appel ; et le permis d'importation. S'il est actif, le GTU peut être une ressource utile. L'agent de la technologie de l'information et de la télécommunication (TIC) du PAM, ou le siège du PAM sur ictemergency@wfp.org , peut être contacté pour obtenir des informations et des conseils sur les systèmes de communication.

En général, l'autorité qui octroie la licence d'exploitation octroie aussi les fréquences. Notez que généralement le permis sera valable pour les communications nationales ; en ce qui concerne les communications radio internationales, les autorités d'autres pays peuvent aussi être contactées. L'autorité peut allouer un indicatif d'appel individuel et prélèvera un droit. Les questions qui seront probablement soulevées lors d'une demande concerneront, entre autres :

- Le type d'équipement utilisé, notamment sa fabrication, ses spécifications techniques, le numéro de modèle et la hauteur de l'antenne au-dessus du sol.
- Le nombre de stations de base et de postes mobiles et leur emplacement.
- Les fonctions de l'équipement (p. ex. voix uniquement ou fax/transmission de données également).
- Les heures d'opérations.
- Les langues qui seront utilisées pour les communications.
- L'encodage éventuel des communications.
- Les fréquences.

Une licence d'exploitation pourrait être une condition pour obtenir un permis d'importation. Renseignez-vous au préalable sur les droits et procédures d'importation et sur les procédures de dédouanement. Le non-respect de ces procédures pourrait signifier que l'équipement sera mis en attente aux points d'entrée.

Les équipements télécoms sont des ressources précieuses. Décidez, dès le début d'un projet, si ces ressources seront éliminées à la fin du projet. Certains pays insistent, au stade de l'importation (surtout lorsqu'une organisation a

demandé à être exonérée des taxes concernant le matériel « d'aide ») que les ressources du projet soient offertes au gouvernement hôte à la fin du projet.

7.1.3 Types d'équipement

Radios Haute fréquence (HF)

Les avantages des radios HF sont les suivants :

- communication de faible à très longue portée, sans station de relais ;
- moins affectées par les variations topographiques ;
- fort degré d'indépendance ;
- permettent de créer facilement des réseaux, avec multiples stations pouvant partager la même fréquence ;
- les messages peuvent être envoyés simultanément vers de multiples destinations ;
- contrôle simple ;
- bien adaptées pour être utilisées dans des véhicules ;
- adaptables aux conditions opérationnelles changeantes ;
- prix d'achat relativement peu élevé ; pas de frais d'appels ;
- il est relativement facile de diversifier les fonctions du réseau (voix, fax, localisation GPS, transmission de données SITOR ou PACTOR) ;
- possibilité d'intégration avec d'autres réseaux (téléphone/email) ; et
- demandent peu d'entretien

Les inconvénients sont les suivants :

- pas sûres - n'importe qui peut écouter ;
- nécessitent une immatriculation et un permis dans la majorité des pays ;
- la force du signal de transmission varie au cours de la journée en fonction de l'activité solaire ;
- « zone de silence » : pas de réception entre la longueur maximum de l'onde directe (onde terrestre) et le plus long rayon qui commence avec les réflexions les plus proches de l'ionosphère ;
- le personnel doit être formé pour pouvoir tirer tous les avantages du réseau ;
- nécessitent un équipement supplémentaire compatible pour permettre la communication avec les partenaires des NU ; et
- une expertise technique est nécessaire pour l'installation, et il peut y avoir interférences entre les HF et d'autres équipements électroniques si les radios ne sont pas installées correctement.

Un appareil radio doit avoir les capacités suivantes :

- Télédiagnostic : un poste peut en interroger un autre pour obtenir des détails sur les facteurs opérationnels tels que la puissance de sortie, la force

du signal et la tension de batterie. Cela permet le diagnostic d'obstacles possibles par un technicien qui ne devra pas être nécessairement présent.
- Appel d'urgence : les signaux de détresse sont automatiquement envoyés à un nombre de stations préprogrammées, en indiquant le degré d'urgence de l'appel au récepteur.
- Un GPS connecté à un ordinateur personnel possédant un logiciel de localisation peut interroger un GPS connecté à un poste portatif sans que les occupants du véhicule s'en aperçoivent. Les mouvements des véhicules peuvent ainsi être surveillés.

Les marques de radio HF les plus couramment utilisées sont Codan et Barrett.

Radios Très haute fréquence (VHF)

Les avantages des radios VHF sont les suivants :

- relativement peu chères ;
- utilisation facile ;
- construction solide : résistent aux chocs, à la pluie, etc. ;
- des réémetteurs bien positionnés peuvent augmenter la couverture de la zone ; et
- contact continu si les utilisateurs surveillent la VHF.

Les inconvénients sont les suivants :

- durée limitée de la batterie (des batteries de rechange ou rechargeables sont nécessaires) ;
- des relais mal positionnés limitent considérablement l'utilité du réseau ;
- les postes portatifs sont fréquemment perdus ou volés ;
- les relais sont très vulnérables aux dommages intentionnels ; et
- elles sont fortement dépendantes de la topographie de la région (portatif-à-portatif, 2–5 km ; portatif à base, mobile ou relais, 7–15 km. Les obstacles entre postes, tels que les hauts bâtiments ou les collines, causent une interférence avec le signal ; le positionnement sur un point élevé peut augmenter la portée).

La marque la plus couramment utilisée est Motorola.

7.1.4 Installer un système radio

Une expertise technique est nécessaire pour installer convenablement un équipement radio et pour former les utilisateurs à s'en servir correctement. Les organisations peuvent réduire les coûts en partageant cette expertise. Dans ce cas également, contactez le PAM ou le groupe de travail local en TIC pour savoir quelles ressources peuvent être partagées.

Positionner la station de base

La station de base doit être suffisamment proche du bureau de l'organisation pour être facilement accessible, mais suffisamment éloignée pour que le bruit venant de la pièce où se trouve la radio ne dérange pas l'activité du bureau et qu'il n'y ait aucune interférence avec l'équipement du bureau, tel que les ordinateurs, les photocopieurs ou les téléphones satellite. Une connexion pratique à une source d'alimentation est nécessaire, de même qu'un accès facile à l'extérieur pour les câbles. Dans une zone à haut risque, où une surveillance radio permanente est envisagée, pensez au confort des opérateurs radio. Pour des raisons de sécurité, tout l'équipement doit être alimenté par un interrupteur d'isolation. Cela peut assurer la sécurité de toute la station en cas de mauvais fonctionnement ou d'incendie.

Choisir et monter l'antenne

Tenez compte des caractéristiques de l'antenne, telles que la polarisation, la largeur de bande, la hauteur effective, l'impédance ainsi que la visibilité, et assurez-vous de sélectionner le bon type d'antenne (dipôle, verticale, en V inversé, large bande). En général, les antennes fonctionnent le mieux lorsqu'elles sont installées sur un terrain découvert et aussi haut que possible, p. ex. sur un toit. Une installation correcte de l'antenne est essentielle à la bonne performance du système radio.

Installer une radio HF dans une voiture

Le poste radio lui-même peut être composé d'une console de contrôle et d'un poste principal ; la console de contrôle doit être installée à un endroit où elle pourra être utilisée facilement, mais le poste principal peut être monté dans le compartiment à gants, sous ou derrière le siège. Il est indiqué d'effectuer une mise à la terre correcte de la radio et il est important que personne ne pose le pied sur quelque partie de l'installation que ce soit en entrant dans le véhicule ou en en sortant. Le positionnement et l'installation de l'antenne sont des facteurs cruciaux. Une mauvaise installation est souvent cause de pannes. Le support de l'antenne doit être boulonné ou soudé au châssis de la voiture pour garantir une bonne mise à la terre. La partie principale de l'antenne ne doit pas être en contact avec la carrosserie du véhicule. Pour des raisons de sûreté et de sécurité, il est judicieux de retirer l'antenne lorsqu'elle n'est pas utilisée. Celle-ci peut être stockée dans le véhicule. Effectuer des transmissions avec le moteur arrêté déchargera vite la batterie et doit donc être évité.

Alimentation en électricité

Aucune radio ne fonctionne sans électricité, et les générateurs et batteries fournissent généralement une alimentation de secours. Un mauvais entretien et de mauvaises révisions du générateur, un mauvais stockage et les déchargements/rechargements de la batterie sont des problèmes opérationnels courants.

Électricité

Étant donné les dangers de travailler avec l'électricité, tous les équipements doivent avoir une mise à la terre séparée et aboutir à des prises mâles et femelles adéquates. Un limiteur de surtension peut permettre d'éviter les dommages causés par des sautes de tension. Vérifiez que les fusibles et les disjoncteurs sont en bon état, qu'ils ont la taille appropriée et qu'ils ne sont pas surpassés ni court-circuités. Utilisez toujours des câbles à double isolation. Pour éviter les accidents, les câbles ne doivent pas être laissés à même le sol et ne doivent pas pendre.

Radiation

Les antennes émettent une énergie électromagnétique sous forme de radiation, qui peut être nuisible au corps humain. N'utilisez pas de radio portative dont l'antenne est endommagée ou dont la « boule » est manquante. Ne placez pas les radios portatives trop près de votre visage (une distance de 18 cm est recommandée). Les terminaux satellites, dont la densité d'énergie est très haute et orientée principalement dans une direction, constituent un danger particulier : lorsque vous utilisez un téléphone satellite, respectez la notice de danger de radiation, placez-vous comme indiqué et veillez à ce que personne ne traverse la zone de danger.

Danger de la foudre

N'oubliez pas que les antennes peuvent attirer la foudre. Une accumulation de tension statique dangereuse peut occasionner un foudroiement. Des précautions techniques peuvent être prises pour réduire le risque, notamment veiller à la mise à la terre de tout l'équipement.

Choc électrique

Si une personne reçoit un choc électrique, ne vous précipitez jamais pour la toucher ou pour essayer de la dégager. La première chose à faire est de couper le courant. Ce n'est que dans le cas où le courant ne peut être coupé que vous pouvez dégager la victime en la tirant ou en la poussant à l'aide de matériaux non conducteurs comme une corde sèche, un bâton sec ou des vêtements secs. Obtenez une aide médicale aussitôt que possible.

Brûlure occasionnée par la fréquence radio

Lorsque vous installez l'antenne sur le véhicule ou que vous la retirez, coupez le moteur pour éviter d'être victime d'une brûlure causée par l'antenne pendant la transmission. Ces brûlures sont particulièrement douloureuses car elles apparaissent sous la peau et la guérison peut prendre beaucoup de temps.

7.1.5 Téléphones mobiles

Les téléphones mobiles sont faciles à utiliser, relativement peu coûteux,

de petite taille et très répandus, donc discrets. Leur portée s'est étendue même dans les parties très isolées du monde. La possibilité d'envoyer des messages textes et des emails permet d'envoyer et de recevoir l'information discrètement (bien que les messages textes puissent être contrôlés). Une nouvelle génération de téléphones offre aussi l'accès à l'Internet. De nombreuses ONG prennent un téléphone mobile international et remplacent la carte SIM par une carte locale afin de réduire les coûts. Si l'intention est d'utiliser un téléphone de société pour ONG lorsque vous êtes à l'étranger, il sera important de vous assurer qu'il est déverrouillé. Certains téléphones sont livrés verrouillés et un fournisseur de services local pourra les déverrouiller pour permettre l'insertion de cartes SIM étrangères. Dans les lieux où il y a des fournisseurs de téléphones mobiles privés, il n'y a en principe pas de problème de permis, mais certains pays exigent une preuve d'identité et une adresse locale avant de vous fournir une carte SIM locale.

Très logiquement, dans de nombreux contextes opérationnels, les téléphones mobiles sont aujourd'hui le principal outil de communication des organisations humanitaires. C'est en partie pour cette raison qu'il est important de connaître quelques inconvénients spécifiques liés aux téléphones mobiles :

- Comme pour tous les systèmes de téléphonie, les utilisateurs ne peuvent généralement parler qu'à une personne à la fois, à moins de programmer un appel en conférence au préalable. Pour cette raison, les téléphones mobiles ne sont quelquefois pas aussi efficaces que les radios pour la diffusion rapide d'informations d'urgence ou de sécurité. De nombreux téléphones mobiles sont livrés aujourd'hui avec la fonction « parler pour parler » qui permet à ceux qui partagent le même réseau de communiquer (p. ex. Blackberry Messenger).
- Beaucoup de réseaux de sécurité intra et inter organisationnels reposent sur des messages textes qui peuvent très vite circuler dans une chaine de communication. Bien que la plupart des messages textes puissent arriver très rapidement, il y a parfois des délais assez longs. Pour les alertes importantes, certaines organisations demandent une réponse au texte pour en confirmer la réception, et appellent ceux qui n'ont pas répondu. La surcharge et la fermeture des réseaux peuvent être un problème.
- Les téléphones mobiles ont des limites de batterie. Si un téléphone mobile est un élément de sécurité majeur, il restera probablement allumé jour et nuit, et il sera donc important d'avoir une source d'alimentation en électricité fiable tout près, ainsi que le temps de recharger le téléphone. Autrement, ayez toujours avec vous une batterie de rechange ou un second téléphone.
- Parler et envoyer des messages textes avec des téléphones mobiles n'est pas entièrement sans risques. Tout comme les lignes fixes, les téléphones satellite et les emails, les communications par téléphone mobile peuvent

être écoutées ou interceptées. Le fait qu'un fournisseur de téléphonie mobile soit une société privée plutôt que publique n'est pas un obstacle majeur pour intercepter les appels.

- La plupart des téléphones mobiles qui ont la fonction GPS peuvent localiser l'utilisateur par un système GSM, c'est-à-dire qu'un satellite détermine la latitude et la longitude exactes du téléphone. Cela peut représenter un avantage ou pas, selon la personne qui localise l'utilisateur. Bien que cette fonction de localisation soit disponible dans le commerce, les ONG n'ont commencé à l'utiliser que récemment.

7.1.6 Communications satellite

La technologie satellite connecte les utilisateurs à des satellites en orbite plutôt qu'à des stations. Elle peut être utilisée pour la connectivité voix et données. Les communications satellite ont élargi la portée des communications sur le terrain beaucoup plus qu'il ne l'était possible auparavant et de nouvelles technologies font leur apparition tous les jours.

Le VSAT (terminal à très petite ouverture) est un appareil de communication satellite de grande puissance. Un VSAT comporte une parabole et une antenne satellite relativement petites et peut fournir une connectivité à l'Internet à tout un quartier. Les avantages du VSAT sont qu'il est compact et mobile, fiable lorsqu'il a été bien installé et relativement indépendant. Les inconvénients sont qu'il est relativement coûteux et vulnérable au vol, que l'installation des services de données peut nécessiter une expertise technique et qu'il peut être surchargé en temps de crise.

Certains fournisseurs de communications par satellite couramment utilisés par les organisations humanitaires sont Thuraya, Iridium et Inmarsat. Ces sociétés offrent différents types de communications phoniques et de données. Thuraya fournit des combinés, en particulier pour la connexion phonique, par son réseau satellite global. Il est utilisé surtout en Europe, en Afrique et au Moyen-Orient. Iridium offre des services similaires, principalement dans la région du Pacifique. Utiliser ces deux fournisseurs pour la connexion de données est également possible, mais le haut débit est limité et cela peut être coûteux. Récemment, Inmarsat a introduit BGAN (réseau global haut débit), qui permet un accès voix et Internet plus mobile et plus rentable qu'il ne l'était possible auparavant. BGAN peut permettre d'établir rapidement un bureau provisoire n'importe où dans le monde sans expertise technique nécessaire.

7.1.7 Téléphones fixes

Les téléphones fixes sont moins fréquemment utilisés car les services de téléphonie mobile sont aujourd'hui plus courants. Les problèmes perpétuels des fixes peuvent inclure de longues attentes pour l'installation et de fréquentes

pannes de service. Ceci dit, avoir un fixe n'est probablement pas une mauvaise idée. Ils sont en général plus avantageux financièrement et constituent une autre option lorsqu'un réseau de téléphonie mobile ou d'autres télécoms sont inaccessibles. L'accès à l'Internet par un téléphone fixe est généralement plus lent que par les autres moyens.

7.1.8 Discipline opérationnelle

Les principes clés de la discipline opérationnelle en matière de télécommunications sont la clarté, la brièveté et la sécurité.

Clarté et discipline dans la communication

Les consignes suivantes sont axées vers les utilisateurs de radios mais beaucoup concernent également les conversations téléphoniques.

La clarté et la brièveté sont obtenues par l'utilisation de termes précis de procédure et de signaux de communication (comme « over » [à vous] ou « say again » [répétez]). La clarté est également renforcée lorsque :

- les messages sont préparés à l'avance ;
- les messages sont présentés point par point ;
- les utilisateurs arrêtent de parler lorsqu'ils n'ont rien à ajouter ;
- les utilisateurs s'expriment avec des phrases courtes, dans un langage simple et standard de radiodiffusion, plutôt qu'en dialectes locaux ;
- les utilisateurs ne parlent pas trop rapidement, surtout lorsque l'interlocuteur doit écrire le message ; et
- ils parlent d'un ton normal (crier nuira à la qualité de la réception).

Il existe plusieurs moyens d'imposer la discipline, par exemple par l'identification automatique de l'appelant à l'aide de codes ID dans un système VHF, en limitant l'utilisation des radios au personnel autorisé et, dans le pire des cas, en retirant la licence d'exploitation pour cause d'abus répété.

Un carnet de bord est un élément essentiel d'une bonne gestion des communications radios. Les éléments essentiels de l'enregistrement des messages sont, entre autre, l'heure de la transmission, l'heure de l'enregistrement, la source du message ou de la transmission, l'identité de la personne qui tient le carnet de bord, le destinataire final du message, les points essentiels du message (écrits textuellement pour les messages importants), l'action de suivi à effectuer par l'opérateur radio ou par d'autres personnes, l'accomplissement ou pas de l'action et les défauts ou problèmes de l'équipement. Un bon opérateur radio a une bonne connaissance technique et une très bonne ouïe, une voix claire, un esprit clair et structuré et une écriture lisible, il a une bonne capacité de

concentration et un grand sens de la discipline. Pour le recrutement, les caractéristiques de la personnalité sont donc aussi importantes que les qualifications techniques.

Pour des raisons de sécurité, il est conseillé de toujours garder la radio « ON », sauf si des conditions de sécurité immédiates empêchent de le faire. Les radios éteintes ne peuvent recevoir les appels d'urgence ou d'autres appels relatifs à la sécurité.

Appels de détresse et de sécurité

Il existe, pour les urgences, un protocole international de radio approuvé (avec de nombreuses variations locales). L'appelant cherche à dégager la ligne en répétant trois fois : « MAYDAY MAYDAY MAYDAY » (SOS) ou « PAN PAN PAN » (MESSAGE D'URGENCE), généralement suivi de « ALL STATIONS » (À TOUTES LES STATIONS). Il est absolument impératif d'accepter les appels d'urgence et d'interrompre les conversations en cours. Un message de sécurité qui n'indique pas une menace envers la vie ou un bien (p. ex. un avis de troubles civils dans une ville qui doit donc être évitée) peut être lancé en répétant « SÉCURITÉ SÉCURITÉ SÉCURITÉ ».

L'encadré ci-dessous fournit des recommandations sur la façon de communiquer par radio en cas d'urgence. Il peut être attaché à tous les appareils de communication radio, téléphonique ou autre ou accroché dans les salles radio et sur les poteaux téléphoniques. S'entraîner à répéter cette séquence permettra de réduire les erreurs dans une situation d'urgence.

Comment communiquer en cas d'urgence

Suivez le modèle et l'enchainement d'informations suivants :

1) **Votre nom :** Bob Smith
2) **Votre organisation :** ONG ou organisation
3) **Votre lieu :** localisation GPS, ou routes, villes principales les plus proches, etc.
4) **Le type d'urgence :** accident de mine, mitraillage, évacuation médicale, etc.
5) **Le nombre de blessés**
6) **L'activité négative actuelle :** une opération de sauvetage peut-elle à présent être organisée en sécurité ?
7) **L'activité négative passée**
8) **L'heure de la prochaine communication**
9) **Comment contacter l'appelant :** numéro de téléphone, fréquence radio, etc.
10) **Autres informations**

Il faut répondre aux appels d'urgence, c.à.d. la réception doit être confirmée et l'identité de la station réceptrice donnée. Toutes les stations recevant l'appel d'urgence doivent confirmer, même si d'autres confirmations ont déjà été reçues. Les communications radio normales ne doivent pas être reprises jusqu'à ce que l'urgence ait été annulée. C'est généralement la station qui lance l'appel d'urgence qui a la responsabilité d'indiquer la fin de l'urgence. Les messages de sécurité ne nécessitent pas confirmation à moins qu'un protocole n'ait été établi dans ce sens. Ils peuvent être répétés à intervalles réguliers pour maximiser les chances d'être reçus par tous.

Dans des situations de crise, les décideurs peuvent être submergés d'une telle quantité d'informations qu'il est impossible de distinguer les faits des rumeurs. Pour être efficace dans ces situations, il sera important de limiter les communications à celles dont le sujet a une importance directe. Encore une fois, cela peut être réalisé avec une formation et de la discipline.

7.1.9 Préparation, formation et entretien de l'équipement

Au cours des dernières années, l'utilisation des radios a baissé en raison de la dépendance accrue vis-à-vis des téléphones mobiles. Cela indique que les pratiques actuelles peuvent être améliorées. Une approche sensée serait que le siège fournisse une formation de base pour tout le personnel recruté à l'échelon international, et que le bureau national fournisse une formation pour tout le personnel recruté à l'échelon national.[2] Il faudrait également des remises à niveau ou des formations spécifiques au contexte pour le personnel international. Des consignes écrites sur le langage standard de radiocommunication et les procédures d'utilisation de la radio ne peuvent se substituer à une formation pratique. Comme pour toutes les formations, les premières questions auxquelles les responsables doivent répondre sont : qui doit recevoir une formation, sur quel sujet (entretien et opération du matériel ; compétences en communication) et à quel niveau. Bien entendu, les opérateurs radio ont besoin d'une formation et de remises à niveau, comme tout membre du personnel qui utilisera la radio (p. ex. les responsables de projet à la base sur le terrain, ou tout membre du personnel ayant un équipement VHF). Les conducteurs de véhicules qui ont un poste mobile devront peut-être également recevoir une formation, par exemple sur l'entretien technique ou sur les procédures d'utilisation de la radio.

Si le véhicule d'un projet roule pendant des jours et des jours dans un contexte où la radio est son seul moyen de communication, au moins un membre de l'équipe doit être en mesure d'effectuer l'entretien et les réparations de base. Assurez-vous également que des pièces de rechange

2 L'ICT Humanitarian Emergency Platform fournit une formation aux organisations humanitaires aussi bien au siège que sur le terrain. Voir http://ictemergency.wfp.org

essentielles sont disponibles pour le véhicule. Si, au cours de leur travail, les membres du personnel qui ont été formés s'éloignent du véhicule, le conducteur doit savoir comment se servir de la radio ou du téléphone satellite en cas d'accident ou d'incident de sécurité.

7.2 Protéger l'équipement de communication

Comme toutes les ressources, l'équipement de communication et les ordinateurs peuvent être perdus, volés ou endommagés. Étant donné le rôle important que jouent ces ressources dans la gestion de la sécurité et dans le fonctionnement du programme en général, il est important de prendre les mesures nécessaires pour éviter ces problèmes. L'encrassement et les chutes sont les causes les plus fréquentes d'endommagement ou de destruction des équipements de communication. Chaque téléphone et chaque radio doivent être équipés d'un étui protecteur qui absorbera les chocs. Le coût de l'étui est beaucoup moins élevé que celui d'un nouvel appareil.

En plus des précautions usuelles contre le vol (voir Chapitre 9 : « Sécurité du site »), des mesures supplémentaires doivent être prises dans les zones où le risque de vol ou de sabotage est particulièrement élevé. Le nom de l'organisation ou un numéro d'identification peut être gravé sur l'équipement afin d'empêcher le vol ou d'identifier l'appareil s'il a été volé. Les ordinateurs peuvent être fixés aux bureaux avec un câble de sécurité pouvant être verrouillé.

7.3 Sécurité de l'information

L'information est cruciale pour le succès des opérations de toute organisation humanitaire. Grâce à l'amélioration des technologies, il existe de plus en plus de moyens de stocker l'information, d'y accéder et de la partager. Mais avec ces technologies, il y a aussi une plus grande nécessité de sécuriser l'information. Cela comporte deux éléments : la protection contre le vol et la protection contre des personnes ayant des intentions potentiellement hostiles. Les informations sur les membres individuels du personnel, les activités de l'organisation, les bénéficiaires visés et les contacts peuvent être utilisées pour nuire à l'organisation. Dans certains cas, le personnel pourrait dire ou écrire des choses qui ne reflètent pas réellement la mission et les objectifs de l'organisation et qui ne sont pas censées être partagées à l'extérieur. Dans d'autres cas, les informations pourraient simplement être mal interprétées ou prises hors contexte.

Étant donné que les valeurs de nombreuses organisations d'aide sont basées sur la franchise et la transparence, la question : jusqu'où aller pour protéger l'information, est très discutée. Néanmoins, de nombreux types de documents doivent être protégés. L'encadré qui suit énonce certains éléments liés à

la sécurité de l'information. Ces points peuvent être incorporés dans une politique de sécurité générale de l'organisation.

Éléments d'une politique de sécurité de l'information

- Une définition de ce qui constitue « des informations sensibles ».
- Qui est autorisé à prendre connaissance des informations sensibles.
- Comment les informations sensibles doivent être :
  - Stockées
  - Communiquées
  - Transportées
  - Épurées
  - Détruites.

7.3.1 Tenue et protection des documents clés

Selon la situation, les documents clés pourraient inclure :

- des copies des passeports, y compris des visas, du personnel international ;
- les listes du personnel international et national ;
- les dossiers individuels de santé, y compris les groupes sanguins ;
- les listes des plus proches parents ou autres personnes à contacter en cas d'urgence ;
- les listes des cartes d'identité de l'organisation et les détails qu'elles comportent ;
- l'inventaire des biens ;
- les numéros de châssis et de moteurs, et les copies des documents d'achat/d'importation ;
- les numéros d'identification de l'équipement des bureaux et les copies des documents d'achat/d'importation
- les numéros d'identification de l'équipement radio et les copies des documents d'achat/d'importation ;
- les listes des clés de maisons et de voitures, le nombre de jeux qui existent et qui les a en sa possession ;
- les contrats du personnel, les contrats avec les fournisseurs ou les prestataires de services, les contrats de location ; et
- les listes de numéros de téléphone (habitations, bureaux, contacts en cas d'urgence) et des fréquences radio.

Toutes ces informations, ainsi que des renseignements à jour sur les travailleurs internationaux qui sont enregistrés auprès de leurs ambassades respectives, doivent être immédiatement disponibles dans le bureau sur le terrain et au

siège. De nombreuses organisations encouragent leurs employés à conserver des copies de leurs passeports dans un fichier ou email provisoire dans leur compte email personnel (p. ex. Gmail, Yahoo). Il est possible d'accéder à ces fichiers numériques partout où il y a un accès à l'Internet.

De nombreuses informations sur les ressources humaines doivent rester confidentielles. Cela inclut les informations sur les troubles médicaux ou psychologiques, les salaires, les évaluations des employés et les actions disciplinaires. Gardez trace aussi des cartes d'identité de l'organisation et assurez-vous qu'elles sont rendues lorsque le personnel quitte l'organisation ou lorsque le personnel international quitte un bureau sur le terrain. Les travailleurs internationaux garderont leur passeport sur eux en fonction de la situation. En principe, il faut l'éviter ; donnez-leur plutôt une carte d'identité comportant les informations les concernant, avec une traduction dans les langues locales, ainsi que des photocopies de leur passeport. Les passeports sont une marchandise de valeur et peuvent être volés. Ayez-les sur vous uniquement lorsque les circonstances le demandent. En règle générale, les travailleurs doivent avoir sur eux une liste de contacts d'urgence, ainsi qu'une liste des fréquences radio, des autorités locales, de l'ambassade et, sauf si cela est jugé aggraver les suspicions et donc le risque, ils doivent aussi avoir des cartes. Des documents peuvent être confisqués, et le personnel doit donc mémoriser ces numéros. Il pourrait être nécessaire de faire des exercices de mémorisation des contacts clés et de leurs détails. Dans des situations très hostiles, où une personne pourrait être ciblée simplement parce qu'elle appartient à une organisation d'aide internationale, il sera sans doute déconseillé aux membres du personnel de porter sur eux tout document pouvant les identifier.

Les principes clés pour protéger l'information sont d'avoir des copies de sauvegarde et de les conserver ailleurs. Cela vous protègera contre les pertes, mais bien entendu ne vous protègera pas contre le vol. Des copies de sauvegarde des documents individuels fondamentaux et de tous les documents programmatiques et organisationnels doivent être conservées. Les documents fondamentaux doivent être sauvegardés à la fois sur support numérique et sur support papier. La base des bonnes pratiques pour protéger les informations sur papier incluent :

- Ne pas laisser traîner de papier près des imprimantes ou des fax.
- Les informations privées doivent être verrouillées et une copie doit être conservée dans un autre endroit, de préférence à l'étranger.
- Les informations potentiellement sensibles sur papier doivent également être verrouillées et une copie doit être conservée ailleurs, idéalement au siège.

- Ne pas mettre de documents sensibles dans une corbeille de recyclage de papier ou dans une poubelle. Déchiquetez-les ou brûlez-les.

Dans certaines circonstances, il pourrait être nécessaire de détruire les documents sensibles dans un bref délai. Détruire des dossiers est difficile et prend beaucoup de temps, et il pourrait donc être bon de minimiser la quantité de documents gardés au bureau, par exemple en tenant des fichiers électroniques plutôt que sur papier, et en transférant les dossiers de plus de deux mois dans des bureaux à l'étranger. Un moyen plus strict d'assurer la sécurité de l'information est de limiter le nombre de personnes qui prendront connaissance de sujets sensibles et qui auront accès aux documents fondamentaux.

7.3.2 Cybercriminalité

La cybercriminalité, c'est-à-dire le fait que des criminels cherchent à tirer profit de l'accès à des informations concernant le public, est une activité en plein essor, et tous ceux qui utilisent un ordinateur connecté à l'Internet sont vulnérables.[3] En général, les principales menaces sont l'introduction de logiciels malveillants (ou « virus ») ; la perte de confidentialité dans les communications ou le vol d'identité ; et les ordinateurs qui sont envahis par des pirates informatiques qui envoient des spams ou d'autres contenus négatifs tels que la pornographie. Pour la plupart, ces menaces seront traitées principalement par le service technologie de l'information. Les principales mesures à prendre sont l'introduction d'un logiciel antivirus et anti-espion, l'installation d'un pare-feu et avoir toujours des mots de passe forts. Le personnel doit également être formé sur l'utilisation des clés USB (memory sticks), car elles peuvent être une source de virus. Le personnel doit également être prudent en ce qui concerne l'ouverture d'attachements suspicieux et ne doit utiliser que les réseaux Wi-Fi (internet sans fil) protégés par un mot de passe.

Les intrus peuvent rapidement installer un logiciel espion, comme les programmes d'identification par touches de clavier (qui révèlent ce qui est tapé sur un clavier d'ordinateur). Ne laissez pas votre ordinateur allumé sans surveillance. Réglez votre ordinateur de sorte qu'il se verrouille automatiquement après quelques minutes de non-utilisation, et qu'on ne puisse le déverrouiller qu'avec un mot de passe fort. Les dispositifs de réseau, tels que les commutateurs, les routeurs, les serveurs et les modems, doivent être dans une pièce ou un placard sécurisé et bien ventilé. Cela évitera que des intrus installent des logiciels malveillants sur le réseau pour voler des données en transit ou pour attaquer d'autres ordinateurs sur le réseau.

3 Une excellente ressource sur le sujet est *Security-in-a-box : Tools and Tactics for Your Digital Security* (Trousse de sécurité : Outils et tactiques de sécurité numérique) (http://security.ngoin-abox.org), disponible en anglais, arabe, espagnol, français et russe.

Les emails peuvent être contrôlés par des ordinateurs qui scannent le trafic et recherchent certains mots clés, certains expéditeurs ou certains destinataires. Les mesures à prendre pour rendre le trafic email plus sûr comprennent entre autres :

- Créez un compte en utilisant un nom qui n'est pas lié à votre vie personnelle ou professionnelle.
- Utilisez un compte email plus sûr (https: au lieu de http:).
- Utilisez un logiciel d'anonymat pour cacher votre choix de service email à quelqu'un pouvant surveiller votre connexion internet.
- Utilisez un système de cryptage à clé publique sur le contenu des emails. Outlook, par exemple, permet d'ajouter une signature numérique qui authentifie l'expéditeur du message. Toutefois, l'utilisation d'emails cryptés peut vous rendre « visible » et attirer l'attention, et est illégale dans certains pays.

Même avec un système email très sûr, n'oubliez pas qu'il est impossible de contrôler ce qu'il advient d'un message quand il est dans la boite de réception du destinataire.

Comme pour les documents sur papier, les circonstances pourraient exiger d'annuler ou de détruire des fichiers sensibles enregistrés sur l'ordinateur. Malheureusement, annuler simplement un fichier ne signifie pas que l'information est supprimée et un pirate déterminé peut trouver beaucoup d'informations sur un disque dur. Supprimer un fichier efficacement exige des procédures particulières ou un logiciel spécial. Un spécialiste en technologie de l'information sera en mesure de vous conseiller à ce sujet. Dans des situations très tendues, où une action rapide est nécessaire, le moyen le plus rapide de se débarrasser d'information électronique est d'endommager ou de détruire physiquement le disque dur de l'ordinateur. Ceci est valable aussi pour les clés USB. En ce qui concerne les CD ou DVD, le meilleur moyen est de les couper en morceaux et de les éparpiller dans différents endroits. Une autre option est de les brûler.

Les endroits clés à ne pas oublier en effectuant le « nettoyage » sont :

- Les fichiers temporaires et les fichiers dans la corbeille.
- Les fichiers effacés mais pas « épurés » sur votre ordinateur ou sur un appareil de stockage externe (p. ex. les clés USB).
- Les informations sensibles sur CD et DVD ou stockées sur un serveur local.
- Les noms et contacts sensibles dans les répertoires de téléphones mobiles ou sur les cartes de contacts.
- Les photos sensibles sur les cartes mémoire des appareils photos et les films vidéo sur les cassettes vidéo.

- Les documents sur papier qui n'ont pas été déchiquetés.

7.3.3 Sécuriser les communications verbales

Les appels téléphoniques d'une ligne fixe, d'un téléphone mobile ou d'un téléphone satellite sont tous automatiquement enregistrés (numéro appelé, heure, durée de l'appel et parfois lieu) par le service de facturation de la société de téléphone. Les conversations de Skype à Skype (autrement dit entre deux terminaux d'ordinateurs), SMS voix et VOIP, sont plus privées que les conversations par téléphone fixe ou mobile, parce que Skype est sécurisé et crypte ou brouille d'une autre façon l'information transmise sur l'Internet. Skype protège entièrement contre l'espionnage occasionnel. Gardez présent à l'esprit, pourtant, que les conversations sur Skype ne sont pas totalement privées : un logiciel malveillant sur un ordinateur peut révéler des informations sur les conversations Skype échangées sur cet ordinateur, quelqu'un pourrait enregistrer la conversation du côté du destinataire et les noms d'utilisateur et mots de passe peuvent être volés. Utiliser Skype pour parler à un téléphone fixe ou mobile implique que la conversation se fait sur un réseau téléphonique public standard et qu'elle peut être surveillée sur ce réseau. Envoyer des messages textes ou échanger des fichiers sur Skype n'est pas nécessairement plus sûr que par email. D'autres canaux « plus sûrs » sont, entre autres, les téléphones payants publics ou les nouveaux téléphones mobiles prépayés, s'ils sont changés régulièrement.

En général, à partir du moment où un échange ne se fait pas face à face, il faut présumer qu'il peut être entendu par un tiers. Il est conseillé de vous exprimer de manière modérée, factuelle et non partisane. Si vous vous trouvez dans une situation où vous pourriez être visé par des actes criminels, terroristes ou militaires, il vous faudra peut-être encoder certaines informations qui pourraient révéler votre position ou vos mouvements. Il existe divers moyens de le faire. Utilisez des mots codes pour désigner des bureaux, des personnes, des routes et des points sur les routes, des véhicules et des types de cargaison, etc. C'est un procédé très répandu mais rarement bien utilisé et donc pas très efficace. Il nécessite des instructions méticuleuses et des accords préalables. Des expressions métaphoriques peuvent être utilisées pour faire référence aux événements sensibles sur le plan politique, comme par exemple « le ciel est couvert » peut indiquer qu'un lieu particulier est sous les feux de l'aviation ou de l'artillerie. Idéalement, les mots ou phrases codes sont connus par cœur (et non pas écrits dans un carnet de codes). Pour les événements sensibles sur le plan politique, les expressions métaphoriques doivent permettre un démenti plausible. Changez les codes occasionnellement parce que les observateurs les déchiffreront après un certain temps. Un code déchiffré peut constituer une vulnérabilité majeure. Notez aussi qu'avoir un trop grand nombre de mots codes peut induire le personnel en erreur.

Un moyen plus sophistiqué et plus difficile à déchiffrer est d'introduire un système comportant des références temporelles et spatiales approuvées par l'organisation. Par exemple, 14.00 heures peut être compris comme étant l'heure de référence interne (TEMPUS) et dans une communication toute référence à l'heure est en conséquence exprimée comme « TEMPUS plus 3 » ou « TEMPUS moins 6.45 ». Les positions spatiales peuvent également être déguisées, par exemple, en ajoutant toujours 50 km à la distance réelle, ainsi « Je suis à 75 km de la destination » signifie en réalité, à 25 km. Utilisez un langage que ceux qui pourraient écouter ne comprendront probablement pas. Ce système n'est efficace, bien entendu, que si les deux interlocuteurs se comprennent mutuellement.

7.4 Communiquer avec les médias

Ces dernières années, de nombreuses organisations humanitaires ont élargi leur action d'information auprès des médias. L'objectif principal est de sensibiliser le public sur une crise, de faire passer des messages de plaidoyer et d'augmenter la visibilité et le profil d'une organisation, ce qui peut ensuite aider à la collecte de fonds. Nouer le dialogue avec les médias peut également avoir des implications de sécurité. Une déclaration mal formulée, inexacte ou provocatrice peut mettre le personnel en danger direct et peut même entraîner l'expulsion d'un pays. Un service médias basé au siège et le personnel basé sur le terrain pourront parfois avoir des objectifs opposés. Ce qui renforce le profil d'une organisation à l'échelon international pourrait ne pas aider à créer un climat de confiance avec les communautés et les autorités sur le terrain. Un système clair doit être instauré pour nouer le dialogue avec les médias. Par exemple :

- Qui sera responsable d'engager les contacts avec les médias ? Qui rédigera les communiqués de presse ? Travailler avec les médias demande des compétences particulières qui ne seront peut-être disponibles qu'au siège ou dans les bureaux régionaux. D'autre part, le personnel chargé des médias pourrait ne pas avoir les connaissances locales et ne pas être en mesure de nuancer l'information de manière à respecter les sensibilités politiques. Pour les communiqués de presse, il peut être utile de travailler en collaboration, mais cela demande des efforts supplémentaires (et des télécommunications fiables). Pour cela, les rôles de chacun doivent être clarifiés avant une crise. En dernier ressort, les opinions du directeur pays et de son équipe doivent être respectées, quelles que soient les priorités médiatiques du siège. Dans la plupart des cas, la décision d'impliquer les médias doit être celle du directeur pays.
- Qui approuvera la version finale d'un communiqué de presse ? De nombreuses organisations ont découvert que, pour des raisons de sécurité, il était justifié qu'un directeur d'une organisation dans le pays ait l'autorité

absolue sur tous les messages médiatiques. D'autres membres du personnel régional et central devront peut-être avoir un rôle, selon l'importance et le profil global de la crise. Pour les organisations qui font partie d'une confédération, il sera important de fixer des règles de base qui détermineront quelle organisation peut publier ou approuver les communiqués de presse, puisqu'il faut présumer que les acteurs locaux ne feront pas la distinction entre, disons, « Save the world UK » et « Save the world Belgique ». Dans certaines circonstances, un forum inter organisationnel décidera de faire une déclaration commune. Négocier une déclaration faite par ce type de processus et se mettre d'accord sur son contenu prennent souvent un temps considérable. Dans certains cas les organisations ne pourront se mettre d'accord que sur une déclaration nuancée.

- Quelles personnes sont autorisées à donner des interviews ? Souvent, les professionnels des médias voudront parler aux personnes qui sont proches de l'action, mais ces acteurs ne sont pas toujours correctement formés à communiquer avec les médias. Identifiez au préalable les personnes qualifiées et offrez éventuellement une formation aux personnels clés sur la façon de répondre à une interview. Il pourrait être utile de limiter cette formation au représentant du pays uniquement.
- Il existe de nombreuses approches différentes pour travailler avec les médias ; décidez de la meilleure approche si possible avant qu'une crise majeure n'éclate. Par exemple, une organisation pourrait avoir des programmes de longue date au Pakistan. Elle devra avoir des plans en place sur les rapports avec les médias dans divers scénarios, tels qu'une grande catastrophe naturelle, une augmentation du terrorisme contre les organisations d'aide étrangères ou un accès de violence localisée non dirigée sur les entités étrangères. Il est utile d'avoir des déclarations et des communiqués de presse préparés, de sorte que lorsqu'une urgence survient, ou qu'une crise devient critique, les médias puissent être contactés rapidement. Il n'est pas très utile d'impliquer les médias sur un problème survenu une semaine auparavant.

7.4.1 Décider de nouer le dialogue

Dans certaines situations, le rôle des organisations internationales pourrait être si controversé que le fait d'attirer une plus grande attention sur ce rôle en travaillant avec les médias serait contre-productif. Dans ce cas, élaborez une bonne stratégie défensive, soit en refusant de commenter, soit en limitant vos remarques aux informations factuelles de base ou en clarifiant la désinformation par le biais de déclarations réactives brèves. Une telle approche serait utilisée en cas de rapt (voir Chapitre 14). Cependant, ne présumez pas que l'adoption d'une stratégie de sécurité discrète sur le plan des mouvements physiques (véhicules non marqués, établissements sans enseigne, etc.) impose automatiquement une stratégie médiatique discrète.

Certaines organisations ont découvert qu'elles n'agissaient pas suffisamment pour expliquer leur rôle et promouvoir leurs principes. Envisagez de sensibiliser les médias locaux, nationaux ou internationaux respectés comme moyen d'influencer les faiseurs d'opinions et les communautés locales.

7.4.2 Définir des objectifs et déterminer le message

Pourquoi nouer le dialogue avec les médias ? Qu'est-ce qui définit le succès ? Certains membres du personnel des services médias pourraient définir le succès par le nombre de « succès », ou par la couverture donnée à l'organisation (ou à la crise). Cela peut être utile pour renforcer le profil de l'organisation ou pour aider à demander des fonds au public avec un appel d'urgence. Mais cela rend-il les opérations plus sûres ? Cela pourrait-il même les mettre en danger, si les messages ne sont pas correctement exprimés ? Par exemple, lors d'une interview, si un membre du personnel exagère le nombre de personnes affectées par la sècheresse, le gouvernement, qui pourrait vouloir dédramatiser la crise, pourrait être irrité. Si l'objectif du travail avec les médias est en grande partie de faire avancer les objectifs de plaidoyer, mettez bien cet objectif en balance avec les préoccupations de sécurité. Par exemple, un communiqué de presse accusant un groupe rebelle particulier de violence envers la population civile pourrait irriter ce groupe et mettre les équipes sur le terrain en danger. Les messages qui renforcent la neutralité et l'indépendance pourraient favoriser la sécurité du personnel. Il pourrait être utile de préparer une liste de questions et réponses (Q&R) possibles avant une interview en vue de centrer les messages uniquement sur les personnes dans le besoin, sur la façon dont l'organisation les aide et sur les changements généraux qui doivent se produire pour que la population soit en plus grande sécurité.

7.4.3 Choisir le média

Si l'objectif principal d'une stratégie médiatique est de renforcer le profil international d'une organisation, la collecte de fonds ou le plaidoyer auprès d'acteurs internationaux (gouvernements étrangers, donateurs, les NU, etc.), la cible sera probablement les grands médias internationaux ou régionaux, voire peut-être les publications dans le pays où l'organisation est basée et où elle a des groupes intéressés actifs. Mais si l'objectif est également d'augmenter la sécurité du personnel en préconisant une meilleure compréhension de la mission et des intentions de l'organisation, les médias nationaux, locaux et même non traditionnels (comme les blogs Internet et le théâtre communautaire) seront très importants et demanderont une sensibilisation considérable au niveau du terrain. Clarifier les objectifs facilitera le choix d'un média. Définissez le type de public et identifiez les publications qu'il lit, les chaînes de télévision qu'il regarde et les stations de radio qu'il écoute. N'oubliez pas qu'une bonne stratégie médiatique locale sera toujours un supplément, et non pas un remplacement, d'une bonne

stratégie de sensibilisation des autorités locales, de la communauté et des acteurs qui pourraient être une source de menace. Le personnel local sera bien mieux placé pour déterminer la fiabilité et le professionnalisme des journalistes locaux – ces deux éléments peuvent grandement varier.

7.4.4 Établir des règles de base du dialogue

Le travail avec les médias, ne serait-ce qu'accepter de donner une simple interview, demande un entraînement et de l'expertise. Il est facile d'être pris au dépourvu par une question provocatrice et de dire quelque chose que vous pourriez regretter. Un examen complet des techniques des médias n'entrent pas dans le cadre de cette RBP. Cependant, les conseils pour assurer la bonne sécurité du personnel sont entre autres :

- La prudence lorsque vous imputez la responsabilité d'une crise. Dans de nombreuses urgences complexes, il ne sera pas possible de dire, sans équivoque, qui est responsable. Il est important de se mettre d'accord au préalable sur une réponse institutionnelle à donner aux médias. Soyez prudents lorsque vous transmettez l'information. Assurez-vous qu'elle a été vérifiée par une source fiable ; si ce n'est pas le cas, dites-le clairement. Répandre de fausses rumeurs pourrait attiser les tensions.
- Lorsque vous donnez aux journalistes des informations générales à titre confidentiel, assurez-vous que le journaliste est professionnel et objectif et mettez-vous d'accord sur ce que vous entendez par « à titre confidentiel ». Vérifiez comment la source d'information sera présentée. Certains moyens courants de masquer une partie de l'information dans les rapports médiatiques, tels que « une source haut placée aux NU » ou « les organisations humanitaires qui opèrent dans la zone de conflit » pourraient ne pas être très efficaces. Ces organisations pourraient être au nombre de quelques-unes uniquement, et il pourrait être évident à certaines personnes qui est la source haut placée.
- Tous les problèmes ne nécessitent pas l'attention des médias et il pourrait être approprié d'évoquer au préalable des problèmes possibles avec les autorités locales ou nationales, pour savoir s'ils peuvent être résolus par d'autres moyens.

Partie 5
Gérer des situations de menaces et de risques spécifiques

Chapitre 8
Sécurité des voyages et des déplacements

8.1 Sécurité à l'arrivée

8.1.1 Instructions avant le départ et à l'arrivée

Une connaissance du contexte et de la situation du lieu opérationnel est critique pour réduire les risques. Cela s'applique aux personnels, aux collègues et aux visiteurs. Les organisations doivent s'assurer que des procédures sont en place pour informer pleinement le personnel et les visiteurs sur le contexte général et sur les aspects de sécurité spécifiques à leur pays, leur région et leur zone d'opération. Dans toute la mesure du possible, ces informations doivent être fournies avant l'arrivée d'une personne dans le pays d'opération et complétées immédiatement à son arrivée.

Les préparations avant un déploiement sont une responsabilité partagée entre l'employeur et l'employé. La direction de l'organisation a la responsabilité de s'assurer que le voyageur a accès aux informations et à la formation nécessaires. Le voyageur a la responsabilité de s'assurer qu'il est suffisamment informé et préparé. Les éléments critiques à étudier avant le voyage incluent :

- Les risques de santé et la prévention.
- Les risques criminels et les risques violents.
- Les risques de catastrophe naturelle.
- Les risques d'accident (p. ex. les problèmes de sûreté relatifs aux compagnies aériennes ou aux services de transport maritime ou routier).
- Les numéros de téléphone essentiels (bureau, téléphones mobiles du personnel clé, centres médicaux, police, ambassades principales).
- Idéalement, un plan de la ville indiquant clairement les lieux principaux (notamment le bureau et l'hôtel). Si des plans ne sont pas facilement disponibles, des sources ouvertes telles que Google Earth peuvent fournir suffisamment d'informations géographiques.

L'information qui n'est pas sujette à des changements rapides peut être communiquée dans une note d'information avant le départ. Lorsque vous voyagez, assurez-vous d'avoir les numéros de téléphone essentiels sur vous – pas uniquement dans votre téléphone mobile : la batterie pourrait se décharger ou le téléphone pourrait être volé. Une séance d'information à l'arrivée complètera les orientations initiales.

8.1.2 Aéroports, ports, gares et taxis

Les aéroports, les gares et les ports sont souvent des zones à forte criminalité. Dans la mesure du possible, les nouveaux arrivants doivent être accueillis de préférence par une personne qu'ils connaissent. Si vous êtes attendu par une personne inconnue, obtenez au préalable le nom du chauffeur, son numéro de plaque d'immatriculation et son numéro de mobile ou, si cela n'est pas possible, demandez à voir sa pièce d'identité. S'il n'est pas possible d'avoir un chauffeur, essayez d'obtenir un taxi agréé prépayé. Montrez de l'assurance à tout moment : les criminels seront à l'affut de voyageurs perdus et désorientés.

Il pourrait être nécessaire, pendant une mission, d'utiliser des taxis plutôt que les véhicules de l'organisation. Les taxis peuvent être dangereux. Dans certaines villes, les risques de vol ou même d'agression sont importants. Les représentants locaux doivent avoir une liste de taxis fiables et de leurs numéros de téléphone, ou doivent identifier un chauffeur et une voiture fiables.

8.1.3 À l'hôtel

Lorsque vous signez le registre d'un hôtel, n'acceptez pas simplement la première chambre qui vous est offerte. Vérifiez son emplacement et ses points d'accès (portes et fenêtres) sur le plan de la sécurité. Si vous n'êtes pas satisfait de la chambre qui vous a été réservée, demandez-en une autre. Si cela n'est pas possible, envisagez de changer d'hôtel. Les facteurs susceptibles d'augmenter votre vulnérabilité sont, entre autres :

- Une chambre au rez-de-chaussée, en particulier si sa voie d'accès est couverte (p. ex. par la végétation).
- Une chambre à l'étage étage située près d'un escalier de secours ou d'une porte de service accessible à un intrus ; se sauver en cas d'incendie sera plus difficile si votre chambre se trouve à un étage très élevé.
- Une chambre située au bout d'un long couloir, loin des principaux mouvements du personnel et des clients, où des bruits suspicieux seront moins susceptibles d'attirer l'attention.
- Une chambre dont on peut facilement forcer la porte et la fenêtre, surtout si elle se trouve au rez-de-chaussée, et qui n'a ni verrou ni chaine de sécurité.
- Une chambre sans rideaux adéquats pour dissimuler qui se trouve à l'intérieur et sans ligne de téléphone qui fonctionne pour appeler le personnel de sécurité de l'hôtel.
- Un hôtel qui n'a pas de gardes ou qui est mal gardé, et qui n'a pas de service de nuit pouvant répondre à un appel d'urgence.
- Mettez en balance le besoin de vie privée avec le besoin de sécurité : envisagez de partager une chambre avec un collègue ou tout au moins d'avoir des chambres adjacentes et de rentrer à l'hôtel ensemble.

Ne laissez pas entrer dans votre chambre une personne que vous connaissez peu, par exemple quelqu'un que vous avez rencontré au cours de la journée, le chauffeur de taxi qui apporte vos bagages ou quelqu'un que vous n'avez pas appelé, par exemple le « personnel de service » vous apportant de la nourriture ou des boissons que vous n'avez pas commandées.

8.2 Véhicules et sécurité routière

Les accidents de la route, les détournements de voiture, le banditisme et autres attaques sur des véhicules sont, de loin, les causes les plus fréquentes de décès et de blessures chez les travailleurs humanitaires.

8.2.1 Choix d'un véhicule

Le choix d'un véhicule peut avoir un impact sur la sûreté et la sécurité. Les nouveaux véhicules passagers tous terrains sont très appréciés par les organisations humanitaires, mais ils attirent aussi les seigneurs de la guerre et les pirates de la route. Dans certains contextes à forte criminalité, les organisations utilisent délibérément de petites voitures non marquées, des motos ou même des charrettes tirées par des ânes, qui sont moins attrayantes pour les pirates de la route et qui constituent donc un moins grand risque pour les organisations. Des véhicules plus modestes peuvent également réduire le ressentiment de la population envers les organisations humanitaires, surtout lorsqu'ils se trouvent en transit ou dans des villes de base/bureaux où l'aide n'est pas distribuée directement à la population.

8.2.2 Sûreté des véhicules

La sûreté des véhicules dépend, en partie, du bon état de fonctionnement du véhicule : les niveaux d'eau, d'huile et d'essence doivent être vérifiés, les pneus doivent être en bon état, les ceintures de sécurité doivent être installées et utilisées, et l'équipement essentiel (cric, pneus de rechange, trousse de premier secours, etc.) doit être présent. Assurez-vous que les conducteurs vérifient leur véhicule quotidiennement, que les véhicules sont de nouveau vérifiés avant les voyages importants, que les mécaniciens sont compétents et que le responsable de la logistique tient un programme de révisions et d'entretien. Les utilisateurs des voitures doivent être formés pour effectuer les réparations de base.

8.2.3 Conduire en sécurité

La sécurité routière dépend également d'une conduite sûre, ce qui est en général un grand problème pour les expatriés tout comme pour les conducteurs locaux. Les conditions de route dans les contextes d'urgence comportent généralement un risque accru : le comportement au volant peut être moins discipliné, les routes principales peuvent être utilisées par des animaux, des cyclistes et des charrettes à bras, des tronçons de route

en travaux peuvent ne pas être signalés et les routes peuvent ne pas être éclairées la nuit ; les sentiers ruraux peuvent être boueux et les routes de montagne, dangereuses.

La conduite sûre nécessite la maîtrise de son véhicule, du terrain et de la circulation. Être maître de son véhicule signifie, par exemple, savoir comment conduire correctement un véhicule à quatre roues motrices, connaître la capacité du moteur dans diverses circonstances (accélération, côtes abruptes, etc.) et être conscient de la stabilité du véhicule sur différents terrains. Avoir la maîtrise du terrain signifie être apte à conduire prudemment et avec compétence, par exemple sur des sentiers sablonneux ou verglacés ou sur des routes de montagne, ou pouvoir traverser le lit d'une rivière. Maîtriser la circulation signifie reconnaître que d'autres utilisateurs de la route pourraient ne pas respecter les règles de la circulation ou pourraient conduire de manière indisciplinée. Il sera important d'adopter un style de conduite préventive ou défensive. Savoir conduire avec sûreté est particulièrement important pour le personnel international. Les personnes qui ne savent pas conduire (ou qui ne savent conduire que certains types de véhicules, par exemple les transmissions automatiques) devront apprendre à conduire avant leur déploiement et devront avoir la possibilité de s'entraîner au cours de leur déploiement.

Vitesse

Respectez toujours les limitations de vitesse imposées par les lois nationales, lorsqu'elles existent. Les excès de vitesse accroissent toujours le risque d'accident de la route et les coupables ne seront pas appréciés par les autochtones. Certaines organisations ont installé des appareils qui contrôlent la vitesse à laquelle la voiture roule. Les excès de vitesse ne peuvent être justifiés que dans des circonstances exceptionnelles, par exemple lorsqu'un tireur isolé constitue un risque.

Ceintures de sécurité

Les ceintures de sécurité doivent toujours être attachées. Ce n'est que dans les circonstances où une sortie rapide de la voiture pourrait être nécessaire, par exemple pendant une attaque aérienne ou un vol à main armée, que l'on pourra se dispenser d'attacher sa ceinture de sécurité.

Zones interdites et conduire la nuit

Certaines organisations définissent clairement des zones interdites dans les villes ou les régions dans lesquelles elles travaillent et elles appliquent également une politique d'interdiction de conduire la nuit pour tous les déplacements, professionnels ou personnels, hors du centre ville. Cette politique ne peut généralement pas être imposée au personnel national, mais elle peut sensibiliser aux risques possibles.

8.2.4 Les chauffeurs

Recrutement

Le recrutement d'un chauffeur est un aspect critique de la gestion pour au moins trois raisons :

- Les chauffeurs doivent être techniquement compétents et sûrs.
- Voyager beaucoup et être en mesure d'influencer les décisions à des moments critiques signifie que les chauffeurs ont un rôle important à jouer dans la gestion de la sécurité.
- Étant donné qu'ils sont en contact avec un grand nombre de personnes, les chauffeurs représentent, de manière informelle, l'organisation et influent donc sur l'image que la population en a.

Les chauffeurs doivent avoir :

- Un permis de conduire valide.
- Des compétences en langues (essentielles ou désirées).
- Une bonne acuité visuelle (elle doit être contrôlée).
- Une expérience de la conduite et un bon dossier de conducteur.
- Des compétences techniques pour l'entretien et les réparations (vérifiez-les).
- La capacité de conduire sur des terrains difficiles et dans une circulation chaotique (vérifiez cela aussi).
- Du sérieux. Vérifiez les références de la personne et ses réseaux possibles. Une référence sociale ou morale est un bon moyen de définir le sérieux d'une personne.

Dans les contextes dangereux, d'autres facteurs peuvent aussi entrer en ligne de compte, par exemple l'appartenance ethnique, l'âge, le tempérament, les compétences d'analyse et d'observation et les connaissances de la région d'opération.

Formation, mise au courant et supervision

Les chauffeurs doivent être formés et supervisés. Étant donné qu'ils représentent l'organisation de manière informelle, ils doivent être en mesure de faire un tableau bref mais exact de ce qu'elle représente et de ce qu'elle accomplit. Ils doivent recevoir également une formation en sécurité et assister à des réunions régulières avec le responsable de la logistique et le responsable de la sécurité.

Politique de conduite

Élaborez une politique de conduite pour les travailleurs qui ne sont pas chauffeurs. D'autres travailleurs nationaux et internationaux peuvent-ils conduire les véhicules ? Si oui, dans quelles conditions ? Cela pourra entraîner l'introduction de tests de conduite et de formations. Cette politique doit clarifier

les responsabilités en cas d'accident causé par un chauffeur ou par un autre membre du personnel. Prenez en considération également les dispositions d'assurance nécessaires pour les chauffeurs et les autres membres du personnel qui pourraient conduire.

8.2.5 Politiques organisationnelles relatives aux passagers et aux accidents

Passagers

Les chauffeurs et autres travailleurs à bord des véhicules doivent bien comprendre la politique de l'organisation en ce qui concerne le transport de passagers qui ne sont pas employés par l'organisation et les accidents mettant en jeu d'autres personnes. Dans la pratique, les politiques pourraient devoir être interprétées en fonction du niveau d'insécurité, ce qui pourrait amener l'organisation à introduire des règles strictes sur certains sujets tout en étant plus flexible sur d'autres. Les règes pourraient interdire de transporter des armes dans les véhicules de l'organisation (des autocollants avec le symbole d'un fusil barré d'une ligne peuvent être collés sur les vitres du véhicule pour rappeler cette règle à tout le monde) ; aucune cargaison autre que celle de l'organisation ne peut être transportée ; les véhicules ne peuvent être conduits par des personnes non-employées par l'organisation ; et les véhicules en mission ne doivent pas être laissés sans surveillance.

Des consignes peuvent également être établies sur la politique concernant les passagers. Elles peuvent être imprimées sur une carte laminée dans la langue locale pour permettre aux chauffeurs de montrer qu'ils respectent les ordres. Il est bien entendu possible d'insister sur le fait que personne d'autre que le personnel identifié de l'organisation ne peut voyager en tant que passager, mais cette décision pourrait être indéfendable et aller à l'encontre du but recherché : dans de nombreuses situations, un autochtone pourrait être emmené en voiture comme guide, ou le personnel pourrait offrir de déposer des personnes pour les remercier de leur hospitalité et essayer de créer de bonnes relations. Des exceptions pourraient aussi devoir être faites pour les malades et les blessés ayant besoin d'une aide médicale. Un document d'exonération de responsabilité, gardé dans la voiture, pourrait décharger l'organisation si quelque chose arrivait, quoique dans certaines circonstances une signature sur un papier aura probablement peu de poids. Évoquez au préalable avec les dirigeants de la communauté toute inquiétude concernant la responsabilité et les compensations en cas d'accident et, le cas échéant, consultez un juriste local.

Conduire des soldats en voiture est une autre difficulté. En général, évitez de prendre toute personne armée, en uniforme ou connue pour avoir des liens avec un groupe armé, surtout dans les régions où plusieurs parties adverses circulent. Ici encore, une part de jugement pourrait entrer en jeu, par exemple :

- Si l'organisation a besoin de protection armée temporaire et si une escorte militaire ne peut pas voyager dans un véhicule séparé.
- Si un soldat oblige un chauffeur sous la contrainte à le conduire quelque part, et si ne pas obéir à ses ordres pourrait mettre les passagers en danger (ceci doit être déclaré comme incident de sécurité).
- Si un soldat est blessé ou malade et nécessite des soins médicaux urgents (ceci doit également être déclaré comme incident de sécurité, surtout si cela pouvait compromettre la perception de neutralité).

Accidents

Des consignes devront être établies sur la façon de réagir en cas d'accident, surtout s'il occasionne des blessures ou la mort de personnes de la région. Dans certains pays, les conseils pourraient être de s'arrêter et d'aider la victime ; dans d'autres, ils pourraient être au contraire de ne pas s'arrêter mais de continuer jusqu'au prochain poste de police ou bureau de l'organisation si des observateurs sont susceptibles d'attaquer le chauffeur et son véhicule, qu'il soit responsable ou pas de l'accident. Si c'est le cas, l'organisation, ainsi que peut-être les agents de police locaux, devra revenir sur les lieux pour régler l'affaire. Ne laissez jamais des problèmes non résolus.

8.2.6 Appareils de protection

Protection contre le vol

Un certain nombre d'appareils permettent de protéger contre le vol, entre autres des capuchons de réservoirs d'essence pouvant être verrouillés, des écrous de roues antivol et des antivols de direction. Le nom de l'organisation peut être gravé sur les fenêtres et autres pièces détachées, pour décourager le vol ou pour aider à récupérer les pièces volées, le cas échéant. Un dispositif d'immobilisation électronique pourrait nécessiter les services d'un spécialiste. Un interrupteur caché servant à couper l'alimentation en carburant peut empêcher des voleurs de voiture d'aller très loin ; évitez les dispositifs servant à couper immédiatement l'alimentation en carburant, car les voleurs pourraient être furieux ou frustrés s'ils ne pouvaient pas faire démarrer le véhicule.

Radios

Les radios permettent à d'autres personnes de surveiller les mouvements d'un véhicule et aux conducteurs de signaler un problème et d'appeler à l'aide. Cependant, rouler avec une énorme antenne fixée à la voiture met en échec toute tentative de discrétion et pourrait aussi signaler la voiture comme cible intéressante pour les milices ou les criminels. Les téléphones mobiles sont des outils plus utiles, et les téléphones satellite peuvent servir de réserve. Arrêtez toujours la radio avant d'installer, de retirer ou de toucher l'antenne, afin d'éviter les brûlures occasionnées par les fréquences radio (voir Chapitre 7 : « Gérer la sécurité de la communication » pour plus de renseignements).

Système de localisation de véhicules

Un système de localisation suit un véhicule et peut indiquer sa position sur une carte stockée sur l'ordinateur de la station de contrôle. Il peut également être programmé pour envoyer un signal d'alarme lorsque le véhicule s'approche d'une zone d'exclusion. Il peut donc avoir une fonction de prévention en signalant aux occupants du véhicule qu'ils entrent dans une zone à haut risque ou qu'ils traversent une frontière, par exemple. De bonnes cartes avec des coordonnées géographiques précises sont nécessaires. Localiser un véhicule suite à un appel de détresse est utile mais ne renseigne pas sur le type de problème dont il est question et n'améliore pas la capacité d'intervention. Dans les contextes à forte criminalité où les détournements de voitures sont très répandus, les dispositifs de localisation peuvent être utiles pour localiser et retrouver les véhicules volés.

Feux clignotants

Dans les régions où les attaques aériennes sont un risque, les organisations ont installé des feux clignotants bleus ou orange sur les toits de leurs véhicules pour augmenter leur visibilité et faciliter leur identification. Cependant, si d'autres acteurs copient cette pratique, elle perd sa fonction de protection. Si cette stratégie est appliquée, communiquez avec les parties au conflit qui utilisent les bombardements aériens dans le cadre de leur action militaire. Dans ces cas, des déplacements coordonnés ou des procédures consultatives en matière de voyage doivent être envisagés. Par exemple, en 2006 au Liban, les Forces israéliennes de défense ont été informées des mouvements des convois humanitaires afin que les véhicules ne soient pas pris, par erreur, pour des cibles militaires.

Documents essentiels

Ayez une liste des :

- Numéros de moteur et de châssis de tous les véhicules (envisagez de prendre des photos des véhicules pour aider à leur identification en cas de perte ou de vol, et prenez note des signes distinctifs tels que les décalcomanies ou les couleurs).
- Documents et coordonnées des polices d'assurance.
- Détails sur le propriétaire du véhicule.
- Contrats de location.
- Contrats d'approvisionnement en carburant et d'entretien.

8.2.7 Planification des déplacements

Planifier les déplacements prend du temps, mais ce n'est pas une raison pour ne pas le faire.

- S'il y a un risque d'attaque ciblée, gardez le plan de voyage confidentiel.
- Étudiez la route et tous les points pouvant présenter des problèmes

(naturels, tels que les inondations et les passages enneigés ; et créés par l'homme, tels que les points de contrôle ou les endroits propices aux embuscades).

- Estimez la durée des voyages plutôt que la distance, et planifiez le voyage de sorte à arriver bien avant la tombée de la nuit ou avant le couvre-feu. Prévoyez du temps pour les demandes de renseignements locaux, p. ex. sur les risques de mines (voir Chapitre 15 : « Menaces liées aux combats et débris de guerre »). Prévoyez des délais possibles. Vous pouvez ensuite indiquer les heures estimées de départ, d'arrivée et de retour.
- Options d'urgence : existe-t-il d'autres routes ou des endroits de secours où vous pourriez obtenir de l'aide ou trouver refuge ?
- Créez un système de surveillance : les heures des appels radio, leur provenance et les intervalles des appels ; qui décide de dévier de l'itinéraire prévu ? Définissez des mots de code ou des phrases codées si nécessaire (voir Chapitre 7).
- Inspectez et préparez les véhicules au préalable : ont-ils eu une révision et sont-ils prêts ? Toutes les personnes concernées ont-elles l'équipement nécessaire ? Les conducteurs et les passagers savent-ils se servir de l'équipement ? Avez-vous tous les documents nécessaires pour les véhicules et les passagers ? Des copies de tous les documents essentiels sont-elles disponibles à la base ?

Avant le départ, il est utile d'organiser, pour l'équipe, une séance d'information au cours de laquelle le plan du voyage sera revu et analysé. À son retour, l'équipe devra être interrogée sur tous les changements survenus dans l'itinéraire adopté.

Si vous vous aventurez sur un territoire inconnu, prenez le temps de vous renseigner sur le paysage qui vous attend : posez des questions à la population locale et arrêtez-vous régulièrement sur la route. Si un guide local vous accompagne, obtenez des renseignements avant de partir. Demandez des renseignements sur la route, les points de référence utiles et l'état des routes, et tracez ensemble une carte comportant ces détails. Prenez des notes sur l'itinéraire et tracez des cartes pouvant servir à ceux qui vous suivront. Contrôlez les distances à l'aide du compteur. Si la situation sécuritaire le permet, envisagez d'utiliser un système GPS pour suivre l'itinéraire.

8.2.6 Points de contrôle

Les organisations humanitaires ont tendance à diriger principalement leur attention sur les points de contrôle, qu'elles considèrent comme des moments critiques d'un voyage. C'est en général exact : des hommes armés à un point de contrôle peuvent harceler, intimider et même menacer les travailleurs humanitaires. La situation peut déraper hors de tout contrôle s'ils

sont tendus ou saouls, ou s'ils sont offensés par ce que vous représentez, transportez, dites ou faites. Les échanges du personnel avec les gardes au point de contrôle influenceront la façon dont l'organisation est perçue et dont le personnel qui essaiera de passer par la suite sera traité. Soyez conscients des pratiques courantes des organisations humanitaires pour aborder les points de contrôle et tentez de les observer, par exemple en refusant de verser toutes « taxes » illégales ou des pots-de-vin.

Évaluation rapide

Les points de contrôle ne sont pas tous critiques au même niveau. L'une des compétences essentielles à développer est l'évaluation rapide du type de point de contrôle : où il est situé, qui y est en faction et quelle semble être l'humeur des gardes. Les points de contrôle aux carrefours, aux ponts, aux cols de montagne et à l'entrée et la sortie des villes sont à prévoir, et ils auront probablement été établis pour le contrôle général de tous les passants. Les points de contrôle au milieu d'une forêt ou sur une route de montagne loin des habitations pourraient être plus inquiétants. Les points de contrôle gardés par les forces régulières de l'armée et de la police peuvent être moins problématiques que ceux gardés par des forces irrégulières.

Lorsque vous vous approchez d'un point de contrôle, signalez clairement que vous n'avez aucune mauvaise intention :

- Informez la base avant d'arriver au point de contrôle et reprenez contact avec elle après l'avoir passé, mais pensez à éteindre la radio si vous jugez qu'elle pourrait attirer une attention négative lorsque vous passez au point de contrôle.
- Ralentissez.
- Baissez la vitre.
- La nuit, éclairez l'intérieur de la voiture afin que tous les passagers soient nettement visibles.
- Arrêtez la voiture à quelques mètres de la barrière, mais gardez le moteur en marche à moins que l'on vous ordonne de le couper. S'il y a plus d'un véhicule, celui qui vous suit devra garder ses distances.
- Enlevez vos lunettes de soleil afin que l'on voie votre visage et vos yeux.
- Évitez tout mouvement brusque dans la voiture et laissez vos mains bien en évidence.

Un porte-parole devra être identifié au préalable. Les chauffeurs jouent souvent un rôle principal soit parce qu'ils parlent pour l'équipe pour passer le point de contrôle soit parce qu'ils jouent aussi le rôle d'interprète. Ils doivent bien comprendre quand passer du rôle de porte-parole à celui d'interprète.

Tout membre de l'équipe pourrait potentiellement être interrogé. Il est donc nécessaire pour tous de savoir quelle cargaison le véhicule transporte et d'avoir la même version sur ce que fait l'organisation et le but du voyage. En plus de leur passeport, les passagers doivent également avoir une pièce d'identité établie dans la langue locale. Si l'on peut l'éviter, les passeports ne doivent pas être remis aux gardes. Si l'on vous demande d'aller dans une salle de garde, essayez de ne pas laisser le véhicule sans surveillance. Si l'un des occupants du véhicule est jugé être vulnérable ou en danger, accompagnez cette personne si les gardes lui demandent de sortir du véhicule pour l'interroger ou pour contrôler ses documents.

8.2.7 Convois

Les convois peuvent prendre différentes formes selon leur composition et ce qu'ils transportent ; le nombre de véhicules, le type de véhicules et le type de cargaison détermineront la longueur et la vitesse du convoi. Un long convoi pourrait réduire le risque par la force du nombre, mais il pourrait également se déplacer plus lentement ; il pourrait transmettre une image de pouvoir et de richesse. Cela pourrait éveiller le ressentiment et, de loin, le convoi pourrait être pris pour une colonne militaire en déplacement. Les petits convois pourraient être plus vulnérables aux embuscades mais il pourrait être plus facile de négocier le passage aux points de contrôle et ils sont moins susceptibles d'être ciblés par une attaque aérienne.

Les convois doivent être gérés et avoir un chef. Lorsque plusieurs organisations prennent part à un convoi, ou lorsqu'elles rejoignent un convoi sous protection armée exercée par des troupes de l'armée nationale ou par des soldats de la paix internationaux, il y a souvent une hésitation pour accepter le commandement. Cela peut affecter la discipline. Il n'est pas acceptable de rejoindre un convoi pour sa propre sécurité et ensuite de changer les règles ou de ne pas respecter la discipline du convoi.

Planifier le voyage

Élaborez un plan de voyage et définissez un point et une heure de rassemblement bien avant le départ. Obtenez des détails précis sur tous les véhicules attendus, ainsi que sur les passagers et les cargaisons. Rassemblez tous les documents qui seront nécessaires.

Organiser le convoi

L'ordre dans lequel les véhicules du convoi seront placés dépendra du nombre et du type de véhicules (camions, bus, véhicules passagers tous terrains, un véhicule citerne, une ambulance, un véhicule de transport du personnel armé) et de la cargaison et des biens qu'ils transportent, ainsi que du type de menaces et de problèmes anticipés (un véhicule embourbé lors

de la traversée d'une rivière, des camions lourds qui ne peuvent franchir une route enneigée, un barrage routier surveillé par des gardes irréguliers, des mines, une agression physique, etc.).

En fonction de ces scénarios possibles, réfléchissez à l'organisation du convoi. Si des problèmes créés par l'homme sont anticipés, envisagez d'envoyer un véhicule en reconnaissance en avant du convoi. Ce véhicule devra pouvoir maintenir le contact radio ; il devra probablement transporter le chef adjoint du convoi, plutôt que le chef lui-même. Demandez-vous également si le guide local partira avec le véhicule de reconnaissance ou s'il restera avec le convoi principal. Le chef de convoi devra voyager en tête, mais une personne ayant de l'expérience et une autorité décisionnelle devra également se trouver en queue. Décidez si vous allez avoir une communication par radio ou par un autre moyen entre la tête et la queue du convoi ; établissez peut-être un signal codé à l'aide des klaxonnes et des phares. Les escortes armées devront voyager dans des véhicules séparés. Si les escortes n'ont pas leur propre transport, vous pourrez leur fournir un véhicule, mais toutes les marques d'identification de l'organisation devront être retirées. Idéalement, une escorte armée devra être répartie sur plus d'un point du convoi. Enfin, les bus ou autre véhicules passagers devront être placés au centre, avec les fournitures médicales, la nourriture, l'eau et les couvertures. Ayez un nombre suffisant de véhicules, de sorte que si l'un d'entre eux tombait en panne, le convoi puisse continuer.

Vérifications avant le départ

Avant le départ, le chef de convoi doit s'assurer que tous les véhicules ont été vérifiés :

- Les véhicules sont-ils adaptés pour le voyage (p. ex. les camions ont-ils la taille et le poids indiqués pour négocier tous les ponts et les tunnels sur la route ?).
- Ont-ils tous suffisamment de carburant et de pneus de secours ?
- Peuvent-ils aborder des terrains difficiles ?
- Tous les documents nécessaires sont-ils prêts ?

Il est très important que le chef de convoi connaisse les détails des cargaisons et il doit avoir le droit de les contrôler avant le départ.

Communiquer les règles du convoi

Tous les conducteurs du convoi doivent savoir qui est le chef de convoi et son adjoint, et tous doivent connaître les règles du convoi. Les règles générales de déplacement doivent inclure la vitesse du convoi (qui doit être celle du véhicule le plus lent), les distances minimales et maximales entre chaque véhicule, l'allumage des phares pour un meilleur contact visuel, les

régulations sur l'utilisation de la radio ou les communications par téléphone mobile dans le convoi et entre le chef de convoi et le bureau de contrôle, ainsi que les arrêts et haltes de repos convenus.

Les règles générales incluent : déterminer comment le convoi réagira à l'approche d'un point de contrôle, ce qu'il fera si un véhicule a des problèmes à un point de contrôle alors que les autres ont l'autorisation de passer et ce qui arrivera si un véhicule tombe en panne mais ne peut être réparé immédiatement. Il est arrivé que des conducteurs de camions soient tués lorsqu'ils sont restés près de leur véhicule tombé en panne.

Garder la distance

Garder la distance adéquate entre les véhicules du convoi peut être difficile. La distance entre chaque véhicule ne doit pas être trop important afin de toujours garder le contact visuel ; mais elle ne doit pas non plus être trop courte et exposer ainsi tous les véhicules aux mêmes incidents (une embuscade, une bombe placée sur le bord de la route, une collision avec le véhicule qui vous précède ou qui vous suit due à un dérapage sur une route verglacée, les dégâts occasionnés par l'explosion d'une mine). La distance appropriée varie selon le terrain, les conditions météorologiques et les conditions de sécurité, et devra sans doute être ajustée au cours du voyage.

Si vous ne voyagez pas en convoi, il est généralement souhaitable d'essayer de garder une grande distance entre votre véhicule et les convois ou véhicules individuels des forces de sécurité. Les acteurs militaires et leurs véhicules pourraient être la cible d'une bombe sur le bord de la route (EEI). S'ils se rapprochent trop, ralentissez et laissez-les vous doubler. Si vous vous trouvez à proximité d'une explosion, évitez, tout au moins immédiatement, de répondre à votre impulsion naturelle et de vous approcher pour examiner la situation ou porter assistance. La meilleure réaction est de vous arrêter, de sortir de votre véhicule et de vous abriter à même le sol ou sur le bord de la route pour éviter les feux croisés possibles[1].

8.3 Déplacements sur la route : préparation et réponse à un incident

Cette section porte principalement sur les vols à main armée sur la route et sur les détournements de voiture. D'autres types de menaces non liées à la sécurité en voyage et en déplacement sont abordés dans un autre chapitre de la Partie V.

1 Tiré de l'ouvrage de David Lloyd Roberts, *Staying Alive : Safety and Security Guidelines for Humanitarian Volunteers in Conflict Areas* (Rester en vie : Consignes de sûreté et de sécurité destinées aux bénévoles humanitaires dans les zones de conflit) (Genève : CICR, 2006).

8.3.1 Analyse de la menace et préparation

Les pirates de la route chercheront à voler votre véhicule. Les voleurs armés ne voudront peut-être que des objets de valeur, mais ils pourraient utiliser votre voiture pour prendre la fuite.

Une bonne analyse des caractéristiques des incidents peut aider à identifier les zones à haut risque. Elle peut également indiquer des heures à haut risque, par exemple les pirates de la route s'emparent des véhicules le matin, au moment où leurs propriétaires les prennent pour partir ou le soir lorsqu'ils rentrent chez eux. Dans ces cas, regardez bien autour de vous avant d'entrer et de sortir de votre voiture. Ou bien, les détournements de voitures ont lieu à un point d'arrêt : à un feu rouge, par exemple. Essayez donc de ne jamais être la première voiture en attente à un feu rouge afin de réduire le risque. Plus fréquemment, les pirates de la route et les voleurs armés sont dans une voiture et peuvent suivre le véhicule visé puis soudain le doubler et le forcer à s'arrêter. S'ils connaissent la route empruntée habituellement par la victime et si l'attaque a été prévue, les agresseurs peuvent attendre et brusquement bloquer la route en garant leur véhicule devant la voiture ciblée. Une autre technique utilisée par les voleurs est de simuler un accident en heurtant un véhicule pour l'immobiliser et forcer le conducteur à sortir. Si cela arrive, ne vous arrêtez pas immédiatement mais indiquez à l'autre voiture de vous suivre et essayez d'aller dans un lieu bien éclairé et où il y a du monde. Vérifiez constamment si un autre véhicule vous suit. Si vous pensez être suivi, retournez au bureau. Appelez avant d'arriver pour avertir les gardes et l'agent de sécurité.

Serrures et ceintures de sécurité

Verrouiller les portières de la voiture ou pas en conduisant est également une décision contextuelle. Dans les régions où les voleurs opèrent généralement sans armes (p. ex. lorsqu'ils s'emparent d'un sac déposé sur le siège d'une voiture arrêtée à un feu) ou avec un couteau, verrouiller les portières offre une protection et vous donne quelques secondes pour pouvoir accélérer et vous éloigner du danger. Cependant, si une analyse des incidents révèle que les voleurs armés sont susceptibles de tirer s'ils rencontrent un obstacle qui gêne leur tentative, il pourrait être plus sûr de ne pas verrouiller les portières.

8.3.2 En cas d'accident

Essayer de s'échapper

La formation spécialisée dans le domaine de la sécurité enseigne aux conducteurs comment mettre rapidement leur véhicule en marche arrière, percuter un véhicule pour le faire quitter la route ou foncer sur un véhicule qui vous bloque le passage. Sauf si vous jugez être un expert, ces tactiques ne sont pas conseillées. Vous provoqueriez probablement une fusillade ou un accident de voiture. Présumez toujours que les agresseurs sont armés et

qu'ils tireront si vous tentez de vous échapper. Ceci dit, si votre analyse des menaces indique que des personnes sont souvent la cible de tirs et sont tuées pendant un détournement de voiture, vous déciderez sans doute d'adopter une action d'évitement.

Types d'agresseurs

Il existe deux catégories de voleurs armés : les voleurs sans expérience, opportunistes, souvent des adolescents, et les voleurs expérimentés. Les voleurs expérimentés pratiqueront probablement des techniques d'intimidation et de soumission : ils pourraient vous forcer à vous placer face à la voiture, à vous agenouiller ou à mettre les mains derrière la tête et pourraient pointer leur arme sur votre tête. Ils pourraient vous frapper fortement sur la tête ou le cou pour indiquer qu'il ne faut pas résister ; ce que vous ignorez, c'est s'ils seront susceptibles de tirer s'ils pensent que vous résistez. Les voleurs expérimentés pourraient également pratiquer des techniques d'embuscade, c'est-à-dire bloquer votre voiture à l'avant et à l'arrière pour vous empêcher de fuir. Tenter de faire une marche arrière ou d'accélérer pour vous sortir de l'embuscade pourrait être anticipée par les agresseurs et déclencher une fusillade. Les voleurs inexpérimentés pourraient être plus dangereux : ils pourraient être beaucoup plus nerveux, stimulés par la drogue ou l'alcool et ne pas être maîtres de leur arme ou d'eux-mêmes ; un coup peut partir très vite et presque involontairement.

En général, les voleurs seront attentifs à tout signe de résistance et nerveux s'ils sont retardés. N'oubliez pas :

- Aucune somme d'argent ou aucun véhicule n'est plus précieux que votre vie.
- Ne mettez jamais votre vie en danger en opposant une résistance à un vol armé.
- Gardez vos mains bien en évidence et ne faites pas de gestes brusques.
- Évitez les signes de colère, d'impolitesse ou d'agression.
- Remettez votre véhicule et les objets précieux comme on vous l'ordonne.

Si on vous ordonne de quitter le véhicule, ne tentez pas d'emporter quoi que ce soit avec vous (par exemple un sac personnel). Obéissez rapidement aux ordres des agresseurs, mais ne prenez pas l'initiative d'une action, par exemple sortir de la voiture ou remettre aux agresseurs votre portefeuille ou les clés de la voiture, à moins qu'ils ne vous en donnent l'ordre.

Moments dangereux

Les mouvements spontanés peuvent déclencher une réaction de vos agresseurs. Ne saisissez jamais la poignée de la portière, ne détachez jamais votre ceinture de sécurité et ne touchez jamais le frein à main par exemple, sans alerter les

agresseurs de ce que vous faites : ils pourraient penser que vous allez prendre une arme. Gardez vos mains en évidence et dites ou signalez ce que vous avez l'intention de faire avant tout mouvement. Laissez la portière de la voiture ouverte après être sorti. Remettez vos objets personnels si on vous le demande. Ne montrez aucune résistance, crainte ou colère.

Négocier

Dans certaines circonstances, il vous sera peut-être possible d'essayer de négocier : par exemple, pour garder votre passeport ou la radio, pour avoir l'autorisation de lancer d'abord un appel de détresse ou pour garder une quantité d'eau ou de nourriture (lorsque l'embuscade a lieu dans une zone isolée loin de toute assistance). Encore une fois, il faudra juger de la situation : en général, évitez de négocier lorsque les agresseurs sont très nerveux, visiblement anxieux de quitter les lieux aussi rapidement que possible, ou très agressifs.

8.4 Voyager en avion et en bateau

Les organisations humanitaires utilisent les lignes commerciales et les services maritimes, et peuvent également affréter un avion ou un navire. Les petites lignes commerciales peuvent émerger et disparaître très rapidement. Toutes ne répondent pas aux normes de l'aviation internationale en matière de sécurité. Certains transporteurs nationaux ne répondent pas non plus à ces normes. Les entités telles que la Commission Européenne ont une liste des compagnies aériennes interdites par l'Union Européenne pour raisons de sécurité. Songez donc à éviter ces compagnies.

Il peut également y avoir des problèmes considérables avec les navires commerciaux opérant d'un pays à un autre ou à l'intérieur d'un même pays, surtout dans les régions où le temps est fréquemment mauvais. Si les normes de sécurité officielles ne sont pas appliquées, les navires pourraient être surchargés et avoir un nombre insuffisant de canots ou de gilets de sauvetage pour tous les passagers, un équipement incendie inadéquat et une cargaison mal arrimée, ce qui accroît le risque de chavirer sur une mer agitée. Évitez, si possible, d'utiliser ces navires. Si vous devez les utiliser, amenez votre propre gilet de sauvetage et restez sur le pont pendant la traversée afin de pouvoir quitter rapidement le bateau si la situation se dégradait.

Si vous affrétez un avion, un hélicoptère ou un bateau, définissez clairement quelles normes de sûreté et de sécurité vous voulez voir en place ; et vérifiez qu'elles le sont.

- La sûreté de l'avion ou du navire. Existe-t-il un dossier d'entretien ? S'il s'agit d'un navire voyageant sur la mer, a-t-il des pièces de rechange, un

deuxième moteur et une batterie de secours ? L'équipement de navigation et de communication fonctionne-t-il correctement ? Y a-t-il des gilets de sauvetage, des fusées de détresse, des lampes électriques, des extincteurs en bon état de fonctionnement et des rames de secours pour les canots de sauvetage ? Y a-t-il suffisamment de carburant, au-delà de la capacité estimée nécessaire pour le voyage ? Le poids de la cargaison est-il dans les paramètres de sécurité et la charge est-elle bien arrimée ?

- Les qualifications du pilote/capitaine et de l'équipage. Le pilote/capitaine a-t-il un permis ? Les membres de l'équipage ont-ils des compétences mécaniques adéquates ? Parlent-ils les langues nécessaires ?
- Voyager en sécurité dans un contexte potentiellement hostile. Quelles sont les prévisions météorologiques ? Le pilote/capitaine utilise-t-il des cartes ou diagrammes corrects et connaît-il les conditions de sécurité actuelles ? Quelles informations pouvez-vous lui donner ? L'autorisation préalable des autorités est-elle nécessaire ? La situation de sécurité sur la piste d'atterrissage prévue ou au port de destination est-elle confirmée ? Que ferez-vous si vous ne pouvez pas obtenir plus de carburant sur la piste d'atterrissage ? Comment l'avion/l'hélicoptère/le navire est-il identifiable (couleur, logos) ? êtes-vous sûr que l'avion ou le navire n'est pas impliqué dans le trafic (d'armes ou de minéraux par exemple) et que l'on ne pourrait pas penser que telle est leur activité en opérant sous contrat pour vous ?

8.5 Liste de contrôle pour la préparation du personnel

Voyageurs et nouvelles recrues

- Consultez vos responsables et assurez-vous que vous recevez vos instructions avant le départ. Faites également vos propres recherches ; ayez les numéros de téléphone essentiels sur vous et demandez conseil sur les moyens de transport locaux fiables si personne ne vous attend à l'aéroport.
- Veillez à recevoir des instructions complètes sur la sûreté et la sécurité à votre arrivée.

Conducteurs et personnel sur le terrain : compétences et équipement essentiels

- lecture de cartes et utilisation d'une boussole ;
- maîtrise du véhicule, du terrain et de la circulation ;
- un kit de réparation de voiture de base pour vous permettre de rentrer ;
- les instructions sur la conduite et la discipline des convois ;
- les messages clés sur l'organisation et sa mission ; et
- une formation par simulation : sous une attaque aérienne, dans une zone minée, face à un vol à main armé sur la route, à un point de contrôle, la planification d'un voyage, s'aventurer sur un territoire inconnu.

Responsables de la logistique : compétences clés

- compétences en réparations avancées d'un véhicule ;
- compétences de formation de chauffeurs ou critères précis pour identifier un bon formateur de chauffeurs ;
- compétences dans l'installation et l'utilisation d'appareils de protection ;
- gestion du parc de véhicules et programmation des entretiens et des réparations ;
- simulations sur la planification de voyages ;
- simulations sur la formation d'un convoi ; et
- gestion de la sécurité.

Responsables sur le terrain

- s'assurer que les notes d'instructions avant le départ et à l'arrivée sont fournies ;
- définir les critères de recrutement des chauffeurs ;
- définir la politique pour les chauffeurs et la politique de discipline (qui est autorisé à conduire, quel véhicule et quand) ;
- définir la politique pour les passagers et les accidents (procédures et consignes) ; et
- simulations sur la formation d'un convoi.

Chapitre 9
Sécurité du site

La protection du site peut empêcher les intrusions ou y mettre fin, retarder une attaque et atténuer les effets d'un incident survenu à proximité immédiate.[1] « Site » fait ici référence aux biens immobiliers utilisés par l'organisation de manière régulière, notamment les bureaux, les habitations et les entrepôts. Ce chapitre porte essentiellement sur la protection des bureaux et des habitations. Cependant, il est également nécessaire de considérer la sécurité du site pour le personnel qui passe du temps dans des contextes programmatiques, par exemple les personnes qui logent dans des camps de réfugiés, dans un centre médical ou un établissement scolaire. Il faut également considérer la sécurité des lieux d'exécution des projets, par exemple les sites de distribution dans les camps, et celle des distributions générales pouvant être effectuées hors d'un camp. En plus des installations primaires et des habitations du personnel international, des mesures de protection peuvent également être nécessaires près des lieux d'habitation du personnel national.

9.1 Choix d'un site pour les bureaux

La protection du site commence avec le choix du site. À des fins de sûreté et de sécurité, les lieux potentiels devront satisfaire des critères spécifiques au-delà des considérations d'espace, d'esthétique et de prix.

9.1.1 Considérations clés pour le choix d'un site

Critères physiques

Critères physiques pour le lieu et le bâtiment :

- S'il y a un risque de conditions météorologiques extrêmes et de catastrophes naturelles connexes, telles que les inondations ou les glissements de terrain, déterminez si le bâtiment est situé dans un lieu potentiellement vulnérable et si la structure est suffisamment robuste pour faire face aux éléments.
- Évitez les endroits qui offrent de nombreuses possibilités de s'approcher ou de fuir sans être vu, par exemple les endroits qui ont une forte densité de buissons ou un lit de rivière asséché, des passages étroits et sombres, des enceintes d'usine, des lieux de stockage et des entrepôts essentiellement abandonnés la nuit, ou des bâtiments endommagés ou détruits.

1 Les risques changent considérablement dans les situations d'insurrection et de guerre, où des mesures additionnelles sont exigées. Celles-ci sont étudiées au Chapitre 15 (« Menaces liées aux combats et débris de guerre »).

- Le bâtiment même ou l'appartement constitue le périmètre intérieur. Si un appartement fait partie d'un immeuble, ou d'un bâtiment situé à l'intérieur d'une enceinte ou d'une zone protégée plus large, celle-ci constitue un périmètre extérieur. Un double périmètre est généralement préférable à un périmètre simple.
- Demandez-vous s'il serait facile d'évacuer le bâtiment ou la zone immédiate en cas d'incendie : existe-t-il différentes routes de sortie et le corps de pompiers local pourrait-il atteindre le bâtiment ?

La zone au sens large

Lorsque vous envisagez un quartier particulier, vérifiez minutieusement une zone sur un rayon d'au moins 1,5 km pour avoir une impression générale. Les questions à poser aux résidents locaux et aux autorités sont entre autres :

- De quelle sorte de quartier s'agit-il ? La plupart des personnes sont-elles résidentes ou y a-t-il un grand nombre de travailleurs qui viennent dans le quartier quotidiennement ? Y a-t-il beaucoup de voyageurs de passage dans cette zone ? S'il y a peu de personnes locales, il sera plus facile à un étranger d'entrer dans le quartier sans se faire remarquer.
- Quels sont les services fournis par les autorités locales et quels sont les services de secours dans le quartier ? Où se trouve la caserne de pompiers la plus proche ? Où se trouvent les postes de police ? Où vivent les dirigeants locaux influents ? Demandez s'il y a une patrouille de police et quelles sont les zones les plus régulièrement visitées par les patrouilles.
- Quels types de mesures de contrôle d'accès sont utilisés par les personnes du quartier ? Y a-t-il des gardes à l'extérieur des maisons ? Les maisons sont-elles fortement sécurisées ?

Vulnérabilités possibles

Tenez compte également des vulnérabilités potentielles du quartier.

- Y a-t-il des installations militaires, des locaux de police ou des bâtiments gouvernementaux ? Y a-t-il des cibles socioéconomiques ou religieuses importantes (le temple d'une minorité religieuse, le siège d'un syndicat militant, le bureau d'un journal d'opposition, une station de radio, etc.) ?
- Dans l'éventualité d'une agitation politique, les manifestations seront probablement axées sur les bâtiments gouvernementaux. Cependant, si une intervention étrangère n'est pas acceptée, les manifestations pourraient viser les bâtiments diplomatiques ; une zone universitaire pourrait être le lieu d'une agitation étudiante, et les marchés pourraient être ciblés par des attaques terroristes. Un quartier qui abrite un groupe minoritaire pourrait être vulnérable aux attaques de bandes.
- Les niveaux de crime peuvent être élevés dans les zones aisées tout

comme dans les zones défavorisées. Quel que soit le niveau d'affluence du quartier choisi, tentez de ne pas donner une image de richesse.

Dans un environnement à forte criminalité, il pourrait être conseillé de choisir un site proche d'un poste de police (mais n'oubliez pas que les postes de police peuvent être les cibles d'une insurrection ou d'une agitation sociale ou politique). Bien que les conditions de sécurité puissent l'exiger, positionner des bureaux ou des habitations dans un quartier relativement aisé, dans une enclave diplomatique ou une enclave protégée, donnera une certaine image et influencera la façon dont l'organisation est perçue.

Locataires uniques ou multiples

L'avantage des locataires multiples c'est que la présence d'autres personnes permet d'avoir de meilleures connaissances et une protection supplémentaire. Il est possible de tirer certains avantages de la force par le nombre lorsque plusieurs organisations occupent des sites à proximité les uns des autres. Les agences des NU regroupent de plus en plus leurs bureaux dans des lieux uniques, à la fois pour des raisons de sécurité et pour des raisons économiques, et certaines ONG en font de même. La colocation comporte des avantages évidents : le coût de la sécurité et des services de garde peut être partagé et un plus grand nombre de personnes sont présentes pour effectuer une surveillance informelle et offrir de l'aide en cas d'urgence. Mais elle comporte également des risques. Les sites regroupés ont tendance à devenir des enclaves protégées, séparées du reste de l'environnement social, et la concentration de cibles possibles signifie qu'une attaque aura un impact beaucoup plus grand si elle aboutit. Assurez-vous que les stratégies d'acceptation et que les considérations concernant l'image de l'organisation sont partagées avec les colocataires. L'organisation pourrait avoir un plus grand contrôle d'un site à occupation unique.

Il est souvent conseillé de louer un espace bureau ou un appartement situé dans les étages du bas, mais pas au rez-de-chaussée (le rez-de-chaussée est plus vulnérable aux intrus et les étages plus élevés pourraient être difficiles d'accès avec un équipement d'urgence et il pourrait être difficile de s'en échapper par exemple en cas d'incendie). De plus, si le toit est accessible, par exemple d'un bâtiment voisin, prendre la partie du bâtiment située juste en dessous du toit pourrait être risqué. Savoir si le choix d'un immeuble augmente ou diminue le risque dépend fortement de la stabilité et de la cohésion sociale de ses résidents. S'il y a une forte stabilité et cohésion sociale, il existera probablement un bon programme implicite de surveillance de quartier. Dans le cas contraire, il pourrait y avoir un manque d'intérêt général dans la sécurité des voisins et les étrangers pourraient accéder facilement au bâtiment.

Exemple de cas : un site sûr en Ossétie

Pour des raisons de sécurité, une organisation humanitaire en Ingouchie décide de se relocaliser en Ossétie du Nord. En recherchant un site sûr, elle remarque que le personnel international d'une autre organisation est logé dans des appartements (selon la politique de l'organisation les membres du personnel sont tenus de trouver eux-mêmes leur logement). L'organisation se méfie des entrées et des passages sombres aux alentours des appartements et décide de chercher une enceinte où les bureaux et les logements peuvent être rassemblés sur le même lieu et où l'on peut garer les véhicules et installer des télécoms. Le responsable de la logistique (un homme) trouve ce qui semble être l'endroit idéal en termes d'accès et d'espace. Cependant, le personnel féminin soulève des inquiétudes concernant le quartier. L'organisation se renseigne et découvre qu'il y a effectivement une activité criminelle dans le quartier. Finalement, un autochtone, qui avait déjà agi en tant que conseiller pour une autre organisation, trouve une enceinte à la périphérie de la ville. Le bâtiment réunit toutes les exigences en matière de sécurité physique, la zone est relativement affluente et on y trouve un grand nombre de chiens de garde et une forte sensibilisation à la sécurité.

Considérations de genre

Dans certaines circonstances, il pourrait être culturellement inacceptable ou simplement dangereux que les collègues femmes, nationales ou internationales, vivent seules, et il pourrait être nécessaire de trouver des arrangements acceptables de partage de logement pour les collègues femmes, qui ne se heurtent pas aux normes sociales. Envisagez d'avoir des lieux d'habitation séparés pour le personnel masculin et le personnel féminin. (Pour plus d'informations à ce sujet, voir la section sur les considérations de genre dans l'évaluation des risques, au chapitre 2.)

Le propriétaire

Essayez d'en savoir le plus possible sur le propriétaire : son occupation, son milieu social, son rôle possible dans la communauté, son affiliation politique, etc. Si possible, évitez de louer les locaux d'une personne impliquée dans des affaires suspectes, d'une personne ayant une influence politique ou d'un dirigeant (ou d'un membre proche de la famille d'un dirigeant) d'une partie en conflit. Dans certains contextes, l'affiliation du propriétaire à un clan sera également importante. La tradition tribale selon laquelle un hôte a le devoir de protéger ses invités pourrait entrer en jeu si un propriétaire considère ses locataires comme des invités. Dans d'autres endroits, le fait que le propriétaire appartienne à un groupe minoritaire constitue un facteur de risque.

Dans la pratique, il sera nécessaire de mettre en balance diverses considérations. Le choix parfait sera rarement possible. Pesez les avantages et les inconvénients de chaque site du point de vue de la sécurité, en fonction de la façon dont l'agence sera perçue, de sa stratégie de sécurité et de son plan d'urgence. Une fois que vous aurez choisi le site, identifiez quels sont ses points faibles et tentez d'y remédier. Quels sont les avantages et les faiblesses physiques du site concernant la sécurité ? Qu'est-ce qui est acceptable et qu'est-ce qui doit être amélioré ? Le propriétaire autorisera-t-il que des améliorations physiques y soient apportées ? Combien coûteront ces améliorations et ce coût est-il abordable ? Avant de signer le contrat de location, négociez en détail l'autorisation de transformer le bâtiment pour en améliorer la sécurité. Cela devra également être reflété dans le contrat de location.

9.2 Renforcement du périmètre physique

9.2.1 Le périmètre extérieur

Plusieurs facteurs doivent être pris en compte lorsque vous étudiez le périmètre extérieur d'un site. Si la végétation à l'approche du site ou sur le périmètre extérieur donne aux voleurs et aux agresseurs la possibilité de se cacher, taillez-la légèrement, coupez-la ou remplacez-la par des buissons épineux. Demandez-vous si les détritus et les gravats vont gêner les agresseurs ou plutôt aider une personne malveillante à surveiller le bâtiment ou à y accéder, et s'ils gêneront les gardes. S'il y a un risque qu'un engin explosif y soit déposé, tous les gravats et les détritus devront être retirés.

Construire un mur d'enceinte autour du site donnera une meilleure protection. La hauteur des murs doit être de 2,5 mètres au minimum et ils peuvent être surmontés de fil barbelé ou de tessons de verre. Remédiez à tout arbre se trouvant à proximité et pouvant être utilisé pour franchir le mur. Les murs hauts ne seront pas d'une grande utilité si les portails sont un point faible parce qu'ils sont faciles à escalader ou qu'ils ne sont sécurisés que par un cadenas et une chaine, pouvant tous deux être sectionnés rapidement. Assurez-vous que des judas sont installés pour vérifier qui se présente au portail sans devoir l'ouvrir. Dans certaines circonstances, par exemple si une zone est sujette à la violence de bandes ou si les vols à main armée sont un risque, il pourrait être souhaitable d'avoir une deuxième sortie. Celle-ci devra également être sécurisée contre une incursion.

Un éclairage amélioré pourrait réduire certains risques, mais il pourrait également mettre un site plus en évidence et attirer l'attention sur le fait qu'il contient quelque chose que l'on veut protéger. Les détecteurs de lumière qui ne sont activés que lorsque quelqu'un s'approche, pourraient être un bon compromis, mais, comme tout éclairage, ils dépendent d'une alimentation

en électricité fiable. Idéalement, les lumières ne doivent éclairer que les endroits sombres de l'enceinte plutôt que le local même ou ses occupants. En l'absence d'électricité, ou s'il y a régulièrement des coupures de courant, envisagez d'utiliser un générateur, surtout si c'est de toute façon une pratique courante dans le quartier. Une alternative moins coûteuse et plus modeste est le positionnement stratégique de lampes tempêtes, si un garde est disponible pour les surveiller. L'éclairage par énergie solaire est de plus en plus courant et abordable. N'oubliez pas que l'éclairage de sécurité n'est vraiment utile que si quelqu'un est présent pour surveiller la zone.

Décider de placer le logo de l'organisation sur le périmètre extérieur se fera en fonction des circonstances, et après avoir déterminé si cela réduira ou augmentera les risques. En règle générale, les logos sont appropriés dans les lieux où il y a un haut niveau d'acceptation du travail et de la présence de l'organisation. Si un logo est exposé, ajoutez une traduction du nom de l'organisation et peut-être un bref énoncé de sa mission dans la langue locale.

Si un site est inoccupé pendant une durée plus ou moins longue, un membre du personnel devra le visiter régulièrement pour allumer et éteindre les lumières et pour ouvrir et fermer les volets, afin de donner l'impression que le site est occupé.

Garer les véhicules

Lorsque le vandalisme, les vols de voiture, la violence des bandes ou les bombardements sont une menace, les véhicules doivent être garés à l'intérieur de l'enceinte à tout moment. Lorsque vous choisissez le site, assurez-vous qu'il y a suffisamment de place pour garer les véhicules. Ceux-ci doivent être verrouillés lorsqu'ils ne sont pas utilisés et des procédures opérationnelles doivent être en place pour le contrôle des clés des véhicules, pour les dispositions sur le stationnement des véhicules, et pour l'utilisation des véhicules en cas d'urgence. En règle générale, les dispositions concernant le stationnement et le carburant doivent permettre un départ facile de l'enceinte. Il faudra, par exemple, s'assurer que les véhicules ont un plein d'essence à la fin de chaque journée, et qu'ils sont garés de telle sorte qu'ils permettent un chargement et un départ rapides.

9.2.2 Le périmètre intérieur

Faites le tour du bâtiment avec l'œil d'un intrus et cherchez les points faibles, en particuliers ceux des portes et des fenêtres. Toutes les portes d'entrée doivent être solides, y compris les encadrements et les charnières. Évitez les portes contenant du verre, ou remplacez-les, et installez un judas ainsi qu'un verrou primaire et un verrou auxiliaire sur les portes extérieures. Sur la face intérieure de la porte, installez une chaîne de sécurité et un pêne dormant

coulissant ou une barre solide en travers de la porte. Les cadenas industriels à l'intérieur, en haut et en bas de la porte, constituent des éléments de sécurité supplémentaires, surtout si les anneaux du cadenas sont soudés. Ne posez pas de boutons d'appel d'urgence ou de téléphones près de la porte d'entrée, car un intrus pourrait en bloquer l'accès.

Les fenêtres peuvent être protégées à l'aide de barres, de grilles ou de volets, surtout au rez-de-chaussée (à condition qu'on puisse les ouvrir facilement de l'intérieur en cas d'urgence). Vérifiez s'il est facile d'atteindre les fenêtres des étages et agissez en conséquence. Les buissons épais épineux sous les fenêtres du rez-de-chaussée peuvent en gêner l'accès. Assurez-vous que les barres ou les grilles ne peuvent être facilement dévissées ou retirées de l'extérieur. Vérifiez s'il est possible de pénétrer dans la maison par les portes d'un garage, par une cave ou par la fenêtre d'une salle-de-bain. La nuit, fermez régulièrement les rideaux pour qu'on ne puisse pas voir de l'extérieur, qui et combien de personnes se trouvent à l'intérieur. En sortant, laissez une lumière allumée pour donner l'impression que le bâtiment est occupé. Vérifiez régulièrement que tous les verrous et serrures fonctionnent bien et, à la tombée de la nuit ou avant de vous coucher, verrouillez régulièrement portes et fenêtres. Limitez le nombre de clés disponibles et surveillez de près qui y a accès.

En cas d'incendie, d'intrusion ou d'émeute, une autre porte de sortie pourrait être nécessaire. Les sorties de secours, y compris les barres ou grilles, doivent pouvoir être ouvertes facilement de l'intérieur. Si des barres sont déjà installées, elles doivent être modifiées pour permettre de les ouvrir de l'intérieur. Cela peut être fait en mettant des charnières sur un côté des barres et en les sécurisant à l'aide d'un cadenas, tout en s'assurant que les occupants peuvent accéder rapidement à la clé du cadenas.

Les alarmes antivol et les caméras de télévision en circuit fermé (CCTV) sont rares dans la plupart des contextes d'aide humanitaire. Elles dépendent en général d'une alimentation en électricité, bien que certaines alarmes antivol fonctionnent avec des piles. Une caméra CCTV n'aura pas un grand effet dissuasif si les intrus ne savent pas ce que c'est et à quoi elle sert, ou s'il y a peu de chances qu'ils soient appréhendés. Les appareils à très forts décibels peuvent constituer une protection très efficace. Ils sont contrôlés à distance et agissent de manière directionnelle : ils émettent un son intenable (mais qui n'endommage pas les oreilles) et empêchent de manière efficace les intrus ou même une foule excitée de s'approcher plus près des locaux. Ils sont munis d'une protection contre le sabotage et fonctionnent avec des piles.

Une note sur la sécurité des bases concernant les risques d'incendie est ici justifiée. Installez des détecteurs de fumée et de monoxyde de carbone ainsi

que des extincteurs dans la cuisine et à chaque étage. Les feux électriques et les feux d'huile ont besoin d'un extincteur CO2 ou à poudre ; pour d'autres types de feux, utilisez un extincteur à mousse ou à eau. Vérifiez les extincteurs et faites-les réviser au moins une fois par an. Identifiez l'accès aux sorties de secours et assurez-vous que, lorsqu'elles sont verrouillées de l'intérieur, elles peuvent être ouvertes sur-le-champ. Dans les bâtiments plus grands, organisez régulièrement des exercices d'évacuation en cas d'incendie, surtout si le roulement du personnel est élevé. Assurez-vous que les chauffages individuels à gaz sont munis d'un dispositif d'aération et vérifiez s'ils ont des thermocouples (dispositifs qui coupent l'alimentation en gaz s'il n'y a pas de flamme pilote ou autre source d'allumage). Les chauffages sans thermocouples ne doivent pas être laissés sans surveillance et ne doivent pas être utilisés la nuit.

9.2.3 La pièce de sécurité

Une pièce de sécurité est un endroit où l'on peut rapidement se mettre à l'abri d'un intrus ; elle diffère d'un abri anti-bombes, et n'est pas blindée. Elle doit être facilement et rapidement accessible, et située de préférence au centre du bâtiment. Autrement, un étage élevé peut être converti en pièce de sécurité en installant une grille sur l'escalier qui peut être verrouillée la nuit. Les pièces de sécurité doivent être munies d'une porte renforcée, d'un téléphone ou d'autres moyens de communication (de préférence ne pouvant être coupés) afin de pouvoir appeler à l'aide, d'une liste de numéros de contacts importants et d'une lampe électrique ou de bougies et d'allumettes. Envisagez d'y stocker également une petite quantité d'eau, de nourriture et d'articles sanitaires. L'objectif d'une pièce de sécurité est de protéger les personnes, et non pas les biens. Tout mettre dans une pièce de sécurité ne fera probablement qu'encourager les voleurs à faire de plus grands efforts pour en forcer l'entrée. Laissez-leur quelque chose, sinon tout, à voler.

9.3 Gestion de la sécurité du site

La sécurité du site est la responsabilité de tous. Chacun doit rester vigilant et signaler tout ce qui est inhabituel ou suspicieux, ainsi que les violations des procédures de sécurité (portes ou fenêtres laissées ouvertes, clés non rangées). Efforcez-vous d'entretenir de bonnes relations avec vos voisins sans être trop indiscret. Les gens sont plus susceptibles de réagir lorsqu'ils voient quelque chose de suspicieux si des relations de base ont été créées et qu'ils vous connaissent un peu.

9.3.1 Les gardes

Les organisations d'aide utilisent fréquemment des gardes et des veilleurs de nuit pour leurs logements, leurs entrepôts et leurs bureaux. Les gardes peuvent

être soit recrutés directement, soit engagés sous contrat auprès d'une société locale. Cependant, trop souvent les gardes sont inefficaces parce qu'ils ne sont pas formés, ne reçoivent pas les instructions adéquates, sont mal payés, mal équipés et mal gérés. Il n'est pas rare de trouver un lit dans les postes de garde des enceintes d'organisations d'aide, ce qui garantit pratiquement que le garde s'endormira à son poste. Pendant la journée, les gardes pourraient être occupés à autre chose et être distraits. Lorsque vous recrutez des gardes, fournissez des termes de référence clairs et incorporez-les dans leur contrat.

Pour le recrutement et la gestion des gardes, considérez les points suivants :

- Choisissez une personne physiquement apte.
- Obtenez des références fiables et si possible recrutez des personnes du quartier. Elles connaîtront ainsi la zone et ses occupants réguliers et seront mieux motivées pour identifier des malfaiteurs potentiels.
- Les occupants principaux d'un bâtiment doivent être en mesure de communiquer avec le garde. Vérifiez les aptitudes linguistiques des candidats.
- Recrutez et déployez suffisamment de gardes afin qu'ils puissent faire face au moins à deux intrus travaillant ensemble.
- Comme pour tout le personnel, veillez à ce que les gardes aient une présentation complète de l'organisation.
- Si le garde doit porter une arme (mortelle ou autre), les circonstances dans lesquelles elle pourra être utilisée doivent être régies par le contrat signé avec la personne ou la société ayant fourni le garde, et doivent refléter la politique de sécurité de l'organisation. Il est recommandé que cette politique soit revue par le conseiller juridique de l'organisation. Incluez des clauses contractuelles interdisant l'utilisation de substances néfastes (p. ex. l'alcool) pendant les heures de travail, et les emplois additionnels pouvant affecter la performance du garde.
- Fournissez un équipement essentiel, des instructions et une formation : des vêtements imperméables, des lampes électriques, un sifflet ou autre dispositif d'alarme, une radio portative ou un téléphone supplémentaire pour le poste de garde. Fournissez un carnet de bord et des instructions sur la façon de le tenir et sur les déclarations d'incidents, ainsi qu'une liste de numéros de contacts clés. Fournissez des instructions précises et une formation sur la façon de réagir face à des visiteurs et face à un intrus. Donnez des instructions claires sur la surveillance des alentours, les patrouilles dans l'enceinte et les règles concernant les portails, portes, fenêtres et clés.
- Les gardes doivent normalement n'avoir accès qu'au périmètre extérieur, surtout dans les lieux résidentiels. Dans l'enceinte des bureaux, ils doivent avoir accès aux couloirs, aux escaliers et au toit, mais pas nécessairement aux bureaux mêmes.

- Dans les lieux où les vols à main armée constituent un grand risque, envisagez des procédures de déploiement, telles qu'un programme d'inspections régulières alternées avec des rondes à des heures moins prévisibles. Répartissez les gardes, et positionnez au moins un garde à un endroit où il ne peut être observé et dominé facilement, par exemple sur la terrasse d'un toit.
- Être de garde pendant de longues périodes peut être ennuyeux, surtout si rien ne se passe, et les gardes seront susceptibles d'être moins attentifs et distraits. Essayez d'éveiller leur attention : parlez-leur, montrez-leur de l'intérêt et demandez-leur comment ils vont et ce qu'ils pensent de la situation dans le quartier.

Trois autres groupes jouent également un rôle direct et important dans la sécurité du site : les réceptionnistes et les standardistes, les membres de la famille du personnel, le personnel d'entretien des bureaux. Les réceptionnistes et standardistes doivent contrôler les visiteurs et les appels téléphoniques, les lettres et les colis livrés, et ils doivent signaler toute chose et toute personne pouvant représenter une menace de sécurité. Les membres de la famille du personnel, tout comme les membres du personnel, doivent être conscients de la sécurité des logements, et le personnel d'entretien, y compris les jardiniers, ne doivent pas laisser entrer des personnes inconnues, donner des informations à des visiteurs inconnus, donner des renseignements sur la disposition des bureaux ou permettre que l'on fasse des doubles de leurs clés. Toute chose inhabituelle doit être immédiatement signalée.

Les chiens de garde spécifiquement entraînés peuvent être très utiles pour donner une alerte précoce et peuvent avoir un effet dissuasif. N'oubliez pas que si un chien est potentiellement dangereux pour les personnes qu'il ne connaît pas, des mesures de contrôle seront nécessaires pour protéger les visiteurs légitimes et le personnel.

9.3.2 Les clés

Les serrures et les clés ne sont utiles que si elles sont bien gérées. Notez toutes les personnes qui ont des clés et lesquelles. Le nombre de clés, et leur accès, doit être étroitement contrôlé. Si vous avez un doute, changez les serrures. Les clés doivent être identifiées, généralement par un code. Les doubles doivent être gardés sous serrure, dans une armoire à clés comportant une vitre sur le devant qui peut être brisée en cas d'urgence. Tout le personnel possédant des clés, y compris le personnel d'entretien, doit être clairement informé que :

- Les clés doivent être portées sur soi et ne doivent pas être laissées sur les bureaux, dans les voitures ou dans des manteaux ou sacs non surveillés.
- Les clés ne doivent jamais être reproduites, sauf si des instructions spécifiques ont été reçues de la direction de l'organisation.

- Toute perte de clés doit être immédiatement signalée.

D'autre part, il pourrait être dangereux d'être trop strict, par exemple si les employés ne peuvent s'échapper d'un bâtiment en flammes parce qu'ils n'ont pas la clé de la porte de secours, ou s'ils ne peuvent répondre à un appel d'urgence d'un collègue parce que les clés de la voiture sont sous verrou et que le responsable de la logistique vit à l'autre bout de la ville.

D'autres mesures techniques de contrôle d'accès comprennent les cartes d'accès magnétiques, les serrures à code (un système électronique de contrôle d'accès à boutons qui autorise l'accès uniquement aux personnes qui connaissent le code), les lecteurs magnétiques, les cartes à puce et les appareils biométriques. Certains de ces systèmes peuvent être coûteux et certains ne fonctionneront pas si le courant est coupé ou si le mécanisme est défaillant.

9.3.3 Gérer l'accès

Contrôler l'accès a généralement deux fonctions : établir l'objectif et la légitimité d'un visiteur et assurer que les visiteurs ne constituent pas une menace. La façon dont l'accès est géré est une question délicate et influera sur la façon dont une organisation est perçue. En général, la majorité des visiteurs seront les bienvenus, mais dans certaines circonstances l'accès pourrait être très strictement contrôlé ; les visiteurs pourraient être activement dissuadés d'entrer ou être dirigés vers un bâtiment séparé du local principal de l'organisation. Dans tous les cas, il est utile d'avoir un espace d'attente réservé aux visiteurs. Il devra être facilement visible par le personnel de la sécurité et le réceptionniste. Il devra être proche des toilettes mais l'accès non contrôlé au bâtiment ne doit pas être possible pour un visiteur attendant d'avoir l'autorisation d'entrer.

Il y a plusieurs degrés de contrôle de la sécurité. Par exemple, demander aux visiteurs de signer à leur arrivée et à leur départ n'est pas vraiment une mesure de sécurité en soi, car tout le monde peut entrer. Des procédures standard plus strictes sont entre autres :

- Tous les employés portent une pièce d'identité visible avec photo lorsqu'ils se trouvent sur les lieux. Elle leur sera reprise à la fin de leur contrat ou de leur emploi.
- Tous les visiteurs montrent une pièce d'identité.
- Tous les visiteurs reçoivent une pièce d'identité ou un laissez-passer, qu'ils rendent lorsqu'ils partent.
- Aucun visiteur ne peut entrer à moins que l'autorisation explicite en soit donnée par la personne qu'il souhaite voir ou qui accepte de le recevoir.
- Aucun visiteur ne peut entrer à moins d'être accompagné par un membre du personnel.

Des procédures encore plus strictes comprennent des vérifications régulières des sacs des visiteurs et des fouilles corporelles régulières, manuelles ou électroniques (des gardes femmes et une formation spéciale sont nécessaires pour cela). Les bureaux plus importants, généralement dans les grandes villes, peuvent contrôler l'accès en installant des portes ou des tourniquets que l'on actionne avec des cartes magnétiques.

Dans les contextes à haut risque, il faut refuser l'accès à toute personne inconnue, non autorisée ou incapable de fournir une pièce d'identité convaincante. La vérification superficielle pour établir si un visiteur pourrait représenter une menace doit donc être effectuée sur le périmètre extérieur, avant qu'il ne soit admis dans l'enceinte. Un visiteur sera autorisé à entrer uniquement quand il aura été établi qu'il ne semble pas constituer une menace. Une seconde étape distincte, dans les locaux, sera d'établir l'objectif exact de la visite, de contacter le service hôte, d'enregistrer la personne et de lui donner un laissez-passer, ce qui réduit le nombre de personnes attendant à l'entrée principale. S'ils ont un doute, les gardes devront avoir pour instruction de contacter un responsable.

Politique concernant l'accès : questions à considérer

- Les véhicules des visiteurs sont-ils autorisés dans l'enceinte ? Si oui, où doivent-ils être garés ? Par exemple, s'il y a une menace de bombe, assurez-vous qu'aucun véhicule n'appartenant pas à l'organisation ne se trouve dans l'enceinte et envisagez d'interdire aux visiteurs de se garer aux alentours de l'enceinte. Les gardes pourraient également avoir comme instruction de fouiller les véhicules, mais il s'agit d'un travail spécialisé et ils devront avoir été formés pour le faire correctement.
- Les visiteurs qui arrivent avec leur propre garde du corps doivent-ils être autorisés à les faire entrer et si oui, avec ou sans leur arme ? Êtes-vous responsable si quelqu'un porte atteinte à la vie d'un visiteur dont le garde du corps n'a pas été autorisé à entrer ? Envisagez de tenir la réunion dans une annexe du bâtiment ou sur une véranda où les gardes du corps pourraient être autorisés.
- Pensez à l'accès des services, notamment le personnel d'entretien, des réparations, des services d'utilité publique et des livraisons. Ces personnes doivent-elles être autorisées dans les locaux en votre absence ? Leurs visites peuvent-elles être prévues et programmées ? Quelle pièce d'identité doivent-elles fournir ? En ce qui concerne les marchands ambulants, dites aux gardes et au personnel domestique qu'ils doivent acheter les marchandises à l'extérieur des grilles.

9.3.4 Lettres et appels téléphoniques menaçants

Les appels téléphoniques problématiques peuvent aller des appels loufoques

relativement innocents au harcèlement sexuel et aux menaces de bombardement. Les membres du personnel qui reçoivent des appels difficiles doivent :

- insister pour que l'appelant donne son identité et établir l'objectif de l'appel ;
- donner aussi peu d'informations que possible sur eux-mêmes et tenter d'en obtenir autant que possible sur l'appelant ;
- ne donner aucune information sur leurs mouvements, quand ils seront présents ou absents, s'ils sont seuls ou pas ;
- demander un numéro de téléphone où ils peuvent rappeler la personne ; et
- signaler ces appels au responsable de la sécurité.

Le harcèlement sexuel par téléphone peut parfois prendre fin lorsqu'un co-résident masculin répond au téléphone. Si l'appelant persiste, changez de numéro de téléphone. Les femmes, en particulier, ne doivent pas mettre leur numéro personnel sur leurs cartes de visite professionnelles.

Dans le cas d'appels téléphoniques menaçants, restez calme et courtois. Si la menace est vague et générale, essayez d'obtenir plus de détails sur le motif et la cible précise et de savoir si le problème peut être résolu d'une autre manière. Si l'appel est une menace de bombe, la question fondamentale est de savoir quand et où la bombe explosera. Dites le nom de votre organisation, suivi de « nous avons plusieurs locaux - à quel local faites-vous référence ? », et faites préciser à l'appelant quelle est la cible visée. Demandez quelle est la raison de la menace et écoutez avec bienveillance. Déclarez qu'il y a un grand nombre de personnes dans et autour du bâtiment et que beaucoup seront atteintes si une bombe explose. Essayez d'écrire exactement ce qui est dit, ou tentez de le mémoriser. Détectez tout indice sur l'identité de l'appelant : homme ou femme, ton, agité ou calme, langue et accent, et bruits de fond spécifiques. À moins d'être absolument sûr que la menace n'est pas réelle, évacuez immédiatement le bâtiment.

Si le bureau reçoit une lettre de menace, celle-ci doit être traitée sérieusement et les cadres supérieurs, les autorités appropriées et les autres organisations de la région doivent en être informés. Toute menace constitue un incident de sécurité et doit faire l'objet d'un rapport.

9.3.5 Lettres ou colis suspicieux

Bien que ce type de menace ne soit pas courant pour les organisations humanitaires, il est possible que l'on dépose une lettre ou un colis délibérément contaminé par un produit chimique nocif ou une substance biologique (comme l'anthrax) ou contenant un explosif. Les indicateurs possibles sont des traces de poudre sur l'enveloppe, une odeur étrange et,

dans le cas d'une bombe, le son d'un tic-tac ou des fils électriques visibles. Le colis pourrait être particulièrement lourd pour sa taille, l'adresse pourrait être mal orthographiée ou le courrier pourrait être adressé à quelqu'un qui ne travaille plus pour l'organisation. Il pourrait ne pas avoir de timbre ou en avoir trop, ce qui indiquerait qu'il n'a pas été affranchi dans un bureau de poste.

Ces lettres ou colis doivent être laissés où ils se trouvent, la pièce doit être évacuée et le personnel de sécurité doit être alerté. Toute personne ayant touché l'objet doit être identifiée et doit se laver immédiatement au savon, surtout les mains. La lettre ou le colis devra sans doute être détruit ou ouvert par un personnel de sécurité ayant été spécialement formé à cet effet, avec l'équipement adéquat (la contamination par une substance nocive exige, au minimum, le port de gants de protection totale, et un masque de protection totale, car certaines substances pénètrent dans le corps par inhalation).

9.4 Zones sous menace terroriste

Atténuer la menace d'attaque terroriste est coûteux et nécessitera généralement les conseils et l'aide d'un spécialiste. Les menaces possibles les plus courantes incluent les tirs sur le personnel par un individu qui se trouve à l'extérieur du périmètre, une bombe humaine à l'entrée du bâtiment, une voiture ou un camion piégé laissé dans le périmètre ou qui a percuté le portail, des agresseurs armés portant des explosifs qui se précipitent dans le bâtiment, et un visiteur qui dépose un colis contenant une bombe derrière le bâtiment. Lorsque vous abordez ces menaces, la première question doit toujours être : devrions-nous être là si la menace est si importante ?

Les divers éléments énoncés ici qui permettent de durcir les sites ont des implications importantes sur la sélection du site. Il est peu probable qu'un bâtiment répondra à toutes les exigences, et certaines vulnérabilités devront donc être abordées. En général, le bâtiment doit avoir les caractéristiques suivantes :

- Il ne conduit pas directement à un endroit que l'organisation ne peut contrôler, tel qu'une route publique. Il doit être situé à une certaine distance de cet endroit.
- Les entrées principales du bâtiment ne se trouvent pas dans la ligne de tir directe partant d'un espace que l'organisation ne peut contrôler.
- Les bureaux sont séparés des entrepôts et garages auxquels les véhicules ont accès, et ont leur propre périmètre de sécurité.
- Il y a un périmètre extérieur qui réduit le nombre de points d'accès à l'espace intérieur et au site.
- Évitez les garages souterrains. Une voiture piégée sous un bâtiment peut causer des dommages considérables. Si vous utilisez un garage souterrain,

seul le personnel (et dans des circonstances très exceptionnelles, les visiteurs) doit être autorisé à y accéder ; envisagez d'ajouter des barrières que l'on actionne pour l'accès des véhicules.
- Délimitez des espaces dans le périmètre extérieur où les visiteurs peuvent se garer ou être déposés.

Des mesures de limitation de vitesse doivent être établies pour les voies d'accès de tous les points d'entrée principaux dans le périmètre extérieur, afin d'empêcher les véhicules d'accélérer et d'entrer à grande vitesse. Un équipement spécialisé peut être installé, ou bien utilisez des tonneaux remplis de gravier et de pierres, ou des grands pots en béton, enchaînés les uns aux autres, contenant des fleurs ou des buissons. Si le périmètre extérieur est près du bâtiment, érigez des barrières supplémentaires telles que des blocs en béton ou des buissons dans des pots en béton. Une explosion qui se produit loin du bâtiment aura un impact amoindri. Il est souhaitable de garder une distance de 30 m entre le bâtiment et le périmètre extérieur, mais cela ne sera pas souvent réalisable. Si possible, ayez des entrées et des parkings séparés pour le personnel et les visiteurs. Les véhicules du personnel doivent malgré tout être soigneusement inspectés au cas où le véhicule d'un travailleur aurait été secrètement chargé d'explosifs dont la détonation est déclenchée à distance, ou au cas où un kamikaze aurait réquisitionné la voiture. Fouillez les véhicules et les visiteurs autorisés à pénétrer dans le bâtiment par le périmètre extérieur.

Essayez de garder un espace libre, sans obstruction, d'au moins 10 m entre les périmètres intérieur et extérieur. Si les véhicules ou les visiteurs doivent circuler dans cet espace, établissez des couloirs de circulation. Toute tentative de circuler en dehors de ces couloirs désignés devra déclencher une réponse immédiate du personnel de sécurité. À l'intérieur du bâtiment, séparez les espaces accessibles aux visiteurs et les espaces réservés au personnel. Tous les visiteurs (et éventuellement tout le personnel) doivent être contrôlés de nouveau à l'entrée et les sacs doivent être fouillés ; le point d'accès ou hall doit être suffisamment grand pour permettre ces fouilles et ne doit pas mener directement à d'autres espaces, au cas où une explosion se produirait dans le hall. Les biens importants, tels que le système informatique central, doivent être situés plus loin dans la zone limitée et leur emplacement ne doit pas être facilement identifiable par des panneaux placés dans le couloir.

Si possible, créez des espaces tampons sur les côtés du bâtiment pour atténuer les effets de l'explosion d'une bombe. Dans ces espaces, les personnes ne doivent pas être assises parallèlement aux fenêtres. Un film de sécurité de bonne qualité réduira le risque de projection de morceaux de verre ; les objets

à l'extérieur du bâtiment qui peuvent être transformés en débris volants, comme les poubelles, les bancs et les pots de fleurs, doivent être retirés ou solidement ancrés dans le sol. Réaménager le bâtiment pour le rendre plus sûr en cas de vague d'explosion serait coûteux et prendrait beaucoup de temps, mais envisagez de renforcer certains endroits comme le hall d'entrée, où une explosion est plus susceptible de se produire.

9.5 Contre-surveillance

Une attaque grave ou un raid demandera probablement une planification. La contre-surveillance peut identifier une menace pendant la phase de planification, avant que l'attaque n'ait lieu. [2] Les phases de la planification d'une attaque comportent généralement :

- La sélection initiale de la cible.
- Une surveillance avant l'attaque.
- La planification de l'attaque.
- Des répétitions avant l'attaque, avec peut-être des recherches et des passages devant le lieu ciblé.

En termes simples, la contre-surveillance consiste à surveiller si l'on vous épie. Elle inclut :

- Identifier les points d'observation possibles et les indiquer au personnel.
- Donner instruction aux gardes de faire des rondes de surveillance aux points d'observation possibles.
- Donner instruction à tout le personnel de rester en état d'alerte et de signaler tout comportement indiquant une observation active sur le site ou dans la circulation sur le site, par exemple le même véhicule qui passe fréquemment ou garé tout près pendant de longues périodes et des piétons qui rôdent près du site.
- Créer des relations avec les voisins et les propriétaires de magasins locaux. Demandez-leur s'ils ont remarqué un comportement suspicieux ou des individus inconnus près du site.
- Varier les routines et les routes empruntées pour aller au bureau et pour le quitter.

Bien que la contre-surveillance puisse avoir une connotation militaire déplaisante pour un acteur humanitaire, elle ne nécessite pas des mesures et matériels de protection lourds, ou l'utilisation de la force. Elle peut, en fait, être un aspect utile d'une stratégie d'acceptation, puisqu'elle exige d'entretenir

2 Cette section est tirée de « Counter-surveillance and Surveillance Detection » (Contre-surveillance et détection de surveillance), présentation faite par John Schafer, directeur de la sécurité, InterAction, janvier 2010.

des relations et une communication quotidiennes avec les résidents locaux. En faisant partie de la communauté, en observant et en connaissant bien votre environnement et les personnes qui y vivent, vous pouvez potentiellement parer aux menaces, et vos voisins peuvent vous y aider.

9.6 Sites de distribution

Un certain nombre de mesures peuvent accroître la sécurité du personnel et des bénéficiaires de l'organisation d'aide aux sites de distribution.

- Comprenez vos bénéficiaires. Il est important de savoir comment ils considèrent la distribution. Sont-ils prêts à tout pour les articles distribués ? Y a-t-il des tensions possibles entre les bénéficiaires ? L'intervention politique est-elle possible ou probable ? Certains éléments auraient-ils intérêt à manipuler la distribution ?
- Ayez un périmètre bien défini, approprié à la situation ; dans certains cas, une clôture ou des murs pourraient être nécessaires, dans d'autres, des barricades quelconques pourraient être acceptables, avec une surveillance supplémentaire.
- Le site doit être à un endroit où la circulation ambiante (des véhicules et des piétons) n'est pas gênée. Il ne doit pas inviter des observateurs non désirés.
- Il doit avoir un point d'entrée et un point de sortie. La foule au point d'entrée doit être bien gérée afin que l'organisation puisse rapidement séparer les bénéficiaires légitimes et illégitimes ; ayez un plan et le personnel à portée de main pour faire face aux individus indisciplinés. Les points de sortie doivent être gérés avec autant de détails, pour s'assurer que les bénéficiaires peuvent quitter le site de distribution de manière ordonnée et sûre. Le personnel ou les autorités doivent s'assurer que les foules (y compris les membres de la famille qui pourraient être venus pour aider à transporter la charge) ne sont pas rassemblées à la sortie et ne gênent pas le départ. Il est très important de faire circuler les personnes. Les organisations doivent être conscientes des questions potentielles de protection en ce qui concerne les personnes qui quittent le site de distribution, surtout les femmes et les jeunes enfants.
- À l'intérieur du site de distribution, l'organisation doit avoir une procédure claire qui permette aux personnes d'entrer et de sortir rapidement ; des problèmes peuvent surgir lorsque des personnes sont obligées d'attendre en groupes. Pensez à la façon dont les articles distribués seront empaquetés. Les personnes qui les reçoivent pourront-elles les porter de telle sorte à ne pas être plus vulnérables lorsqu'elles quitteront le site de distribution ? Pensez aux moyens de rendre les articles distribués moins évidents pendant le retour des bénéficiaires chez eux.

Chapitre 10
Foules, bandes et pillage

Dans les situations tendues et controversées, les foules peuvent devenir menaçantes ou violentes. Cela peut entraîner le pillage de biens et l'agression du personnel. Les scénarios courants comportent l'agitation civile, la violence ethnique ou communautaire, les troubles liés aux distributions d'aide et les vagues de pillage par les soldats ou les combattants armés. Une telle violence peut faire irruption spontanément, mais elle peut également être planifiée et fomentée.

10.1 Suivi et analyse de la situation

Anticiper la violence des foules et des bandes n'est pas une science exacte. Cependant, il est important de considérer cette possibilité dans le cadre d'une analyse et d'un suivi constants de la situation, au niveau national (souvent avec un risque plus important dans les villes), ou au niveau opérationnel local (surtout dans les camps de personnes déplacées ou dans les bidonvilles). La montée de la tension et de la frustration peut souvent être décelée à l'avance. La population locale, à l'écoute des médias locaux et des circuits informels d'information, est souvent consciente que quelque chose se prépare, mais elle n'est pas nécessairement mieux placée pour prédire exactement ce qui arrivera, quand et où. Il faut noter que les situations tendues peuvent se développer à la suite d'un événement particulier, tel qu'une distribution (p. ex. une dispute au sujet d'une place dans la queue, des allégations de fraude) ; même en l'absence de facteurs prédictifs, il doit toujours exister des plans pour calmer les tensions qui naissent (p. ex. en ayant toujours des articles supplémentaires à distribuer et un personnel chargé principalement d'observer et de contrôler l'humeur des personnes qui attendent).

Demandez-vous si l'organisation est une cible ou pourrait le devenir, et où elle est potentiellement exposée. Quelle est la cause de la tension et contre qui la colère est-elle dirigée ? Les organisations d'aide et les étrangers en sont-ils l'objet ? Les autorités locales peuvent-elles détourner le ressentiment éprouvé envers elles-mêmes et le reporter sur les étrangers ou les organisations d'aide ? Le personnel local est-il plus en danger en raison de son appartenance ethnique ou de son identité sociale ? Y a-t-il déjà eu des agitations publiques dans le passé ? Si oui, où ont-elles commencé et comment ont-elles évolué ? Certaines caractéristiques pourraient-elles être répétées dans cette situation ? L'organisation est-elle indirectement exposée, par exemple parce que ses bureaux ou entrepôts sont proches d'une zone où les manifestations ont lieu, ou sont situés dans un quartier de minorités ?

Exemple de cas : les bureaux du PAM sont pris d'assaut

Le 30 juillet 2006, une bande furieuse a pris d'assaut le bâtiment du PAM à Beyrouth, au Liban. Ce matin-là, les manifestations contre Israël et les États-Unis s'étaient transformées en protestations visant les NU. Se sentant en sécurité dans ses bureaux, à l'intérieur des grilles du périmètre, le personnel a continué à travailler, même lorsque les manifestants en colère ont tenté d'entrer par effraction dans le bâtiment. Les alarmes ont retenti lorsque la bande est entrée, et le personnel de la sécurité a donné instruction aux travailleurs de se barricader dans les bureaux du PAM. Lorsque la situation s'est dégradée, les agents de la sécurité ont conduit de toute urgence les travailleurs à l'escalier du fond du bâtiment qui mène à un parking souterrain, où ils se sont verrouillés dans les véhicules pour se cacher. La situation a finalement pu être contrôlée ; il n'y a eu que quelques blessures mineures, mais deux étages de bureaux ont été saccagés. Cet incident montre qu'une situation qui peut paraître courante, dans ce cas une manifestation dans la rue, peut rapidement devenir très menaçante.

Le personnel doit-il traverser des zones critiques où la situation tournera inévitablement à la violence ?

Des tensions qui montent depuis longtemps peuvent soudain éclater avec violence suite à un événement déclencheur. Il est possible d'identifier les déclencheurs potentiels, par exemple une décision des pouvoirs étrangers d'intervenir militairement, une crise économique soudaine provoquée par les conditions des échanges internationaux, ou la décision d'un gouvernement de mettre fin aux subventions d'articles essentiels tels que la nourriture ou le carburant, ou de fermer un camp de réfugiés avant que les personnes n'expriment le souhait de rentrer chez elles. D'autres déclencheurs ne peuvent être prévus mais peuvent être reconnus en tant que déclencheurs probables, par exemple l'arrestation ou l'assassinat d'un acteur important.

10.2 Action préventive

Plus la désinformation concernant l'organisation sera répandue, plus le risque que la frustration et la colère collectives soient dirigées contre elle sera grand. Les attentes devront être gérées de manière proactive. Par exemple, évoquez avec les personnes ce à quoi elles peuvent réellement s'attendre, et informez-les immédiatement s'il y a un retard ou un changement de plan. Il peut être utile de les rencontrer pour écouter leurs critiques et chercher d'autres solutions afin d'éviter que la frustration ne tourne à la colère. Ne

Exemple de cas : une foule attaque une organisation humanitaire

Un article de la presse nationale paru dans le seconde moitié de 1995, accusait l'ONG *Forum on Sri Lanka* de soutenir les rebelles Tigres tamouls dans leur guerre contre le gouvernement sri-lankais. L'article est paru quelques jours seulement avant la réunion annuelle du *Forum*, qui devait se tenir au Sri Lanka, et alléguait que la réunion était en fait un rassemblement contre le gouvernement et son effort de guerre. Les détails de la réunion ont été diffusés par une station de radio locale. Une foule de 3000 personnes en colère s'est rassemblée sur le lieu de la réunion et a menacé les participants. Le *Forum* a changé son lieu de réunion mais, encore une fois, les détails ont été diffusés à la radio locale et les protestataires ont de nouveau perturbé la réunion. L'hôtel où certains des participants étrangers résidaient a également été attaqué. La situation ne s'est calmée qu'après l'intervention de membres du parlement et de ministres, et la suspicion et l'hostilité envers les ONG au Sri Lanka ont persisté pendant plusieurs semaines.

parlez pas uniquement avec quelques représentants : tentez de rendre l'information publique par le biais de nombreuses parties prenantes diverses, notamment les médias locaux.

N'encouragez jamais le rassemblement d'une foule à moins de pouvoir répondre à ses attentes. Organisez les événements à l'avance (réunions, distributions) dans des lieux où les personnes se rassemblent. Établissez les procédures avec les représentants locaux. Tentez d'éviter ou de limiter les mouvements incontrôlés de la foule, les longues queues et les temps d'attente : multipliez les points de distribution, programmez les distributions tout au long de la journée pour différents segments de la population, créez des zones d'attente où il y aura de l'ombre et de l'eau et demandez aux personnes qui attendent de s'asseoir, donnez des informations précises sur la nature et la quantité des articles distribués, désignez des membres du personnel qui contrôleront la foule, refouleront les personnes qui ne doivent pas être là, renseigneront, expliqueront les procédures de mouvements, orienteront physiquement les personnes pour former une queue plus gérable ou les dirigeront dans de petits couloirs, et établiront une voie de sortie éloignée des points d'entrée.

L'identification préalable des bénéficiaires est essentielle pour faire face aux attentes. Beaucoup utilisent des listes, mais la tension peut monter lorsque les individus qui attendent dans une queue s'inquiètent et se demandent

si leur nom sera sur la liste ou pas. Les coupons ou bons (qui devront être raisonnablement difficiles à falsifier) sont un bon moyen de rassurer et de calmer les personnes qui attendent car elles auront la quasi certitude qu'elles recevront effectivement leur part de ce qui est distribué. Cette méthode a bien fonctionné dans l'intervention suite au tremblement de terre d'Haïti en 2010.

10.3 Protection

Envisagez des tactiques telles que limiter les mouvements dans les zones risquées, relocaliser les sites loin des zones à risque, retirer le personnel jugé être en danger, limiter ou réduire les stocks des entrepôts et entreposer temporairement les objets de valeur, tels que l'équipement des bureaux, dans les logements du personnel local. Réduisez la visibilité en retirant les logos et drapeaux de l'organisation des bâtiments et des voitures, en limitant les mouvements du personnel international qui se distingue de la population locale et en louant des voitures locales ou en utilisant des taxis plutôt que les véhicules tous terrains peu discrets de l'organisation. Contrôlez étroitement toute manifestation.

Le mouvement logistique des biens à distribuer, en particulier de la nourriture, doit être soigneusement planifié. Les mouvements doivent être planifiés tactiquement afin de minimiser la visibilité de la cargaison et programmés dans le temps afin d'éviter de traverser les zones dans lesquelles les bénéficiaires dans le besoin pourraient être tentés de piller (p. ex. programmez les routes et les heures du jour et de la nuit).

Informez les autorités sur la situation et envisagez de leur demander une protection spéciale. Cela peut être une stratégie très efficace si les autorités souhaitent et peuvent contrôler les foules. Cependant, cela pourrait ne pas toujours être le cas : les agents de police des commissariats locaux pourraient faire partie de la communauté locale et refuser de mécontenter une foule composée de personnes locales en colère. De plus, le gouvernement pourrait refuser d'intervenir trop rapidement ou trop fermement pour contrôler une foule comprenant des partisans possibles. D'autre part, les autorités pourraient souhaiter utiliser une force excessive pour imposer l'ordre, et pourrait même aller jusqu'à tirer dans une foule. Lorsque vous demandez la protection armée des autorités, veillez à évoquer les règles d'engagement, et indiquez la position de l'organisation en ce qui concerne l'utilisation de la force.

10.3.1 Négocier avec les foules

Il est très important de contrôler étroitement la dynamique de la foule afin d'identifier les indicateurs de problèmes bien avant qu'ils ne surgissent, par exemple lors d'un exercice de distribution. Cela pourrait signifier désigner des membres du personnel spécifiquement pour cette activité. De nombreuses

situations d'indiscipline commencent par des perturbations relativement légères. Il est important d'avoir des plans adoptés pour intervenir rapidement et gérer utilement les situations avant qu'elles ne s'aggravent.

Lorsque vous êtes confronté à une foule en colère, tentez de calmer la tension. Les tactiques clés incluent :

- Demandez conseil aux travailleurs locaux qui comprennent ce que la foule crie. Ils pourraient identifier qui sont les manifestants et qui semble les contrôler ou les mener.
- Gagnez du temps : essayez d'identifier le chef ou le porte-parole du groupe et de négocier avec lui, à condition que les discussions aient lieu avec un petit nombre de représentants du groupe. Demandez à ces représentants de communiquer la décision prise ou les informations ; les gens seront anxieux et impatients de connaître les résultats s'ils savent qu'un représentant négocie peut-être en leur nom ; de plus, le message aura une plus grande crédibilité. Prenez en considération le fait que les membres du personnel local du programme pourraient être considérés comme partiaux s'ils ont des liens avec un élément particulier de la communauté.
- Tenez ces discussions dans l'enceinte de l'organisation, mais pas au centre du bâtiment. Considérez le risque de sortir de l'enceinte pour négocier ; soyez sûr de ne pas être agressé.
- Écoutez attentivement et avec respect ; évitez de faire des promesses hâtives sur le problème en question. Signalez que vous prenez note des plaintes et que vous êtes d'accord pour poursuivre la discussion mais pas sous la menace ou la contrainte. Autrement dit, essayez d'obtenir que les discussions aient lieu dans un endroit où la foule en colère ne sera pas derrière la porte.
- Tous les employés doivent se préparer à évacuer le bâtiment. Demandez-vous si les objets essentiels, tels que les ordinateurs portables, les téléphones satellites, l'équipement radio et les dossiers principaux devront être emportés. Verrouillez toutes les pièces évacuées ; quittez l'enceinte en utilisant une sortie loin de la foule et où le personnel ne peut être vu. Un site bien choisi aura une sortie de secours séparée non visible des points d'entrée et de sortie principaux. Le personnel devra connaître les autres voies secondaires.
- Si une évacuation sûre n'est pas possible, rassemblez tout le personnel à un endroit où il sera difficile d'accéder une fois toutes les portes verrouillées.
- Si les personnels locaux pensent que la foule est énervée par les meneurs qui ne sont pas les dirigeants de la communauté habituels, ils pourront contacter ces derniers et leur demander de venir sur le lieu de la confrontation pour calmer la foule.
- Désignez une personne qui contactera d'autres organisations pouvant encourir un risque similaire.

Suite à un incident, veillez à :

- Maintenir une forte sécurité pendant quelques jours jusqu'à ce que la situation se soit visiblement calmée et qu'il n'y ait pas de risque de représailles individuelles.
- Considérer la position de l'organisation en matière de relations publiques et quels messages, le cas échéant, l'organisation communiquera.
- Tenir parole : ayez des discussions, même si la protection de la police est renforcée. Communiquez non seulement avec les autorités officielles mais aussi avec le reste de la population ; vous devrez rétablir les relations et peut-être l'acceptation.

10.3.2 Survivre au pillage

Le pillage d'entrepôts, de convois, de bureaux et de logements, est fréquent. Tout comme pour le vol à main armée, la règle essentielle pour survivre à un pillage est de ne pas résister et d'éviter l'agression des membres du personnel en laissant les pilleurs prendre ce qu'ils veulent. Ne montrez aucune crainte : les signes de grande vulnérabilité pourraient rendre les pilleurs sûrs d'eux et ils pourraient se retourner contre vous (p. ex. ils pourraient avoir prévu de ne prendre que de la nourriture mais pourraient aussi décider de s'en prendre à d'autres biens). Restez calme, gardez votre dignité et essayez de calmer la tension. En général, il est conseillé de quitter le lieu de pillage au cas où la situation s'aggraverait. Cela pourrait ne pas être toujours possible et la situation pourrait être plus dangereuse à l'extérieur. Si c'est le cas, vous devrez sans doute vous préparer à des heures, si ne n'est des jours, d'anarchie permanente et de pillage général. Les pilleurs pourraient arriver par vagues, et finalement dévaliser complètement les lieux.

Anticipez une augmentation possible des risques. Au fil du temps, il y aura moins de biens matériels pour satisfaire les pilleurs. Essayez de rester discret et gardez un moyen de communication. Il pourrait être possible de garder une radio portative, un téléphone mobile ou un téléphone satellite, ou de négocier pour qu'un téléphone vous soit laissé (si les lignes ne sont pas coupées). Reprenez ou rétablissez le contact avec vos collègues dès que possible.

Chapitre 11
Sécurité de l'argent liquide

Ce chapitre porte uniquement sur le vol et le vol à main armé perpétrés par des personnes externes à l'organisation. Cependant, la sécurité de l'argent liquide est un sujet plus large, et les protocoles opérationnels doivent également inclure la sécurité de l'argent liquide en cas d'événements tels qu'un incendie ou une catastrophe naturelle. Les organisations doivent également être conscientes de la nécessité de protéger le personnel contre la fraude et la tentation de détourner l'argent.

11.1 Réduire l'utilisation d'argent liquide

De toutes les formes de paiement, l'argent liquide est le plus susceptible d'être perdu ou volé. Les organisations peuvent réduire leur utilisation d'argent liquide en utilisant d'autres mécanismes financiers formels, tels que les paiements par chèque et par carte de crédit, les opérations bancaires par téléphone mobile, les cartes prépayées et les cartes smart. Si possible, demandez à tout le personnel d'ouvrir un compte bancaire et envisagez de couvrir tous les frais encourus pour l'ouverture de ce compte. Gardez à l'esprit que les cartes de crédit d'entreprise peuvent être très vulnérables à la fraude. L'utilisation des cartes de crédit doit faire l'objet de consignes et doit être régulièrement contrôlée. Les organisations qui ont des flux de trésorerie importants doivent se renseigner sur la possibilité de contracter une assurance spécifique contre la perte ou le vol.

Les mécanismes informels de crédit et de transactions tels que le système *hawala* offrent une autre solution. Certains de ces réseaux n'opèrent que localement, tandis que d'autres ont des liens internationaux. Les contacts locaux devraient être en mesure de vous conseiller. Le système *hawala* a subi des pressions, surtout après le 9/11, suite à des inquiétudes sur des transactions qui auraient aidé au transfert illégal de fonds à des organisations terroristes, mais il reste très utilisé dans de nombreux pays en développement.

11.2 Discrétion

Lorsque vous utilisez de l'argent liquide, soyez discret. Si peu de personnes le savent, le risque sera moindre. Les communications par téléphone ou par radio doivent être codées. Si vous retirez de l'argent à la banque, organisez la transaction au préalable et, de nouveau, soyez discret. Pour régler les fournisseurs, il est préférable d'utiliser l'une des autres méthodes

mentionnées plus haut, autres que l'argent liquide. Si le personnel utilise régulièrement le même hôtel ou le même fournisseur, envisagez de créer un compte chez ce prestataire.

La quantité et le volume d'argent liquide sont un problème fréquent et parfois inattendu. En Somalie, par exemple, la monétisation de l'aide alimentaire au début des années 1990 a donné lieu à des paiements en shillings somaliens qui ne représentaient pas moins de 17 mètre cubes. Même les sommes relativement modestes de monnaie internationale peuvent représenter des liasses très considérables de billets de banques. Gardez cela à l'esprit lorsque vous retirez de l'argent à la banque et demandez que l'argent vous soit versé en grosses coupures.

11.3 Limiter l'exposition

Il existe plusieurs moyens de réduire l'exposition d'une organisation à la perte ou au vol. Les règlements juste-à-temps des fournisseurs réduisent la quantité d'espèces détenue au bureau. Une autre pratique courante est de fixer un plafond d'argent liquide pouvant être retiré, transféré ou gardé dans le coffre-fort de l'organisation, mais n'oubliez pas que réduire la taille des transactions individuelles augmentera probablement le nombre de transactions, ainsi que leur coût. Si l'argent liquide encourt le plus grand risque lorsqu'il est physiquement déplacé, envisagez de déplacer de plus grosses sommes moins fréquemment, surtout si des moyens plus sûrs de transport d'argent liquide sont périodiquement disponibles, tels que les hélicoptères ou les grands convois. Considérez les divers risques à différents points dans la chaîne du transfert, depuis la banque jusqu'au coffre-fort de l'organisation et finalement jusqu'au bénéficiaire, et représentez cette chaîne sur un organigramme. Il pourrait être possible de réduire le nombre de maillons de la chaîne, par exemple en demandant aux fournisseurs de se présenter au bureau pour se faire payer, plutôt que de se déplacer pour effectuer le paiement en argent liquide.

Si les cambriolages, les hold-up et les vols sont des facteurs de risque, il sera conseillé de répartir le risque : ne conservez pas tout l'argent en un seul lieu et ayez une certaine quantité sous la main, dans un endroit évident, afin d'apaiser les voleurs et de les encourager à vous laisser tranquille. Une certaine somme d'argent doit être facilement accessible sur vous, dans la voiture et dans le logement ; le reste sera de préférence caché. Lorsque vous voyagez, cachez votre argent personnel sur vous, dans un portefeuille, dans une ceinture autour de la taille, dans une autre pochette pendue à votre cou et peut-être aussi dans vos chaussures. Si une personne voyage accompagnée, répartissez l'argent entre les différents voyageurs. En périodes de forte

tension, lorsque le retrait, la relocalisation ou l'évacuation pourrait être nécessaire, distribuez l'argent liquide au personnel qui part, non seulement pour répartir le risque mais aussi pour que les personnes aient de l'argent liquide sous la main si elles étaient séparées. Dans les pays où l'évacuation est une forte possibilité, cela devra être organisé au préalable et planifié de sorte que le personnel sache à quoi s'attendre. Assurez-vous que les personnes acceptent de porter de grosses sommes d'argent liquide sur elles dans des situations de forte tension.

11.3.1 Réduire la prévisibilité

La routine augmente le risque. Les risques prévisibles courants incluent :

- La somme d'argent liquide accumulée pour le paiement des salaires.
- Les paiements spéciaux au personnel national juste avant une évacuation.
- L'arrivée du personnel international à l'aéroport, son transfert à l'hôtel ou au bureau en ville (les voleurs professionnels pourraient contrôler les heures d'arrivée des vols internationaux et s'attaquer aux véhicules sur la route principale qui mène à la ville).
- Les déplacements entre le bureau et la banque, effectués par les comptables ou les directeurs financiers, surtout s'ils empruntent toujours la même route et voyagent approximativement aux mêmes heures. Bien que le trajet en soi puisse ne pas être problématique, le fait d'avoir des routes et des heures prévisibles pourrait augmenter le risque de vol.
- Les comptables ou les directeurs financiers accompagnés d'une autre personne lorsqu'ils vont à la banque, ce qui indique qu'ils vont retirer une somme d'argent plus importante que d'habitude.

Dans ces situations, prenez des précautions de sécurité supplémentaires et essayez de réduire la prévisibilité. Par exemple :

- Utilisez un véhicule loué ou le véhicule d'un membre du personnel local, non identifiable, ou une route secondaire pour amener le personnel de l'aéroport au bureau ou à l'hôtel.
- Changez les périodes de versement des salaires et les heures des paiements afin d'en réduire la prévisibilité, mais cela sera probablement mal accueilli par le personnel.
- Autorisez plus de membres du personnel à aller à la banque ; changez l'itinéraire ainsi que les heures des visites.

11.3.2 Réduire la vulnérabilité

Idéalement, ancrez le coffre-fort au sol afin qu'il ne puisse pas être emmené. Placez une serrure devant être ouverte avec deux clés, et donnez les clés à deux

personnes différentes. Ou bien, utilisez une clé et un cadenas à combinaison. Lorsque vous étudiez la sécurité du coffre-fort, demandez-vous si les voleurs armés seraient susceptibles d'utiliser la violence contre le personnel si le coffre-fort n'était pas ouvert lorsqu'ils l'ordonnent. Si l'un des détenteurs de clés est sur le point de partir en vacances ou autre, assurez-vous qu'un comptage de caisse est effectué en présence du nouveau détenteur de clé, que le montant est juste et qu'il est approuvé par les deux parties.

La voiture est la méthode la plus courante de transporter de l'argent liquide. Pour réduire la vulnérabilité, deux personnes au minimum, et de préférence plus d'une voiture, devront être utilisées, mais, encore une fois, évitez la prévisibilité et envisagez de varier le nombre de passagers et de voitures. Dans les cas extrêmes, une escorte armée ou un véhicule blindé pourrait être utilisé, mais cela attirera probablement une attention non désirée. Pour retirer de l'argent liquide d'un distributeur automatique de billets (DAB), choisissez un guichet situé dans une rue fréquentée, ayant une file d'attente, retirez l'argent pendant la journée et idéalement soyez accompagné d'un collègue qui pourra surveiller les alentours. N'oubliez pas que l'on peut vous observer lorsque vous retirez l'argent et que vous pourriez être suivi : n'allez pas dans des rues calmes ou dans des endroits plus douteux après avoir utilisé un DAB.

11.4 Sécurité électronique de l'argent

11.4.1 Facilités bancaires en ligne

Les organisations d'aide humanitaire utilisent de plus en plus les facilités bancaires en ligne pour les transferts monétaires internationaux, et dans certains pays, cela pourrait également être une option viable pour les opérations financières à l'intérieur du pays. Les règles usuelles de sécurité sur Internet sont applicables (voir Chapitre 7) : utilisez un pare-feu efficace et un logiciel de sécurité à jour, ne téléchargez jamais de matériels provenant de sources non fiables et effacez les fichiers Internet temporaires. N'utilisez jamais les facilités bancaires en ligne sur un ordinateur public, par exemple dans un cybercafé. Attention aux messages (que l'on appelle de « filoutage ») qui vous invitent à visiter un site Web pour vérifier votre compte, ou qui vous demandent de confirmer votre mot de passe ; ces messages sont conçus pour vous soutirer des informations confidentielles ; aucune banque ne vous enverra ce type de message.

11.4.2 Vol d'identité

Le vol d'identité et la fraude financière, notamment la fraude à la carte de crédit, sont de grandes industries en expansion. Les formes les plus courantes comprennent entre autres le simple vol physique de cartes ; la fraude aux chèques (imprimer de faux chèques ou voler des chèques) ; la fouille de

Bonnes pratiques de sécurité de l'argent liquide

- Faites tout ce qui est possible pour limiter l'utilisation d'argent liquide.
- Faites une évaluation du risque concernant le flux d'argent liquide dans l'organisation.
- Aux points à haut risque, mettez en place des actions et stratégies pour réduire ce risque.
- Fixez des limites raisonnables de crédit et de retrait d'argent liquide.
- Vérifiez les relevés bancaires et faites des recherches sur les paiements non reconnus.
- Gardez des listes de numéros de téléphone à appeler en cas de perte ou de vol de cartes de crédit.
- Gardez vos codes confidentiels en sécurité (noter un code dans votre carnet d'adresses est dangereux).
- Faites bloquer ou annuler une carte de crédit dès que vous l'avez perdue.
- Lorsque vous remettez une carte de crédit pour faire un achat, ne la perdez pas de vue.
- Si les voleurs vous obligent à leur donner votre numéro confidentiel pour retirer de l'argent, faites-le.

Atténuer les risques des programmes de distribution d'argent liquide

En Afghanistan et en Somalie, des organisations ont utilisé avec succès des organismes de versement pour remettre de l'argent aux personnes qui habitent dans des régions isolées et dangereuses. En Éthiopie, Save the Children contracte une police d'assurance contre le risque de perte lors du transport d'argent liquide dans les zones de projets où il n'y a pas de banques. En Zambie, Oxfam a sous-traité les versements dans les régions rurales isolées à Standard Bank, qui utilisait des véhicules de société de sécurité pour livrer l'argent liquide, accompagnés d'agents de police locaux. D'autres mesures de sécurité incluent par exemple varier les jours et les lieux des paiements, limiter le nombre de personnes qui savent quand l'argent sera retiré et transporté, et utiliser différentes routes pour atteindre les points de distribution.

poubelles (voler des documents financiers dans une poubelle) ; le transfert de comptes (remplir un formulaire de changement d'adresse) ; et tout simplement voler un portefeuille ou un porte-monnaie. Dans certains cas, les personnes sont retenues, parfois même chez elles, pendant que des complices utilisent

leur carte de crédit et leur code confidentiel dans un DAB à proximité. Lorsque ce type de risque existe, convenez d'un plafond, avec votre banque, pour les retraits bancaires.

11.5 Utilisation d'argent liquide dans les programmes

Certaines organisations choisissent, dans leurs programmes, de verser de l'argent liquide plutôt que de fournir une assistance en nature. Les transferts d'argent liquide sont souvent considérés comme un risque de sécurité plus sérieux que l'aide en nature. Les organisations d'aide humanitaire qui mettent en œuvre des projets basés sur l'argent liquide ont créé des moyens intéressants et novateurs de réduire les risques potentiels de sécurité. Tout comme les pratiques organisationnelles internes concernant l'utilisation d'argent liquide, l'utilisation des banques et d'autres institutions financières réduit potentiellement les risques de sécurité associés aux transferts d'argent liquide aux bénéficiaires. Ceci dit, la plupart des projets de distribution d'argent liquide dans les contextes dangereux sont à une échelle relativement petite, et les risques de sécurité peuvent augmenter au fur et à mesure que les programmes se développent.[1]

1 Paul Harvey, *Cash-based Responses in Emergencies* (Interventions sous forme de prestations monétaires), HPG Rapport 24 (Londres : ODI, 2007).

Chapitre 12
Agression sexuelle

12.1 Définitions et cadre

Le viol et autres formes d'attaque et d'agression sexuelles doivent être abordés en tant que catégorie spécifique de menace qui nécessite des mesures distinctes de prévention, d'atténuation, de gestion de crise et de prise en charge post-incident. Le viol est défini ici comme la pénétration sexuelle (vaginale, anale ou orale, par un pénis ou un objet) sans le consentement et contre le gré de la victime. D'autres types d'attaque sexuelle peuvent inclure des attouchements non désirés ou le déshabillage forcé. Le viol et autres attaques sexuelles sont généralement perpétrés en utilisant ou en menaçant d'utiliser la violence.

L'intimidation et le harcèlement sexuel ont des effets psychologiques qui peuvent se transformer en symptômes physiques, quelquefois longtemps après l'incident. L'organisation doit avoir une politique sur le harcèlement sexuel et s'assurer qu'elle est appliquée par le personnel. Cependant, ce chapitre porte principalement sur les atteintes directes à l'intégrité physique d'une personne. Les hommes aussi bien que les femmes peuvent être victimes d'attaque sexuelle, mais les femmes le sont de manière disproportionnée, et une grande partie de ce qui suit est donc écrit dans cette perspective.

L'agression sexuelle est une question de pouvoir et d'humiliation, tout autant que de sexe. L'agression sexuelle a divers motifs. Dans les contextes dans lesquels les organisations humanitaires opèrent, ils incluent :

- Certaines catégories de femmes (un groupe ethnique particulier, une caste inférieure ou une « occidentale ») sont perçues comme moralement faciles ou indignes de respect, et peuvent donc être utilisées à des fins sexuelles.
- Le viol et la domination des femmes renforcent les sentiments de pouvoir du violeur, qui pourrait s'étendre au groupe social ou ethnique auquel il appartient.
- Pour ceux qui y participent, le viol collectif peut être utilisé comme rituel d'attachement, pour renforcer la cohésion d'un groupe et l'identification à ce groupe.
- Le viol peut constituer une arme de guerre, destinée à détruire les liens sociaux dans la société ennemie et à affaiblir la détermination des hommes du groupe opposé.
- Le viol en tant que tactique terroriste peut avoir des motivations politiques

et peut avoir pour but d'intimider l'organisation ou les intervenants internationaux en général.

Porter atteinte et démoraliser l'ennemi en violant et en humiliant « ses » femmes est une tactique courante de violence. Lutter contre le viol peut donc devenir un aspect important des efforts de protection civile. Comme indiqué dans l'introduction, ces problèmes de protection n'entrent pas dans le cadre de ce rapport.

L'exploitation sexuelle, telle que l'extorsion de faveurs sexuelles en échange de protection matérielle et physique, se produit souvent lorsque des hommes ont le contrôle de ressources (rations alimentaires, accès à en endroit sûr ou documents fondamentaux) ou exercent d'une autre façon un pouvoir sur les femmes. Bien qu'il n'y ait aucune menace directe de violence, il s'agit malgré tout d'une forme de consentement forcé. Les femmes en déplacement (PDPP, rapatriées, résidentes des camps de réfugiés, migrantes économiques) peuvent être particulièrement vulnérables, surtout si elles ont une position sociale ou juridique faible.

12.2 Réduction du risque

12.2.1 Sensibilisation et compréhension générale du risque

La réduction du risque commence lorsque l'organisation et l'individu reconnaissent que l'agression sexuelle constitue un risque réel. Actuellement, ce n'est pas le cas : les attaques sexuelles et les viols des travailleurs humanitaires restent des sujets très sensibles qui reçoivent souvent trop peu d'attention dans les consignes de sécurité. Inclure des consignes claires sur l'agression sexuelle dans les protocoles de sécurité de l'organisation peut aider à encourager une plus grande attention, une plus grande discussion et une plus grande action sur ce sujet éprouvant pour de nombreux membres du personnel, y compris les coordinateurs de la sécurité.

Il est important de reconnaître que les hommes et les femmes de tous âges courent le risque d'être victime d'agression sexuelle. Il est également important d'être conscient que travailler dans des contextes violents peut accroître le risque de formes particulièrement traumatiques d'attaque sexuelle et de viol. Pendant une période de captivité, par exemple, il pourrait y avoir un plus grand risque de viols collectifs ou de viols répétés. Les femmes, plus souvent locales qu'étrangères, peuvent être enlevées et forcées à l'esclavage sexuel ou à un « mariage » avec un combattant.

12.2.2 Cartographie et caractéristiques du risque

Les actes d'agression sexuelle peuvent être perpétrés dans toute société et à

tout moment. Cependant, les organisations humanitaires doivent avoir une idée des pays dans lesquels cette forme de violence constitue un plus grand risque pour les travailleurs humanitaires : la RDC et l'Afghanistan comparativement au Sri Lanka, par exemple. L'absence d'une analyse du risque et la sous-déclaration systématique des incidents donnent lieux à des évaluations basées sur des impressions, qui sont souvent plus fréquentes que les évaluations reposant sur des informations fiables. Parmi les facteurs généraux qui augmentent le risque, même sans enquête ciblée, on trouve : la présence de nombreux hommes jeunes qui ont accès à des armes ; une guerre ou un conflit dans lequel le viol a souvent été utilisé comme arme ; les régions dans lesquelles un gouvernement a peu ou pas de contrôle ; une société traditionnelle qui limite le contact entre les femmes et les hommes non mariés ; ou des situations où l'extorsion de faveurs sexuelles est une pratique courante. Cette extorsion pourrait expliquer la sous-déclaration systémique du viol.

Une analyse ciblée du risque identifiera les lieux, les heures, les situations et les catégories de personnes qui courent un plus grand risque. Les zones où le risque est le plus élevé peuvent inclure des quartiers dans lesquels une milice opère ; l'espace qui entoure un camp de réfugiés ou la périphérie d'un camp ; certains quartiers dans une ville ; les prisons (les hommes et les femmes détenus dans les commissariats ou en prison sont souvent victimes de viol) ; certains types d'hôtels ; et les points de passage des frontières et les postes de contrôle. À certains moments, le risque pourrait être accru : la nuit ; pendant les festivals et les fêtes ; pendant les distributions d'aide ; lorsque les femmes vont chercher de l'eau ou du bois de chauffage ou lorsqu'elles vont aux toilettes ; lorsque les groupes armés sont vaincus et fuient ; ou lorsque les troupes entrent dans une ville dont ils viennent de s'emparer. Certaines catégories de personnes peuvent être en plus grand danger : le personnel national d'un groupe ethnique particulier ; les femmes autochtones (ou les jeunes hommes) membres du personnel qui ont été relocalisés et qui vivent dans un environnement où ils ont peu ou pas de liens sociaux ; les femmes occidentales ; les veuves ou les femmes qui dirigent un ménage ; ou les jeunes filles (parce que les violeurs pensent qu'elles sont moins susceptibles d'être séropositives au VIH).

Certains groupes ou individus sont peut-être plus susceptibles de perpétrer une attaque sexuelle et un viol que d'autres, p. ex. les paramilitaires ou les agents de police qui sont réputés ne pas respecter les normes du droit international ; les soldats indisciplinés du gouvernement ; les groupes rebelles et les mouvements violents de jeunes ; les soldats démobilisés et au chômage ; et les voleurs armés dont l'intention principale est de voler mais qui souvent violeront une femme qui se trouve dans le logement qu'ils cambriolent.

12.2.3 Sources d'information

En raison de la sensibilité du sujet, il n'est pas toujours facile d'obtenir des informations fiables ou des statistiques exactes sur les incidents d'agression sexuelle. Des sources possibles incluent le personnel local féminin, les groupes locaux de femmes, les organisations des droits de l'homme, les juristes des droits de l'homme, les groupes de femmes dans les camps de réfugiés, les expatriés qui ont de bons contacts dans la communauté tels que les travailleurs religieux ou les travailleurs humanitaires long terme, et les points focaux de sécurité dans les ambassades. Il pourrait ne pas toujours être conseillé de poser des questions directes ; abordez plutôt le sujet avec discrétion et soyez sensible aux normes culturelles et sociales. Une approche consisterait à demander des statistiques aux autorités locales et aux centres médicaux locaux : leur réaction pourrait vous donner une indication de la sensibilité du sujet. Elle pourrait également donner lieu à une discussion sur les exigences légales et les réponses locales à la violence sexuelle et vous donner des ressources légales et médicales complémentaires sur la région.

12.2.4 Réduire la vulnérabilité

Mesures individuelles

Les recommandations générales concernant la compétence personnelle sur le plan de la sécurité (voir Chapitre 6 : Le personnel de la gestion de la sécurité ») sont également pertinentes ici. Le personnel doit s'habiller et se comporter de façon discrète et doit s'efforcer de ne pas attirer l'attention. Cependant, il est également important de montrer clairement de la détermination, une connaissance de l'environnement et de l'assurance. Le but est de donner l'impression à toute personne pouvant vous observer que vous ne serez pas facilement surpris ou accablé.

L'apparence personnelle est une question délicate car elle est jugée faire partie du domaine privé. Toutefois, la façon dont une femme s'habille, son style de coiffure et son comportement peuvent aussi être interprétés à tort par autrui comme étant explicitement sexuels ou peuvent être utilisés comme excuse d'agression. Cela peut arriver dans n'importe quelle société, mais pourrait être plus courant dans les communautés opposées au style d'habillement occidental, qui peut être considéré comme informel. Les membres du personnel, hommes et femmes, doivent adopter une approche culturellement sensible concernant leur apparence et privilégier la pudeur. Dans de nombreux contextes sociaux et culturels cela facilitera l'acceptabilité sociale des membres masculins et féminins du personnel, ce qui en général contribuera à l'acceptation de leur rôle et de leur travail.

Dans des sorties sociales, la consommation excessive d'alcool rend ceux qui s'y adonnent particulièrement vulnérables à un éventail de menaces, notamment

l'agression sexuelle. Les agressions sexuelles sont parfois commises après avoir drogué la boisson de la victime. Les recommandations de base sont : n'acceptez pas de boissons offertes par des étrangers (ou même par des personnes connues en qui vous n'avez pas encore entièrement confiance) ; dans les endroits où des boissons sont servies soyez parfaitement conscient de votre environnement et ne laissez jamais votre verre sans surveillance.

Mesures organisationnelles

Examinez soigneusement les hôtels utilisés par le personnel et insistez pour avoir une chambre qui offre le maximum de protection contre les intrus. Dans certains cas, l'évaluation du risque pourrait indiquer que le personnel féminin doit loger avec des collègues. Les consignes générales concernant la sécurité du logement et le choix du site doivent être observées (voir Chapitre 9 : « Sécurité du site »). Dans des contextes particulièrement dangereux, les femmes qui font partie du personnel doivent être vues le plus souvent possible avec des collègues hommes de la communauté ou avec des membres masculins du personnel d'une organisation partenaire locale, pour donner l'impression qu'elles ne sont pas seules ou isolées. La civilité de la personne (Mademoiselle, Madame) ou un prénom féminin reconnaissable ne doit pas être affiché à l'extérieur du logement ou paraître dans l'annuaire téléphonique. Envisagez d'employer un aide ménager pour ouvrir la porte aux visiteurs pendant la journée. Si vous utilisez un répondeur téléphonique, faites enregistrer le message d'accueil par un homme.

Des mesures supplémentaires possibles pourraient inclure :

- Les employées jugées être à risque (internationales et nationales) doivent être accompagnées de chez elles à leur lieu de travail dans un véhicule de l'organisation. Si une employée vit seule ou loge à l'hôtel, le chauffeur doit avoir pour instructions de l'accompagner jusqu'à la porte de son logement et d'en vérifier l'intérieur pour s'assurer qu'il n'y a aucun intrus.
- Dans les situations à haut risque, les employées doivent voyager en groupe ou être accompagnées par une femme ou (si c'est culturellement acceptable) par un membre du personnel masculin, aussi bien pendant les heures de travail que pendant les heures de repos. Elles doivent être informées des procédures de sécurité appropriées et ne pas s'exposer à un risque ou exposer les personnes qui l'accompagnent.
- Dans un contexte hostile, les employées ne doivent jamais être laissées seules, même pendant de courtes périodes.

Procédures de sécurité différentes pour les personnels hommes et femmes

Dans certaines circonstances, les procédures de sécurité pourraient être différentes pour les hommes et les femmes. Par exemple, la politique

pourrait être qu'aucune employée ne dorme dans une zone du projet, même si le personnel masculin y est présent. Ces mesures ont tendance à être contestées parce qu'elles sont jugées discriminatoires. Cependant, leur intention est de réduire un risque identifié, et non pas de discriminer. Dans une certaine perspective, il pourrait être affirmé que les personnes, si elles sont pleinement informées du risque, devraient être en mesure de prendre leurs propres décisions. Le revers de cet argument est que les répercussions d'un incident vont au-delà de l'individu et pourraient affecter les opérations de l'organisation entière, ce qui justifie que l'organisation prenne la décision finale. Des exemples de ces décisions pourraient inclure les employées qui sont relocalisées loin des quartiers ou des camps à haut risque, ou le retrait ou l'évacuation du personnel féminin en temps de risque accru. Ces politiques doivent être expliquées par une évaluation du risque à jour dans le lieu en question et doivent être appliquées de manière sélective en fonction de cette évaluation. Par exemple, des mesures pourraient être adoptées pour le personnel féminin national uniquement, pour les jeunes femmes, ou pour les femmes appartenant à un groupe ethnique particulier.

12.3 Survivre à une agression sexuelle

Les consignes données pour survivre à une agression sexuelle sont principalement basées sur des modèles psychologiques occidentaux. Ces modèles sont axés sur l'individu et se concentrent sur la thérapie par la parole, selon laquelle la survivante est aidée à mettre l'incident, ses émotions et ses réactions en perspective. Les personnes issues de milieux culturels différents pourraient réagir différemment face à la violence sexuelle. Celle-ci pourrait, par exemple, affecter non seulement leur bien-être psychologique mais également leur avenir social, notamment la possibilité de mariage. Les victimes pourraient chercher à oublier ou à refouler leur expérience plutôt que de la recadrer, ou pourraient avoir recours à des pratiques de guérison traditionnelles. En offrant leur soutien, les organisations doivent être ouvertes et sensibles à d'autres moyens de rétablissement.

12.3.1 Être victime d'une attaque sexuelle

Le message clé à communiquer au personnel doit être : protégez et préservez votre vie. Cependant, au-delà de ces conseils il n'y a pas de règle générale sur la façon de se comporter face à une menace imminente d'attaque sexuelle et de viol. Les réactions les plus courantes sont :

La résistance active

- hurler, klaxonner, crier à l'aide ;
- se sauver ; et
- se défendre.

Résistance passive

- parler à l'agresseur pour tenter de le faire changer d'avis (connaître quelques phrases dans la langue locale serait très utile).

Ce qui arrive et ce que fait le membre du personnel dépendra des circonstances, p.ex. s'il y a une montée progressive de la menace ; combien d'agresseurs il y a ; s'ils sont armés ; où l'agression se produit (un lieu public ou privé) ; s'il y a de l'aide à proximité ; et la préparation mentale d'une personne. Il est également important de ne pas oublier que l'agresseur pourrait être quelqu'un que la victime connaît. Survivre doit être la priorité, et ensuite minimiser l'atteinte physique et psychologique durant l'agression sexuelle ou le viol. Cela pourrait signifier devoir se soumettre et ne pas résister physiquement.

Réactions psychologiques possibles

Comme dans d'autres situations graves, les mécanismes de défense psychologique seront probablement actifs. Ceux-ci comprennent :

- La dissociation : comme si la victime regardait un film et observait l'action.
- Le déni : « ce n'est pas à moi que cela arrive ».
- Le refoulement : « cela sera fini dans quelques minutes ; ce n'est pas la fin du monde ».
- La rationalisation: « quel moyen mesquin de satisfaire ton besoin de pouvoir. Tu ne peux pas vraiment me faire de mal ».

Bien qu'il s'agisse de réactions normales pendant une attaque, elles ne doivent pas induire la victime en erreur et la laisser penser qu'elle n'a pas été profondément blessée.

Réactions physiques possibles

Il peut également y avoir des réactions physiologiques ou psychosomatiques durant ou immédiatement après un viol, telles que le vomissement, la diarrhée, l'hyperventilation, l'étouffement ou des difficultés pour avaler sa salive, la perte de connaissance et la désorientation. Ce sont des réactions normales suite à l'expérience psychologique et physique d'une attaque sexuelle. Les réactions physiologiques et psychosomatiques seront fonction de l'ampleur de l'attaque, du lieu, du type d'agresseur et de la durée de l'attaque. Dans certains cas, les victimes pourraient être accablées et traumatisées psychologiquement. Les membres du personnel qui apporteront un soutien immédiat à la victime devront être conscients des implications possibles.

Les attaques sexuelles sont souvent sous-reportées, en raison des sentiments de honte et des craintes des réactions de la famille, des amis et des collègues. D'autres membres du personnel pourraient vouloir encourager le silence par respect des

sentiments de la victime ou en raison de leur propre gêne. Ces réactions sont compréhensibles, mais ne pas déclarer une attaque sexuelle pourrait priver la survivante de l'assistance médicale et du soutien psychologique dont elle a besoin pour son rétablissement. Cela privera également de l'information d'autres acteurs et ce manque pourrait entraîner d'autres attaques similaires.

12.3.2 Être témoin d'une attaque sexuelle

Il faut aussi prendre en considération ceux, souvent des hommes, qui pourraient être forcés par les agresseurs à assister au viol, ou qui pourraient être empêchés d'intervenir pour arrêter le viol d'une collègue, de leur mère, leur femme ou leur fille qui est commis dans une autre pièce ou tout près. Le risque est réel et la sensibilisation et la préparation sont nécessaires. Ne pas pouvoir empêcher un viol est, en soi, une expérience profondément choquante. Le témoin devra, par la suite faire, face à ses propres émotions et aura besoin de soutien.

Comme pour les victimes, le principal message à communiquer aux témoins doit être de se protéger et de préserver leur vie. Il faut conseiller aux membres du personnel :

- De s'efforcer de ne pas être séparé d'une collègue menacée de viol, de raisonner les agresseurs, de tenter d'offrir quelque chose d'autre pour prévenir l'agression, et d'insister sur le fait qu'ils ne peuvent pas laisser la femme seule.
- Si résister met leur vie en danger, il faut renoncer. Personne ne sera aidé si les témoins sont gravement blessés ou tués ; si la violence est utilisée en premier lieu contre les collègues masculins ou contre les membres de la famille, elle sera plus susceptible d'être utilisée envers la femme, soit pendant le viol soit après. Il faut conseiller aux collègues qui se trouvent dans de telles situations d'éviter de provoquer inutilement la violence des agresseurs, et de se concentrer plutôt sur leur propre préparation mentale pour aider et soutenir la victime du viol quand l'attaque aura pris fin. Se concentrer sur la meilleure façon de soutenir la survivante du viol immédiatement après l'agression peut être un mécanisme d'adaptation important pendant le supplice.

12.4 Gestion de la crise

L'agression sexuelle et le viol doivent être gérés comme une urgence médicale et une menace de sécurité grave. Ils doivent faire l'objet d'une gestion attentive dans quatre domaines majeurs : les soins médicaux, le soutien psychologique, l'action juridique et la confidentialité. L'action dans tous ces domaines doit être lancée immédiatement et simultanément ; elle sera plus facile si une équipe de gestion de crise est déjà en place avant un incident.

12.4.1 Soins médicaux

La victime pourrait avoir subi des blessures causées par la violence de l'agresseur ; elle court également un plus grand risque de grossesse involontaire et de maladie infectieuse. Elle doit avoir accès à des soins médicaux immédiats pour traiter les blessures graves. Les mesures suivantes pourront également être prises, avec l'accord de la victime :

Contraception post-coïtale

La contraception post-coïtale (également connue sous le nom de contraception d'urgence ou pilule du lendemain) doit être administrée dans les 72 heures qui suivent un rapport sexuel. La décision doit être celle de la personne concernée, mais ne doit pas attendre les résultats d'un test de grossesse ; en effet, ceux-ci ne sont généralement pas fiables dans un temps si court.

Traitement prophylactique du VIH et d'autres maladies sexuellement transmissibles (MST)

Les traitements médicaux peuvent éviter le Chlamydia, la Gonorrhée et la Trichomonase. Dans les cas où l'on ignore si l'agresseur est séropositif au VIH, présumez qu'il l'est, et des précautions devront être prises au cours du traitement médical de la survivante. Le risque de contracter le VIH augmente si la pénétration a été violente et a occasionné des lésions des tissus. Il n'existe pas de traitement préventif efficace à 100 %. Le traitement offert par certaines organisations est une association AZT/3TC, qui doit débuter sous 72 heures et se poursuivre pendant quatre semaines. Ce traitement peut avoir des effets secondaires, tels que maux d'estomac, nausées, maux de têtes et inflammation du foie, et ne doit être pris que sous contrôle médical. Les examens médicaux de dépistage des maladies sexuellement transmissibles et du VIH doivent être répétés de façon intermittente jusqu'à un an après l'incident.

La prophylaxie post-exposition (PPE) est un traitement médical d'urgence qui peut être utilisé pour protéger les personnes contre le VIH. La PPE comprend un traitement, des examens de laboratoire et un soutien psychologique. Idéalement, la PPE doit être démarrée 2 à 4 heures (et pas plus tard que 48 à 72 heures) après une exposition possible au VIH et doit se poursuivre pendant approximativement quatre semaines. Bien qu'il n'ait pas été prouvé de façon certaine que la PPE empêche la transmission de l'infection au VIH, les recherches indiquent que si le traitement est démarré rapidement après une exposition possible, il pourrait être bénéfique. L'efficacité de la PPE est probablement plus forte si le traitement démarre quelques heures après l'exposition au VIH et est progressivement réduite s'il commence plus tard. Après 48 à 72 heures, les avantages sont probablement minimes ou non existants, et les risques d'intolérance et d'effets secondaires associés aux traitements antirétroviraux seront plus importants que tout avantage potentiel de prévention.

Certaines ONG et agences des NU gardent dans leurs bureaux des kits de démarrage de PPE pour le personnel et le personnel associé. Chaque kit de PPE contient les médicaments nécessaires pour les cinq premiers jours de traitement, un test de grossesse, une contraception orale d'urgence, des consignes pour le médecin et le patient et un formulaire de consentement.

Infection par le virus de l'hépatite B

Si la victime du viol n'est pas immunisée contre l'hépatite B suite à une infection par le virus et si elle n'a pas reçu la vaccination complète contre ce virus, celle-ci devra être proposée. Elle est efficace lorsqu'elle commence dans les 14 jours qui suivent l'exposition. Une protection supplémentaire peut être obtenue avec l'administration d'immunoglobuline anti-hépatite B.

12.4.2 Soutien psychologique

Les principaux objectifs pour ceux qui apportent une aide immédiate sont de créer un sentiment de sûreté, d'empathie et de soutien positif. Il sera également important de fournir un soutien au reste de l'équipe. La principale personne qui apporte un soutien doit être quelqu'un ayant de la maturité et de la sensibilité, une personne en qui la victime a confiance. Cela ne sera pas nécessairement son responsable.

Rétablir une sensation de sûreté

Il sera important de trouver un endroit où la victime peut se reposer, se rétablir et se sentir complètement en sûreté et en sécurité. Le lieu aura une influence sur ce sentiment de sûreté et de sécurité, de même que les personnes qui entourent la victime. Une expatriée pourra être relocalisée à l'intérieur du pays ou dans un pays voisin. La personne affectée est la mieux placée pour indiquer où elle se sent le plus en sûreté et en sécurité ; elle devra donc être consultée et encouragée à prendre part au processus décisionnel. Demandez-lui avec qui elle se sent le plus à l'aise et en qui elle a le plus confiance. Cette personne devra se trouver à proximité et rester en contact étroit.

Soutien positif

Les réactions émotionnelles immédiates après un viol peuvent varier : une survivante pourrait pleurer abondamment et souffrir d'anxiété extrême ; une autre pourrait être très calme, sembler être maîtresse d'elle-même et soucieuse de continuer comme d'habitude, comme si rien ne s'était passé. Quelle que soit la réaction :

- Montrez de la compassion envers la survivante et aidez-la à identifier et à reconnaître ses émotions. Ne lui imposez rien.
- Évitez de dire ou de faire quelque chose qui pourrait impliquer que la victime est mise en cause ou critiquée. Il n'y a aucun doute que la seule

personne à incriminer est le violeur. Bien que la survivante ait pu se rendre plus vulnérable par ses actions, elle n'a pas demandé à être attaquée et n'a pas consenti à ce qui s'est passé.

- Laissez la victime maîtriser autant que possible la situation. Après avoir subi une attaque sexuelle ou un viol une personne se sentira impuissante, aussi bien physiquement que psychologiquement. À tous moments, consultez-la et cherchez à obtenir son consentement, ne prenez pas de décision pour la victime.

Messages clés à communiquer aux survivantes d'agression sexuelle :

- Le but profond de l'attaque n'est pas le sexe mais le pouvoir.
- Vous n'êtes pas responsable, c'est l'agresseur qui doit être incriminé.
- Vous n'êtes pas seule. Il y a quelqu'un pour vous soutenir et s'occuper de vous.
- Vous pouvez survivre à cette expérience et vous en remettre. Cela prendra du temps et demandera de l'attention, mais ce n'est pas la fin de votre vie ou de votre bonheur.
- Des personnes qui ont vécu la même expérience vous accompagneront dans votre rétablissement lorsque vous serez prête à leur parler.

Soutien du reste de l'équipe

Les personnes qui étaient présentes mais qui n'étaient pas en mesure d'empêcher l'agression auront également besoin d'un soutien. Si une plus grande partie de l'équipe est au courant de ce qui est arrivé, l'organisation devra aborder le sentiment de choc, de désorientation, de dépression, de colère et de confusion que cela pourrait provoquer chez les autres membres du groupe. D'autres membres de l'équipe pourraient également avoir été victimes de viol dans le passé. En fonction de leur propre processus de rétablissement, elles pourraient être bien placées pour fournir un soutien à cette nouvelle victime. Si l'incident réveille leur propre traumatisme, elles auront aussi besoin de soutien.

Aider les aidants

Fournir un soutien aux victimes du viol est stressant et éprouvant. Ceux qui le fournissent doivent également contrôler leurs propres émotions, qui pourraient être agitées. Ils devront trouver quelqu'un avec qui partager dans la confidentialité ce qu'ils ressentent et qui a la maturité de parler avec l'aidant pour évaluer de manière constructive ses émotions.

S'occuper de la famille

La responsabilité de s'occuper de la famille de la victime est celle du siège, sauf si le partenaire de la victime et peut-être ses enfants, se trouvent également dans le pays d'opérations, ce qui sera incontestablement le cas du personnel

national. Demandez conseil à la victime ainsi que son consentement. Il est important qu'elle puisse décider qui doit être informé et quand, et ce qui doit être dit. Cependant, dans le cas d'un rapatriement, il faudra donner une raison à la famille et il sera nécessaire pour cela de consulter la victime. Si la presse mentionne l'incident, une approche plus proactive sera nécessaire avec la famille, et l'organisation désignera probablement une personne de contact qui communiquera régulièrement et étroitement avec les proches, tout comme dans le cas d'un rapt (voir Chapitre 14).

12.4.3 Poursuite juridiques et questions de confidentialité

Déclarer l'incident à la police

Informer ou pas la police est également une question délicate. Demandez préalablement au conseiller juridique de l'organisation quels sont les procédures et les délais pour faire une déclaration à la police. Il pourrait sembler bureaucratique, insensible et non urgent d'obtenir les documents officiels, mais ultérieurement cela pourrait être important. C'est le cas, par exemple si la victime décide de porter plainte et d'engager des poursuites, pour accéder aux services d'avortement légal ou obtenir un traitement VIH à un prix abordable.

Preuves médico-légales recevables devant un tribunal

Si une action en justice est envisagée, les poursuites auront lieu dans le pays où l'agression s'est produite. Les poursuites judiciaires nécessitent des preuves médicales. Pour être acceptables, ces preuves doivent être recueillies et traitées sous certaines conditions prescrites. Consultez au préalable un juriste fiable et expérimenté (l'ambassade pourrait vous aider à en trouver un). Demandez au juriste :

- qui a l'autorisation légale de recueillir les preuves médico-légales en cas de viol ;
- quelles preuves médico-légales sont recevables en cas de poursuites pour viol ; et
- quelles procédures de recueil, d'examen et de conservation des preuves doivent être suivies pour qu'elles soient recevables.

Si un professionnel de la santé reconnu est nécessaire, envisagez d'en identifier un (de préférence une femme) avant que tout incident ne se produise.

Toute cette procédure est délicate et exige de la sensibilité. Les deux principes essentiels sont :

- Les preuves médico-légales ne doivent pas être recueillies sans en donner entièrement la raison à la victime au préalable et sans expliquer ce que

Exemple de cas : une deuxième expérience traumatisante

Il n'est pas rare que la victime subisse un deuxième traumatisme par un traitement indélicat de la police. C'est le cas d'une travailleuse humanitaire expatriée qui a subi une agression sexuelle pendant son travail à l'étranger. Personne dans cette organisation (bien connue) ne savait quoi faire immédiatement après l'incident : ni sa responsable sur le terrain, ni l'équipe des ressources humaines au siège. Le lendemain, elle s'est rendue, seule, à son ambassade pour déclarer l'incident. L'ambassade l'a envoyée au commissariat local, accompagnée d'un autochtone, agent de sécurité à l'ambassade. Arrivée au commissariat, quatre policiers armés lui ont posé des questions détaillées sur l'incident. Comme ses réponses étaient hésitantes, ils l'ont accusée de mentir. Pendant l'interrogatoire, d'autres policiers curieux venaient sans cesse regarder ce qui se passait. Le policier chargé de l'interrogatoire a insisté pour qu'elle leur montre ses blessures avant de la laisser quitter le commissariat. Ils ont ensuite insisté pour qu'elle leur montre où l'incident s'était produit, pour une reconstitution qui, selon eux, était essentielle pour l'enquête. Aucune enquête réelle n'a jamais eu lieu. L'agresseur n'a jamais été pris et la survivante a appris plus tard qu'il était très rare dans ce pays de juger ou de reconnaître une personne coupable d'agression sexuelle. Son expérience au poste de police a en fait été une deuxième agression et une nouvelle expérience traumatisante.

Une personne bien informée et digne de confiance doit toujours accompagner la victime au poste de police pour s'assurer qu'elle ne subit aucune intimidation ou qu'elle n'est à aucun moment davantage persécutée, que l'interrogatoire est conduit dans une langue que la victime comprend et que les documents et l'assistance appropriés sont fournis. Ce défenseur doit être prêt à intervenir si les droits et la dignité de la victime ne sont pas respectés. Il est important qu'il assume son rôle de défenseur en tant que représentant de l'organisation et que l'on ne pense pas qu'il agit à titre personnel.

cela représente dans la pratique. Elles ne doivent être recueillies qu'avec le consentement écrit de la victime.

- Recueillir les preuves n'engage pas la victime à une action en justice, mais cela permet de le faire si la victime souhaitait engager des poursuites plus tard.

Les preuves comprennent généralement les vêtements de la victime (non lavés), les poils pubiens, les blessures génitales ou autres et le sperme. Il existe trois problèmes courants pour recueillir les preuves :

- La victime veut se laver et changer de vêtements aussitôt que possible et pourrait souhaiter se débarrasser de tout ce qui lui rappelle son supplice. Cela ne détruit pas toutes les preuves, mais il sera plus difficile de les recueillir.
- Recueillir certaines preuves physiques nécessitera une personne ayant reçu une formation médicale et un équipement approprié.
- Les preuves doivent être scellées, manipulées et conservées correctement et de manière appropriée, par exemple dans des sacs en papier et non pas en plastic, scellés et identifiés ; certaines devront être réfrigérées. Les mouvements devront être limités et le moins de personnes possibles devront manipuler les preuves ; un registre des personnes qui ont eu accès à ces preuves devra être tenu à jour avec les dates et les heures (la chaine de possession des prélèvements doit être préservée). Des dates limites pourront être imposées pour le recueil des preuves, sous peine de non-recevabilité devant le tribunal.

Poursuites judiciaires

La décision d'engager des poursuites judiciaires doit être prise par la victime, qui doit être en mesure de prendre une décision éclairée. Pour l'aider dans cette décision, le responsable doit se renseigner sur les détails pratiques d'une arrestation et des procédures judiciaires. La victime devra-t-elle identifier un suspect avant qu'il ne puisse être inculpé ? Comment cela se passe-t-il dans la pratique ? Le suspect peut-il être libéré sous caution ? La victime doit-elle témoigner au tribunal, et peut-être devant son agresseur ? Les poursuites peuvent-elles être engagées si la victime ne réside pas dans le pays de façon permanente, ou devra-t-elle revenir plusieurs fois ? Quelles sont les pénalités encourues si l'agresseur est reconnu coupable ? Étant donné les faits de l'affaire, quelle est la probabilité qu'il soit déclaré coupable ? Quels sont les antécédents du pays en ce qui concerne les normes internationales de protection des droits de l'homme et les poursuites pour agression sexuelle ? Les tribunaux sont-ils prédisposés à rejeter les cas d'agression sexuelle ou de viol ? Une survivante d'agression sexuelle doit être assistée par une personne suffisamment compétente et objective afin d'étudier et de trier avec elle toutes ces informations.

Les responsables doivent également considérer les implications de sécurité possibles pour la survivante et pour les autres membres du personnel si des poursuites sont engagées, mais aussi si elles ne le sont pas. Porter plainte et engager des poursuites judiciaires pourraient exposer la survivante, sa famille et les personnes qui la soutiennent et l'accompagnent à des menaces et à des agressions supplémentaires.

Secret médical

Dans la mesure où le viol constitue une urgence médicale, la survivante doit bénéficier du secret médical. Celui-ci est souvent garanti par la loi (p. ex. la

loi sur la protection de la vie privée aux USA). Le but de la confidentialité est de permettre à la personne qui demande une aide médicale d'évoquer ses inquiétudes et problèmes médicaux et psychologiques ouvertement et pleinement. Les sentiments de honte, de culpabilité et d'humiliation ainsi que la crainte d'être jugée par autrui, expliqueront que la survivante souhaite garder son expérience aussi confidentielle que possible. C'est une préoccupation légitime.

Même si l'on sait que quelqu'un dans l'organisation a été victime d'agression sexuelle, la survivante ne voudra pas que les détails soient divulgués et discutés. L'équipe, son responsable et l'organisation entière ont la responsabilité de protéger l'identité individuelle de la victime et la confidentialité des détails sur son supplice. Le responsable doit entreprendre une action immédiate. Il doit :

- S'assurer que les autres membres du personnel ne mentionnent pas l'incident. Si des questions sont posées, il est conseillé de donner une réponse standard (p. ex. « Je ne peux pas répondre à cette question, contactez le représentant résident »).
- Établissez une ligne directe de communication avec le chargé de liaison désigné au siège. La communication entre le terrain et le siège devra être gérée et contrôlée et ne devra pas impliquer une série d'intermédiaires ou un grand nombre de suppléants. La situation ne devra pas être évoquée dans les lieux où la discussion pourrait être entendue par d'autres personnes.
- Entreprenez une action proactive avec la presse s'il semble qu'elle va couvrir l'incident, et faites bien comprendre aux rédacteurs en chef et aux journalistes qu'ils ne doivent utiliser, tout au plus, que les initiales de la victime, et non pas son nom complet.

Il est conseillé de se mettre d'accord sur un nom codé, un mot codé ou un numéro de cas pour faire référence à la victime, plutôt que d'utiliser son nom.

Alerter autrui

Comme pour tout incident de sécurité, il est important que le viol et les autres agressions sexuelles, y compris les tentatives d'agression, les menaces ou l'intimidation, soient non seulement rapportés à l'organisation mais aussi signalés à d'autres organisations pertinentes sur le terrain (sans révéler l'identité de la victime, à des fins de confidentialité). Cela permettra à d'autres organisations d'évaluer le risque et d'adapter leurs plans de sécurité en conséquence.

Il est possible de protéger la vie privée des victimes de diverses façons, par exemple en n'identifiant pas la victime lors d'une déclaration d'incident. Mais il est extrêmement important de déclarer l'incident et de le signaler à d'autres organisations travaillant dans la région. Il faut comprendre et expliquer à la

Exemple de cas : obligation de sonner l'alarme

Un certain nombre d'organisations ont des bureaux sur le terrain, dans des villes qui, bien que situées en dehors de la zone de guerre, sont sujettes à des tensions entre la population locale et les autorités, et elles sont considérées comme une force d'occupation. En presque 20 ans de guerre, de nombreux civils ont été brutalisés et sont donc armés. Une nuit, trois voleurs armés forcent l'entrée d'un logement d'une organisation. Ils violent une femme expatriée pendant que sa collègue est tenue sous la menace d'un fusil. La femme est rapatriée mais, afin de protéger sa vie privée, l'organisation décide de ne pas mentionner l'incident. Trois semaines plus tard, des voleurs armés forcent l'entrée d'un autre logement. Cette organisation déclare ultérieurement qu'une expatriée avait été menacée de viol mais que l'un des voleurs avait empêché ses complices de mener à bien l'attaque. Le personnel est bouleversé et l'organisation décide de le retirer de la ville. Ce n'est qu'alors qu'un plus grand nombre d'organisations qui travaillent dans la ville apprennent le viol perpétré plus tôt, et que des mesures ont été prises pour réduire la vulnérabilité du personnel.

victime du viol que ne pas mentionner l'incident pourrait empêcher d'autres personnes et organisations de prendre des précautions et pourrait ainsi contribuer à d'autres viols. La stratégie doit donc être de protéger la vie privée de la victime, mais de donner l'alerte pour éviter à d'autres personnes de subir la même épreuve.

Il sera également important de rédiger un rapport complet qui pourra être remis à un nouveau responsable. Celui-ci devra peut-être donner suite aux procédures judiciaires et il devra gérer les conséquences émotionnelles à long terme du personnel restant. Il pourrait également être conseillé d'informer l'ambassade, même si son assistance n'est pas recherchée (auquel cas il ne sera pas nécessaire de révéler l'identité de la victime).

12.5 Préparation et formation

12.5.1 Au niveau organisationnel

- Une organisation humanitaire qui déploie du personnel dans un contexte où le viol est un risque connu doit être en mesure de mobiliser un soutien expert et efficace pour les responsables sur le terrain qui se chargent des victimes de viol. Si cette expertise ne peut être développée ou retenue à l'intérieur de l'organisation, elle doit être facilement accessible auprès de sources externes.

- Selon la politique, tous les expatriés (pas uniquement les femmes) doivent être informés du risque de viol, ainsi que des autres risques évalués, avant de signer leur contrat, plutôt que juste avant leur déploiement.
- Les bonnes pratiques organisationnelles doivent inclure des déclarations de principe sur le soutien qu'une victime de viol peut s'attendre à recevoir de l'organisation et comment l'organisation a l'intention de concilier le besoin de confidentialité et celui d'alerter d'autres personnes sur la menace.
- Il doit exister des consignes détaillées pour les responsables sur le terrain. Qu'ils soient hommes ou femmes, ils doivent être préparés à gérer une situation de viol grâce à une formation et à des exercices de simulation.
- Il doit exister des consignes claires sur la façon dont l'organisation protègera et soutiendra le personnel national dans ce contexte spécifique.
- Les responsables devront envisager des options possibles en ce qui concerne les droits aux congés ou à une pause pour repos et récupération, pour les femmes qui travaillent dans des zones à haut risque d'agression sexuelle.

12.5.2 Au niveau du terrain

- Les consignes pour répondre au viol et à l'agression sexuelle doivent être claires, documentées et immédiatement disponibles pour tous les membres du personnel. Elles pourraient inclure les politiques ou pratiques sur le rapatriement, la relocalisation (temporaire ou permanente), le soutien juridique disponible localement et au siège, et la possibilité de congé pour raisons personnelles.
- Il est conseillé aux responsables d'évoquer avec le personnel la menace de viol et les consignes de base sur une conduite appropriée, comme suggéré dans ce chapitre. Au niveau du terrain, si le viol n'est plus ignoré, si les discussions sur le viol ne sont plus considérées comme taboues et si le personnel a été sensibilisé au risque et à la nécessité d'obtenir un soutien adéquat, il sera beaucoup plus facile d'employer les mesures nécessaires pour gérer la situation si elle se présentait. Il doit y avoir une sensibilisation active des membres masculins du personnel, y compris les responsables de la sécurité, aux risques et au stress auxquels sont exposées les femmes qui travaillent dans des zones à haut risque.
- Il sera important d'évoquer avec le personnel issu d'autres milieux culturels quels sont, selon eux, les protocoles et le soutien les plus appropriés. Les employées locales pourraient être moins en mesure de contrôler les résultats et pourraient donc être plus hésitantes à rapporter un incident de violence sexuelle dans l'organisation, et elles pourraient être très inquiètes au sujet de la confidentialité.
- L'équipe de la haute direction doit décider qui se chargera des divers aspects de la gestion immédiate d'une crise.
- Dans une zone à haut risque, il faut conseiller aux couples de parler entre

eux de la façon dont ils perçoivent l'agression sexuelle et de leurs attentes mutuelles en cas d'incident.

- En règle générale, il sera important d'obtenir des connaissances détaillées sur les exigences légales, les pratiques policières et judiciaires, ainsi que le soutien médical spécialisé, de la zone opérationnelle. Ces connaissances seront ainsi disponibles si un incident se produisait.
- Si la contraception post-coïtale et d'autres traitements spécialisés ne sont pas facilement disponibles auprès des institutions médicales dans la zone opérationnelle, veillez à les avoir sous la main au bureau et à les administrer sous contrôle médical. Vous pouvez également veillez à ce que la victime puisse être transportée immédiatement dans un lieu où elles seront disponibles.

12.5.3 Au niveau individuel

Les travailleurs humanitaires, mais surtout les femmes, doivent examiner leur propre capacité de faire face. Les femmes ont en général une plus grande sensibilisation aux risques d'agression sexuelle où qu'elles se trouvent, mais il est important de noter que, dans des contextes de conflit, il pourrait exister un plus grand risque de viol collectif, d'agression avec circonstances aggravantes (c.à.d. être menacé avec une arme) et d'infection au VIH suite à un viol.

- Il est important de reconnaître vos propres forces et limites émotionnelles. Pouvez-vous faire face au risque ? Pourriez-vous survivre émotionnellement et vous rétablir de cette expérience ?
- Décidez si vous être réellement prête à accepter un poste pouvant présenter un risque accru d'agression sexuelle.
- Serez-vous prête à observer les mesures de sécurité visant à contrôler le risque, même si vous les ressentez comme une atteinte à votre liberté personnelle ou à votre droit d'égalité ?
- Envisagez comment vous réagiriez face à votre partenaire, votre famille et vos enfants si vous étiez violée. Pourriez-vous parler du risque et des résultats potentiels d'un incident avec votre partenaire, et établir précisément ce que vous vous pourriez attendre l'un de l'autre, afin que cela ne soit pas une inquiétude et une anxiété supplémentaires ?
- Connaître quelques phrases dans la langue locale pourrait être critique pour changer l'intention d'un agresseur potentiel. Prenez des leçons de langue et penchez-vous, avec vos collègues, sur ce que vous pourriez dire ou faire si vous étiez menacée.

Chapitre 13
Détention, arrestation et enlèvement

Ce chapitre et celui qui suit traitent de la détention et de l'arrestation ainsi que de l'enlèvement, du rapt et des situations d'otages. Ces termes sont souvent employés de façons différentes. Ils ont tous en commun la même caractéristique : des personnes sont privées de leur liberté de mouvement et peuvent subir diverses contraintes allant de la pression polie à la menace de mort, mais la nature et la motivation des ravisseurs pourront différer selon le type de scénario. De ce fait, les stratégies de réponse en matière de gestion de crise ne seront pas nécessairement les mêmes.

La bonne gestion de ces incidents exige une préparation poussée et un haut niveau d'expertise et d'expérience, soit à l'intérieur de l'organisation soit sur demande. La condition indispensable est une formation appropriée pour tout le personnel ayant des activités dans des régions exposées aux rapts ou aux enlèvements. Dans ces circonstances, une organisation doit également avoir un plan de gestion d'incidents pleinement développé (voir Chapitre 5 « Déclaration d'un incident et gestion d'un incident critique »), qui définit les rôles et responsabilités de l'organisation (au siège et sur le terrain) et du personnel dans ces circonstances. Dans tous ces scénarios, les organisations pourraient également envisager de rechercher l'assistance de tiers, par exemple les NU, les gouvernements internationaux ou la Croix-Rouge.

13.1 Terminologie

En termes juridiques, « détention » a une signification spécifique, mais elle fait référence ici uniquement aux membres du personnel gardés en captivité sous le contrôle d'un individu ou d'un groupe. Bien que leur vie ne soit pas gravement ou immédiatement en danger, il n'y a pas de condition préalable à leur libération. Être détenu peut être un aspect courant du travail humanitaire. Le personnel de l'organisation peut être détenu par un groupe de villageois, une autorité locale, un groupe de soldats ou une milice. La détention peut être déclenchée par le mécontentement local au sujet d'un projet ou d'un programme de cette organisation ou d'une autre organisation (souvent, la population ne fait pas la distinction entre différentes organisations), par le ressentiment que le projet fournit de l'aide à d'autres personnes, ou par la frustration parce que les autorités ne nouent pas le dialogue avec un groupe particulier ou ne le font pas de manière satisfaisante.

Le terme « arrestation » décrit la détention de personnes par les autorités du gouvernement (généralement la police mais également l'armée) ou par les autorités présumées. Ce qui la distingue du type de détention plus général mentionné plus haut, c'est le rôle des autorités officielles. Cela signifie que le droit peut, en principe, être invoqué. La situation peut être plus difficile et plus dangereuse lorsque les autorités du gouvernement arrêtent une personne de manière extrajudiciaire (c.à.d. sans mandat d'arrêt légitime) ou lorsque la personne arrêtée « disparaît ». Les autorités pourraient alors nier que l'arrestation a eu lieu ou bien refuser de révéler où se trouve la personne arrêtée.

Le terme « enlèvement » fait référence à l'acte qui consiste à emmener une personne contre son gré et de manière illégale, mais n'entraîne pas la demande d'une rançon. L'enlèvement peut avoir divers motifs : le travail forcé, la conscription, le sexe ou des raisons politiques.

13.2 Réduction du risque

Soyez conscient des zones et des groupes qui bénéficient de l'aide humanitaire et de ceux qui n'en bénéficient pas et qui pourraient penser, en conséquence, qu'ils sont victimes de discrimination. Assurez-vous que le plus de personnes possible dans la zone d'opération comprennent qui est l'organisation et le rôle qu'elle joue. La façon dont les programmes sont exécutés et les compétences relationnelles du personnel du programme sont importantes. Il en va de même de la connaissance des lois et des règlements locaux. La transparence, une bonne communication, l'intégrité, l'impartialité et le respect sont également utiles.

Éviter une arrestation suite à des procédures judiciaires est, bien entendu, généralement impossible. Une arrestation qui ne suit pas la procédure juridique légale peut être contestée mais n'est pas évitable. Si l'on craint la disparition possible de la personne après son arrestation, l'organisation doit immédiatement se mobiliser pour jouer un rôle très actif, qui signalera que la situation est suivie de près.

Le personnel national peut être détenu, arrêté ou enlevé pour des raisons politiques sans rapport avec le travail de l'organisation, et les organisations humanitaires pourraient craindre de donner l'impression de se mêler à la politique locale. Cependant, cela ne doit pas être une excuse pour ne pas assumer l'entière responsabilité de tout le personnel dans cette situation ni pour faire tout ce qui est possible pour son retour sain et sauf.

13.3 Répondre à un incident et gestion de crise

Lorsque des membres du personnel disparaissent, la première difficulté pour le responsable sur le terrain est de découvrir la nature exacte de la situation, d'établir les faits. Cela pourra prendre plusieurs heures ou plusieurs semaines. Des informations fondamentales devront être établies et communiquées dans un rapport d'incident. Les éléments essentiels devant être inclus sont :

- Un énoncé du problème (une personne est manquante, arrêtée ou détenue).
- Qui est la victime (nom, nationalité, âge, genre, position occupée dans le bureau, affiliation, état connu (médical, etc.), famille, clan, tribu).
- Ce qui est arrivé (ce que l'on sait, ce que l'on suppose, ce que l'on ne sait pas en précisant suivant les cas).
- Où l'incident s'est produit, avec le plus de précision possible.
- Quand il s'est produit, avec le plus de précision possible.
- Qui l'a commis (on en est sûr, on le soupçonne, on le suppose ou on ne sait pas).
- Pourquoi il s'est produit (motivation déclarée, supposition).
- Si des témoins ont été identifiés.
- Si d'autres personnes étaient impliquées ou ont été blessées au cours de l'incident.
- Qui a été informé ou qui est au courant en dehors de l'organisation ; qui vous suggérez d'informer en dehors de l'organisation ; si la police, les forces de sécurité ou les autorités sont au courant, ont été informées ou le seront ; si la presse ou d'autres personnes sont au courant de l'incident ; ce que sait le reste de l'équipe ; si la famille a été informée.
- Quelles actions sont en cours ou proposées.
- Une surveillance des médias locaux et nationaux pour mesurer l'impact, le cas échéant.

13.3.1 Détention

En cas de détention, il est essentiel que les personnes détenues respectent les consignes données pour survivre lorsque l'on est pris en otage (voir Chapitre 14). Lorsqu'il juge la situation et le moment appropriés, le détenu pourrait tenter d'obtenir sa libération inconditionnelle (voir plus loin). Pour l'organisation, faire appel aux autorités nationales ou adopter une approche autoritaire peut faire plus de tort que de bien et peut accroître plutôt que réduire la tension avec l'organisation. En général, l'objectif de la détention est de forcer l'organisation ou une autre entité à prêter attention aux ravisseurs et à entamer avec eux un échange sérieux. Répondre à cette attente et nouer un dialogue sérieux suffisent généralement à mettre fin à l'incident. Mais gardez à l'esprit que dans

certaines circonstances, ce qui débute comme une détention peut dégénérer en incident beaucoup plus grave et prolongé.

Lorsqu'ils négocient leur libération, les détenus doivent :

- Ne pas oublier que l'objectif de la négociation est de pouvoir retourner à la base en sécurité et rapidement.
- Souligner leur travail humanitaire et la nature neutre, impartiale et indépendante de leur organisation et de ses activités.
- Rester conciliants ; éviter de devenir hostiles.
- Écouter leurs ravisseurs et tenter de découvrir ce qui les motive et ce qu'ils souhaitent ou espèrent.
- Ne pas faire de promesses dans le but d'obtenir une libération, et toujours préciser qu'ils ne sont pas en mesure de prendre des décisions finales ou de s'engager fermement.
- Demander l'autorisation de contacter leur organisation ou leur ambassade.

13.3.2 Arrestation

Si un membre du personnel est arrêté et si l'on ne sait pas où il se trouve, la première priorité sera d'établir où il est et sous autorité de qui. Faites preuve d'assurance et rendez visite à toutes les autorités locales pertinentes, informez son ambassade (s'il s'agit d'un membre du personnel international), soyez très persévérant et insistez pour obtenir des informations. N'oubliez pas qu'un membre du personnel pourrait être arrêté pour raisons légitimes et pourrait devoir expliquer ses actes. Quoi qu'il en soit, consultez un bon juriste local qui connaît les langues et le système locaux, qui a l'expérience de ce type de situation et qui a peut-être des contacts utiles.

Lorsque vous saurez clairement qui a arrêté le membre du personnel et où il se trouve, veillez à ce que ses droits soient protégés. Insistez pour qu'il ait le droit de visite ainsi que le droit à une assistance médicale et juridique, et exigez des améliorations dans ses conditions de détention si celles-ci sont inacceptables. Protestez si ces exigences sont ignorées. Souvent, les personnes sont arrêtées sans qu'aucune accusation formelle n'ait été faite, auquel cas, insistez pour qu'une accusation soit formulée dans un délai spécifié. L'accusation pourrait porter sur la personne (par exemple, elle est accusée d'avoir pris part à un crime) ou sur l'organisation (par exemple une accusation d'espionnage sous couvert de travail humanitaire). Quelle que soit la situation, la première priorité est de s'efforcer d'obtenir la libération rapide et sans danger du membre du personnel. Dans la plupart des circonstances, ce n'est que lorsque la personne sera dégagée d'accusations injustifiées, que des mesures devront être prises pour disculper la personne ou l'organisation.

Dans le cas d'une arrestation, restez en contact avec la famille de la personne disparue et prenez soin d'elle (voir Chapitre 14). Dites-lui que des mesures sont prises, entretenez avec elle une ligne directe et régulière de communication, demandez-lui quelles mesures elle a prises ou elle a l'intention de prendre, et mettez-la en garde s'il semble que ce qu'elle envisage de faire sera contre-productif.

13.3.3 Enlèvement

Un enlèvement peut être une situation extrêmement difficile. Il est possible que l'on ne sache pas où le détenu se trouve et qu'il soit impossible de contacter les ravisseurs. L'organisation ciblée pourrait s'efforcer de générer un haut niveau de publicité sur l'incident mais, comme dans tous les cas où la presse est impliquée, cela pourrait être contre-productif si cela fait de la publicité inutile aux ravisseurs et les valorise. Autrement, cela pourrait être une bonne approche si elle indique aux autorités que beaucoup de personnes sont au courant du sort du détenu et que prolonger sa captivité nuirait considérablement à l'image des autorités ainsi qu'à leur capacité d'établir ou de conserver la primauté de la loi. Les organisations des droits de l'homme et de défense d'autres causes sont généralement plus en mesure de créer ce type de publicité que les organisations humanitaires, il pourrait donc être possible de coopérer avec elles. Dans d'autres cas, il ne sera pas possible de faire grand-chose, à part diffuser des informations et des photos du détenu et tenter de trouver quelqu'un qui puisse fournir une piste ou un contact.

Chapitre 14
Rapt et situations d'otages

14.1 Définitions

Le rapt est défini comme l'enlèvement et la détention forcée d'une personne dans le but explicite d'obtenir une contrepartie pour la libération de la personne. L'objectif et, de ce fait, le motif du rapt varient : souvent c'est l'argent, mais les ravisseurs pourraient également exiger des concessions politiques. Dans d'autres cas, ce qui pourrait être apparemment une cause politique, pourrait en fait n'être rien d'autre qu'un racket.

Les termes « prise d'otages » et « rapt » sont parfois employés de manière interchangeable, mais prise d'otages fait ici référence à un état de siège. En fait, les auteurs du crime et leurs otages ont été localisés et encerclés par les forces de sécurité, et les ravisseurs menacent de tuer les otages s'ils n'obtiennent pas un moyen de prendre la fuite. Un rapt peut se transformer en prise d'otages ou en état de siège lorsque les forces de sécurité découvrent où sont les ravisseurs et les encerclent.

Globalement, le nombre de rapts s'est accru au cours des dernières années, notamment dans le monde humanitaire. Les pays à haut risque comprennent le Yémen, l'Irak, la Somalie, le Darfour (Soudan), l'Afghanistan et le Pakistan. Il peut être difficile d'éviter le rapt, tout au moins si l'on a affaire à un groupe de criminels organisés et déterminés. Il peut être un moyen très efficace d'obtenir des fonds et de renforcer sa visibilité politique et constitue donc une menace très grave.

14.2 Stratégies de réduction du risque

Un certain nombre de mesures peuvent contribuer à réduire le risque, entre autres une évaluation des risques du programme, une formation et une orientation spécialisées pour le personnel, ainsi que des procédures opérationnelles standard bien conçues. Les organisations pourront aussi déclarer certaines zones temporairement interdites.

14.2.1 Préparation, coordination et sensibilité culturelle

La préparation comprend l'élaboration d'un plan de gestion d'incident (voir Chapitre 5) et une formation spécialisée connexe pour le personnel sur le terrain et au siège. Rappelez constamment au personnel qu'il est important d'observer les procédures de sécurité. La coordination comprend la création de liens aux niveaux local et international afin de pouvoir bénéficier d'une expertise en

matière de gestion d'incident au fur et à mesure des besoins. La sensibilité culturelle est essentielle, car le comportement du personnel n'est jamais examiné aussi minutieusement que lorsque celui-ci est victime d'un enlèvement ou d'un rapt ou lorsqu'il est pris en otage. Cela doit s'appliquer au personnel national tout comme au personnel international, car les employés nationaux sont souvent recrutés dans une région différente de la leur et pourraient ignorer les spécificités de la zone opérationnelle tout autant que leurs collègues internationaux. Cela doit s'appliquer également au personnel qui se rend dans un pays pour une période limitée seulement, ainsi qu'aux employés qui vivent et travaillent dans la zone pour une plus longue période. La sensibilité culturelle comprend tous les aspects que vous pourriez inclure dans une stratégie d'acceptation, par exemple comprendre le type de comportement considéré comme approprié ou inapproprié dans un contexte social ou culturel particulier, ainsi que les dimensions de genre et le respect des normes culturelles et religieuses.

14.2.2 Réduire l'exposition

Éviter la routine

Évitez la prévisibilité dans vos déplacements entre le logement et le bureau, ainsi qu'en dehors des heures de travail, par exemple lorsque vous déposez les enfants à l'école ou lorsque vous allez faire des courses. Variez les heures de vos déplacements et prenez des routes différentes. Ceci est plus facile à dire qu'à faire, et très difficile à observer pendant une période prolongée.

Évitez d'attirer l'attention

Des travailleurs humanitaires expatriés ont été victimes de rapt sur le chemin de l'aéroport. Éviter d'attirer l'attention pourrait impliquer que le personnel voyage en taxi plutôt que dans un véhicule de l'organisation facilement identifiable (assurez-vous qu'il s'agit d'un taxi légitime). Si l'on soupçonne que les communications radio sont écoutées, les travailleurs expatriés ne devront pas s'identifier lorsqu'ils sont en déplacement. Par exemple, seuls les travailleurs locaux pourraient être autorisés à parler à la radio (dans leur langue maternelle), comme ils le feraient s'ils ne voyageaient pas avec un collègue expatrié. Les informations sur les plans de déplacement, les itinéraires et les heures de voyage doivent être codées (voir Chapitre 8 « Sécurité des voyages et des déplacements »).

Contrôle de sécurité du personnel dans le pays

Pour les ravisseurs, le moyen le plus facile d'obtenir des informations sur une cible potentielle est de placer un contact dans l'organisation. Le contrôle de sécurité du personnel dans le pays peut permettre de se protéger contre cette pratique mais il est difficile, et souvent négligé, et l'opportunisme pourrait empêcher ce contrôle (par exemple si le chauffeur de l'organisation est malade et appelle son frère pour le remplacer).

Éliminer des vulnérabilités potentielles

Une mesure plus drastique consiste à retirer les membres du personnel jugés être exposés à un grand risque. À la fin des années 1990, alors que le risque de rapt grandissait en Tchétchénie, les organisations se sont relocalisées dans un premier lieu à Nazran en Ingouchie, puis à Vladikavkaz en Ossétie du Nord. En 2003 et 2004, suite à une vague d'attentats à la bombe et de rapts en Irak, la plupart des membres du personnel international ont été relocalisés en dehors du pays. La même situation s'est produite dans les régions somaliennes. Notez que le personnel national peut être exposé à un risque similaire à celui des travailleurs internationaux, sinon plus grand ; en fait, la tendance à long terme montre que les travailleurs nationaux courent un risque de plus en plus élevé comparativement aux travailleurs internationaux.[1]

Protection du site

La protection du site et les règles strictes qui régissent l'identification des étrangers ainsi que les limites d'accès (y compris les mesures et procédures de contrôle d'accès – voir Chapitre 9 « Sécurité du site ») compliquent la situation pour des ravisseurs potentiels. Bien que le rapt soit encore un risque dans les logements, les hôtels et les maisons d'hôtes, la plupart des incidents se produisent lorsque la cible est en déplacement, généralement en voiture.

Sensibilisation accrue et contre-surveillance

En termes simples, la contre-surveillance signifie « surveiller si l'on est épié ». Pour qu'un rapt aboutisse, il faut généralement le planifier, et avant d'agir les criminels surveilleront pendant un certain temps le logement, le bureau et les mouvements de la cible qu'ils ont identifiée. Ils pourraient tenter d'en savoir plus sur le logement en se présentant comme membre du personnel d'entretien, ou en examinant les serrures des portes et des fenêtres pendant que le personnel est absent. Ils pourraient suivre en voiture une personne ciblée pour définir sa routine et identifier le moment idéal pour agir. Observez tout ce qui peut être inhabituel. Pour bien le faire, il vous faudra faire preuve d'attention constante et avoir une connaissance de l'environnement local, notamment savoir qui est de la région et qui ne l'est pas. Voir le chapitre 9 pour de plus amples renseignements sur les méthodes de contre-surveillance.

Rechercher une protection et un soutien locaux

Dans les contextes où un hôte est responsable du bien-être de son invité et mobilisera des hommes pour le protéger comme s'il faisait partie de sa famille, il pourrait être utile d'obtenir une protection (traditionnelle) locale. De même, demander à des notables respectés de se joindre à vous pour une visite pourrait

1 Stoddard, Harmer et DiDomenico, *Providing Aid in Insecure Environments : 2009 Update* (L'aide humanitaire dans les contextes dangereux : mise à jour 2009)

être une forme de protection. Certaines organisations ont une politique selon laquelle les expatriés, lorsqu'ils voyagent, sont toujours accompagnés par une personne de la région; envisagez également de partager un logement avec un travailleur local. Toutefois, dans les contextes où cette tactique a eu du succès dans le passé, notamment au Yémen, en Somalie et en Afghanistan, elle ne garantit plus une protection, car le contrôle des autorités traditionnelles et les normes sociales qu'elles soutiennent se sont affaiblis avec l'afflux d'éléments criminels et de combattants étrangers. Seule une bonne connaissance du contexte déterminera si cette tactique réduira le risque.

Protection armée

Une autre option est d'avoir une protection armée dans le logement, le bureau et en déplacement, y compris pendant les heures de loisir (voir le chapitre 3 pour de plus amples informations sur la protection armée). Cela pourrait nécessiter des gardes armés aux alentours du site ou une protection étroite (gardes du corps). Il y a cependant des exemples d'incidents où, malgré une protection armée, une cible a été enlevée. Les gardes armés pourraient être surpris, surpassés en nombre et en armes, et pourraient se rendre ou être tués.

Politique publique : « Aucune rançon » et aucune autre concession importante

Dans leurs documents de politiques et de communication publique, les gouvernements et les organisations humanitaires déclarent souvent qu'ils ne verseront aucune rançon et ne feront aucune concession importante, dans aucune circonstance, pour résoudre un incident de rapt. Bien entendu, publiquement il ne pourrait en être autrement : déclarer ouvertement que des rançons seront payées reviendrait à déclarer que l'on peut cibler votre organisation et son personnel. Cependant, dans la réalité, les familles, les sociétés privées, les gouvernements et les organisations d'aide versent de l'argent dans de nombreux cas. Ne surestimez pas l'effet dissuasif d'une politique publique de non-paiement : des mesures d'atténuation, une formation et une préparation sont malgré tout nécessaires.

Depuis quelques années, l'assurance contre les rapts et les demandes de rançon est de plus en plus répandue. Son coût varie considérablement et dépend principalement de la taille de l'organisation, des lieux où le personnel travaille et de la couverture éventuelle du personnel national aussi bien qu'international. Selon la police, certains régimes d'assurance donnent la possibilité de déduire 10 % de la prime annuelle à des fins de préparation et de formation. Ils peuvent également couvrir les frais d'évacuation, de communication, de soins médicaux, de soutien psychologique pour cause de traumatisme et d'autres éventualités n'entrant pas dans le cadre de l'organisation, ainsi que l'attribution d'une personne chargée du dossier pour mener les négociations.

14.3 Survivre à une situation de rapt ou de prise d'otages

En termes généraux, le rapt comprend quatre étapes principales :

- Le moment de l'enlèvement.
- La période durant laquelle la victime est détenue et les négociations sont menées.
- La libération de la victime (ou la confirmation de son meurtre).
- Après la libération.

Être victime d'un rapt est une énorme épreuve psychologique et quelquefois aussi physique. Un rapt peut durer d'un jour ou deux à des mois et parfois des années. Les moments les plus dangereux sont la période immédiatement après l'enlèvement de la victime, pendant un état de siège et pendant la libération. À ces moments, les ravisseurs se sentiront menacés, seront tendus et donc plus susceptibles d'avoir recours à la violence. Restez calme et évitez d'ajouter à la tension des ravisseurs. D'autres moments extrêmement difficiles sont lorsque la victime parle à sa famille et à ses collègues, peut-être pour montrer qu'elle est toujours en vie, ou lorsqu'elle est forcée à faire une déclaration sur vidéo qui aura été écrite à l'avance et qui sera envoyée aux médias. Apprendre que d'autres personnes enlevées en même temps ont été relâchées ou tuées peut également être extrêmement difficile. Les victimes pourraient aussi être soumises à des tortures psychologiques, telles que de fausses promesses de libération imminente, ou de fausses exécutions.

Préparez-vous mentalement du mieux que possible. Rappelez-vous que la vaste majorité des victimes de rapt sont finalement remises en liberté et que le corps et l'esprit de l'homme ont des capacités d'adaptation et de résilience considérables, qui permettent aux victimes prises en otage, même à long terme, de supporter physiquement et psychologiquement le supplice, et de s'en rétablir.

14.3.1 Le moment de l'enlèvement

Lors d'un rapt, des personnes peuvent être blessées par balle, recevoir d'autres blessures ou être tuées : un chauffeur, un membre de la maison, un garde résidentiel, un garde du corps. Attendez-vous à être menacé d'une arme, peut-être même à avoir les yeux bandés et à être battu, et dans certains cas même à subir la torture ou le viol. Ces actes ont pour objectif de briser la résistance physique et mentale de la victime et de montrer quelles seront les sinistres conséquences de toute tentative de fuite ou de déjouer les plans des ravisseurs. De plus, les victimes pourraient être droguées. Ces tactiques sont toutes destinées à faire taire la victime. Ne résistez pas ; en fait, rester calme et silencieux vous aidera à retrouver votre sang-froid, à recueillir des informations

sur l'endroit où vous vous trouvez et sur l'identité de vos ravisseurs, et à vous adapter à cette nouvelle situation choquante dans laquelle vous vous trouvez. Au cours des premières heures et des premiers jours, les victimes seront probablement déplacées plusieurs fois car les ravisseurs tenteront de brouiller les pistes. Soyez calme et coopératif, ne parlez que lorsque l'on vous adresse la parole, écoutez attentivement et évitez les gestes brusques. Ne soyez pas agressif et n'essayez pas d'être un héro : acceptez la situation. Vos actes influeront sur votre sécurité et sur votre bien-être.

14.3.2 Pendant votre détention

Préparez-vous à être détenu pendant longtemps et peut-être par plus d'un groupe. Les victimes pourraient être vendues par leurs ravisseurs à un autre groupe de criminels ou à un groupe politique cherchant à se servir du rapt pour obtenir des concessions politiques. L'endroit où les victimes sont détenues et les conditions de la détention varieront considérablement. Elles pourront être détenues au même endroit ou déplacées plusieurs fois ; elles pourront être seules ou avec d'autres détenus. Dans certaines situations, les victimes devront marcher pendant des semaines avec leurs ravisseurs, dans la brousse ou dans la montagne. Certaines seront détenues dans des conditions acceptables, tandis que d'autres seront enchaînées à un lit ou à un radiateur. Si vous êtes à plusieurs, essayez de ne pas être séparés. Être détenu avec d'autres personnes, probablement dans des circonstances difficiles et pendant longtemps, comporte ses propres difficultés, mais la possibilité de pouvoir partager son expérience avec au moins une autre personne sera dans l'ensemble une source de soutien. Si vous êtes détenu avec un groupe important, identifiez un porte-parole qui communiquera avec les ravisseurs ; choisissez cette personne en fonction de ses capacités plutôt que de son rang.

Rappelez-vous qu'obtenir votre libération n'est pas votre problème mais celui de votre organisation. Soyez sûr que votre organisation fait tout ce qui est possible pour vous et qu'elle soutient votre famille et vos amis, même si vous n'entendez rien ou si vos ravisseurs vous disent le contraire. Attendez-vous à des périodes d'isolement et à d'autres méthodes d'intimidation et préparez-vous à une longue attente. Ne croyez pas tout ce que l'on vous dit.

Essayez de créer une relation respectueuse tout en gardant votre dignité : ne quémandez pas, ne suppliez pas, soyez coopératif et obéissez aux ordres sans être servile ou agressif ; ne discutez pas de politique ou de religion, restez sur des sujets communs tels que la famille et les enfants et encouragez vos ravisseurs à vous considérer comme une personne. Évitez d'échanger vos vêtements avec ceux de vos ravisseurs car cela pourrait gêner votre identification lors d'une tentative de sauvetage, ou les vêtements pourraient être utilisés abusivement s'ils comportent un nom et un logo. Soyez conscient

du langage corporel et des styles de communication non verbale ; ne menacez pas de témoigner contre les ravisseurs ; s'ils masquent leur identité, n'indiquez pas que vous les reconnaissez ; mangez et buvez même si vous n'avez pas d'appétit ou si ce n'est pas bon ; maintenez une routine de repos et d'activité ; essayez de prendre de l'exercice chaque jour et gardez la notion du temps ; maintenez une hygiène personnelle, gardez vos valeurs et demandez des médicaments si vous en avez besoin. Soyez discret et essayez de ne pas montrer que vous étudiez vos ravisseurs. Ne vous impliquez jamais directement dans les négociations pour votre libération. Cela ne fera que compliquer les choses. Si l'on vous demande de parler à la radio, au téléphone ou sur vidéo, dites uniquement ce que l'on vous demande de dire ou ce que l'on vous autorise à dire et refusez de négocier, même si vos ravisseurs vous y poussent.

14.3.3 La libération

Les ravisseurs peuvent conduire la victime (les yeux bandés) dans un lieu inconnu et la faire sortir de la voiture, ou bien un tiers pourrait venir la chercher et la conduire aux autorités. Il est moins probable qu'il y ait une forme d'échange direct car cette situation est très dangereuse pour les deux parties. Dans une opération de sauvetage, le lieu peut être pris d'assaut ou encerclé par les forces de sécurité et un état de siège pourrait être créé. Ces situations sont très dangereuses :

- Comme indiqué, essayez d'éviter d'échanger vos vêtements avec ceux de vos ravisseurs : les sauveteurs pourraient penser que vous êtes l'un d'entre eux.
- En cas de tentative de sauvetage, jetez-vous à terre, cherchez un abri et mettez vos mains sur la tête.
- Soyez prêt à crier votre nom. Vous ne serez pas immédiatement reconnu par vos sauveteurs et vous pourriez être traité durement jusqu'à ce que vous soyez identifié comme la victime du rapt et non pas comme l'un des criminels.

14.3.4 Après la libération

Une fois relâché, vous voudrez vous concentrer sur vos proches et vous souhaiterez probablement rester tranquille pendant un certain temps afin de vous rétablir. Cependant, tout de suite après un incident, la presse manifestera certainement un grand intérêt et les autorités voudront aussi vous parler pour obtenir des informations sur les ravisseurs et sur les circonstances du rapt. Vous n'obtiendrez pas tout de suite la tranquillité et l'intimité de la vie privée que vous pourriez souhaiter. Être victime d'un rapt est une énorme épreuve psychologique : attendez-vous à en ressentir les effets pendant des mois et peut-être même des années, mais soyez sûr qu'avec de l'aide vous pourrez vous en remettre et reprendre le cours de votre vie.

14.4 Gestion d'incident critique

En règle générale, les situations de rapt ne peuvent être traitées au niveau du terrain uniquement ; elles doivent impliquer le siège et les bureaux régionaux de l'organisation. Un rapt est une situation très complexe et éprouvante et exige inévitablement la participation d'un certain nombre de personnes et d'organisations diverses, notamment la police, les agences gouvernementales, les médias et les compagnies d'assurance. Des capacités de gestion d'incident critique seront nécessaires, notamment la formation, la planification, des exercices de préparation et l'affectation de ressources adéquates.

14.4.1 La réponse immédiate

La première chose à faire est d'établir les faits et de préparer un rapport d'incident critique. Les éléments essentiels de ce rapport sont évoqués au chapitre 5. Ensuite, assurez la sécurité des autres membres du personnel de l'organisation, peut-être en les cantonnant dans leurs logements ou en les déplaçant dans un lieu différent, plus sûr. Demandez-vous si le risque est tel que les programmes devraient être interrompus. Alertez d'autres organisations qu'un rapt s'est produit afin qu'elles puissent prendre des mesures de précaution pour protéger leur propre personnel.

14.4.2 Les équipes de gestion d'incident critique

La prochaine étape est de mobiliser ou de créer l'Équipe de Gestion d'Incident Critique (EGIC). Décidez comment l'organisation communiquera avec les parties prenantes clés, y compris la famille de la victime, les autres membres du personnel, le gouvernement hôte et le gouvernement du pays de la victime, ainsi que les médias. Un haut responsable informera également le conseil d'administration de l'organisation et, le cas échéant, contactera la compagnie d'assurance et les bailleurs de fonds.

Plusieurs équipes de gestion d'incident pourraient être nécessaires, une sur le terrain, une autre au siège et peut-être aussi une troisième au bureau national principal. Les principaux membres de l'équipe devront avoir été identifiés, les ressources affectées et les procédures établies au préalable. Les membres de l'équipe devront avoir reçu une formation, idéalement comprenant une simulation. L'EGIC du siège a normalement l'autorité suprême, autrement dit l'équipe sur le terrain ne devra prendre aucune décision sans son accord.

Le cœur de l'équipe du siège doit être de petite taille. L'équipe doit comprendre un haut responsable ou plus, un ou deux agents de sécurité ayant une expérience pertinente (une expérience des situations de rapt et de prise d'otages ou une bonne connaissance du contexte où l'incident s'est produit). D'autres membres possibles sont les conseillers juridiques,

Étude de cas : Survivre à un rapt au Pakistan

À la fin 2008, un docteur membre du personnel national d'une organisation active dans la province du Nord-Ouest du Pakistan, a été victime d'un rapt organisé par un groupe d'attaquants armés dans une Toyota break blanche. Durant sa captivité, ils l'ont changé d'endroits plusieurs fois. Tout au long de son épreuve, il a été poli et a suivi les instructions de ses ravisseurs. Il leur demandait le jour de la semaine et l'heure, et il priait lorsque ses ravisseurs priaient pour tenter de gagner leur confiance et leur respect. Il essayait de garder le moral et une attitude positive. Un jour, le docteur a été informé que sa famille avait été contactée et qu'un accord avait été conclu pour sa libération. Les ravisseurs avaient demandé une rançon considérable et la famille du docteur avait refusé. Tous les docteurs de la région se sont mis en grève et ont déclaré que tous les hôpitaux et centres médicaux seraient fermés jusqu'à ce que la victime soit relâchée.

le personnel des ressources humaines et les responsables des médias. Un spécialiste en matière de rapts et de prises d'otages, externe à l'organisation, pourrait se joindre à l'équipe. Il pourrait venir du gouvernement hôte, du gouvernement d'origine ou de la compagnie d'assurance, ou il pourrait être recruté sous contrat auprès d'une société privée de sécurité. Le directeur de l'organisation pourra faire partie de l'équipe ou pas, selon son emploi du temps. Chaque équipe de gestion d'incident critique devra garder un registre de tous les événements, documentés avec précision : ce qui s'est produit, ce qui a été dit, quel jour et à quelle heure, qui était impliqué, quels sujets ont été abordés, ce qui a été décidé, sur la base de quels arguments, et quelle était l'attribution des responsabilités détaillées de chacun. La confidentialité de ces informations doit être respectée.

La gestion d'incident dans le cas d'un rapt est, tout au moins initialement, un travail à temps complet. Le personnel intervenant doit être déchargé de ses autres obligations et protégé d'intrusions inutiles afin de pouvoir se concentrer sur sa tâche. Il devra avoir son propre espace et ses propres installations de travail, notamment une salle de crise temporaire, il devra contrôler la situation tous les jours et choisir et revoir la politique à employer vis-à-vis des ravisseurs, de la famille, des autorités, de la presse et des autres organisations impliquées. Les membres de l'équipe devront se reposer et se relaxer régulièrement, et devront être soutenus pendant et après la crise. Si la crise se prolonge pendant longtemps, les membres de l'EGIC pourraient devoir être remplacés. Dès le déclenchement de la crise, préparez-vous à une transition en douceur : assurez-vous qu'un dossier de

transition est mis à jour avec des rapports et des analyses, et planifiez la transition de sorte à avoir un temps de chevauchement entre les membres de l'équipe.

La gestion d'incident critique devient extrêmement difficile lorsque des personnes de différentes nationalités et de différentes organisations ont été victimes d'un rapt ensemble ou sont détenues par les mêmes ravisseurs. Différents gouvernements et différentes familles seront impliqués et les organisations touchées devront adopter une approche collaborative. Les approches individuelles risquent de fragiliser les organisations ou de donner aux ravisseurs la possibilité de monter une agence contre une autre. Dans l'idéal, les différentes parties prenantes devront constituer des équipes de gestion d'incident critique communes, sur le terrain et au siège. Chaque organisation impliquée voudra y participer, mais les membres de l'équipe doivent être choisis pour leurs aptitudes et leurs compétences en matière de gestion d'incidents, plutôt qu'en tant que représentants de leurs organisations respectives. Des experts externes, qui ne sont affiliés à aucune organisation, pourraient être invités à aider l'équipe à garder son objectivité et son orientation.

14.4.3 Gérer les relations avec la famille de la victime

Cette section porte principalement sur les familles du personnel international. Elle peut également s'appliquer au personnel national. Des consignes supplémentaires spécifiques sur ce sujet se trouvent à la fin de la section.

Contact immédiat

Comme pour tout autre incident grave, la famille de la victime doit être informée immédiatement. Il est essentiel qu'elle apprenne le rapt en premier lieu par l'organisation, plutôt que par la presse ou par un tiers. Tout doit être fait pour rendre visite en personne aux membres de la famille proche, mais cela pourrait ne pas toujours être possible. Si la prise de contact initiale doit se faire par téléphone, organisez, par la suite, une rencontre face à face dès que possible, et envisagez d'inviter les membres de la famille au siège pour qu'ils se rendent compte de la façon dont l'incident est géré.

Au cours des premiers contacts avec la famille, tentez d'en savoir plus sur la victime, sa personnalité, son état mental avant le rapt, son état physique et les besoins spéciaux qu'elle pourrait avoir. Clarifiez l'engagement de l'organisation envers la victime, précisez notamment que son salaire continuera d'être versé, et indiquez quels coûts l'organisation est prête à couvrir pour la famille, tels que ceux des voyages périodiques au siège ou dans le pays où l'incident a eu lieu. Informez-la également du soutien psychologique que l'organisation est en mesure de lui offrir et d'offrir à la victime après sa libération. Un soutien psychologique en situation de

stress pourrait être nécessaire. Une coordination préalable avec d'autres organisations pourra renforcer les ressources internes en la matière.

Comment gérer la famille

La famille a le droit de savoir ce qui se passe. Il sera essentiel de créer et d'entretenir avec elle une relation de confiance. Si la famille n'a pas confiance en l'organisation, elle pourrait agir de sa propre initiative. Même si l'aboutissement de la situation est favorable, la famille pourrait se retourner contre l'organisation avec une plainte publique ou juridique sur une gestion présumée incompétente. Ceci dit, essayez d'éviter d'en dire trop sur la stratégie de négociation et de gestion d'incident critique de l'organisation, car un membre de la famille pourrait malencontreusement dévoiler des informations qui pourraient arriver aux oreilles des ravisseurs ou des médias. Soyez conscient que le gouvernement et les médias du pays de la victime souhaiteront également prendre contact avec la famille, ou vice-versa. Dans l'intérêt de la famille, l'idéal serait d'avoir une approche commune ou tout au moins cohérente entre l'organisation et le gouvernement du pays de la victime.

Liaison avec la famille

Un membre du personnel de l'organisation d'un niveau relativement « élevé », possédant de bonnes compétences interpersonnelles, doit être nommé en tant que chargé de liaison avec la famille. Certaines organisations ont des postes créés expressément pour ces circonstances. L'une des fonctions du titulaire du poste est d'agir en tant que personne contact désignée pour la famille. La même personne doit avoir ce rôle tout au long de l'incident. Il s'agit d'une responsabilité lourde qui nécessitera le soutien de l'organisation.

Il est important de programmer un moment opportun pour informer les familles et, dans la mesure du possible, veillez à ce que l'organisation les appelle, et non pas l'inverse. Dans les cas qui se prolongent, expliquez clairement à la famille que les appels quotidiens des premiers jours de l'incident deviendront progressivement moins fréquents s'il n'y a rien de spécial à signaler. Il est également utile d'encourager la famille à nommer elle-même un chargé de liaison, qui pourra agir comme personne contact avec l'organisation et en tant que porte-parole de la famille. Au fur et à mesure que l'incident évoluera, l'état d'esprit de la famille fluctuera probablement et celle-ci pourra commencer à exprimer des doutes au sujet de l'organisation, des autorités ou de la stratégie suivie. C'est une réaction normale, mais qui doit néanmoins être contrôlée.

Attentez-vous à des initiatives de la part de la famille

Les membres de la famille et les amis proches de la victime pourraient être tentés d'agir de leur propre chef, en particulier si l'incident se prolonge trop :

ils pourraient contacter la presse, se rendre dans le pays où le rapt a eu lieu ou tenter d'établir leur propre ligne de négociation. La famille sera également plus disposée que l'organisation à payer une rançon et pourrait décider de vendre des biens pour collecter des fonds. Les familles ont leurs propres droits d'action, mais conseillez-les sur les conséquences possibles de leurs actes et sur les risques que leurs négociations pourraient entraîner pour d'autres parties.

Les familles des membres du personnel national

Dans le cas du personnel national, les familles pourraient préférer traiter l'affaire elles-mêmes. Certes, elles pourraient être mieux placées pour le faire grâce à leurs connaissances de la culture et de la société locales et de leurs propres réseaux de contacts. Ceci est particulièrement vrai si le rapt est motivé par des rivalités sociales ou politiques entre des groupes ou clans. Toutefois, dans le cas d'un rapt à motivation criminelle ou politique, la famille ne sera sans doute pas mieux placée que l'organisation.

Lorsque des travailleurs nationaux sont victimes de rapt à des fins financières, souvent leur famille versera une rançon, mais pourrait demander une aide à l'organisation, telle qu'une compensation. Dans ces circonstances, il est important d'informer les familles que le paiement de la rançon ne garantit pas la remise en liberté des victimes et pourrait encourager des demandes d'argent supplémentaires. Rappelez à la famille que la libération de la victime est l'une des étapes les plus critiques et les plus risquées d'un rapt. Elle doit être consciente de la position de l'organisation en tant qu'employeur et du soutien que celle-ci peut apporter. Cependant, la décision finale d'impliquer ou pas l'organisation reste celle de la famille. La coordination des activités avec la famille peut être difficile, car souvent les ravisseurs voudront avoir affaire uniquement aux membres de la famille. Cela sera inévitablement plus stressant aussi pour les membres de la famille qui se sentiront directement menacés. Un autre facteur à prendre en considération est le fait que l'assurance contre les rapts et les demandes de rançon ne couvre pas le personnel national, ou que sa couverture comporte des limites et des restrictions.

14.4.4 Gestion d'incident critique et les autorités

« Autorités » fait ici référence au gouvernement hôte et, dans le cas d'un membre du personnel international, au gouvernement de son pays. Dans la pratique, divers départements et institutions du gouvernement pourraient être impliqués.

Dans les cas de détention, une organisation pourrait tenter de résoudre la situation elle-même. Cependant, lorsqu'il s'agit d'un rapt, il est généralement conseillé d'informer immédiatement les autorités car elles l'apprendront probablement à un moment ou à un autre et seront mécontentes si elles n'ont pas été informées. Même si un rapt se produit dans une région du pays

qui n'est pas sous le contrôle du gouvernement, celui-ci doit en être informé. Donnez-lui les faits sur le rapt ainsi que des renseignements sur la victime.

Le personnel du siège et sur le terrain doit choisir quelle politique adopter envers le gouvernement hôte et celui de la victime. Les autorités nationales auront accès à l'information et aux renseignements confidentiels, aux réseaux et aux services (p. ex. mise sur écoute des téléphones et réseaux GSM) qui ne sont pas disponibles aux étrangers ou aux particuliers nationaux et elles pourraient donc être dans une meilleure position pour obtenir une libération. De même, leurs décisions pourraient être guidées par des considérations autres que le simple bien-être de la victime. Elles pourraient vouloir donner l'impression qu'elles assument leurs responsabilités en matière d'ordre public ou qu'elles font preuve de fermeté en matière de terrorisme. Elles pourraient vouloir principalement décourager d'autres ravisseurs potentiels ou utiliser l'incident pour justifier des tactiques brutales envers des adversaires connus. Elles pourraient également se méfier de la capacité d'une organisation humanitaire à gérer correctement la situation d'un rapt ou pourraient vouloir l'empêcher de nouer le dialogue avec les ravisseurs qu'elles considèrent comme des terroristes ou des rebelles (dans certains pays, prendre contact avec les ravisseurs est illégal). Si les autorités sont désireuses de clore rapidement l'incident, elles pourraient être prédisposées à employer la force pendant les négociations ou au lieu d'entrer dans des négociations, ce qui présenterait des risques potentiels pour la sécurité de la victime.

Décidez d'un commun accord avec les autorités, et confirmez :

- La stratégie globale qui sera suivie.
- Que la sûreté et le bien-être de la victime du rapt doivent être la première préoccupation.
- Que les autorités ne feront pas de tentative de sauvetage en utilisant la force sans le consentement de la famille et de l'organisation.
- La confidentialité vis-à-vis des médias, sauf si une stratégie différente est approuvée.
- La participation de l'organisation dans l'équipe de gestion d'incident créée par les autorités. Si cela n'est pas acceptable, essayez d'obtenir la participation d'un représentant de l'ambassade ou tout au moins un accord sur une structure de contacts entre les autorités nationales et l'organisation.
- Une approche commune de la famille.
- Un accord sur le choix d'un interlocuteur (voir plus loin).

Les mêmes sujets doivent être abordés et, idéalement, approuvés d'un commun accord avec le gouvernement du pays de la victime. Demandez conseil à l'ambassade et obtenez son soutien pour communiquer avec les

autorités nationales. Les principales préoccupations du gouvernement du pays de la victime sont en général son retour sain et sauf et traduire les ravisseurs en justice. Cependant, selon le contexte politique plus large, et la relation entre le gouvernement hôte et celui du pays de la victime, d'autres considérations, pas nécessairement énoncées, pourraient également entrer en jeu. Une collaboration sera également nécessaire entre le siège et le gouvernement du pays de la victime concernant sa famille. Dans certains contextes, le gouvernement de la victime pourra établir un contact direct avec la famille et ne pas impliquer l'organisation dans cette procédure.

Il est possible que les autorités nationales ou celles du pays de la victime disent tout simplement à l'organisation qu'elles prendront la direction de la gestion de la situation de rapt. Dans l'idéal, un membre du personnel de l'organisation sera accepté au sein de l'équipe de gestion de crise du gouvernement. Si ce n'est pas le cas, demandez au minimum les garanties décrites plus haut, et essayez d'obtenir des réunions d'informations régulières et une consultation avec l'organisation avant la prise de décisions importantes. Précisez à la famille qui a la responsabilité de la gestion de la situation.

14.4.5 Experts externes

Des experts en gestion des rapts pourront se présenter à vous spontanément, être proposés par le gouvernement hôte ou le gouvernement du pays de la victime, ou être recherchés par l'organisation. Ils pourront également être disponibles par le biais de l'assureur. Ces experts peuvent jouer un rôle utile en offrant une perspective objective basée sur une plus grande expérience. Ils pourront anticiper des scénarios et offrir une meilleure préparation, présenter les options avec leurs avantages et leurs risques respectifs, et confirmer que ce qui a été fait a été bien fait, et qu'avoir des hauts et des bas est tout à fait normal. Le soutien d'un expert est utile si celui-ci agit en tant que conseiller et accompagnateur, notamment en apportant des conseils à l'équipe des médias, un soutien juridique et psychologique à l'EGIC et une expertise régionale ou locale. Cependant, l'expert peut devenir un problème s'il poursuit d'autres objectifs. Un expert fourni par le gouvernement, surtout s'il s'agit de son représentant, suivra la politique officielle du gouvernement, qui ne sera peut-être pas en parfaite harmonie avec celle de l'organisation. Aucun conseiller externe ne doit entrer en négociations directes avec les ravisseurs.

14.4.6 Gérer les médias

Désignez un chargé de liaison avec les médias au siège et sur le terrain. Si un membre du personnel international est captif, les médias internationaux et ceux du pays de la victime suivront probablement l'affaire. La durée pendant laquelle ils s'y intéresseront dépendra d'autres événements qui méritent d'être publiés et de l'importance politique de l'incident. Étant donné que l'incident

sera médiatisé de toute façon, soyez proactif et tentez d'avoir une influence sur le message communiqué. Tous les messages doivent rester concis. Un message clé doit être que l'organisation tient les ravisseurs responsables de la sécurité et du bien-être de leurs captifs. Les médias nationaux (radio, télévision, journaux, Internet dans les langues locales) pourront présenter le fait sous un angle différent. Consultez toujours le point focal avec les médias en ce qui concerne les déclarations qui leur sont destinées.

Un moyen de gérer les demandes de renseignements des médias et l'intérêt du public est de publier des mises à jour hebdomadaires sur le site de l'organisation. Celles-ci permettront de réduire le nombre d'appels téléphoniques et de s'assurer que les messages communiqués par l'organisation sont cohérents. Présumez toujours que les ravisseurs suivent l'actualité et qu'ils pourraient apprendre ce que vous avez déclaré dans votre pays. Il n'est pas conseillé de tenter de communiquer, et encore moins de négocier avec les ravisseurs par l'intermédiaire des médias publics. Les messages médiatiques sont déformés et fragilisent les messages « réels » ainsi que le processus de négociation. Nouez le dialogue avec les rédacteurs et les journalistes afin qu'ils travaillent avec l'organisation plutôt que contre elle. La famille pourrait insister pour lancer un appel public par le biais de la presse : gérez cette demande de manière constructive.

Selon les circonstances, la publicité des médias pourra aider ou gêner la gestion d'une situation de rapt. La publicité pourrait être utile si les ravisseurs s'inquiètent de leur réputation. Cela ne sera probablement pas le cas des bandes criminelles ou des groupes terroristes qui utilisent le rapt précisément pour générer de la publicité. Dans ce cas, ce sont les ravisseurs qui invitent la presse, ce qui est très dangereux : la situation est transformée en spectacle international, et la mise à mort des captifs est une « fin tragique » possible. Contrecarrer cela implique de persuader la presse de ne pas aller dans ce sens. Comme indiqué plus haut, la famille et les amis d'un captif pourraient lancer une campagne de publicité pour faire pression sur le gouvernement de leur pays et sur le gouvernement hôte. Le public ciblé n'est pas les ravisseurs mais les autorités officiellement responsables de la sécurité, et les messages sont conçus pour s'assurer qu'elles continuent leurs efforts pour résoudre la situation. Les indications pourraient être que les captifs sont autorisés à lire les journaux, à écouter la radio, à regarder la télévision ou à utiliser l'Internet. Si c'est le cas, envisagez d'utiliser la presse pour envoyer un message de soutien. Il semble que le fait d'entendre leur nom mentionné aux actualités peut remonter le moral des captifs.

14.4.7 S'occuper des autres membres du personnel

La communication interne avec les autres membres du personnel de l'organisation est importante et doit être proactive et bien gérée. Attendez-

vous à être questionné et entretenez le moral du personnel et sa confiance dans l'organisation, tout en essayant d'écarter le personnel non essentiel des activités de gestion de la crise. La communication doit comprendre :

- Des séances d'information hebdomadaires pour tout le personnel du siège, dirigées par le chef de l'équipe de gestion de la crise.
- Une feuille d'information hebdomadaire rédigée par le directeur de la communication interne, accessible à tout le personnel du siège et sur le terrain (en plusieurs langues si nécessaire), publiée sur l'intranet ou par d'autres moyens de communication.
- Des opportunités pour le personnel de prendre part à l'affaire et de montrer son soutien à la victime, par exemple en signant des messages de soutien. D'anciens captifs disent avoir beaucoup apprécié ces efforts.

14.4.8 Informer d'autres organisations

Les rapts sont des situations très délicates et doivent être gérés avec discrétion. Cependant, comme pour les cas d'agression sexuelle et de viol, le besoin de discrétion doit être mis en balance avec la responsabilité de l'organisation d'assurer la sécurité de tous les travailleurs humanitaires, y compris ceux d'autres organisations. Ceci n'est généralement pas compris. Des discussions pourraient naître entre les différentes organisations, au sujet des stratégies de contrôle du risque et des aspects de la gestion de la situation, surtout sur le rôle des autorités et la question des rançons. Il est difficile de donner des règles, mais les principes directeurs pourraient comprendre :

- L'action d'une organisation a des implications sur la sécurité d'autres organisations dans la même région. La responsabilité en matière de sécurité est donc collective.
- Une organisation dont un travailleur est victime d'un rapt est responsable de choisir l'approche qu'elle adoptera. Cependant, il sera judicieux d'écouter les conseils d'autres organisations ayant une expérience dans la région, surtout en ce qui concerne les implications de sécurité possibles de stratégies particulières.
- En principe, aucune rançon ne doit jamais être versée car cela augmente le risque général d'incidents similaires ciblant la même organisation ou d'autres organisations dans la région. En réalité, dans de nombreux cas une rançon est versée, mais les organisations le nient. Bien que cette hésitation soit compréhensible, il n'en reste pas moins que le versement d'une rançon change considérablement la situation globale, et si une rançon est versée il pourrait être conseillé d'en informer les autres organisations dans la plus stricte confidentialité. Si un travailleur d'une autre organisation est ultérieurement victime d'un rapt, la moindre des

choses est d'informer cette organisation si une rançon a été versée lors du premier incident pour tenter de le résoudre.

14.5 Communiquer et négocier avec les ravisseurs

14.5.1 Communiquer avec les ravisseurs

Un élément fondamental des négociations sera la nature des demandes et qui, dans la pratique, peut ou doit les satisfaire. Nous avons déjà indiqué que les objectifs et les demandes des ravisseurs peuvent changer et qu'une détention peut se transformer en rapt. Il existe également de nombreux exemples de demandes qui étaient tout d'abord politiques et qui se sont transformées en demande d'argent. Mais l'inverse peut également être vrai : si aucune rançon n'est payée, une bande criminelle pourrait « vendre » un captif à un groupe ayant des motivations politiques. Si les ravisseurs demandent des concessions politiques à un gouvernement hôte ou au gouvernement du pays de la victime, la situation sera hors du contrôle de l'organisation.

Dès que l'on soupçonne ou que l'on signale un rapt, un registre devra être ouvert sur le terrain et au siège dans lequel on notera l'heure et les moyens de communication avec les ravisseurs, les noms des personnes impliquées et le contenu des conversations. Ce registre s'ajoutera à celui de la gestion d'incident critique. Les autorités pourraient conseiller d'enregistrer les communications, car le choix d'un mot particulier, le ton de la voix et les bruits de fonds peuvent donner des indices utiles sur l'identité et le lieu où se trouvent les ravisseurs. Les conversations peuvent être enregistrées avec la plupart des équipements de télécommunication, notamment les téléphones mobiles. Souvent toutes les parties, y compris les ravisseurs, s'attendront à ce que les conversations soient enregistrées.

14.5.2 Négocier avec les ravisseurs

L'EGIC au siège devra garder le contrôle de toutes négociations, tout au moins en ce qui concerne les questions plus larges de stratégie et de politiques (pour savoir si le contact direct est permis, par exemple, et quelles sont les procédures standard). Cela vous donnera du temps pour la consultation interne et externe ainsi que pour l'analyse avant de répondre. Les principes clés pour communiquer avec les ravisseurs incluent :

- Examinez leurs motivations, et envisagez si elles ont les mêmes caractéristiques dans le temps. Comment les ravisseurs sont-ils perçus : semblent-ils agressifs et menaçants, sensés et factuels ou très émotionnels ? Quel ton de voix et quel style de discours seraient les plus efficaces pour apaiser la situation et créer un rapport ?
- Examinez le profil des ravisseurs et la façon dont ils ont agi dans le passé.

- Demandez des preuves d'identité et de détention de la victime pour être sûr que celle-ci n'a pas été tuée ou transférée dans un autre groupe de ravisseurs. Un enregistrement sur cassette ou sur vidéo n'est pas une preuve absolue que la victime est toujours en vie. Demandez à la famille ou à un ami intime de la victime de vous donner un détail personnel à son sujet que les ravisseurs ne peuvent connaître (p. ex. le nom d'un bon ami d'école ou quelque chose qui s'est produit pendant des vacances mémorables). Au fil des jours, vérifiez régulièrement que la victime est toujours vivante. La meilleure preuve est d'entendre la personne parler en direct. Si les ravisseurs ne peuvent prouver l'identité de la victime et que celle-ci est toujours en vie, ne poursuivez pas les négociations.
- Convenez, avec les ravisseurs, d'un mot de code qui servira à les identifier, pour être sûr que vous parlez aux réels ravisseurs et non pas à des imposteurs.
- Adressez-vous toujours aux ravisseurs en utilisant leur nom. Encouragez-les à bien traiter leurs captifs : mentionnez les besoins spéciaux qu'ils pourraient avoir, par exemple le port de lunettes, ou un traitement médical spécial. Mentionnez leurs inquiétudes pour d'autres personnes (leur famille, leurs enfants) et demandez s'il y a un moyen d'échanger des messages.
- Soulignez que vous n'avez aucun pouvoir décisionnel et que vous devez parler à d'autres personnes qu'il vous sera peut-être impossible de contacter immédiatement. Cela vous donnera le temps de réfléchir et donnera à l'organisation une marge de manœuvre. Ne donnez aucune indication qu'un tiers (les autorités ou un expert en sécurité, par exemple) vous conseille. Dans certaines circonstances, les ravisseurs pourraient demander à parler au décideur plutôt qu'au messager. Soyez prêt à cette éventualité et mettez-vous d'accord sur une approche au préalable.
- Réaffirmez la politique de non-versement de rançon pour montrer que l'organisation est cohérente et que le temps n'affaiblit pas votre détermination.
- Mettez-vous d'accord sur les heures de communication. Essayez d'obtenir un accord sur le prochain contact ; demandez comment vous pourrez contacter les ravisseurs, par exemple par le biais d'une tierce personne ou d'un message dans un journal spécifique. Prévoyez d'éventuels problèmes de communication, y compris la perte ou les perturbations du réseau de téléphone mobile.
- Entretenez la communication : ne coupez pas le contact de votre propre initiative à moins d'être certain que votre interlocuteur n'est pas le réel ravisseur ou que les captifs ne sont plus en vie. Expliquez bien aux ravisseurs que vous voulez qu'ils communiquent avec vous.
- N'acceptez pas de vous rendre dans un lieu indiqué pour une rencontre. S'il y a une forte pression pour le faire, insistez pour obtenir des garanties

précises pour votre propre sécurité. Vous pourriez être vous-même victime d'un rapt.

14.5.3 Communiquer avec la victime

L'interlocuteur pourra, à un moment, parler directement au membre du personnel captif. Il sera alors très important d'être clair sur le genre d'information et de messages que vous voulez passer. Ne donnez pas à la victime des informations que les ravisseurs ne doivent pas connaître, mais rassurez-la que tout est fait pour obtenir sa libération. L'une des principales préoccupations d'une victime d'un rapt est de savoir comment sa famille fait face. Essayez de la rassurer le mieux possible.

14.5.4 L'interlocuteur

Les interlocuteurs sont un lien entre les décideurs (le groupe de gestion d'incident) et les ravisseurs ; ils ne sont pas les décideurs. Étant donné qu'un rapt peut durer longtemps, il pourrait être nécessaire d'avoir plus d'un interlocuteur. La tâche de l'interlocuteur est uniquement de transmettre des messages. Cependant, il devra pour cela avoir été bien préparé par le biais d'exercices de simulation par exemple, car il y aura inévitablement des demandes imprévues et des pressions exercées par les ravisseurs.

L'interlocuteur devra être un autochtone, il devra maîtriser la langue locale et comprendre la culture et les mœurs de la population. Il devra être fiable, intelligent, équilibré, d'humeur égale, capable de travailler sous extrême pression, être disponible 24 heures sur 24, sept jours sur sept, et disposé à agir sous les directives de l'EGIC. Les interlocuteurs n'ont pas connaissance des discussions de l'EGIC, qui envisage des scénarios et des hypothèses et formule des réponses. Si les ravisseurs insistent pour parler à une personne particulière qui n'est pas l'interlocuteur désigné, assurez-vous que l'interlocuteur que vous avez choisi écoute discrètement la conversation.

Utiliser un intermédiaire local

Un intermédiaire venant de la communauté pourra également se présenter, ou pourra avoir été recherché par l'organisation, proposé ou approché par les autorités ou même suggéré par les ravisseurs. Il n'est pas rare que des personnes locales respectées et influentes s'impliquent elles-mêmes dans la résolution d'un rapt. Des notables ont joué un rôle influent en Somalie et en Afghanistan par exemple, ainsi que des hommes d'affaires dans le Caucase.

Dans une situation de forte acceptation, où la communauté garde une certaine influence sur les ravisseurs, une personne locale digne de confiance pourrait être en mesure d'obtenir une libération. Il doit être précisé, cependant, que ces personnes ne peuvent s'engager au nom de l'organisation sans son

consentement préalable. Face à des criminels bien organisés, plus indépendants de la communauté, des dirigeants traditionnels pourraient être inefficaces. La question de confiance est cruciale. Pour qui l'intermédiaire agit-il ? Est-il de votre côté ou bien a-t-il des liens avec les ravisseurs ? Qui contrôle les négociations ? Il y aura également la question de rémunération. Envisagez de rembourser certains frais généraux, en fonction des taux locaux. Ceux-ci pourront couvrir les déplacements, le logement, la nourriture et les communications. Ces paiements pourraient ne pas être appropriés si l'organisation a affaire à une personne qui, selon les normes locales, est considérée comme relativement aisée.

Négociateurs officiels

Les autorités pourraient proposer un négociateur officiel. La première chose qu'il fera sera certainement d'établir un climat propice au dialogue. Tout d'abord, le centre de l'attention sera probablement les questions mineures sur lesquelles un accord peut être conclu. Cela préparera le terrain pour des discussions sur des sujets plus difficiles. Si le négociateur est présenté par les autorités, il y a toujours le risque que des considérations autres que la sécurité et la libération des captifs entrent en ligne de compte. Ou bien une entité prestigieuse non gouvernementale pourrait proposer un envoyé qui interviendrait en qualité de médiateur pour obtenir la libération des victimes.

14.5.5 Libération par la force

Il n'est pas rare que les forces de sécurité essaient de retrouver les captifs et tentent de les sauver ou de créer un état de siège pour forcer les ravisseurs à se rendre. C'est une stratégie risquée car les captifs pourraient être tués par leurs ravisseurs lorsque ceux-ci se retrouveront piégés. Ou bien, un ou plusieurs captifs pourraient être blessés ou tués dans la confusion, sous les feux croisés qui accompagnent souvent une libération forcée. Les sièges ou les tentatives de libération forcée ne doivent pas être entrepris sans l'accord de la famille et de l'organisation. Cependant, cette approche ne doit pas être totalement rejetée : si les ravisseurs se mettent à mutiler ou à tuer les victimes pour faire monter la pression, ou s'il y a un risque que les captifs meurent de faiblesse ou d'épuisement après une captivité prolongée, une tentative de sauvetage par la force peut être l'option de dernier recours.

Les situations de siège peuvent mal tourner pour un certain nombre de raisons. Du point de vue de l'organisation, deux éléments sont particulièrement importants :

- Ceux qui dirigent le siège ont-ils manifestement le commandement global ? Si ce n'est pas le cas, des actes non coordonnés pourraient mettre la vie des otages en danger.

- Les troupes ont-elles une description précise des otages afin de pouvoir les distinguer des ravisseurs, et ont-elles reçu des instructions de ne tirer que sur les personnes qui tirent sur elles ? N'oubliez pas que les captifs pourraient porter le même type de vêtements que leurs ravisseurs.

14.6 Gérer les suites d'un rapt

14.6.1 Gérer le retour d'une victime d'un rapt

Le retour d'une victime d'un rapt doit également être correctement organisé et géré. Plusieurs exigences contradictoires devront être prises en compte :

- Les besoins émotionnels du captif, de sa famille et de ses amis.
- La communication entre le captif, sa famille et ses amis.
- Le besoin de repos, de se soumettre à un contrôle médical, et éventuellement de recevoir des soins médicaux.
- Le souhait des autorités (gouvernement hôte et gouvernement du pays de la victime) d'interroger la personne libérée.
- Le désir de la presse de s'emparer de l'histoire.
- La relocalisation de la victime hors du pays, pour un repos et une récupération prolongés.
- Le besoin d'informer d'autres organisations que la situation a été résolue.

Soyez conscient que si plusieurs personnes travaillant pour diverses organisations étaient impliquées dans le rapt, la situation pourrait ne pas être résolue pour toutes les parties prenantes. Si c'est le cas, les déclarations publiques devront être faites avec extrême prudence jusqu'à ce que la crise soit résolue pour tous.

Exemple de cas : contrôler la rumeur

Durant la dernière phase des négociations avec les ravisseurs d'un travailleur humanitaire en Somalie, contrôler les rumeurs est devenu une réelle difficulté. Alors que la situation était encore tendue, une autre organisation humanitaire a annoncé, contre toute attente, que les captifs avaient été libérés et avaient pris un avion le jour précédent. Cette rumeur a immédiatement circulé dans la communauté humanitaire et a été reprise par la presse locale. L'organisation impliquée dans le rapt a découvert, après deux heures d'angoisse, d'où venait l'annonce et a démenti l'information.

Les EGIC, aussi bien sur le terrain qu'au siège, doivent donc être prêtes à :

- Pourvoir aux besoins de la victime, notamment prendre des dispositions pour lui permettre de parler à ses proches et de les retrouver.
- Donner des informations exactes aux autres organisations ; si c'est jugé nécessaire, demandez-leur de ne pas émettre de commentaire public, et indiquez-leur quand des informations supplémentaires seront fournies.
- Gérer la presse ; organisez une conférence de presse avec la victime et/ou sa famille et gardez le contrôle des contacts avec la presse (p. ex. la durée des interviews et le nombre de questions permises).
- Organiser une réunion pour que les autorités interviewent la victime.

L'idéal serait que la victime du rapt soit accueillie par une personne qu'elle connaît, peut-être par un proche collègue. Une femme sera préférable si la victime est une femme. Faites en sorte que les victimes reprennent le contrôle de leur situation aussi rapidement que possible. Amenez-les à prendre des décisions qui les concernent directement, mais faites-le progressivement et après avis médical. De plus, l'organisation devra prévoir :

- Un vol pour le retour de la victime chez elle dans les 48 à 72 heures qui suivent sa libération (si le captif n'est pas un membre du personnel local). La victime devra être accompagnée.
- Un accueil privé à l'aéroport (dans le salon d'honneur), sans représentants de la presse.
- Un compte-rendu de mission au siège.
- Une conférence de presse au siège (une heure au maximum).
- Un congé, avec une couverture d'assurance complète et sans perte de revenu.

Un rapt ou une situation d'otages est une expérience traumatisante. Les survivants auront besoin d'aide à long terme et d'un soutien professionnel ; il pourrait en être de même pour leurs proches, qui auront également vécu des moments très éprouvants. Choisissez des conseillers professionnels avec soin : un type de soutien psychologique inadéquat peut être une expérience stressante et peut désorienter.

14.6.2 L'analyse après action et rendre des comptes

Une fois le problème du rapt résolu, l'organisation concernée souhaitera probablement conduire une analyse après action pour définir les leçons à tirer. Si les choses se sont mal passées – si le captif a été blessé ou tué par exemple, la famille de la victime pourrait remettre en question la façon dont l'organisation a géré la crise et pourrait intenter une action en justice contre elle. Dans cette éventualité, les dossiers que l'organisation aura gardés sur

l'incident au fur et à mesure qu'il s'est déroulé seront une source de preuves importante. Si les choses tournent mal dans un incident géré par les autorités, l'organisation pourra insister pour qu'une enquête soit faite sur la façon dont l'opération a été menée et si ce qui est arrivé aurait pu être évité. Si des otages ont été tués, leurs familles pourraient également demander une enquête.

Des préparations spécifiques doivent être faites en cas d'aboutissement négatif. Les dépouilles mortelles doivent être prises en charge et une autopsie devra être faite, soit dans le pays concerné soit ailleurs, surtout pour le personnel expatrié et si l'objectivité est une préoccupation. Il sera important pour l'organisation de savoir comment la victime est morte et qui l'a tuée.

14.7 Préparation et formation

14.7.1 Au niveau organisationnel

- Identifiez les membres d'une EGIC et leurs suppléants.
- Formez-les, notamment par le biais de simulations de scénarios de rapt, et obtenez la participation des services opérations, technologie de l'information, personnel, finances, presse et juridique, ainsi que des hauts responsables.
- Demandez à votre gouvernement quelle aide est disponible si un membre du personnel est victime d'un rapt.
- Identifiez les experts externes qualifiés en gestion de crise et en soutien des victimes potentielles et de leurs familles après une crise.
- Gardez des dossiers sur tous les membres du personnel international, contenant les coordonnées de leurs proches parents et leurs problèmes médicaux éventuels.
- Précisez quelles sont les responsabilités de chacun en cas d'enlèvement, d'arrestation ou de rapt selon les accords avec les autres organisations régissant le détachement de personnel.
- Énoncez les responsabilités et obligations que l'organisation assume envers le personnel victime d'enlèvement, de rapt ou d'arrestation et les familles.
- Ayez une politique claire spécifiant que le personnel ne doit pas être déployé dans des régions dangereuses sans être pleinement informé du risque au préalable et sans son accord explicite.
- Contrôlez constamment les zones à haut risque afin de détecter des menaces possibles de rapt.

14.7.2 Au niveau du bureau sur le terrain

- Établissez et maintenez le contact avec l'ambassade et d'autres acteurs diplomatiques tels que les NU.
- Dans un contexte à haut risque, sachez qui contacter au gouvernement hôte en cas de rapt.

- Renseignez-vous sur la structure de commandement des forces de sécurité nationales dans la zone d'opérations de l'organisation.
- Identifiez et prenez contact avec un juriste spécialisé en droit criminel local, fiable et compétent.
- Comprenez bien les procédures juridiques qui régissent l'arrestation dans ce pays.
- Comprenez la politique du gouvernement en ce qui concerne les contacts avec les ravisseurs, s'il en existe une.
- Constituez une EGIC, préparez un plan, mettez-le à jour régulièrement et fournissez une formation spécialisée.
- Gardez des dossiers complets sur le personnel, comprenant les pièces d'identité, les coordonnées de la famille et les informations médicales.

14.7.3 Au niveau individuel

- Avant un déploiement, assurez-vous que vos affaires domestiques sont en ordre. Idéalement, les documents suivants doivent être disponibles : certificat de naissance, certificat de mariage/divorce ; polices d'assurance ; dossiers médical et dentaire ; documents de naturalisation, documents d'adoption/de tutelle ; dossier militaire ; procuration écrite ; documents financiers essentiels ; et coordonnées des médecins, avocats et autres professionnels clés.
- Soyez conscient des risques et sachez comment les contrôler.
- Soyez vigilant, à tous moments.
- Familiarisez-vous avec l'environnement physique ; déplacez-vous avec une carte si possible.
- Ayez sur vous une liste de numéros de téléphones importants et des fréquences radio ; mémorisez les plus importants au cas où vous perdriez la liste.
- Ayez sur vous des photos de famille, y compris de vos enfants.
- Si vous prenez des médicaments, ayez-en une petite quantité sur vous ; ayez une paire de lentilles de contact ou une paire de lunettes de rechange. Ayez une note sur d'éventuels besoins médicaux, également dans les langues locales.
- Portez de bonnes chaussures de marche.
- Cachez une petite quantité d'argent sur votre personne

Liste de controle de base

Ces points essentiels peuvent être suivis ou adaptés par le personnel sur le terrain dans les premières heures critiques d'un incident, lorsque le temps est précieux et que tout le monde est sous pression.

Les termes de référence de l'EGIC sont :

- Gestion de la crise au niveau local.
- Contacts avec les intermédiaires.
- Contacts avec les ravisseurs.
- Liaison avec les autorités, en particulier la police.
- Contacts avec les ambassades.
- Transmission d'informations aux NU et aux ONG.
- Soutien à la famille, si présente, et soutien moral et matériel à l'otage si possible.
- Contacts avec les médias locaux.
- Orientations d'autres contacts vers l'EGIC au siège.
- Information et évaluation des risques pour l'EGIC au siège.

Action immédiate suite à un enlèvement :

- Constituer l'EGIC.
- Confirmer que l'enlèvement s'est produit.
- Informer le siège.
- Informer immédiatement les membres de la famille présents.
- Informer le personnel local.
- Informer les autorités.
- Organiser une couverture télécom permanente.
- Revoir les mesures de sécurité.
- Commencer un registre.
- Si possible, installer un appareil enregistreur sur le téléphone ou la radio.

Premier contact avec les ravisseurs

- Enregistrer la conversation.
- Adopter une attitude coopérative.
- Demander à parler aux captifs.
- Insister pour avoir une preuve qu'ils sont en vie.
- Expliquer les responsabilités limitées de l'interlocuteur.
- Fixer un délai pour une réponse.
- Établir une procédure pour rappeler (numéro de téléphone, mot de code).

Liste de controle de base (suite)

Premier contact avec les autorités locales

- Décider, avec le siège, de la ligne de conduite à adopter.
- Joindre un contact connu.
- Informer les autorités des faits.
- Insister sur le fait que la sécurité des otages est la première priorité.
- Obtenir une garantie de confidentialité, surtout en ce qui concerne les médias.
- Établir une procédure de contact.

Preuve que la victime est en vie

Les éléments suivants peuvent être utiles :

- Une photo de la victime tenant une récente édition d'un journal.
- Un message enregistré ou écrit.
- Des réponses correctes à des questions que seule la victime pourrait connaître.

Prouver que les victimes sont en vie est important :

- Pour s'assurer qu'elles n'ont pas été tuées.
- Pour s'assurer que l'on a affaire à un réel intermédiaire et que ce n'est pas un canular.
- Pour contribuer au bien-être de l'otage.
- Pour donner un soutien moral à la victime.
- Pour établir un lien, même ténu, avec l'otage.

Chapitre 15
Menaces liées aux combats et débris de guerre[1]

Ce chapitre porte sur les menaces liées aux combats, notamment les bombardements, les missiles et tirs d'obus, les feux croisés et les tirs isolés, les mines, les engins explosifs improvisés et les munitions non explosées (UXO), ainsi que le phosphore blanc. Il comprend également des détails importants sur les dangers des « débris de guerre ».[2]

15.1 Questions essentielles

Les questions fondamentales, dans les zones de combat actif, concernent la présence même de l'organisation (le seuil de risque acceptable) et les avantages de rester (l'impact du programme) par rapport aux risques. Les risques de tirs d'obus et de bombardements, de feux croisés et de tirs isolés sont-ils au-dessous du seuil de risque acceptable de l'organisation ? Y a-t-il des besoins d'assistance et de protection importants qui justifient la présence de l'organisation ? Les conditions vous permettent-elles malgré tout d'exécuter le programme avec efficacité ou restez-vous uniquement par solidarité ? Combien de membres du personnel doivent rester pour remplir cette fonction ? Le personnel médical, en particulier, reste ou avance généralement plus près pour aider les victimes du conflit. De nouveau, les mêmes questions essentielles doivent être considérées.

Conseils essentiels pour le personnel qui se trouve sous le feu :

- Ne soyez pas machiste, n'essayez pas d'être un héro.
- Ne restez pas sur place pour essayer de découvrir d'où et de qui proviennent les tirs, ou quel type d'arme est utilisé.
- Pour votre survie immédiate, décidez si vous devez rester ou fuir, puis prenez les mesures logiques imposées par votre décision.
- Utilisez les meilleures défenses naturelles que vous possédez : votre peur et votre bon sens.
- Mettez-vous à l'abri, cachez-vous, ne restez pas dans la ligne de tir.

1 Ce chapitre a été rédigé en collaboration avec Michael Niedermayr, coordinateur en sécurité zonale en Asie-Pacifique, Fédération internationale des Sociétés de la Croix-Rouge et du Croissant-Rouge.
2 Un ouvrage particulièrement utile sur ce sujet et les sujets connexes est le *Manuel de sécurité sur les mines terrestres et les débris explosifs de guerre* (2005), publié par le Service de l'Action antimines des Nations Unies et CARE, et disponible en anglais et en français. En plus du guide, il existe également un module de formation et une présentation Powerpoint, une vidéo de formation et un CD-ROM dans diverses langues. Voir également *Staying Alive : Safety and Security Guidelines for Humanitarian Volunteers in Conflict Areas* (Rester en vie : Consignes de sûreté et de sécurité destinées aux bénévoles humanitaires dans les zones de conflit) (2006), du CICR.

15.2 Tirs d'obus et bombardements

15.2.1 Types et tactiques

Les obus et les roquettes peuvent être lancés par des obusiers et par l'artillerie lourde, des chars et des lance-roquettes, ou par des mortiers portables plus petits. Les mortiers les plus courants ont une portée d'environ 6 km, tandis que d'autres types d'artillerie peuvent avoir une portée maximale de 50 km. Se trouver derrière une colline n'offre aucune protection car les obus peuvent être lancés par-dessus la colline. Les roquettes artisanales et certaines armes fournies par l'armée, par exemple les missiles « Scud », sont très imprécises. D'autres sont guidées par satellite ou par laser et sont, en principe, relativement précises. Les avions de chasse peuvent lâcher des bombes, lancer des fusées ou mitrailler le sol. Les hélicoptères peuvent lancer des fusées ou mitrailler. Les drones ou véhicules aériens sans pilote et téléguidés, sont souvent utilisés pour la reconnaissance, mais peuvent aussi lancer des missiles. Ils ont été utilisés en Irak, en Afghanistan, au Pakistan et en Somalie, ainsi que dans le conflit israélo-palestinien. Étant donné que les avions et les drones peuvent lancer leurs armes à distance, vous risquerez de ne pas les entendre ; l'explosion sera sans doute le premier signe d'une attaque.

Sur le plan de la tactique, des distinctions de base peuvent être faites entre les tirs au hasard ou de saturation, les tirs prévus et les tirs observés. Les développements technologiques permettent d'augmenter la précision des tirs. Les tirs au hasard ou de saturation sont très imprécis. Cela peut s'expliquer par les types d'arme utilisés, tels que les lance-roquettes multiples, qui saturent une zone avec des obus (ils ont été utilisés par les Russes à Grozny, la capitale Tchétchène), ou les bombes à fragmentation qui éparpillent des centaines de petites bombes (utilisées par l'OTAN au Kosovo et par Israël à la fin de la guerre contre le Hezbollah au Liban, en 2006). Cela peut également être un choix tactique, par exemple un barrage d'artillerie ou ce que l'on appelle un tapis de bombes.

Pour les tirs prévus, l'artillerie vise d'après les calculs faits sur une carte, mais ne peut ajuster les tirs sur une cible précise, ou bien les pilotes lancent des roquettes ou lâchent des bombes sur une cible lors d'un seul survol. Le comportement des pilotes et donc la précision des tirs à partir d'un avion ou d'un hélicoptère dépendent fortement de la possibilité de l'ennemi de les détecter au préalable par radar. Selon que les pilotes s'attendent à être attaqués par des tirs anti-aériens ou par des avions de chasse, aura également une influence. Les installations radar, les terrains d'aviation ennemis et les installations anti-aériennes sont les principales cibles. Si l'ennemi n'a pas les moyens techniques que nous venons de décrire, il pourrait disposer de

missiles sol-air portatifs. Les avions et les hélicoptères de combat réduisent généralement leur vulnérabilité en lâchant des bombes d'une haute altitude, en s'éloignant de la cible ou en volant à basse altitude pour tenter de la surprendre. Cela n'aide pas à la précision du tir.

Les attaques aériennes ou les tirs d'artillerie observés signifient qu'il y a un ou plusieurs observateurs qui repèrent où les obus, les roquettes ou les bombes tombent et qui transmettent des instructions à l'équipe d'artillerie afin qu'elle ajuste son tir. Il existe deux techniques couramment utilisées pour ajuster les tirs d'artillerie : « marcher dans la direction » de la cible et le « réglage percutant par encadrement sur la ligne d'observation ». Dans les deux cas, l'observateur dirige d'abord l'équipe d'artillerie sur la ligne de tir – une ligne imaginaire entre l'observateur et la cible – puis se rapproche de la cible. Marcher dans la direction de la cible signifie que les obus se rapprochent successivement. Dans le réglage percutant par encadrement sur la ligne d'observation, les obus sont lancés de manière alternée devant et derrière la cible, et « l'encadrement » devient de plus en plus étroit.

La technologie du laser et des satellites a donné naissance à un type entièrement nouveau de bombes et de missiles qui peuvent en principe atteindre une cible désignée avec grande précision, même dans les zones bâties.

15.2.2 Réduction du risque

La première étape est de bien réfléchir au lieu où vous vous trouvez :

- Ne positionnez pas les bureaux et les entrepôts près de cibles militaires évidentes ou possibles, comme les terrains d'aviation, les casernes, les dépôts de carburant, les bâtiments officiels ou les points stratégiques tels que les carrefours, les têtes de ligne, les centrales électriques et les bâtiments de radio et de télévision. Évitez les hôtels situés près de cibles potentielles.
- Si l'organisation travaille dans une ville d'importance militaire stratégique susceptible d'essuyer les tirs, éloignez-vous le plus possible vers la périphérie ou dans la campagne avoisinante, dans la mesure des besoins opérationnels.
- Dans les zones accidentées ou montagneuses, évitez de vous arrêter sur les hauteurs où vous serez très exposé. Cherchez à vous mettre à l'abri des tirs d'obus et des bombardements au pied d'une colline abrupte ou d'une montagne.
- Identifiez l'organisation : peignez le logo en couleurs vives sur les toits et sur les murs des enceintes de l'organisation. N'oubliez pas que le drapeau de l'organisation ne sera pas visible de loin ou s'il n'y a pas de vent. Les tirs d'artillerie à longue distance et les missiles ou les bombes guidées

par des lasers ne reposent pas sur une identification visuelle mais sur les coordonnées préprogrammées de la cible. Si vous être en contact avec les combattants, envisagez de leur donner les coordonnées GPS de votre bâtiment et des informations préalables sur les itinéraires et les horaires des mouvements de vos véhicules.

N'oubliez pas que si la zone est sous le feu, les civils chercheront probablement à s'abriter dans l'enceinte de l'organisation, pensant qu'elle sera mieux protégée et qu'elle ne sera pas ciblée. Considérez si l'enceinte a la capacité d'accueillir un grand nombre de personnes supplémentaires. L'accès leur sera-t-il refusé et qui sera responsable d'appliquer cette décision ? Si l'accès leur sera ouvert, les personnes devront-elles être accueillies dans les endroits plus protégés ou devront-elles rester à l'extérieur des bâtiments de l'enceinte ?

Protection physique

Les mesures physiques pour réduire l'impact potentiel d'une attaque pourraient ne pas être très efficaces en cas de touche directe, mais elles peuvent réduire les dommages des tirs près du but et les effets de souffle et des éclats d'obus. Pour les abris anti-aériens et les bunkers, le meilleur endroit est en sous-sol, souvent dans une cave. À défaut, une pièce blindée au rez-de-chaussée conviendra. Les poutres en béton et en acier sont la structure la plus solide, mais le plafond peut également être renforcé avec des troncs d'arbre. Plus l'abri anti-bombe sera grand, moins la construction sera susceptible d'être solide. Il serait préférable d'avoir deux abris plus petits, mais bien entendu ils doivent être suffisamment grands pour accueillir tout le personnel, ainsi que l'équipement vital, des toilettes et éventuellement de la nourriture et de l'eau. Idéalement, l'abri comportera deux sorties, au cas où l'une d'elles serait bloquée par des gravats. Des pelles et des pioches pourraient être nécessaires si les occupants doivent creuser pour pouvoir sortir. Aucun abri, même pas un bunker en béton, ne protègera contre des bombes très puissantes.

Un abri anti-aérien ne sera pas très utile si le personnel doit courir 800 mètres pour l'atteindre. Déterminez un temps limite pour arriver à l'abri, disons une ou deux minutes. Le personnel qui ne peut atteindre un bunker dans ce délai à partir de l'endroit où il travaille habituellement, devra avoir son propre abri plus près. Si les autorités ont identifié ou construit des abris anti-aériens publics, assurez-vous que le personnel sait où ils sont situés.

Les tranchées et les trous peuvent offrir un abri contre les obus de mortier et les mitraillages au sol par des avions volant à base altitude ou des hélicoptères. Ils doivent être profonds (2 mètres), étroits et suffisamment longs pour abriter

jusqu'à 4 personnes. Une bonne construction est une petite tranchée en forme de L, avec un point d'entrée et un point de sortie. Le haut peut être protégé de rondins et de deux couches de sacs de sable. N'oubliez pas l'entretien : les entrées peuvent causer des éboulements et des inondations. Attention aux serpents : ils peuvent faire leurs nids dans les tranchées ou les trous.

Malgré leur nom, les murs anti-souffle sont conçus pour empêcher les éclats d'obus et les balles mais pas nécessairement le souffle de l'onde de choc d'une explosion. Utilisez des sacs de sable (alternez entre « carreaux » et « boutisses » et construisez des angles solides pour renforcer la construction), des barils ou des boites remplies de terre ou de gravats, ou des carrés de pelouse renforcés par des poteaux de bois verticaux. Construisez les murs anti-souffle à une hauteur supérieure à celle d'une personne se tenant debout, sauf peut-être pour le mur protégeant le chemin de l'abri, sur lequel les personnes peuvent courir en se baissant. Les murs anti-souffle ne doivent pas bloquer le passage, surtout celui conduisant à l'abri. Les endroits à protéger à l'aide de murs anti-souffle sont le corps de garde, les portes et fenêtres du bâtiment, la salle de radio, les dépôts de carburant et le passage conduisant à l'abri. Vous pourrez aussi créer un « espace anti-souffle » dans la maison, de préférence au rez-de-chaussée et dans une pièce intérieure, c'est-à-dire avec au moins deux murs entre l'abri et vous. Construire un bon mur anti-souffle demande de l'expertise. Les murs mal construits peuvent s'effondrer et peuvent donc constituer eux-mêmes un danger.

La principale menace lors d'une explosion d'un gros engin explosif improvisé (contrairement à celle d'un mortier ou d'un obus) est le souffle de l'onde de choc même, et non pas la fragmentation et les éclats d'obus. Contrairement aux éclats d'obus, une onde tourne sur elle-même et autour des obstacles pratiquement sans être entravée. Pour en atténuer les effets, le mur anti-souffle devra être au moins deux fois plus haut et plus large que la structure qu'il est censé protéger et devrait être placé juste à côté de cette structure ou juste à côté de l'explosion même.

La grande majorité des blessures subies lors d'une explosion sont causées par des fragments de verre provenant des fenêtres, propulsés par la force de l'explosion dans les zones occupées. Cela peut être atténué en apposant un film destiné à retenir les fragments, également connu sous le nom de « film anti-éclats » sur la face intérieure des fenêtres. Notez que le film anti-éclats appliqué sur une fenêtre à double vitrage est inefficace, de même que lorsqu'il est apposé à l'extérieur des fenêtres. Le film anti-éclat n'arrêtera pas non plus les éclats d'obus ou les balles. Si un film anti-éclat n'est pas disponible ou est trop coûteux, vous pouvez utiliser plusieurs couches de film adhésif normal (du type utilisé pour couvrir les livres), appliqué en croisé des deux côtés de la fenêtre.

Bien que le film anti-éclat soit conçu pour contenir le verre, il ne le gardera pas dans son cadre. Lors d'une forte explosion, la vitre entière sera propulsée dans la pièce et pourra causer de graves blessures et même tuer. À moins de n'avoir aucune fenêtre, le meilleur moyen de réduire le risque est de positionner les bureaux de sorte que personne ne soit assis dans la trajectoire d'une éventuelle projection de fenêtre. Ou bien, envisagez d'installer des rideaux anti-souffle, des câbles attrapeurs ou des barreaux. Vous pouvez aussi garder les fenêtres ouvertes. Envisagez de laisser les pièces extérieures ou exposées, inoccupées, c'est-à-dire de les utiliser comme entrepôt plutôt que comme bureaux. Dans les endroits à grand risque de feu indirect, le dernier étage d'un bâtiment pourra également être utilisé de la même manière.

Enfin, assurez-vous que l'environnement physique des bureaux et des enceintes, par exemple le gravier, ne constitue pas une source de fragments secondaires.

Que faire sous le feu (tirs d'obus, missiles et bombardements)

Votre comportement sous le feu dépend en partie de l'endroit où vous vous trouvez lorsque les tirs d'obus ou le bombardement commencent, de l'endroit où les missiles atterrissent, de la direction des tirs (s'ils sont ciblés), et de la proximité d'un abri efficace. En général :

- Cherchez à vous abriter immédiatement dans la tranchée d'urgence ou l'abri le plus proche.
- Si vous ne pouvez atteindre un abri anti-bombe, cherchez un autre abri solide. Un arbre, une clôture en bois ou une voiture ne suffiront pas. Il vous faudra un abri beaucoup plus solide : des murs, du béton, un rocher ou un grand trou, par exemple un fossé sur le côté d'une route. Si vous êtes exposé, jetez-vous à plat ventre sur le sol. L'exposition au souffle peut endommager les tympans : n'oubliez pas de vous couvrir les oreilles avec les mains et de garder la bouche entrouverte.
- Si vous êtes en voiture, décidez si vous devez accélérer pour sortir de la zone de tir ou abandonner le véhicule pour chercher un abri. Si les tirs d'obus sont proches ou si vous êtes en convoi, éloignez-vous du véhicule et cherchez un abri. (À l'intérieur du véhicule vous risquez de recevoir des éclats de verre, des éclats d'obus peuvent perforer la voiture ou le réservoir à carburant peut exploser si la voiture est atteinte par un obus.) Si les tirs d'artillerie ne sont pas trop proches et que vous pouvez vous éloigner en voiture, essayez d'atteindre un endroit plus sûr où vous pourrez mieux vous abriter.
- Si vous êtes sous une attaque aérienne, attendez-vous toujours à ce que votre véhicule soit ciblé. Quittez-le et allez vous abriter.
- Si vous devez rouler dans une zone de danger, baissez le volume de la radio, ouvrez légèrement les fenêtres, et restez vigilant.

15.3 Feux croisés et tirs de précision

Les feux croisés font référence aux tirs d'armes légères échangés entre combattants ou au hasard. Ils peuvent provenir de fusils, de grenades et de grenades à fusil. Les tirs de précision sont ciblés. Les tireurs d'élite sont experts et peuvent repérer une cible à longue distance. Ils peuvent être actifs sans qu'un combat général n'ait lieu et peuvent utiliser des fusils spéciaux munis de lunettes télescopiques et à vision nocturne. Les tireurs d'élite sont déployés pour harceler les forces ennemies et perturber leurs mouvements, ou pour terroriser une population ennemie plus importante. Pour cela, ils prennent des postes avancés ou infiltrent le territoire ennemi, par exemple pour cibler des officiers ou retarder un convoi en tuant le chauffeur du premier camion, ou simplement pour semer la terreur en tuant subitement un civil. Ils agissent furtivement et par surprise. S'ils se trouvent en position éloignée et non menacée, ils peuvent la maintenir pendant longtemps. Dans d'autres circonstances, ils peuvent tirer et changer de position pour attaquer ailleurs.

15.3.1 Réduction des risques

La meilleure défense contre les feux croisés et les tireurs d'élite est de ne pas s'approcher des zones où des tirs d'armes légères sont échangés et où les tireurs d'élite opèrent. Cependant, cela peut être difficile dans les guerres contemporaines : vous pourriez subitement être pris entre deux feux. Les tireurs d'élite ne peuvent être évités que s'ils sont statiques ou s'ils couvrent uniquement une zone identifiée et si l'on connaît leur position et la portée de leur arme. Les tirs d'armes légères ne sont généralement efficaces que sur une distance maximale de 100 m, mais les balles de carabine peuvent atteindre des distances supérieures à 3 km et celles des mitrailleuses lourdes de 6 km et plus.

Protection physique

N'oubliez pas que le port d'équipement de protection n'est pas en soi une solution. Une planification globale en matière de sécurité ne doit jamais être marginalisée par la fourniture d'équipement de protection.

Lorsqu'ils sont bien construits et suffisamment épais, les murs anti-souffle offrent une protection contre les tirs d'armes légères (mais pas contre les tirs directs de grenades à fusil, et probablement pas contre un mitraillage soutenu). Les tireurs d'élite peuvent utiliser des balles perforantes qui traversent les murs anti-souffle normaux. Dans ces circonstances, la meilleure option est de rester hors de vue : éloignez-vous des portes et des fenêtres, et essayez d'avoir au moins deux murs entre vous et les balles. Cela vous protègera également mieux contre les balles qui ricochent.

Les gilets pare-éclats sont conçus pour protéger le corps contre le souffle de l'onde choc, les éclats de verre et les éclats d'obus. Ils n'arrêteront pas les balles. Les gilets balistiques ou pare-balles donnent une meilleure protection. Les gilets de base doivent être portés avec des plaques balistiques et un casque, ils sont lourds (jusqu'à 12 kg) et coûteux.

Les véhicules blindés peuvent assurer une certaine protection contre les tirs de fusil et les effets de souffle des obus et des petites mines. Ils ne vous protègeront pas suffisamment contre les tirs directs d'artillerie, une bombe ou des grenades à fusil , ni contre un tireur d'élite, qui pourrait utiliser des balles perforantes. Sauf s'ils sont conçus spécialement pour résister aux mines (avec un dessous de caisse en forme de V), ils ne vous protègeront pas non plus suffisamment contre le souffle et les éclats d'une mine antichar ou contre une bombe placée sur le bord de la route. Les véhicules blindés sont considérablement plus lourds que les véhicules normaux et très coûteux. En général, plus le véhicule est lourd plus sa protection sera efficace. Étant donné leur poids supplémentaire et donc leur plus grande distance de freinage, une formation spéciale est recommandée pour les conduire. Lorsque vous voyagez dans un véhicule blindé, vous devrez porter un casque et un gilet pare-éclats ou un gilet balistique. Comme pour les autres véhicules, les véhicules blindés doivent toujours se déplacer deux par deux.

Manœuvres d'évasion : réduire l'exposition

Si vous ou votre personnel vous trouvez subitement sous le feu, votre réaction dépendra de votre position, de la proximité d'un abri, de la proximité des tirs et du fait que vous soyez ou non la cible.

Lorsque vous êtes en voiture, si les tirs sont en face de vous, vous devrez certainement quitter le véhicule pour vous mettre à l'abri ; s'arrêter, faire marche arrière ou se tourner et exposer le flanc du véhicule prendra trop de temps et fera de vous une cible facile. Lorsque vous prenez des mesures d'évasion contre les tirs d'armes légères, favorisez la vitesse. Évitez les embardées et les zigzags ; ils ne vous empêcheront pas d'être frappé.

Lorsque vous cherchez un abri, n'oubliez pas qu'il vous faut du solide. Vous accroupir derrière une voiture ordinaire vous cachera peut-être mais cela ne vous protègera pas des balles. Comme pour les roquettes et les bombes, un abri solide signifie des rochers, un trou, un monticule de terre, du béton ou plusieurs épaisseurs de briques. Les buissons, les arbres, les clôtures en bois et les voitures ordinaires ne constituent pas des abris solides. Si vous êtes raisonnablement bien abrité, prenez le temps de considérer votre position et vos options. S'agit-il de tirs généraux d'armes légères ? D'où viennent-ils et vous ciblent-ils ? Si vous en êtes la cible, sont-ils un avertissement pour

vous faire battre en retraite ou sont-ils destinés à vous atteindre ? S'agit-il de tirs isolés ? Les soldats disent que si vous vous demandez si vous êtes la cible, c'est que vous ne l'êtes pas. Autrement dit, si vous êtes ciblé, vous le saurez. Avec l'expérience, vous reconnaîtrez les différents sons émis par une balle passant tout près (comme le claquement d'un fouet) et par des balles éloignées (un sifflement ou une plainte aiguë). N'oubliez pas qu'un combat est, à bien des égards, comme un match de boxe, avec de fréquents arrêts pendant que les parties changent de position ou évaluent la réponse de l'ennemi. Restez à l'abri jusqu'à ce que vous soyez certain que vous pouvez sortir sans danger.

15.4 Mines, objets piégés et munitions non explosées

15.4.1 Les mines

Il existe deux catégories de mines : les mines antichars et les mines antipersonnel. Les premières sont de taille plus importante et ont une plus grande puissance explosive. Pour être déclenchées, elles nécessitent en général un poids ou un mouvement important, sauf si elles sont vieilles ou instables. Elles peuvent rompre la chenille d'un char et endommager une partie de sa suspension, mais elles détruisent quasi entièrement un véhicule non blindé. Les mines antipersonnel sont plus petites. Certaines sont conçues pour blesser une personne en lui arrachant une main ou un pied. D'autres peuvent occasionner des blessures beaucoup plus graves, voire mortelles.

Les mines antipersonnel blessent ou tuent par effet de souffle ou de fragmentation. Les mines à fragmentation ont une enveloppe qui éclate en petits fragments ou contiennent des fragments qui se dispersent lorsqu'elles explosent. La plupart des mines antipersonnel sont enfouies dans le sol. Certaines sont posées sur une première charge d'explosifs qui, lorsqu'elle est déclenchée, fait sauter la mine à un mètre au-dessus du sol, où elle explose. Certaines mines sont déclenchées par des fils de traction, qui sont généralement difficiles à repérer et très dangereux. D'autres ont des systèmes qui explosent lorsqu'une pression est exercée sur le fil de détente, ou bien elles sont déclenchées par le relâchement de la tension et explosent lorsque le fil de détente est coupé. Si vous trouvez un fil de traction, ne tentez jamais de le couper, ne vous en approchez pas et ne le touchez pas. Quittez la zone en suivant la même direction d'ou vous venez et vérifiez systématiquement s'il y a des fils de traction sur votre chemin. Notez que les fils de traction ne sont pas placés uniquement à hauteur de la cheville, mais peuvent se trouver plus haut, par exemple au niveau de la poitrine. Certains systèmes de mines antipersonnel sont interconnectés et possèdent des détecteurs. La mine explose si quelqu'un s'en approche. D'autres exposent lorsqu'une seconde personne approche, par exemple une équipe de secours, pour aider la victime de la première mine.

Les mines directionnelles sont placées au-dessus du sol et sont attachées à des arbres ou à des objets fixes. Elles sont généralement déclenchées à distance mais peuvent également être liées à des fils de traction ou à des objets piégés. Certaines mines antipersonnel peuvent tuer dans un rayon maximal de 35 à 50 mètres et causer des blessures graves jusqu'à 100 mètres. Si vous êtes, ou si vous pensez être dans un champ de mines, votre seule option est de quitter la zone avec prudence (voir plus loin, section 15.4.3). Marcher en file indienne ne réduit pas beaucoup le risque.

En général, les mines antichars n'explosent pas lorsqu'une personne pose le pied dessus car elles ont besoin d'une pression plus forte pour être déclenchées. Quelquefois une mine antipersonnel est placée au-dessus d'une mine antichar : la plus petite explosion fait détoner la mine plus importante. Certaines mines antipersonnel et antichars disposent d'un mécanisme de protection qui empêche de les récupérer ou de les désamorcer (elles explosent lorsqu'on y touche).

Un grand nombre de mines ont un contenu métallique, ce qui explique l'utilisation de détecteurs de mines. Dans certaines situations, notamment avec certains types de mines contenant peu ou pas de métal ou dans un terrain saturé de métal, les détecteurs de métaux seront peu utiles. Certaines mines sont équipées de dispositif anti-manipulation à influence magnétique, c'est-à-dire que le champ magnétique du détecteur de métaux déclenchera la détonation. Heureusement, ces mines sont rares.

Emplacement possible des mines

Les mines sont en général posées pour trois raisons :

- Dans le cadre d'une stratégie de bataille. Les groupes armés posent des mines pour défendre leurs positions militaires, pour perturber les mouvements de l'ennemi, pour empêcher l'accès de l'ennemi à certaines routes ou pour diriger l'ennemi vers une route particulière. On peut donc s'attendre à trouver des champs de mines près des bunkers et des tranchées, embossements de chars de combat et sur ou le long de ponts et de routes. Dans le cas de villes assiégées, les deux camps peuvent poser des mines : les défenseurs pour perturber une attaque, les attaquants pour empêcher les défenseurs de s'approvisionner et de fuir. Les mines sont souvent posées de manière non systématique : elles peuvent être éparpillées sur le territoire ennemi par des avions et des hélicoptères, ou elles peuvent être lancées par l'artillerie. Dans le cas des guérillas ou des insurrections, de nombreux groupes posent des mines au hasard sans jamais prendre ou communiquer de notes sur leur emplacement. Il n'est donc pas surprenant que des forces du même groupe se retrouvent dans des champs de mines posées par leurs collègues. Vos connaissances des principaux sièges et

Étude de cas : le minage par anticipation

En 1995, le véhicule d'une ONG a sauté sur une mine antichar sur une route d'Afrique Centrale. La force de l'explosion a projeté le véhicule 12 mètres plus loin en le retournant complètement. Deux passagers ont été tués et trois ont été blessés. Pendant la nuit, des mines antipersonnel ont été posées autour de l'épave. Le lendemain, une femme qui était venue observer la scène a marché sur une mine et a perdu une jambe.

lieux de combats, des principales positions de défense ainsi que du terrain en général, vous rendront plus attentif aux zones à risques évidents.

- À proximité des cibles socioéconomiques. Les pylônes électriques, les centrales d'eau et d'électricité ainsi que les embranchements ferroviaires peuvent également être entourés de mines pour les protéger du sabotage et des attaques.
- Pour semer la terreur générale et provoquer la délocalisation. Les mines sont également posées lors de combats plus classiques pour cibler la population civile et ses ressources : les pâturages et les terres agricoles, les canaux d'irrigation, les puits, les zones forestières dans lesquelles le bois de chauffage est ramassé, les temples et même les sentiers villageois peuvent être minés. Le but est de délocaliser une population locale qui pourrait soutenir l'ennemi et de créer le mécontentement.

Ceux qui posent des mines anticiperont les réactions d'une force ennemie, ou des civils. Ainsi, le pont d'une rivière peu profonde pourra être miné, mais les berges à côté le seront aussi, et cibleront les personnes qui veulent éviter le pont et traverser la rivière à pied. Une route principale pourra être minée, et les routes d'accès secondaires le seront peut-être également. Dans un conflit continu, même de faible intensité, les zones ayant été déminées peuvent être minées à nouveau. Les mines peuvent aussi « migrer », être déplacées par la pluie, les inondations, les glissements de terrain ou par les marées sur une plage. Au début 2000, huit ans après la guerre au Mozambique, de fortes inondations ont éparpillé les mines et ont détruit le balisage des zones minées. Enfin, la population locale peut également poser ou reposer des mines pour protéger ses ressources. Renseignez-vous à ce sujet et déplacez-vous uniquement avec les propriétaires sur leurs propres terrains.

Trouver et partager les informations

Même si vous êtes très attentif, vous ne pourrez pas savoir où se trouvent toutes les zones minées, à moins qu'une personne bien informée ne vous renseigne. Les gens ne viendront probablement pas à vous pour vous donner

des informations ou pour vous demander quels sont vos mouvements afin de vous avertir. Il faudra vous renseigner vous-même, réunir des informations de diverses sources et les communiquer au nouveau personnel ayant des responsabilités similaires. Avant votre départ, obtenez des informations générales sur les mines dans un pays, par exemple en consultant les rapports annuels publiés par la Campagne internationale pour interdire les mines. Des organisations spécialisées dans le déminage humanitaire, dont HALO Trust, Mines Advisory Group, Handicap International et Norwegian People's Aid, pourraient être en mesure de vous fournir des renseignements utiles. Dans le pays même, les principales sources d'informations générales et spécifiques à une région seront :

- L'agence nationale d'action contre les mines ou les autorités locales et les forces de sécurité.
- Les organisations de déminage et un centre onusien d'action contre les mines s'il en existe un.
- Les observateurs militaires ou forces du maintien de la paix des NU.
- Les hôpitaux et postes de santé où les victimes des mines sont traitées.
- Le personnel de l'organisation.
- La population locale.

Les connaissances locales sont particulièrement importantes : lorsque vous vous hasardez dans une nouvelle zone où il y a, ou il y a eu des combats, arrêtez-vous régulièrement et renseignez-vous auprès de la population locale au sujet des mines dans les environs. Cela prend du temps mais cela peut sauver des vies. Prévoyez du temps supplémentaire dans votre plan de voyage. Plus les questions seront précises, plus les réponses le seront aussi. Demandez :

- Depuis combien de temps la personne interrogée est dans la région.
- Quel est l'historique des combats par ici.
- Quels accidents se sont produits dans la région : des véhicules, des personnes ou des animaux ont-ils été atteints par des mines, et si oui, quand et où ?
- Quels sont les mouvements de la population locale, et quelles zones évite-t-elle ?
- La personne interrogée a-t-elle emprunté la route, et si oui quand et jusqu'où ?
- Comment les personnes utilisent-elles la route ? Si elles ne se déplacent qu'à pied ou en bicyclette, les mines antichars pourraient ne pas avoir été déclenchées et seront donc toujours un danger. Attention aux termes employés : au Mozambique, par exemple, les personnes classent les bicyclettes dans la catégorie des véhicules.

Bien que les informations communiquées par la population locale soient importantes, n'en surestimez pas la fiabilité. Par exemple, si vos interlocuteurs sont des réfugiés de retour depuis peu seulement, ils ne sauront pas où se trouvent les mines. Même s'ils sont dans la région depuis longtemps, ils ne connaîtront peut-être pas tous les endroits.

Champs de mines balisés

Ceux qui posent des mines ne vont évidemment pas signaliser leur emplacement. Souvent, la population locale crée elle-même ses propres signaux d'avertissement, mais ils sont difficiles à identifier pour les étrangers et peuvent être ambigus et confus. Les signaux peuvent n'être qu'un petit tas de pierres ou deux branches croisées posées au début d'un sentier. Demandez aux personnes locales quels signaux elles utilisent et si elles ont un système commun (si chacun utilise ses propres signaux, il n'existera donc pas de signal commun). Les opérations de déminage signalisent les champs identifiés de différentes façons selon les pays, mais généralement les signaux sont relativement clairs. La couleur rouge est normalement utilisée. Notez, toutefois, que les signaux pourraient être tombés, être moins visibles ou être cachés.

15.4.2 Objets piégés et munitions non explosées

L'objectif des objets piégés peut être d'empêcher le retrait d'autres explosifs. Plus souvent, ils sont posés par une force en retraite pour compliquer la réoccupation d'une zone – généralement une zone construite – et la rendre plus coûteuse. De nombreux objets piégés sont artisanaux, mais ils sont posés et masqués avec une grande créativité, quoique cruelle : la porte ou la fenêtre d'une maison, un puits, un fusil abandonné ou un cadavre. Un objet piégé peut être attaché à un simple article ménager et même à un jouet. La consigne est simple : ne vous aventurez pas dans des zones abandonnées et ne touchez à rien. Si vous vous occupez du ramassage des corps, vérifiez-les soigneusement avant de les déplacer.

Les munitions non explosées (UXO) font référence au matériel qui était censé exploser au moment de l'impact mais qui ne l'a pas fait. Elles incluent les balles, les roquettes, les missiles, les bombes, les grenades, les armes à sous-munitions et les obus. Les UXO peuvent représenter un danger beaucoup plus important que les mines antipersonnel parce que la dispersion peut en être plus aléatoire et imprévisible et que les munitions sont elles-mêmes susceptibles d'être instables. Les bombes à sous-munitions tirées par des obus d'artillerie ou larguées par des avions constituent un risque particulier. En hauteur, les conteneurs se brisent et laissent tomber une multitude de mini-bombes qui peuvent « saturer » une zone entière. Les bombes à sous-munitions ont été utilisées par les Soviétiques en Afghanistan, par l'OTAN au Kosovo et par la force aérienne israélienne dans le sud du Liban.

15.4.3 Réduction des risques

Lorsque vous conduisez, essayez de n'utiliser que les routes goudronnées, et évitez les nids de poule, qui peuvent être minés. Si la route goudronnée se transforme subitement en sentier de terre et que vous ne savez pas ce qui vous attend plus loin, il sera plus prudent de faire demi-tour. Cherchez des signes évidents de mines : un cratère formé par une explosion, une chaussure déchiquetée, la carcasse d'un animal, l'épave d'un véhicule, une route qui semble ne pas être utilisée, un champ envahi de mauvaises herbes et non cultivé dans une zone habitée, ou un bâtiment sans toit, dont les volets et les portes sont intacts alors qu'ils ont été retirés ou pillés sur d'autres bâtiments. Restez sur les chemins battus. Ne quittez jamais une route ou un sentier et faites attention aux zones marquées. Si vous êtes passager, demandez au conducteur :

- De ne pas dévier des routes empruntées et de ne pas rouler à travers champs.
- De conduire sur des sentiers existants, de ne pas rouler sur les obstacles de la route (une grosse branche ou des débris pouvant cacher une mine) ou de ne pas les contourner sans vérifier au préalable que la surface de la route n'a pas été perturbée.
- De ne pas conduire sur les bords de la route pour éviter un obstacle, pour faire demi-tour, pour doubler un autre véhicule ou pour laisser passer un véhicule venant en sens inverse : les bords de route peuvent être minés.

Par-dessus tout : si vous avez un doute, faites demi-tour.

Un véhicule non blindé ne peut être protégé contre une mine antichar. Cependant, le risque de blessure grave peut être réduit en mettant des sacs de sable d'environ 10 cm d'épaisseur sur le plancher du véhicule sous chaque passager, et une couche ou deux de sacs de sable à l'arrière du véhicule. Malheureusement, cela augmentera aussi le poids de votre véhicule et pourra faire détoner une mine antichar. Vous risquerez aussi d'être aveuglé par le sable si vous roulez sur une mine. Une astuce peut-être un petit peu plus efficace consiste à remplir les pneus d'eau, mais cela est plus efficace avec des roues de gros camion en raison du volume nécessaire pour faire une différence.

Les mines sont rarement posées seules. Votre présomption de base doit être : s'il y a une mine, il y en aura d'autres. Si une mine explose ou si vous soupçonnez que vous êtes dans une zone minée, ne réagissez jamais sous l'impulsion :

- Ne vous précipitez jamais hors de votre véhicule s'il a déclenché une plus petite mine mais n'est pas en feu.

- Ne conduisez pas impulsivement vers un autre véhicule qui a déclenché une mine.
- Contrôlez-vous, contrôlez vos collègues et agissez avec prudence pour éviter d'autres victimes.

Évacuer un véhicule

Si votre véhicule a fait détoner une mine mais n'est pas en feu ou en danger d'une autre explosion, évacuez-le de manière contrôlée. Ne posez pas le pied sur le sol autour du véhicule sauf à l'arrière, sur le sentier où vous avez roulé. Sortez du véhicule par la portière arrière ou par l'arrière en passant par le toit et posez le pied sur votre propre trace. Si le goudron est solide ou si les traces du véhicule sont visibles, vous pouvez retourner à pied, en file indienne espacée, au dernier endroit sûr ou à un point où vous pensez qu'il n'y aura plus de risque de mines. Si les traces ne sont pas visibles, préparez-vous à quitter la zone à l'aide d'une sonde, ce qui prendra probablement plusieurs heures. Si la nuit tombe, préparez-vous à une nuit inconfortable jusqu'à ce que vous puissiez continuer à l'aube.

Sortir d'une zone minée

Les principes de base pour sortir d'une zone minée sont de retracer vos pas ou de retourner sur le sentier que vous avez suivi pour arriver où vous êtes. Ceci est plus facile dans la théorie que dans la pratique.

Sonder

Sonder le terrain signifie examiner soigneusement chaque centimètre avant d'y poser le pied. Avant de commencer, vérifiez qu'il n'y a pas de fils à traction qui peuvent déclencher des mines. Les fils à traction ressemblent à du fil de pêche ou à d'épais fils de toile d'araignée ; ils sont à peine visibles et peuvent être recouverts de feuilles et de branches. Un détecteur de fil à traction, une fine branche qui se courbera au contact d'un fil à traction, vous aidera à les identifier. Placez-le à l'horizontale devant vous, en le tenant entre le pouce et l'index, et soulevez-le en douceur, en le maintenant à l'horizontale. Dès que vous sentez une résistance, relâchez immédiatement la pression et vérifiez s'il s'agit d'un fil à traction. Essayez de trouver un autre chemin pour l'éviter. Ne touchez jamais ou n'essayez jamais de couper un fil à traction : certains feront détoner une mine en exerçant une pression, mais d'autres fonctionnent par relâchement de pression. Si vous coupez un fil à traction, la mine explosera.

S'il n'y a pas de fil à traction, il vous faudra alors délimiter un espace de la largeur de vos épaules et le sonder systématiquement. La meilleure façon de procéder est de dégager un espace et de vous coucher sur le ventre, ou bien de vous agenouiller ou de vous accroupir. Sonder signifie enfoncer délicatement

la sonde dans le sol en formant un angle de 30 degrés, pour sentir s'il y a un objet dur. Si vous en trouvez un, et dans un sol pierreux il peut y en avoir des centaines, dégagez soigneusement les côtés jusqu'à ce que vous découvriez ce que c'est. Si c'est une mine, ne la touchez pas et n'essayez jamais de la retirer, mais signalisez son emplacement et contournez-la pour continuer à sonder.

Le secours

Peu de situations sont aussi difficiles à affronter que la vue d'une personne qui pose le pied sur une mine près de vous. Le personnel doit avoir pour consigne de :

- Ne jamais se précipiter pour aider une victime, même si elle hurle à l'aide et risque de mourir en se vidant de son sang. N'oubliez jamais que la présence d'une mine indique qu'il y en a probablement d'autres : augmenter le nombre de victimes n'aidera personne.
- Ne tenter une opération de secours planifiée et contrôlée que si la personne est toujours en vie, si les équipes spécialisées ne peuvent arriver sur les lieux dans un délai raisonnable, et s'il y a de bonnes chances que cela ne fasse pas plus de victimes.

Une opération de secours consiste essentiellement à :

- Parler à la victime et lui faire comprendre qu'elle ne doit pas bouger car il pourrait y avoir d'autres mines tout près.
- Sonder, à partir de l'endroit sécurisé le plus proche, un espace d'environ 1,5 mètre de largeur.
- Dégager un espace autour de la victime pour pouvoir administrer les soins de premier secours.
- Vérifier avec précaution sous les membres et le corps de la victime s'il y a d'autres mines.
- Dispenser les premiers soins.
- Sortir la victime par le chemin que vous aurez dégagé.

Déclaration

Toute indication qu'il pourrait y avoir des mines, des objets piégés ou d'autres munitions non explosées dans une zone, et bien entendu, tout cas d'incident réel, doivent faire l'objet d'une déclaration aux autorités concernées (y compris à un centre d'action contre les mines) et dans les forums inter organisationnels. Faites un plan du lieu approximatif et pensez à mettre un signal, mais laissez l'enquête aux professionnels. Les organisations humanitaires concernées par le travail médical curatif doivent déclarer toute victime traitée pour blessures causées par une mine.

Consignes essentielles : Ne pas toucher, ne pas s'approcher, signaliser si possible, déclarer

- Munitions non explosées : Généralement visibles, mais peuvent être partiellement ou même entièrement ensevelies. Présumez qu'elles sont instables et qu'elles peuvent exploser si on les touche. Ne les touchez jamais. Marquez leur position et informez les autorités. Dans certains pays, il y a une industrie active de recyclage de métaux, et les UXO sont manipulés. Même si elles ont été touchées plusieurs fois, elles peuvent encore contenir des explosifs et peuvent exploser à tout moment.
- Objets piégés : L'objet piégé est généralement visible mais pas l'explosif auquel il est attaché. Présumez que pratiquement tout objet peut être piégé dans un endroit non dégagé, non repeuplé ou repeuplé récemment et partiellement. Ne touchez à rien, n'ouvrez pas les volets ni les portes. N'entrez pas dans des bâtiments vides ou en ruines, même pour y faire vos besoins.
- Mines : Généralement non visibles. Ne les touchez jamais ; n'essayez pas de les retirer ; n'essayez pas de les faire exploser en leur jetant des pierres. Si vous savez que des mines ont été utilisées dans un conflit, et que vous n'êtes pas absolument certain que la route est dégagée, ne vous y aventurez pas. Si vous voyez une mine, marquez son emplacement très clairement et informez les autorités.
- La population locale peut devenir trop confiante et agir bêtement. Ne comptez pas sur des personnes non formées pour manipuler les mines et les UXO. Vous serez peut-être invité par des villageois à aller voir leur placard rempli de ces curiosités et d'articles recyclés, ou à observer une équipe de travail déterrer les mines. Ces articles pourraient être instables et exploser, même s'ils ont déjà été manipulés. Ne vous en approchez pas ou partez immédiatement.

15.5 Phosphore blanc

Le phosphore blanc est utilisé dans une zone de combat pour former un rideau de fumée. C'est l'un des rideaux de fumée les plus efficaces parce qu'il s'épaissit très rapidement ; non seulement il masque le contact visuel mais il brouille aussi la radiation infrarouge et interfère donc avec l'optique infrarouge et les systèmes de repérage des armes, tels que ceux utilisés par les armes guidées comme les missiles antichars. Il peut être contenu dans les petites grenades fumigènes, les canons antichars, les mortiers ou autre types d'artillerie. Au moment de l'explosion, des particules brûlantes se dégagent, suivies immédiatement de traits de fumée blanche qui se fondent

en un nuage très blanc. Le phosphore blanc a récemment été utilisé pendant la guerre Israël-Hezbollah en 2006, en Irak et pendant la guerre de Gaza en 2008-2009.

Le problème du phosphore blanc est son utilisation dans les zones habitées et ses effets sur la population. Les particules brûlantes collent à la peau et peuvent produire des blessures graves. Les particules continuent à brûler jusqu'à ce qu'elles soient totalement consumées ou jusqu'à ce qu'elles soient privées d'oxygène. De plus, les parties brûlées du corps absorbent le phosphore qui peut endommager le foie, les reins et le cœur ; il peut même occasionner une défaillance d'organe. L'ingestion par voie orale de particules de phosphore est le deuxième type de contact potentiellement mortel. L'inhalation de la fumée est dangereuse et irrite les yeux, le nez et les voies respiratoires mais ne constitue pas la même menace mortelle que les brûlures et l'ingestion.

15.6 Les débris de guerre : un rappel

15.6.1 Débris de guerre explosifs

Vous n'êtes pas à l'abri du danger même si la guerre est finie : les mines antipersonnel et les bombes à sous-munitions resteront un danger pendant des années et même des décennies à venir. Les obus d'artillerie et de mortiers et même les balles peuvent vous sembler des souvenirs intéressants à garder, mais peuvent encore exploser et deviendront de plus en plus instables avec le temps. D'autres bombes et obus pourraient être enfouis profondément et continuer à représenter un danger pour les agriculteurs et les ouvriers du bâtiment. Les véhicules ou bâtiments militaires ou utilisés par l'armée, qui ont été détruits ou abandonnés et qui ont servi aux groupes armés, peuvent contenir des munitions non explosées ainsi que des combustibles, des résidus chimiques (y compris de l'uranium appauvri, un produit utilisé pour les munitions perforantes) et des objets piégés. Le conseil universel est de ne pas s'en approcher.

15.6.2 Préparation et formation

Se préparer à opérer dans une zone potentiellement minée exige de bonnes connaissances et une attention particulière à la discipline concernant les mouvements et le comportement individuels.

Les connaissances essentielles sur les mines, les munitions non explosées et les objets piégés concernent, entre autres, l'endroit où il est possible de les trouver et donc comment les éviter ; les signaux d'avertissement utilisés localement ; les idées fausses concernant les mines ; le déminage et les connaissances locales ; que faire lorsque l'on ne sait pas si une

zone est minée ou pas ; les règles pratiques à observer en présence de mines ; comment sortir d'un champ de mines ; et déclarer les zones minées identifiées ou soupçonnées. Par-dessus tout, la formation en matière de mines doit souligner l'importance d'avoir un comportement discipliné. Le personnel des organisations humanitaires n'écoutera généralement pas le conseil de faire demi-tour en cas de doute, sauf si ce message est inculqué par des exercices de simulation et renforcé dans les opérations quotidiennes par les responsables de programmes. Dans les zones à haut risque, les exercices doivent porter sur la demande de renseignements auprès de la population locale, la discipline dans les déplacements et sortir d'un véhicule et d'une zone en vérifiant s'il y a des fils à traction et en utilisant une sonde. Si l'organisation opère dans une zone où les secours spécialisés sont plus ou moins accessibles partout, comme au Kosovo fin 1999/début 2000, le personnel n'aura peut-être pas besoin d'une formation en soins de premier secours. Mais cela restera une exception. Le personnel qui opère dans les zones où une aide spécialisée ne se trouve pas à proximité devra recevoir une formation médicale de base. Cela prendra du temps, occupera une grande partie du personnel et sera probablement coûteux.

Les nouveaux membres du personnel arrivant dans une zone opérationnelle où l'on sait qu'il y a des champs de mines, doivent recevoir des instructions complètes. Faites-les se familiariser avec les environs et indiquez-leur où se trouvent les zones minées connues et les signaux qui permettent de les identifier. Une réelle exposition sur le terrain et la mémoire visuelle seront plus utiles que des informations verbales ou écrites. Des instructions appropriées doivent également inculquer la nécessité de marquer toute zone suspecte qu'ils rencontreront et d'en faire une déclaration détaillée. Il faudra leur rappeler régulièrement l'importance de rester vigilants face aux dangers que représentent les mines.

L'équipement essentiel inclut :

- Une radio dans la voiture.
- Si possible des radios portatives à utiliser hors de la voiture.
- Une bonne trousse de premier secours.
- Un équipement de sonde et de détection (une sonde peut être un long tournevis ou un long couteau avec une lame de 12 à 15 cm de long. Pour détecter les fils à traction, utilisez une tige légère et flexible de 1 m à 1,30 m de long, un fil de fer mince et solide, une tige flexible ou une branche).

Partie 6
Annexes

Annexe 1
Tendances générales concernant la sécurité du travailleur humanitaire

En 2000, au moment de la publication de la première édition de cette Revue des bonnes pratiques, la majorité des organisations d'aide humanitaire commençait tout juste à reconnaître sérieusement les réalités et les difficultés liées à l'insécurité opérationnelle. Galvanisées par des attentats très médiatisés, tels que l'assassinat, en 1996, de six personnels du CICR en Tchétchénie, les organisations internationales d'aide humanitaire avaient pris des initiatives collaboratives d'apprentissage, destinées à renforcer la sécurité opérationnelle. Ces initiatives ont donné lieu à la toute première formation inter organisationnelle en matière de sécurité et à la première édition de cette RBP. À cette époque, la plupart des organisations internationales ne disposaient pas de personnels désignés responsables de la sécurité ni même de coordinateurs de sécurité, pas d'outils d'évaluation des risques et pas de consignes de bonnes pratiques ; elles avaient peu ou pas de politiques ou de protocoles au niveau de l'organisation concernant la gestion des risques intentionnellement tournés vers le personnel et les opérations.

Au cours des dix années qui ont suivi la première édition, de grands développements ont été observés dans le domaine de la gestion de la sécurité humanitaire, et des changements ont eu lieu dans l'environnement sécuritaire global. Ces changements ont eu de graves implications pour l'assistance humanitaire internationale. Au début de la décennie, l'attaque du 11 septembre 2001 et les guerres contre l'Afghanistan et l'Irak qui ont suivi, ont donné lieu à un grand nombre de programmes d'intervention humanitaire dans des environnements violents. Ces opérations, venant principalement d'occident, ont subi un nombre régulier et croissant d'attaques, en partie parce qu'elles étaient perçues par certains comme des instruments politiques occidentaux. Dans les années qui ont suivi, les NU et le CICR ont subi des attentats à la bombe dévastateurs à Bagdad, le nombre de rapts et d'attaques mortelles visant les acteurs humanitaires a augmenté, et les bureaux des NU ont été ciblés par un important bombardement à Alger, capitale Algérienne.

Cette annexe examine brièvement les tendances générales de la sécurité des travailleurs humanitaires depuis la première publication, ainsi que la culture de la gestion de la sécurité qui se développe au sein de la communauté humanitaire.

D'après les chiffres : révélations et limites des statistiques globales

Ce n'est qu'en 2005 qu'une cartographie rétrospective globale des attentats majeurs contre les travailleurs humanitaires du monde entier a été établie, sous forme d'une base de données sur la sécurité des travailleurs humanitaires : *Aid Worker Security Database* (ASWD). Depuis, la base de données est actualisée régulièrement et est disponible gratuitement en ligne sur : www.aidworkersecurity.org. *Insecurity Insight* (aperçu de l'insécurité) est un autre projet de recherches statistiques sur le sujet (www.insecurityinsight.org).

Il faut noter que ces statistiques globales ont généralement peu de pertinence opérationnelle pour le personnel sur le terrain. Leur principale fonction est de sensibiliser les organisations, les gouvernements et le public en général, de renforcer la compréhension de la portée et de la profondeur des difficultés opérationnelles qui se présentent dans le travail humanitaire, et de fournir des informations sur les tendances et questions globales observées dans les sphères humanitaires et politiques internationales. Elles constituent une base essentielle d'éléments d'appréciation permettant une analyse qui, jusqu'à présent, était basée sur des observations empiriques et des suppositions.

Les conclusions de l'AWSD, ces des dix dernières années, indiquent les tendances générales suivantes :[1]

- Un taux croissant d'attaques importantes contre les travailleurs humanitaires, la plupart étant concentrées dans un petit nombre de contextes très violents, notamment en Afghanistan (et plus récemment au Pakistan), en Irak, en Somalie et au Darfour.
- Dans certains de ces contextes les plus violents, l'utilisation croissante de tactiques plus sophistiquées, mieux organisées et plus meurtrières, le ciblage évident des étrangers et des motivations plus politiques chez les auteurs des attentats.
- Une légère baisse globale, du nombre de victimes parmi les acteurs humanitaires, malgré un nombre croissant de travailleurs sur le terrain. Ceci indique une meilleure gestion de la sécurité dans le secteur.
- Une augmentation de longue date du nombre d'attaques contre les personnels nationaux comparé au nombre d'attaques contre leurs homologues internationaux.

1 Ces conclusions ont été publiées dans les rapports *Providing Aid in Insecure Environments* (L'aide humanitaire dans les contextes dangereux) de 2006 et 2009, disponibles sur http://odi.org.uk/programmes/humanitarian-policy-group.

Base de données sur la sécurité du travailleur humanitaire : résumé des statistiques en Octobre 2010

Incidents de violence grave envers des travailleurs humanitaires	1997	1998	1999	2000	2001	2002	2003	2004	2005	2006	2007	2008	2009*
Total des incidents	35	27	32	42	29	46	63	63	75	106	119	161	139
Total des victimes parmi les travailleurs humanitaires	73	69	65	91	90	85	143	125	172	239	208	274	278
Total des décès	39	36	30	57	27	38	87	56	54	86	78	127	102
Total des blessés	6	15	15	23	20	23	49	46	95	87	84	87	84
Total des victimes de rapt	28	18	20	11	43	24	7	23	23	66	46	60	92
Total des victimes parmi les personnels nationaux	40	52	40	70	62	68	116	101	157	213	173	227	205
Total des victimes parmi les personnels internationaux	33	17	25	21	28	17	27	24	15	26	35	47	73

* Chiffres provisoires

Ces tendances reflètent un environnement de sécurité et géostratégique changeant, ainsi que les réponses des organisations internationales humanitaires en matière de politiques et d'opérations. Elles se résument dans trois domaines principaux :

Le renforcement de la gestion de la sécurité : des développements dans la politique organisationnelle, la formation, la collaboration inter organisations et l'obligation globale de vigilance.

Tout d'abord les bonnes nouvelles : au cours des dix dernières années, les organisations humanitaires ont fait d'énormes progrès pour intégrer et renforcer la gestion de la sécurité dans leurs opérations. Les connaissances générales et le professionnalisme dans l'approche vis-à-vis de la sécurité se sont considérablement améliorés dans tout le secteur, et sont reflétés par l'élaboration de politiques, de protocoles et d'outils pratiques utilisés sur le terrain. Aujourd'hui, pratiquement toutes les grandes organisations humanitaires ont, dans leurs politiques organisationnelles, des responsabilités formalisées en matière de sécurité, même si elles varient en qualité et en application, alors qu'en 2000 seule une petite minorité d'organisations était concernée.

Beaucoup plus de personnels humanitaires sur le terrain prennent part à une formation en matière de sécurité, et les ressources sur le terrain pour ce type de formation se sont multipliées. L'un des principaux prestataires de formation est RedR (www.redr.org.uk), qui dirige des stages de formation dans les pays d'origine des organisations ainsi que dans les contextes opérationnels, partout dans le monde. Un nombre croissant d'autres organisations offrent également une formation et des renseignements en matière de sécurité opérationnelle, par exemple Security Management Initiative, basée à Genève (www.securitymanagementinitiative.org).

Les consortiums internationaux ayant pour thème la sécurité, qui rassemblent les organisations humanitaires, incluent le European Interagency Security Forum (EISF), basé à Londres, et le Security Advisory Group du consortium américain d'ONG InterAction. Ces groupes sont des plateformes de partage d'informations et d'élaboration de politiques et on les retrouve de plus en plus sur le terrain. Le rapport, le suivi et le partage d'informations sur les incidents de sécurité ne sont pas encore ce qu'ils devraient être et dans certains domaines, les organisations hésitent encore à entrer dans des discussions franches et ouvertes (par exemple sur la question de l'utilisation de protection armée dans les opérations humanitaires). Cependant, les progrès sont globalement incontestables. On peut raisonnablement conclure

que le renforcement des capacités de gestion de la sécurité dans la communauté humanitaire est à l'origine, tout au moins en partie, de la baisse des taux d'incidents majeurs dans le monde, en tenant compte des contextes les plus violents.

Une politisation grandissante de la violence envers les travailleurs humanitaires dans les contextes de menace « globalisée »

Maintenant, la mauvaise nouvelle : malheureusement, ces améliorations dans la gestion de la sécurité opérationnelle paraissent dérisoires comparées au niveau croissant de menaces dans les contextes humanitaires où les risques sont les plus élevés. Le nombre croissant d'attaques contre les travailleurs humanitaires dans un nombre restreint de contextes, associé au ciblage de plus en plus important des étrangers dans ces lieux et à la plus grande utilisation de « tactiques terroristes », telles que les attentats suicides, les attentats coordonnés et les engins explosifs improvisés, indiquent que les travailleurs humanitaires sont devenus des cibles politiques. Cet élément est confirmé par les données disponibles relatives aux allégeances et aux objectifs des attaquants (quand il est possible de les déterminer). Dans ces contextes d'extrême violence, les opérations internationales d'aide humanitaire sont exposées à des niveaux de violence sans précédent et l'accès aux populations dans le besoin est de plus en plus difficile. Dans ces endroits, l'espace humanitaire rétrécit car l'accès des acteurs humanitaires n'est plus sûr et les programmes sont réduits ou arrêtés.

Faiblesses persistantes : transmettre le risque au personnel national, et la nécessité d'avoir des approches d'acceptation plus actives

Les organisations d'aide humanitaire qui cherchent à poursuivre leurs opérations humanitaires dans des contextes violents font souvent face aux menaces sérieuses en relocalisant certaines catégories de personnel ou en limitant leurs mouvements, et en transmettant une plus grande responsabilité au personnel local ou à des organisations partenaires locales. Les opérations de secours continuent, souvent à un niveau moindre ou simplifié, et sont gérées à distance. Cette pratique, appelée gestion à distance, est évoquée au chapitre 4 ; elle permet à l'aide de continuer d'affluer pour répondre aux besoins vitaux, mais elle peut également placer une quantité de risque inacceptable sur le personnel national ou local, qui bénéficie souvent de moins de formation, et de ressources et d'équipements moins importants pour gérer la sécurité. Les statistiques montrent une augmentation de longue date des taux d'attentats visant les populations nationales. Cela met en

évidence la gravité du sujet et les implications éthiques pour les organisations d'aide. Cette RBP souligne ce problème dans les pages qui précèdent, et met en exergue la nécessité d'effectuer une bonne évaluation des risques pour les travailleurs nationaux et locaux, de les atténuer en conséquence et de fournir aux travailleurs internationaux et nationaux des ressources équitables en matière de sécurité.

Ce guide souligne également la nécessité d'une approche d'acceptation plus analytique et plus proactive de la part des organisations humanitaires dans les régions contestées (voir Chapitre 3). Cela pourrait être impossible dans les contextes où la communauté humanitaire, dans son ensemble, est déjà considérée comme un outil de la domination politique et culturelle occidentale. Néanmoins, les travailleurs humanitaires recherchent encore l'acceptation pour pouvoir renforcer la sécurité. Dans leur approche sécuritaire, ils cherchent donc des solutions qui soient les plus ancrées dans les valeurs et principes centraux du travail humanitaire, plutôt que des solutions à court terme telles que des mesures extrêmes de protection et de dissuasion. La recherche actuelle des praticiens et des universitaires, telle que l'initiative dirigée par Save the Children US sur les moyens de mesurer l'acceptation et d'appliquer activement les stratégies d'acceptation, est un pas important dans cette direction.

Annexe 2
Le système de gestion de la sécurité des Nations Unies[1]

La responsabilité principale en ce qui concerne la sécurité et la protection du personnel des organisations[2] du système des Nations Unies incombe au gouvernement hôte. Dans le cas d'organisations internationales et de leurs représentants, le gouvernement est censé avoir une responsabilité particulière conformément à la Charte des Nations Unies ou aux accords du gouvernement (appelés « accords avec les pays hôtes ») avec chaque organisation.

La structure du système de gestion de la sécurité au siège

Le système de gestion de la sécurité des Nations Unies a été restructuré après le bombardement de Bagdad en 2003. Le Département de la sûreté et de la sécurité des Nations Unies (DSS) a été établi. Il est dirigé par un sous-secrétaire général. Le sous-secrétaire général (SSG) pour la sûreté et la sécurité est responsable de la direction et du contrôle exécutifs du Système de gestion de la sécurité des Nations Unies (SGSNU), de la sûreté et de la sécurité du personnel civil des Nations Unies et des personnes qui en dépendent, aussi bien au siège que sur le terrain, ainsi que des locaux et des biens des Nations Unies au siège et sur le terrain. Cette personne est responsable devant le secrétaire général de tout ce qui concerne la sécurité et est chargée d'élaborer des politiques, pratiques et procédures en matière de sécurité pour le personnel du système des Nations Unies du monde entier. Les responsables exécutifs des fonds et programmes des Nations Unies sont responsables devant le secrétaire général et sont chargés de s'assurer que les objectifs du SGS sont atteints dans leurs organisations respectives.

Le Réseau inter agences pour la gestion de la sécurité (IASMN) réunit le DSS, les départements du Secrétariat concernés et les agences des NU pour ce qui concerne la politique et les consignes en matière de sécurité au sein des Nations Unies. Les membres se réunissent deux fois par an dans une assemblée plénière pour étudier et valider les recommandations qui sont ensuite présentées au Comité de gestion de haut niveau (HLCM), puis au Conseil des chefs de secrétariat (CSS) ; toutefois les comités spéciaux et les

1 Cette annexe a été rédigée en collaboration avec le Département de la sûreté et de la sécurité des Nations Unies (DSS).
2 Cela inclut les conjoints des membres du personnel des Nations Unies ainsi que les personnes reconnues à leurs charges et leurs biens, ainsi que les biens de l'organisation.

mécanismes de coordination fonctionnent tout au long de l'année. Si le SSG pour la sûreté et la sécurité a la responsabilité globale du système de gestion de la sécurité, l'IASMN soutient le Comité de gestion de haut niveau pour ce qui est de la revue des politiques et des questions liées aux ressources, pour la totalité du système de gestion de la sécurité des Nations Unies. L'IASMN contrôle la mise en œuvre des politiques, pratiques et procédures de gestion de la sécurité élaborées par les NU, par tous les acteurs du système des NU ; cela inclut le budget du programme. Il relève du Comité de gestion de haut niveau, auquel il fait des recommandations.

Financement du système de gestion de la sécurité des Nations Unies

Le DSS reçoit une part de son budget biennal du budget ordinaire des Nations Unies. L'autre part (45 % des dépenses totales) provient des contributions des organisations au partage des frais, calculées sur la base du nombre de leur personnel au niveau global et sur le terrain. À l'origine, on espérait que le DSS serait entièrement financé par le budget ordinaire, mais les États membres, à l'assemblée générale, s'y sont opposés en faisant valoir que le partage des frais renforcerait le sentiment « d'adhésion » et encouragerait une meilleure participation à la prise de décisions.

Le système de gestion de la sécurité au niveau national

Dans chaque pays ou zone définie où les Nations Unies sont présentes, le plus haut représentant est généralement nommé comme représentant désigné pour la sécurité. Le représentant désigné est responsable de la sûreté et de la sécurité devant le secrétaire général par le biais du SSG et est chargé de la sécurité des membres du personnel employés par les organisations du système des Nations Unies et des personnes reconnues comme étant à leur charge, dans toute la zone ou tout le pays désigné.

Les représentants des organisations (ou le « représentant de pays », le « directeur de l'organisation » ou le « chef de mission ») du système des Nations Unies qui participent au système de gestion de la sécurité des Nations Unies sont responsables devant le secrétaire général par le biais de leurs directeurs exécutifs respectifs, sous l'autorité générale du SSG pour la sûreté et la sécurité, pour tout ce qui concerne la sécurité de leur personnel sur leur lieu d'affectation. Chaque chef d'agence sera également représenté sur le terrain dans l'Équipe de gestion de la sécurité (EGS), présidé par le représentant désigné, qui inclut le conseiller en sécurité (voir ci-dessous). L'EGS conseille le représentant désigné sur tout ce qui concerne les questions de sécurité. Pour les missions de maintien de la paix, dans lesquelles le chef d'agence

agit en tant que représentant désigné, l'équipe de gestion de la sécurité peut également inclure les directeurs de bureaux ou de départements de la mission.

Le conseiller en chef pour la sécurité, ou conseiller en sécurité, est un expert en sécurité nommé par le SSG et est chargé de la sûreté et de la sécurité ; son rôle est de conseiller le représentant désigné et l'EGS en matière de sécurité. Le conseiller en sécurité relève du représentant désigné et maintient une ligne de communication technique avec le département de la sûreté et de la sécurité. En l'absence d'un conseiller en sécurité, le représentant désigné, en consultation avec le Département de la sûreté et de la sécurité, doit nommer, pour l'EGS, un chargé de liaison en matière de sécurité dans le pays. Le chargé de liaison en matière de sécurité dans le pays peut être une personne employée par une autre organisation des NU, qui peut avoir d'autres responsabilités principales.

Les coordinateurs de zone de sécurité sont des membres du personnel nommés par le représentant désigné, en consultation avec l'EGS, dans les régions de pays plus grands, distinctes de la capitale en termes de distance et d'exposition. Leur rôle est de coordonner et de contrôler les dispositions de sécurité applicables à tous les membres du personnel employés par les organisations du système des Nations Unies et aux personnes à leur charge, dans leurs domaines de responsabilité. Les coordinateurs de zone de sécurité sont responsables devant le représentant désigné en ce qui concerne leurs obligations en matière de sécurité. Le conseiller régional en matière de sécurité peut bénéficier des services et conseils d'un coordinateur de la sécurité sur le terrain, un expert en sécurité déployé par le DSS.

Les points focaux sont nommés par le représentant désigné, en consultation avec l'équipe de gestion de la sécurité, et s'assurent de la bonne mise en œuvre du plan de sécurité dans une zone déterminée d'une grande ville. Les points focaux sont responsables devant le représentant désigné/coordinateur de zone de sécurité, en matière de sécurité, quelle que soit l'organisation qui les emploie.

Responsabilités des membres du personnel

Toutes les personnes employées par les organisations du système des Nations Unies sont responsables de leur propre sûreté et sécurité, quel que soit le lieu de leur poste, et elles doivent observer toutes les politiques et procédures de sécurité. Les personnes employées par les organisations du système des Nations Unies doivent :

- Se familiariser avec les informations qui leur sont transmises concernant le système de gestion de la sécurité des NU sur leur lieu de travail.

- Recevoir le feu vert de la sécurité avant de se rendre dans un pays dans lequel une phase de sécurité a été décrétée, et informer le représentant désigné de leur pays de destination lorsqu'ils voyagent dans un pays où une phase de sécurité n'est pas en vigueur.
- Assister aux séances d'information et certifier qu'ils y ont participé.
- Savoir qui est leur point focal et/ou chargé de liaison en matière de sécurité pour leur agence et comment le contacter.
- Être correctement équipé pour leurs fonctions sur leur lieu d'affectation (p. ex. s'assurer qu'ils ont reçu tous les vaccins nécessaires et que les dispositions appropriées de transport ont été prises pour les déplacements sur leur lieu d'affectation).
- Appliquer et respecter toutes les règles et procédures de sécurité sur leur lieu d'affectation, pendant et en dehors des heures de travail.
- Se comporter de manière à ne pas mettre en danger leur propre sûreté et sécurité ou celles des autres.
- Mener à bien la formation en matière de sécurité.

Les phases de sécurité des NU et le nouveau système onusien de niveaux de sécurité

L'actuel système onusien de phases de sécurité a été créé en 1980, en réponse aux situations d'urgence et de crise qui menaçaient la sécurité du personnel des Nations Unies. En tant qu'outil principal de gestion de la sécurité pour la préparation dans les lieux d'affectation, le système de phases de sécurité était associé à des mesures de sécurité appropriées, établies en fonction du niveau de classification du lieu d'affectation (allant de 1 à 5), qui étaient exprimées dans le plan de sécurité.

Au cours de 2010, les NU ont décidé d'introduire un nouveau système de niveaux de sécurité (Security Level System – SLS) contenant six niveaux, pour remplacer le système de phases de sécurité. Sa mise en œuvre officielle dans toutes les opérations des NU était prévue pour le 1er janvier 2011. Le système de niveaux de sécurité fait partie du protocole d'évaluation des risques de sécurité du modèle de gestion des risques des NU, et permet une évaluation plus objective du contexte de sécurité dans lequel les NU opèrent. Il fournit une évaluation structurée des menaces, qui décrit le contexte général de sécurité d'une zone géographique et donne aux travailleurs et aux responsables une indication globale du contexte de la sécurité dans une région comparée à une autre. Le système de niveaux de sécurité est censé être plus objectif, basé sur des faits, logique et systématique, et il supprime les mesures de sécurité automatiques et les droits aux ressources humaines qui étaient prévus dans le système des phases de sécurité.

Standards minimaux de sécurité opérationnelle (MOSS)

MOSS est le principal mécanisme de gestion et d'atténuation des risques de sécurité pour le personnel, les biens et les ressources des organisations des NU. MOSS comprend un éventail de mesures conçues pour réduire le niveau de risque. Un système MOSS unique est appliqué dans toutes les opérations onusiennes.

Formation en matière de sécurité

Le système des Nations Unies a introduit une formation obligatoire en matière de sécurité pour les membres du personnel des Nations Unies. Cette formation est fortement recommandée au personnel non employé par les Nations Unies. Le cours, intitulé « Sécurité de base sur le terrain : sûreté, santé et bien-être du personnel », est disponible sur CD ROM dans les six langues officielles des NU, et est recommandé à tout le personnel, qu'il se déplace ou pas hors de son lieu d'affectation. Le « Cours de sécurité avancé sur le terrain » est fortement recommandé au personnel qui se rend dans les lieux de Phase un ou au-delà. Un certificat est fourni une fois le test réussi, et est valable pour trois ans. Voir Annexe 7 pour des renseignements sur l'accès à cette formation.

Annexe 3
Sauver des vies ensemble : un cadre de collaboration pour la sécurité

En 2001, le Comité permanent inter agences (IASC), en étroite collaboration avec le coordinateur de la sécurité des NU (UNSECOORD, précurseur du Département de la sûreté et de la sécurité des Nations Unies (DSS)) a établi un « Menu à options » pour la collaboration en matière de sécurité entre les NU, les ONG et les organisations intergouvernementales. Le Menu à options était une liste de stratégies d'atténuation de risques potentiels visant à améliorer la sécurité collective dans la communauté humanitaire. Il n'a pas eu un grand succès pour un certain nombre de raisons, notamment un manque de ressources, des approches diverses de la sécurité et un manque de confiance et de compréhension chez les participants, et il était peu connu sur le terrain.

En 2006, le Menu a été revu et rebaptisé *Saving Lives Together (SLT): A Framework for Improving Security Arrangements among IGOs, NGOs and the UN in the Field (Sauver des vies ensemble : un cadre pour améliorer les dispositions de sécurité dans les OIG, les ONG et les NU sur le terrain)*. L'initiative Sauver des vies ensemble a établi dix recommandations non obligatoires sur la façon dont les NU, d'autres organisations intergouvernementales telles que l'Organisation internationale pour les migrations (OIM) et d'autres ONG, pouvaient collaborer pour leur sécurité commune. Le cadre Sauver des vies ensemble cherche à encourager cette collaboration sans compromettre la neutralité ou l'indépendance des efforts humanitaires et sans imposer quoi que ce soit aux missions institutionnelles. L'hypothèse sous-jacente est que, par le biais d'efforts communs, la communauté humanitaire peut minimiser les risques dans les contextes dangereux.

Malgré sa révision et sa relance, l'utilisation du cadre Sauver des vies ensemble a été modérée sur le terrain, où son existence et ses objectifs sont peu connus. Ceci est dû, en partie, à un problème de disponibilité de ressources et de personnel. Si l'initiative Sauver des vies ensemble a le soutien des États membres des NU, il reste non formel et non obligatoire et, en tant que tel, toutes ressources supplémentaires nécessaires pour mettre en œuvre ses recommandations doivent provenir de sources extrabudgétaires. De plus, dans certains contextes locaux, il a été difficile de recruter et de déployer du personnel DSS, même lorsque le financement était disponible.

Sauver des vies ensemble : un cadre pour améliorer les dispositions de sécurité dans les OIG, les ONG et les NU sur le terrain

1. Collaboration dans l'Équipe de gestion de la sécurité des NU, avec la participation d'ONG et d'OIG

a) Les OIG et les ONG pourront, de par leurs fonctions, participer à des réunions pertinentes de l'Équipe de gestion de la sécurité des NU (EGS), en tant que représentantes.1
b) La collaboration UN/ONG/OIG en matière de sécurité devra être un point régulier de l'ordre du jour des réunions de l'Équipe de gestion de la sécurité des NU. Comme l'autorise le cadre du système de gestion de la sécurité des NU, il pourra être envisagé d'inviter les hauts responsables des ONG et des OIG à assister aux discussions sur certains points pertinents des réunions de l'Équipe de gestion de la sécurité.
c) Les protocoles du partage et de la diffusion des informations, évoqués dans les réunions de l'Équipe de gestion de la sécurité, seront adoptés au préalable, et d'un commun accord, par toutes les parties présentes.
d) Le cas échéant, le représentant désigné2 devra coordonner les décisions de sécurité avec les acteurs humanitaires ne faisant pas partie du système des Nations Unies.
e) Les partenaires OIG/ONG d'organisations des NU dans des opérations humanitaires spécifiques choisiront, entre elles, un ou un nombre limité de points focaux sur le terrain en matière de sécurité.

2. Organiser des forums diversifiés pour la collaboration et le partage d'informations en matière de sécurité

a) Des forums seront organisés régulièrement pour la collaboration pratique entre tous les acteurs humanitaires aux niveaux des régions, des pays et des bureaux auxiliaires, afin d'évoquer les questions pratiques de sécurité d'intérêt commun.
b) Les forums pourront inclure les participants ordinaires suivants : représentant désigné/agent de sécurité sur le terrain3/coordinateur

1 « De par leurs fonctions » indique que les représentants d'organisations qui ne font pas partie des Nations Unies ne sont pas liés et ne participent pas officiellement aux décisions de politique de l'EGS sur la sécurité.
2 Le représentant désigné est le haut représentant des NU ayant la responsabilité générale de la sécurité et de la protection du personnel du système des NU.
3 L'agent de sécurité sur le terrain est un représentant des NU responsable de la sécurité sur son lieu d'affectation.

Sauver des vies ensemble (suite)

régional de la sécurité ou autre délégué du représentant désigné ; les membres de l'EGS s'il y a lieu ; le(s) chargé(s) de liaison d'ONG en matière de sécurité sur le terrain ; les représentants d'OIG. Le président pourra être choisi par rotation.

c) Les forums pourront inclure des sujets de discussion tels que : L'échange d'informations liées à la sécurité ; les déclarations d'incidents ; l'analyse de la sécurité et des tendances ; la planification opérationnelle commune, s'il y a lieu ; les protocoles pour le partage et la plus grande diffusion d'informations et de documents présentés ou étudiés.

3. Inclure les préoccupations de sécurité du personnel dans les appels globaux

Des mesures structurées seront prises pour inclure des projets de sécurité des NU/ONG/OIG bien conçus et bien élaborés dans les procédures d'appels globaux, afin de couvrir les ressources supplémentaires potentiellement nécessaires pour une collaboration renforcée en matière de sécurité du personnel entre les agences des NU et les ONG/OIG, telles que les télécommunications et la formation en matière de sécurité.

4. Répondre aux besoins communs liés à la sécurité et partager les ressources

Il est reconnu que les ressources financières des ONG individuelles sont souvent moins importantes que celles des NU ou des OIG, néanmoins leurs contributions seront nécessaires et il faudra considérer quelles ressources pourront être mises à disposition pour aborder les besoins communs liés à la sécurité.

Les organisations des NU et leurs partenaires ONG/OIG, qui se sont engagées à collaborer en matière de sécurité dans des opérations humanitaires spécifiques, contribueront, dans la mesure qui leur est possible et en fonction de l'étendue de leur engagement, à répondre aux besoins non couverts de la communauté humanitaire en matière de sécurité.

5. Partager les ressources

Les organisations des NU et leurs partenaires OIG/ONG qui coopèrent dans les opérations humanitaires sur le terrain feront un inventaire local dans le but de partager leurs ressources humaines et matérielles spécialisées, liées à la sécurité.

(suite)

Sauver des vies ensemble (suite)

6. Faciliter la sécurité interorganisationnelle et les télécommunications d'urgence

Les télécommunications entre les organisations des NU et leurs partenaires OIG/ONG au niveau du terrain seront facilitées par :

a) Le représentant désigné, qui préconisera auprès des autorités concernées l'utilisation d'équipements de télécommunications dans le cadre des accords internationaux existants.
b) L'organe des NU concerné, qui négociera avec les autorités une fréquence commune inter organisationnelle pour faciliter une plus grande interopérabilité pour la collaboration en matière de sécurité entre les organisations des NU et les OIG/ONG présentes dans la même région, sans contester le besoin des organisations d'avoir leur propre infrastructure de communications internes et intégrantes.
c) Les acteurs humanitaires engagés dans une collaboration en matière de sécurité utiliseront des procédures de communication standard et, dans la mesure du possible, fourniront à leur personnel des systèmes de communication compatibles.

7. Collaborer et consulter pour la formation relative à la sécurité

Toutes les organisations des NU et leurs partenaires OIG/ONG au niveau central et du terrain :

a) Effectueront, dans la mesure du possible, une formation commune liée à la sécurité, en collaboration et/ou en consultation avec d'autres organisations.
b) Lorsque cela sera possible, mettront en commun les ressources nécessaires pour effectuer une formation sur le terrain en matière de sécurité.
c) Chercheront à renforcer leur capacité en formation en matière de sécurité à tous les niveaux.
d) Étudieront la possibilité de créer des programmes de formation centrés spécifiquement sur l'amélioration de la collaboration en matière de sécurité.

8. Partager l'information

Les organisations des NU et leurs partenaires OIG/ONG partageront l'information sur la sécurité tout en respectant le caractère humanitaire des participants ainsi que la confidentialité des informations sensibles.

Sauver des vies ensemble (suite)

9. Identifier des normes minimales de sécurité

Les organisations des NU et leurs partenaires OIG/ONG identifieront et approuveront d'un commun accord la façon d'appliquer les normes, principes et/ou consignes minimaux de sécurité, adaptés aux circonstances locales. Ce faisant, les acteurs humanitaires tiendront compte des normes, principes et/ou consignes existant déjà, par exemple les Normes minimales de sécurité opérationnelle (MOSS) des NU, qui sont obligatoires pour les membres du système des NU, ainsi que les lignes directrices d'InterAction pour l'élaboration de la sécurité (Security Planning Guidelines).

10. Chercher à adhérer aux règles humanitaires communes

La collaboration des organisations des NU et de leurs partenaires OIG/ONG en matière de sécurité dans des opérations spécifiques sur le terrain, reposera, dans la mesure du possible, sur le respect des règles communes établies localement pour l'action humanitaire.

Annexe 4
Prestataires privés de sécurité

La sécurité privée et commerciale est une industrie en expansion. Un plus grand nombre de sociétés internationales ont émergé dans les premières années d'activités en Afghanistan et en Irak. Les prévisions indiquent que l'industrie militaire et de sécurité privée dans le monde atteindra 202 milliards de dollars en 2010.[1] On utilise le terme « prestataire privé de sécurité » plutôt que sociétés de sécurité privées ou sociétés militaires privées, pour inclure les milices payées qui ne sont pas nécessairement constituées en sociétés ni enregistrées, mais qui fournissent des services similaires. L'éventail de services offerts par les prestataires privés de sécurité est large : protection statique (généralement dans les bureaux et les lieux de résidence), protection mobile (escortes), protection rapprochée (gardes du corps), évaluation des risques et analyse des menaces, audits de sécurité, formation, consultation (c.à.d. conseils sur les protocoles de sécurité), gestion d'incidents critiques, logistique et fourniture d'équipement. Une sous-catégorie de prestataires privés de sécurité, communément appelés Sociétés militaires privées (SMP), peut également offrir des services aux gouvernements et aux militaires, par exemple une réforme du secteur de la sécurité, des conseillers militaires, une formation militaire, le commandement et le contrôle des opérations militaires, un soutien logistique important, l'administration des prisons et des interrogatoires.

En 2008, une étude sur le rôle des prestataires privés de sécurité dans l'action humanitaire a montré que les principaux services qu'ils fournissaient consistaient en une protection non armée, la formation et la consultation.[2] Bien que la fourniture de protection armée reste exceptionnelle, tous les acteurs humanitaires importants ont utilisé des prestataires privés de sécurité dans ce but dans au moins un contexte. La protection non armée étant le service de sécurité le plus fréquemment demandé, la plupart des prestataires privés de sécurité recrutés par des organisations humanitaires sont des sociétés locales, non internationales. L'étude a également révélé que les décisions d'employer un prestataire privé de sécurité sont souvent prises au niveau du terrain, avec peu ou pas de consignes pratiques ou de politique provenant du siège de l'organisation.

1 Deborah Avant, « Privatizing Military Training » (Privatiser la formation militaire), *Foreign Policy in Focus*, vol. 7, issue 3, Mai 2002.
2 Abby Stoddard, Adele Harmer et Victoria DiDomenico, The Use of Private Security Providers and Services in Humanitarian Operations (L'utilisation de prestataires et de services privés de sécurité dans les opérations humanitaires), HPG Rapport 27 (Londres : ODI, 2008).

Considérations sur le recrutement de prestataires privés de sécurité

Un certain nombre de suppositions influencent la décision d'employer un prestataire privé de sécurité : un prestataire fournit des connaissances spécialisées qui n'existent pas à l'intérieur de l'organisation ; cela peut faire gagner du temps ; et c'est financièrement plus avantageux. Ces suppositions doivent être soigneusement examinées.

L'externalisation de ces service est souvent jugée être une option moins coûteuse, réduit les coûts de formation, d'assurance et d'administration et permet au personnel de se concentrer sur des tâches centrales. Ce type de raisonnement pourrait être valable en termes de comptabilité, dans la plupart des organisations humanitaires internationales (et probablement aussi dans beaucoup d'organisations nationales). Cependant, à long terme, les coûts cachés peuvent inclure le manque d'investissement pour apporter des compétences et une expertise au sein de l'organisation même (parce que les compétences en matière de sécurité restent le domaine du prestataire) ; l'atteinte possible à la réputation de l'organisation ; et les frais légaux potentiels et mêmes les versements d'indemnités en cas de problèmes. Les implications possibles de coûts à long terme sont une autre considération pour l'organisation, si elle suit une approche sécuritaire principalement centrée sur la protection et la dissuasion. Une telle approche risque de se perpétuer en partie parce qu'il sera de plus en plus difficile de reprendre une approche d'acceptation, qui peut être moins coûteuse. Enfin, dans les contextes où un prestataire privé de sécurité a un quasi monopole, les prix seront probablement élevés et pourraient devenir exorbitants.

Une autre question cruciale est la perception de l'association entre ces entités (et par extension les organisations humanitaires) avec les acteurs militaires et politiques. Les prestataires privés de sécurité peuvent avoir des liens avec les services de sécurité ou de police, avec les services militaires du gouvernement ou avec des acteurs ayant des antécédents de comportement illégal, criminel ou abusif, y compris de violations des droits de l'homme. Il peut être extrêmement difficile d'évaluer les pratiques, au sens large, de certains prestataires privés de sécurité. En effet, ces sociétés n'attirent généralement pas l'attention du public sur leurs activités dont la légalité peut être remise en question, et les informations concernant d'autres clients sont généralement considérées comme confidentielles. Les prestataires privés de sécurité peuvent également être des filiales de sociétés holdings plus grandes, ce qui rend difficile d'établir qui les possède.

Une autre préoccupation au sujet des services privés de sécurité est l'impact généralement nuisible qu'ils ont sur la sécurité du public :

- La présence de nombreux prestataires privés de sécurité est un signe indirect que les autorités ne sont pas en mesure d'assurer la sécurité publique.
- Une meilleure rémunération dans le secteur privé pourrait conduire les membres du secteur public de la sécurité à le quitter pour prendre des postes dans les sociétés privées.
- Si le personnel de la sécurité privée ne peut être facilement distingué des forces de sécurité publiques, toute faute de conduite créera une méfiance plus généralisée.
- Lorsque les agents d'État (forces de sécurité ou forces civiles, actives ou à la retraite) ont des intérêts commerciaux dans des services privés de sécurité, la motivation pour renforcer le secteur public ne sera pas très grande et il pourrait y avoir des conflits d'intérêts.
- Les États en post conflit peuvent ne pas avoir de cadre réglementaire pour les prestataires privés de sécurité ; si une réglementation est en place, elle ne sera peut-être pas appliquée avec succès.

Une recherche exploratoire en Angola et en Afghanistan indique que la population locale se méfie généralement des prestataires privés de sécurité ; celle-ci pense qu'au lieu de réduire l'insécurité, ils l'augmentent.[3]

En somme, le recrutement d'un prestataire privé de sécurité n'est pas simplement une question de réduire à court terme le risque pour le personnel et les biens ou de réduire les frais. Il peut avoir de profondes implications, pas seulement pour la stratégie sécuritaire de l'organisation à long terme, mais aussi pour d'autres organisations humanitaires et pour l'objectif plus général de rétablir un État efficace et responsable.

Les points suivants donnent un aperçu des mesures que le personnel des organisations humanitaires peuvent prendre en compte pour améliorer leur prise de décision au sujet de l'utilisation de prestataires privés de sécurité et la gestion de leurs relations avec ces prestataires.

Implications stratégiques

- Comment cette option s'inscrit-elle dans le cadre de votre stratégie de sécurité ? L'emploi d'un prestataire privé de sécurité pourrait-il fragiliser votre stratégie ou nécessiter une approche différente ?

3 Ulrike Joras et Adrian Schuster (sous la direction de), Private Security Companies and Local Populations : An Exploratory Study of Afghanistan and Angola (Les sociétés privées de sécurité et les populations locales : Étude préliminaire en Afghanistan et en Angola), Swisspeace, document de travail 1, 2008.

- Réduira-t-il le risque physique direct à long terme, aussi bien qu'à court terme ?
- Comment les prestataires privés de sécurité sont-ils perçus par la population locale ? Quels sont les risques pour la réputation de l'organisation, aux niveaux local et international ?
- Avez-vous une politique sur l'utilisation de prestataires privés de sécurité, armés et non armés ?
- Avez-vous les compétences nécessaires pour gérer un prestataire privé de sécurité ? Comment allez-vous développer les compétences requises dans l'organisation si vous externalisez votre sécurité (surtout la gestion de votre sécurité) ?
- Cela créera-t-il un précédent qui pourrait avoir un impact sur d'autres organisations humanitaires ?
- Contribuez-vous à l'inflation du marché (prix plus élevés) ou à une baisse des normes ? Des négociations collectives pourraient-elles être une option pour les acteurs humanitaires ?
- Y a-t-il des moyens d'utiliser des prestataires privés de sécurité qui renforcent aussi les services publics de sécurité ou qui apportent de plus grands avantages publics (p. ex. des gardes statiques qui assurent la sécurité d'un quartier entier plutôt qu'uniquement celle de maisons individuelles) ?
- Existe-t-il des politiques ou règlements étatiques que vous devez suivre, concernant les prestataires privés de sécurité?
- Quel est le coût financier direct comparativement à votre budget de fonctionnement global dans le pays ? Comment déterminerez-vous le rapport coût-efficacité de l'investissement ?

Questions à considérer pour la vérification des antécédents et le recrutement d'un prestataire privé de sécurité

- Avez-vous des consignes pour faire preuve de la diligence requise lors des vérifications d'antécédents et des contrôles de qualité du prestataire privé de sécurité ? Avez-vous des modèles de contrats pour la provision de services privés de sécurité ? Avez-vous un système pour garder un dossier sur le prestataire que vous recrutez ?
- Quels services le prestataire fournit-il ?
- Si le prestataire offre une protection armée, savez-vous comment il devra manier, entretenir et utiliser ses armes ? A-t-il des règles d'engagement ?
- Est-il enregistré, et où ? Les sociétés internationales peuvent être enregistrées dans différents pays : une question sera de savoir où leur siège est enregistré, et si le prestataire est enregistré dans le pays dans lequel vous êtes actif. Les entités nationales peuvent être enregistrées ou pas, peut-être sous différentes dispositions légales.
- Qui sont ses autres clients ?

- À qui appartient la société (ou, dans le cas d'un groupement non doté de la personnalité morale, qui dirige le personnel) ?
- Que pouvez-vous savoir sur ses antécédents et sa réputation ? Est-il jugé avoir des intérêts particuliers, par exemple une personne éminente, une certaine élite ou une faction locale ? La société a-t-elle été impliquée dans des incidents importants ou a-t-elle été accusée de faute professionnelle ?
- Le prestataire privé de sécurité respecte-t-il en tout point les lois et règlements nationaux ?

Fiabilité et professionnalisme

- Le prestataire privé de sécurité a-t-il une déclaration éthique ou de responsabilité sociale d'entreprise, notamment un engagement de respecter les lois nationales, les lois internationales sur les droits de l'homme et tout autre cadre légal international applicable ?
- Effectue-t-il des vérifications d'antécédents détaillées et tient-il des dossiers à jour sur son personnel ?
- Exige-t-il que son personnel soit nettement identifiable comme faisant partie de la société ?
- A-t-il des permis de port d'arme, et utilise-t-il des armes interdites par le droit international ?
- A-t-il un registre à jour de toutes les armes et munitions ?
- Le prestataire privé de sécurité fournit-il une formation approfondie pour son personnel, portant sur l'utilisation de l'équipement, les règles précises sur l'utilisation des armes et les relations avec le public en général ?
- Offre-t-il des rémunérations et des avantages adéquats à son personnel ?
- Donne-t-il à son personnel des contrats, dans une langue qu'il comprend ?
- Contrôle-t-il régulièrement la conduite de son personnel ?
- Des mesures efficaces sont-elles en place contre la corruption ?
- A-t-il des mécanismes de plaintes, des capacités d'enquête et des procédures disciplinaires concernant la conduite de son personnel ?
- Le prestataire privé de sécurité sous-traite-t-il certains services, et si oui, a-t-il des procédures efficaces pour vérifier et rendre responsables ses sous-traitants ?
- A-t-il la capacité financière d'absorber les dettes ?
- Est-il suffisamment assuré ?

Vous pouvez poser ces questions à un prestataire potentiel lors des premières discussions. Ces discussions fourniront une base pour rédiger un contrat, qui pourra inclure un grand nombre des renseignements ci-dessus. Le contrat devra également spécifier les conditions qui vous permettront de le résilier et quelles clauses pourraient entraîner des pénalités pour le prestataire.

Contrôle, enquête sur les plaintes et déclarations

Les clients des prestataires privés de sécurité ont la responsabilité de surveiller la conduite et la performance de leur prestataire, pas seulement en ce qui concerne leurs propres intérêts mais aussi ceux des tierces parties, y compris de l'ensemble de la population. Lorsque vous employez un prestataire privé de sécurité, envisagez d'établir un mécanisme de surveillance et de plaintes, accessible au grand public et sûr.

Les clients du prestataire privé de sécurité ont l'obligation éthique de contribuer au renforcement d'un régime national et international pour réglementer et surveiller les prestataires privés de sécurité. Les expériences négatives avec des prestataires privés de sécurité doivent être déclarées et communiquées, comme il convient, aux autorités concernées du pays d'opérations et/ou au siège du prestataire. Les mécanismes internationaux sont un autre moyen de s'assurer que les prestataires privés de sécurité sont guidés par des normes de bonne conduite. Celles-ci incluent le code de bonne conduite pour les sociétés militaires et de sécurité privées à travers le monde. Son lancement est prévu en 2010.[4] Un autre mécanisme, le Document de Montreux (septembre 2008), rappelle aux États leurs obligations envers les sociétés militaires et de sécurité privées (celles qu'ils emploient et celles constituées sur leur territoire) et énonce un ensemble de bonnes pratiques. Le document est également considéré comme une référence utile pour les organisations humanitaires. Il inclut un rappel sur le fait que les hauts responsables d'une société militaire et de sécurité privée sont responsables de la conduite de leur personnel. Il en va de même pour l'agent d'un État qui a des relations avec la société.[5]

4 Voir http://www.dcaf.ch/privatisation-security/_index.cfm.
5 Lettre datée le 2 octobre 2008 du Représentant permanent de la Suisse au Secrétaire-général des Nations Unies. New York, NU A/63/467-S/2008/636 (http://www.icrc.org/web/eng/siteengo.nsf/htmlall/montreux-document-170908/$FILE/MONTREUX-Document-eng.pdf).

Annexe 5
L'assurance

Cette annexe souligne quelques questions fondamentales que les travailleurs humanitaires, les responsables de la sécurité et les sièges d'organisations doivent considérer. Elle n'est pas censée être un examen spécialisé des polices d'assurance contre les accidents, les risques de guerre ou les actes malveillants.

Pour les employeurs, assurer leur personnel contre des incidents de sûreté et de sécurité est un aspect important de la responsabilité requise en matière de sûreté et de sécurité. Les travailleurs humanitaires devront être pleinement informés des détails de l'assurance fournie par leur organisation. En tant que travailleur humanitaire, vous avez la responsabilité personnelle de vous informer sur l'assurance qui vous est offerte. En plus des renseignements que vous obtiendrez auprès de votre organisation, il vous est également conseillé de contacter vous-même les compagnies d'assurance et les associations professionnelles pour savoir ce qui est disponible.

Il est important, pour tous, de ne pas oublier que l'assurance fournit une indemnité, non pas une protection.

Le coût de ne pas avoir d'assurance

Les accidents et incidents de sûreté et de sécurité peuvent avoir des conséquences financières majeures pour les travailleurs humanitaires concernés, leurs familles et l'organisation. Il y a des coûts immédiats, tels que l'évacuation médicale et le traitement d'urgence, qui peuvent rapidement s'élever à des sommes très importantes. Il y a également des coûts potentiels à long terme, tels que ceux résultant d'un handicap permanent (par exemple suite à la perte d'un membre) et ceux concernant des besoins de soins à long terme.

Dans le passé, beaucoup d'organisations humanitaires n'avaient pas d'assurance adéquate pour les risques de guerre et les actes malicieux, soit parce qu'elles ignoraient que leurs politiques ordinaires ne couvraient pas ces types d'incidents, soit parce que les coûts impliqués étaient élevés. Bien entendu, dans certains cas les compagnies d'assurance ont refusé de verser des indemnités et les travailleurs humanitaires blessés, ou les familles des travailleurs décédés, ont entamé des poursuites contre l'organisation afin d'obtenir une indemnisation. Ces demandes d'indemnités peuvent conduire une petite organisation à la faillite.

De quelle assurance avez-vous besoin ?

Les besoins en assurance seront différents selon les organisations. L'assurance doit être considérée comme une composante d'une stratégie d'atténuation et, comme tout autre chose, elle nécessite une appréciation complète des risques, qui découlera d'une évaluation globale. Après avoir appris quelques leçons coûteuses sur les dangers d'une couverture d'assurance insuffisante, les organisations sont aujourd'hui plus conscientes du type de couverture qu'il est prudent d'avoir. La plupart des grandes organisations humanitaires internationales qui déploient du personnel dans des contextes difficiles, tels que les contextes de conflit ou de forte criminalité, ont des contrats d'assurance avec les types de couverture suivants :

- Assurance médicale standard.
- Assurance accident standard, comprenant la mort accidentelle et la perte d'un membre.
- Assurance invalidité : partielle ou totale, à long ou à court terme.
- Assurance urgence médicale, comprenant une couverture pour l'évacuation médicale et les soins médicaux sur place et en transit.
- Assurance risque de guerre. Il s'agit souvent d'une police séparée, ou d'un supplément avec un coût additionnel. Elle couvre les blessures ou les décès causés par des actes de guerre ou de terrorisme. Cette couverture peut se faire sous forme de police personnelle d'accident couvrant les actes malicieux ou les tactiques terroristes et prévoyant le versement d'une somme forfaitaire, par exemple cinq fois le salaire annuel.
- Assurance rapt et rançon, couvrant l'expertise technique de gestion de crise et les frais éventuels pour faciliter une libération en sûreté.
- Assurance de responsabilité civile. Elle est généralement destinée au haut personnel et aux directeurs, au cas où ils seraient poursuivis en justice par des membres du personnel ou autres personnes demandant des dommages et intérêts.

Ce que vous devez savoir

Globalement, la couverture d'assurance pour les travailleurs humanitaires s'est élargie et est donc devenue plus complexe. Il est plus important que jamais de lire entre les lignes et de se renseigner explicitement sur ce qui est couvert et ce qui ne l'est pas.

Clauses d'exclusion

Les polices d'assurance peuvent ne pas être applicables dans certaines conditions, et les détails et l'interprétation de ces clauses d'exclusion peuvent avoir une importance vitale. Par exemple :

- La couverture n'est accordée que pendant le travail (p. ex. en Somalie, mais pas pendant une période de repos et de relaxation à Nairobi).
- La couverture n'est accordée que pendant les heures de travail (p. ex. jusqu'à 18.00 heures mais pas après ou pendant le weekend).
- La couverture exclut certains types de risques de guerre ou d'actes malicieux, en particulier les « actes terroristes », par exemple un bombardement dans un lieu public.
- La couverture exclut des zones de conflit spécifiques (vous devrez vous assur-er que la manière dont ces zones sont définies est clairement spécifiée).
- La couverture n'est accordée que si l'organisation a des consignes de sécurité écrites, si elle peut démontrer que ces consignes sont appliquées (le responsable de la sécurité pourrait en avoir la responsabilité) et suivies, et/ou si l'organisation offre au personnel une formation en matière de sécurité.
- La couverture exclut le personnel qui a des contrats à court terme ou le personnel au-delà d'un certain âge (souvent 59 ans).
- Exclusions politiques : pour les organisations dont le siège est basé aux USA, les pays qui sont sous sanctions du Bureau du contrôle des avoirs étrangers (OFAC) ne sont généralement pas couverts par les polices d'assurance, à moins d'obtenir une dérogation de la part du gouvernement américain.

Annulation d'autres polices d'assurance

Lorsque vous travaillez dans des zones dangereuses, vérifiez non seulement l'étendue de la couverture accident et l'étendue de l'assurance, mais aussi l'impact potentiel de souscrire plus d'une police d'assurance. Quelquefois les contrats d'assurance vie (tels que ceux souscrits avec un emprunt immobilier) peuvent ne pas être valables pour le personnel qui travaille dans des zones à risque élevé.

Couverture au début et à la fin du contrat d'emploi

Demandez précisément quand la couverture commence et quand elle prend fin. Il est important de déterminer si un membre du personnel est couvert, même s'il ne perçoit pas encore de salaire ou s'il n'a pas encore été déployé sur son lieu de mission. L'organisation et le membre du personnel doivent également savoir exactement à quel moment, après la fin de la mission, la couverture prend fin.

Primes

Certaines compagnies d'assurance baissent leurs primes pour les personnes qui travaillent dans des zones à grand risque si l'assuré peut démontrer qu'il a pris part à une formation en matière de sécurité, fournie par une

organisation reconnue ou agréée. Cette option a été acceptée par un grand nombre de professionnels du journalisme et pourrait être explorée dans le secteur humanitaire. Bien qu'il n'existe pas de données solides, des données empiriques indiquent que les organisations qui peuvent démontrer une approche sérieuse de la sécurité de leur personnel dans leurs politiques et pratiques peuvent bénéficier de primes moins élevées.

Autres considérations

Assurance et personnel national

Les pratiques des organisations humanitaires internationales varient en ce qui concerne les assurances pour le personnel national. Bien que certaines se soient efforcées d'améliorer l'assurance du personnel national, dans la majorité des organisations la plupart des travailleurs nationaux ne sont pas assurés, et les demandes d'indemnités ou d'aide financière en cas de maladie, de blessure ou de décès sont généralement gérées au cas par cas. Dans de nombreuses situations, soit il est impossible de souscrire une assurance pour les travailleurs nationaux, soit le coût de couvrir tous les employés nationaux est prohibitif. Cependant, ce n'est pas une raison pour éviter la question. Un pays peut avoir un système national d'assurance qui fonctionne et qui peut être consulté. Ailleurs, il pourrait y avoir des pratiques locales régissant comment les membres du personnel et leurs familles peuvent être compensés et les montants de ces indemnités. Même si votre assureur international n'offre pas d'assurance tous risques pour les travailleurs nationaux, il pourrait être possible de les inclure dans certaines polices, par exemple le rapt et la rançon.

Régimes d'auto-assurance

Dans les situations où les organisations ne sont pas en mesure de fournir une couverture d'assurance aux travailleurs nationaux des régions à haut risque, certaines de ces organisations ont créé leur propre système d'assurance en coopérative interne : une caisse d'assurance, ouverte avec une somme forfaitaire versée par l'organisation et à laquelle les employés qui y participent pourront verser des contributions. Les ONG de secours médical offrent souvent des soins de santé gratuits à tout leur personnel comme avantage en nature.

Assurance risque politique

Lorsque le gouvernement du Soudan a expulsé 13 ONG de son territoire en 2009, le coût de retrait des organisations concernées s'est élevé à des millions de dollars, représentés par la perte de biens et par les frais généraux des projets qui ne pouvaient pas être entrepris. En général, l'évacuation est très coûteuse (un événement peu fréquent mais très grave), et certaines grandes organisations humanitaires qui travaillent dans des contextes instables

ont commencé à envisager les risques politiques et de nouvelles formes d'assurance qui pourraient verser des indemnités dans ces éventualités.

Points essentiels à ne pas oublier

Cela pourrait être un cliché, mais on ne soulignera jamais assez l'importance de lire entre les lignes d'un contrat d'assurance. Avant de souscrire une assurance, évaluez soigneusement le risque et déterminez quelles politiques et procédures sont déjà en place, et ce qui doit être ajouté. L'objectif est de parvenir à la bonne configuration de polices d'assurance pour atténuer les menaces les plus probables. Une fois l'assurance souscrite, le travail n'est pas terminé : les organisations doivent mettre les protocoles administratifs nécessaires en place, en termes de formation et de procédures d'information en matière de sécurité.

Annexe 6
Financement des donateurs et gestion de la sécurité

Quelles que soient les approches ou les stratégies de sécurité employées par les organisations humanitaires dans les contextes dangereux, elles engendreront inévitablement des frais. S'assurer que les fonds suffisants sont disponibles pour permettre aux organisations de travailler en sécurité est vital.. Ceci est un sujet sur lequel les organisations et leurs donateurs doivent être prêts à avoir des discussions franches. Cette annexe expose certains points et développements importants concernant le financement des initiatives de gestion et de coordination de la sécurité par les donateurs.

Financer les frais de sécurité

Les administrations des donateurs institutionnels ne sont pas toutes conscientes des préoccupations de sécurité des organisations opérationnelles et elles n'y sont pas toutes réceptives.[1] Cependant, en règle générale, les grands donateurs humanitaires sont prêts à financer les dépenses liées à la sûreté et à la sécurité quand elles sont appropriées et justifiées. Plusieurs donateurs institutionnels, notamment DFID et USAID/OFDA, incluent des références explicites concernant la gestion de la sécurité et les frais connexes dans leurs lignes directrices pour l'établissement de propositions. Certains donateurs nomment des personnes à des postes spécifiques de gestion et de coordination de la sécurité. Ces personnes peuvent fournir des conseils utiles, surtout pendant la phase de planification des programmes et les étapes initiales de la budgétisation. Certains donateurs ont également organisé des ateliers et des conférences pour conseiller les organisations humanitaires sur l'intégration des coûts de sécurité dans leurs propositions. En 2008, ECHO a organisé une séance de travail sur « les défis que représente la gestion des risques en Afghanistan », et a inclus les questions de gestion de la sécurité dans un certain nombre de conférences annuelles de ses partenaires.

Les demandes de financement liées à la sécurité doivent généralement être accompagnées d'un plan de sécurité détaillé comprenant une analyse du contexte et une évaluation des risques. Afin d'éviter d'importantes révisions budgétaires des projets après la signature des contrats, les évaluations des

1 Par « donateur institutionnel » nous entendons les administrations donatrices qui travaillent sous les auspices de gouvernements (comme USAID ou DFID) et les organes intergouvernementaux (comme ECHO).

risques peuvent décrire plusieurs scénarios futurs, et plusieurs besoins, si la sécurité se détériorait. Les donateurs varient en ce qui concerne ce qu'ils sont prêts à financer, mais les domaines de dépenses communes incluent l'équipement de communication et de sécurité, le personnel de sécurité spécialisé, les véhicules, les aménagements physiques de sécurité dans les logements et les bureaux, les évaluations de la sécurité et la formation sur la sécurité. Un soutien additionnel au niveau du terrain, tel que celui offert par les prestataires privés de sécurité, est normalement considéré au cas par cas.

Il n'y a pas de formule budgétaire uniforme ou de définitions de dépenses communes pour les ressources et les activités visant à renforcer la sécurité opérationnelle. Les organisations et les donateurs varient également dans la façon dont ils incluent les coûts liés à la sécurité dans leurs budgets. Certains incluent le financement de la sécurité dans les frais généraux ou les services de soutien de base, tandis que d'autres l'incluent dans un poste budgétaire séparé ou comme un pourcentage fixe des coûts du programme. De nombreuses organisations seraient incapables de fournir un chiffre pour les dépenses de sécurité, parce que leurs coûts de sécurité sont entièrement intégrés dans les coûts de leurs programmes. Par exemple, les véhicules supplémentaires achetés ou loués afin que le personnel puisse se déplacer en convois figureraient au poste « véhicules/transport » ; faire installer des barrières, des barreaux ou des systèmes d'alarmes serait inclus dans « réparations/entretien des installations » ; et le recrutement de nouveaux experts en sécurité ou de personnel de programme additionnel serait ajouté au poste des salaires.

Un certain nombre de donateurs institutionnels encouragent activement une plus grande sensibilisation à la sécurité et de meilleures compétences en matière de sécurité dans les organisations humanitaires qu'ils financent, et ils s'attendent à voir des dépenses liées à la sécurité dans les budgets. Cependant, outre cela, les donateurs ne dictent généralement pas de politiques ou de pratiques particulières concernant la sécurité, et préfèrent laisser aux organisations le soin de déterminer leur propre position et d'exercer leur propre contrôle de qualité dans ce domaine. C'est en partie parce que les donateurs n'ont pas le personnel et donc le temps, les compétences et la présence sur le terrain, pour exercer une influence plus directe. Les donateurs sont également très prudents pour ne pas être perçus comme imposant un modèle de sécurité particulier aux organisations. S'impliquer officiellement dans l'assurance de la qualité les exposerait potentiellement à des réclamations en responsabilité civile.

Un grand nombre de donateurs exigent que leur financement soit mis en évidence et insistent pour que leur logo soit en vue sur les biens qu'ils financent, notamment les bureaux, les véhicules et les biens distribués aux bénéficiaires.

Dans certains cas, cette association peut être considérée comme une menace à la sécurité, en particulier si le donateur en question est peu apprécié dans un contexte particulier, ou si l'organisation essaie d'adopter une approche discrète. Dans ces cas-là, une organisation pourrait demander officiellement une dérogation à la clause de visibilité. Les donateurs peuvent être flexibles sur ces exigences lorsque des préoccupations de sécurité imposent la prudence.

Participation du donateur au-delà du financement des besoins de sécurité opérationnelle

Dans les organisations donatrices, les points focaux de sécurité peuvent, en tant que spécialistes dans les domaines à la fois de la sécurité et du travail humanitaire, jouer un rôle important pour faciliter la promotion de la sécurité des organisations d'aide, au-delà du simple financement des besoins liés à la sécurité. Ils peuvent préconiser une meilleure attention aux besoins de sécurité de leurs partenaires, par exemple en assurant à leurs collègues que des demandes particulières ne sont pas excessives ; aider à quantifier les pertes subies suite à des incidents de sécurité, pour montrer la valeur de l'investissement dans la gestion de la sécurité ; mener des discussions avec des acteurs sur le terrain responsables de la sécurité des travailleurs humanitaires (les discussions bilatérales entre les gouvernements américain et soudanais en sont un exemple) ; et encourager le rassemblement et le partage de bonnes pratiques en matière de sécurité. Les donateurs institutionnels ont également un rôle à jouer pour renforcer les capacités et les compétences inter organisationnelles, notamment en finançant le *Security Advisory Group* d'InterAction et le *European Interagency Security Forum* (EISF). Les donateurs ont fourni un soutien extrabudgétaire pour les officiers de sécurité du Département de la sûreté et de la sécurité (DSS) des Nations Unies, avec un accent particulier sur les postes d'officiers de sécurité ayant des responsabilités de liaison avec les ONG, par le biais de l'initiative Sauver des vies ensemble (voir Annexe 3). Le gouvernement américain a fourni un financement pour permettre aux officiers de sécurité de DSS de travailler à plein temps sur les questions de sécurité des ONG au Darfour et pour permettre à DSS de renforcer sa capacité à offrir des services à la communauté dans son ensemble en Éthiopie, en Côte d'Ivoire et au Liban. Un poste de liaison ONG-DSS à New York a été financé grâce à un soutien extrabudgétaire d'un donateur. Des donateurs institutionnels ont également financé une recherche pour examiner l'évolution des défis en gestion de la sécurité et l'évaluation des pratiques actuelles des organisations humanitaires. Puisque les organisations financent souvent des programmes grâce à des contributions de multiples donateurs, la coordination entre donateurs est importante pour permettre l'harmonisation des exigences et des lignes directrice en matière de budgétisation pour la sécurité.

Annexe 7
Ressources supplémentaires

Il existe une quantité croissante d'ouvrages sur la gestion de la sécurité opérationnelle, comprenant à la fois des documents spécifiques aux organisations et des lignes directrices plus générales. Cette annexe indique certaines des sources d'informations les plus importantes.

Guides généraux sur la sécurité

ECHO, *Guide générique de la sécurité pour les organisations humanitaires*, Office d'aide humanitaire de la Commission européenne (ECHO) (Bruxelles : ECHO, 2004).

ECHO, *NGO Security Collaboration Guide* (Guide de collaboration sur la sécurité des ONG). Commandé par l'Office d'aide humanitaire de la Commission européenne (ECHO) (Bruxelles : ECHO, 2006).

David Lloyd Roberts, *Staying Alive : Safety and Security Guidelines for Humanitarian Volunteers in Conflict Areas* (Rester en vie : Consignes de sûreté et de sécurité destinées aux bénévoles humanitaires dans les zones de conflit) (Genève : CICR, 2006).

FISCR, Rester en sécurité : Guide de la Fédération internationale destiné aux responsables de la sécurité) (Genève : FISCR, 2007). Également disponible en anglais.

InterAction Groupe de sécurité, *Security Risk Management : NGO Approach* (Gestion des risques de sécurité: Approche ONG) (Washington DC : InterAction, 2010).

Comité pernanent inter agences, *Saving Lives Together : A Framework for Improving Security Arrangements Among IGOs, NGOs, and UN in the field* ((Sauver des vies ensemble : un cadre pour améliorer les dispositions de sécurité dans les OIG, les ONG et les NU sur le terrain) (New York : IASC, 2006).

Formation en matière de sécurité

Advance Training Program on Humanitarian Action (ATHA) : www.atha.se. Fournit une formation dans divers domaines, notamment la gestion de la sécurité.

Centre for Safety and Development : www.centreforsafety.org. Fondation à but non lucratif spécialisée dans la sûreté et la sécurité des organisations humanitaires. Organise des conférences et des stages de formation dans le domaine de la sécurité.

Essential Field Training : www.essentialfieldtraining.org. Offre une formation sur la sensibi-lisation à la sécurité pour les travailleurs humanitaires internationaux, les soldats du main-tien de la paix, les représentants de gouvernements, le secteur privé et autres acteurs.

RedR : www.redr.org. Offre une formation sur divers sujets, notamment la gestion du personnel de sécurité, la formation des gardes de sécurité, la sûreté des déplacements sur le terrain et la gestion du bien-être du personnel et des incidents critiques.

Security Management Initiative : www.securitymanagementinitiative.org. Fournit des ressources concernant la formation, l'information et l'éducation sur la sécurité opérationnelle. Basée à Genève.

Nations Unies : https://dss.un.org (pour le personnel NU) ou http://dss.un.org/asitf (pour le personnel non-NU). Offre deux cours de formation interactifs sur CD-ROM : « Sécurité de base sur le terrain : sûreté, santé et bien-être du personnel » et « Cours avancé de sécu-rité sur le terrain ». Disponibles en anglais, arabe, chinois, espagnol, français et russe.

Tendances concernant la sécurité du travailleur humanitaire

Aid Worker Security Database (AWSD) : www.aidworkersecurity.org. Donne une vue d'ensemble des attaques majeures contre les travailleurs humanitaires dans le monde depuis 1996.

Antonio Donini et al., *Mapping the Security Environment : Understanding the Perceptions of Local Communities, Peace Support Operations, and Assistance Agencies* (Cartographie de l'environnement de sécurité: Comprendre les perceptions des communautés locales, des opérations de soutien de la paix et des organisations d'aide) (Medford, MA : Feinstein International Famine Center, 2005).

ECHO, *Report on Security of Humanitarian Personnel : Standards and Practices for the Security of Humanitarian Personnel and Advocacy for Humanitarian Space* (Rapport sur la sécurité des personnels humanitaires: Normes et pratiques relatives à la sécurité des personnels et plaidoyer pour l'espace humanitaire) (Bruxelles : ECHO, 2004).

Abby Stoddard, Adele Harmer et Katherine Haver (2006) *Providing Aid in Insecure Environments* (L'aide humanitaire dans les contextes dangereux), HPG Rapport 23 (Londres : ODI, 2006).

Abby Stoddard, Adele Harmer et Victoria DiDomenico, *Providing Aid in Insecure Environments : 2009 Update* (L'aide humanitaire dans lex contextes dangereux : Mise à jour 2009), HPG Policy Brief 34 (Londres, ODI, 2009).

Assemblée générale des NU, *Sûreté et sécurité du personnel humanitaire et protection du personnel des Nations Unies*, Assemblée générale des NU A/64/336 (New York : NU, 2009).

Les groupes armés militaires et non-étatiques

Max Glaser, Humanitarian Engagement with Non-state Actors : The Parameters of Negotiated Access (Coopération humanitaire avec des acteurs non gouvernementaux : Les paramètres d'un accès négocié), HPN Dossier thématique 51 (Londres : ODI, 2005).

IASC, Civil–Military Guidelines and Reference for Complex Emergencies (Directives et référe-nces civiles-militaires pour les contextes d'urgence) (New York et Genève : IASC, 2008).

Abby Stoddard, Adele Harmer et Victoria DiDomenico, *The Use of Private Security Providers and Services in Humanitarian Operations* (L'utilisation de prestataires et de services privés de sécurité dans les opérations humanitaires), HPG Rapport 27 (Londres : ODI, 2008).

UN, *Use of Military or Armed Escorts for Humanitarian Convoys : Discussion Paper and Non-Binding Guidelines* (L'utilisation d'escortes militaires ou armées pour les convois humanitaires : Document de discussion et recommandations non obligatoires), 2001.

Gerard McHugh et Manuel Bessler, *Humanitarian Negotiations with Armed Groups : A Manual for Practitioners* (Négociations humanitaires avec les groupes armés : guide destiné aux praticiens) (New York L OCHA en collaboration avec IASC, 2006).

UN, *Guidelines on the Use of Military and Civil Defence Assets to Support United Nations Humanitarian Activities in Complex Emergencies* (Directives sur l'utilisation des ressources de protection militaires et civiles pour soutenir les activités humanitaires des Nations Unies dans les contextes d'urgence complexes) (Directives MCDA) (New York : UN, 2003, édition révisée 2006). Disponible en anglais, arabe, chinois, espagnol, français et russe.

UN, Directives sur l'utilisation des ressources militaires et de la protection civile étrangères dans le cadre des opérations de secours en cas de catastrophe (Directives d'Oslo), mise à jour novembre 2006, révision Novembre 2007. Disponible en anglais, arabe, chinois, espagnol, français et russe.

Gestion des personnes et du personnel

Centre for Humanitarian Psychology : www.humanitarian-psy.org. Publie des fiches d'informations sur divers aspects du soutien du personnel.

A. Gaul et al., *NGO Security: Does Gender Matter ?* (Sécurité des ONG : Le genre est-il important?) (Washington DC : Save the Children USA et Elliott School of International Affairs, George Washington University, 2006).

CIRC, L'action humanitaire et les conflits armés : Gérer le stress (Genève : CICR, (2001). Disponible en anglais, espagnol et français.

Interaction, *The Security of National Staff : Essential Steps* (Sécurité du personnel national : Mesures essentielles) (Washington DC : Interaction, 2002).

People in Aid : www.peopleinaid.org. Fournit des conseils d'orientation et des conseils pratiques sur divers sujets liés à la gestion des personnes dans le secteur de l'aide humanitaire, notamment le bien-être, la sécurité, la santé mentale et le soutien psychologique du personnel.

Sécurité et communications

ICT Humanitarian Emergency Platform : www.wfp.org/ict-emergency. Décrit les meilleures pratiques dans l'installation et l'entretien des équipements télécoms et offre une formation aux organisations humanitaires aux niveaux du siège et sur le terrain.

Security in-a-box : http://security.ngoinabox.org. Une collaboration de Tactical Technology Collective et de Front line ; donne des conseils sur la sécurité numérique. Disponible en anglais, arabe, espagnol, français et russe.

Security Management Initiative, *Cyber Security for International Aid Agencies : A Primer* (La cybersécurité pour les organisations d'aide internationale : consignes élémentaires), SMI Professional Development Brief 3 (Genève : Centre de politique de sécurité, 2009).

Mines terrestres

Service de l'action antimines des Nations Unies et CARE, *Manuel de Sécurité sur les mines terrestres et les débris explosifs de guerre*, 2005. Également disponible en anglais, et comme module de formation, vidéo et CD-ROM.

Autres ressources

Aid Workers Network : www.aidworkers.net. A une page sur la « Sûreté et sécurité des travailleurs humanitaires ».

Organisation Internationale de normalisation (ISO) Gestion des risques – Principes et recommandations (Genève : ISO, 2009). Disponible en anglais et en français.

Safer Access : www.saferaccess.org. Offre des conseils sur la sûreté et la sécurité, notamment sur la sécurité incendie, la sécurité des ordinateurs portatifs, des kits sur le traumatisme personnel, l'utilisation des bateaux dans le secours humanitaire et la sécurité en cas de tremblement de terre.