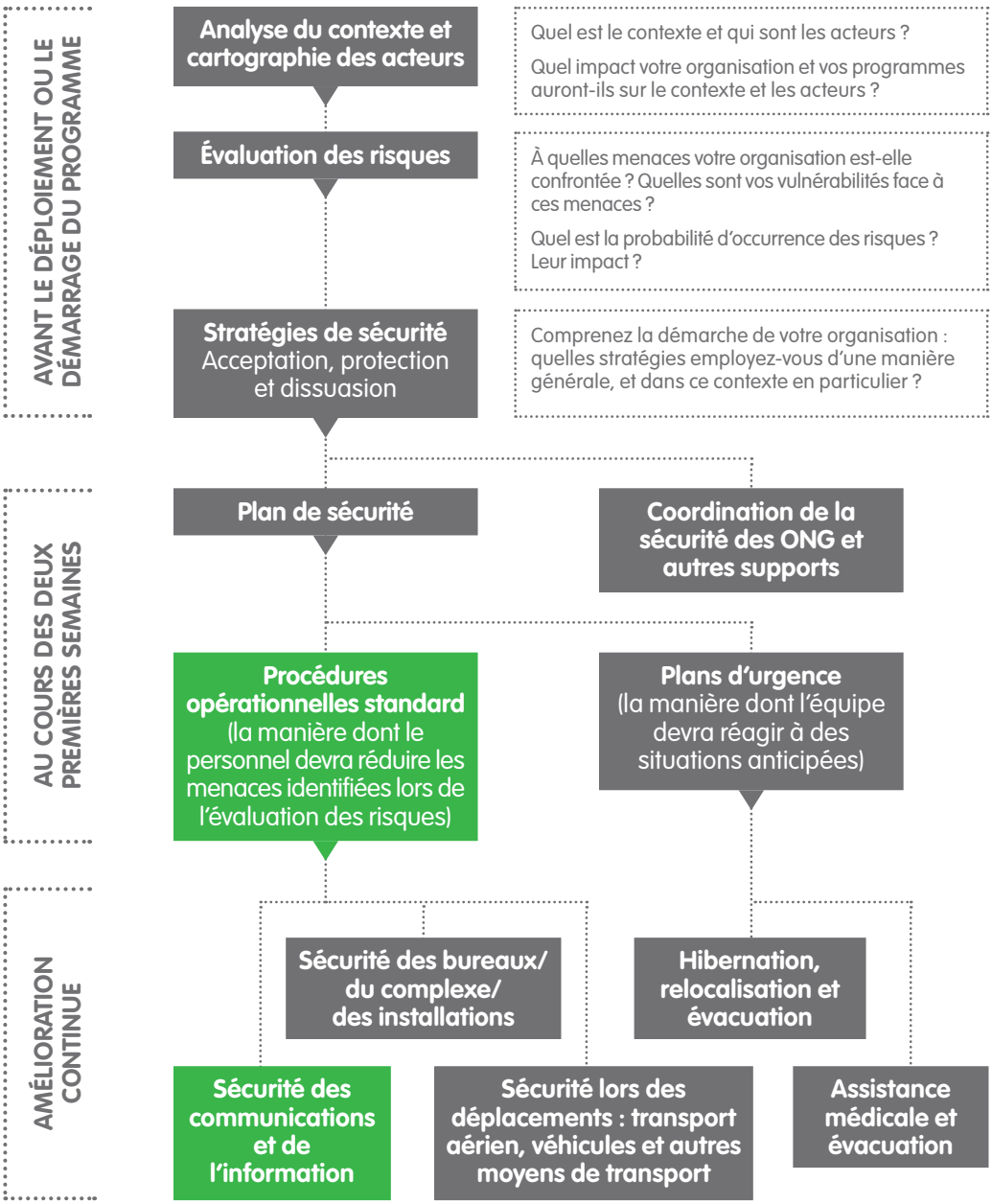
8 Sécurité des communications et de l'information



Lors de la mise en œuvre d'un nouveau déploiement, d'un nouveau projet ou d'une nouvelle mission, il est important de prendre le temps de s'interroger sur les types de communications qui seront disponibles (réseaux fixe et mobile, téléphones satellite, Internet, courrier postal, service de coursiers, etc.) et sur leur fiabilité. De nos jours, les communications sont tout aussi essentielles pour la « survie » que l'accès à de la nourriture, à de l'eau et à un abri.

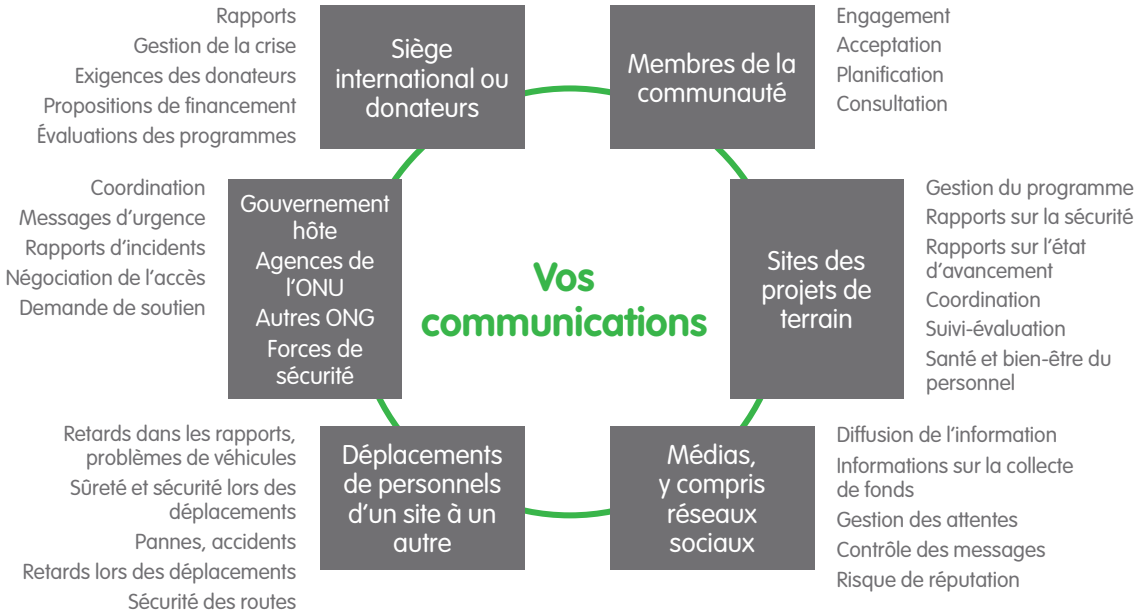
Que ce soit pour assurer la sécurité des personnels ou la réussite des programmes, il est crucial de prévoir à un stade précoce votre budget dédié à des systèmes de communications fiables – y compris à des systèmes alternatifs et de secours pour remplacer les équipements endommagés, perdus ou volés. En outre, certaines formes de communications telles que la radio et le satellite peuvent nécessiter une licence. Les Nations Unies pourront éventuellement vous aider à obtenir cette licence. Votre organisation devra prévoir un budget pour le temps d'antenne et/ou l'obtention de licences le cas échéant.

Renseignez-vous sur les nouvelles technologies susceptibles d'améliorer de manière rentable vos communications, par exemple les « sacs-à-dos satellite » pour téléphone portable ou les dispositifs de messagerie par satellite, au lieu des téléphones vocaux traditionnels. Investissez dans le meilleur équipement possible pour votre budget.

Mais les organisations doivent aussi tenir compte de l'image que donnent ses équipements de communication. Si la discrétion fait partie de leur stratégie de sécurité, la pose de radios HF et d'antennes sur les véhicules les distingueront autant qu'un logo.

Dans les régions en proie à un conflit ou à des troubles civils, ou bien après une catastrophe naturelle, ne présumez jamais que vous pourrez vous servir d'Internet et des réseaux mobiles. Lors d'urgences sécuritaires ou de catastrophes naturelles, il est fréquent que les gouvernements prennent le contrôle des réseaux (voire les verrouillent) – juste au moment où vous en avez le plus besoin. Il est important de ne jamais se fier à un seul système – réseau fixe, mobile, téléphones satellite, Internet, etc.

Faites preuve de créativité. Dans une situation d'urgence, les ONG recourent à toute une chaîne de chauffeurs de taxi se relayant pour maintenir la communication avec leur personnel lorsque les téléphones ou Internet ne fonctionnent plus, ou utilisent des dromadaires pour transporter des messages et maintenir le contact avec les communautés de zones reculées.



Sécurité et procédures en matière de communications

L'instauration et l'entretien d'un vaste réseau de communications sont essentiels pour la sûreté, la sécurité et la réussite des opérations. Si vous disposez de réseaux radio ou de téléphones satellite, apprenez au personnel à s'en servir pendant leur formation initiale et montrez-leur où utiliser les équipements de communication installés (p. ex. faut-il être dehors pour s'en servir ? Y a-t-il certains endroits où ils ne fonctionneront pas ?). Veillez à ce que les membres du personnel puissent communiquer avec leur famille et leurs amis lors de déploiements, surtout en cas d'urgence.

De plus en plus d'organisations et d'organismes de coordination utilisent WhatsApp et d'autres applications sociales de ce type pour diffuser l'information directement entre membres du personnel. Cela peut être bénéfique car l'information est ainsi partagée en temps réel, mais elle n'est pas vérifiée. Veillez à mettre en place des directives claires sur les informations pouvant être partagées ou non, et des procédures à suivre une fois l'information reçue.

D'une manière générale, il faut discuter avec le personnel de toutes les procédures et directives relatives aux communications. Affichez les procédures écrites, ainsi que les informations sur les contacts en cas d'urgence, y compris les numéros de téléphone, les fréquences et les codes, dans le bureau, à bord de chaque véhicule et sur une carte que les membres du personnel garderont sur eux.

Il est important de tester les systèmes régulièrement et d'avoir des équipements et fournitures de secours pour recharger les radios et les téléphones mobiles et satellite.

Bonnes pratiques :

- Le personnel ne transmet jamais d'informations sensibles – notamment sur le transfert d'argent liquide ou des projets de voyage – en langage clair par radio ou via les réseaux téléphoniques.
- Les équipements de communication, dont les radios, les téléphones cellulaires et satellite, ont l'accord du gouvernement du pays hôte et disposent des licences nécessaires avant d'être utilisés.
- En cas d'utilisation de radios, différentes fréquences VHF et HF sont, si possible, obtenues pour chaque bureau.
- L'utilisation de réseaux radio d'autres organisations – par exemple des Nations Unies – a été coordonnée.
- L'envoi de SMS, d'appels par téléphone satellite ou de vérifications par radio avec des bureaux éloignés et les personnes en déplacement a lieu régulièrement, en fonction des besoins. Il existe des règles pour les cas où un membre du personnel ou une équipe ne se signalerait pas ou ne serait pas joignable. Tout le personnel a connaissance de ces règles, qui sont appliquées de manière systématique.
- Des codes de contrainte (mots ou phrases) ont été choisis pour les conditions d'urgence communes telles que les enlèvements et les intrusions. Leur utilisation a été présentée au personnel.
- Les radios et téléphones d'urgence font l'objet d'une surveillance 24 heures sur 24 si nécessaire.

Sécurité de l'information

Quelle que soit l'image que nous ayons nous-mêmes de notre agence, les organisations humanitaires internationales ne sont plus considérées comme des entités neutres et indépendantes. Elles interviennent, exigent des comptes, défendent certains principes et souvent assument des tâches plus généralement associées aux pouvoirs publics (soins de santé, eau, assainissement, secours d'urgence) et, dans de nombreux cas, tout en étant financées par des gouvernements « occidentaux » avec un agenda politique bien précis. Ainsi, aux yeux d'un grand nombre de personnes, toutes les activités des ONG humanitaires semblent suspectes.

▶ *Voir le document d'information de l'EISF « The future of humanitarian security in fragile contexts: an analysis of transformational factors affecting humanitarian action in the coming decade »*

Les gouvernements ont généralement les moyens de contrôler les appels téléphoniques passés par les organisations, leur activité Internet, leurs communications via Facebook, Twitter et RSS, et de récupérer des informations sur vos disques durs. Les organisations criminelles peuvent aussi estimer que les ONG sont riches étant donné les véhicules, les ordinateurs portables et les téléphones satellite qu'elles utilisent, et les annonces publiques relatives aux niveaux de financement des donateurs. Tout cela expose l'information des agences humanitaires à un risque de sécurité. N'oubliez pas que tout ce que vous écrivez dans un courriel peut être lu par des criminels ou des agents du gouvernement.

▶ *Voir le document d'information de l'EISF « Communications technology and humanitarian delivery: challenges and opportunities for security risk management »*

Réfléchissez aux documents que vous voulez enregistrer sur un lecteur commun. Le personnel d'urgence, qui arrive souvent avec ses propres ordinateurs, copiera tout sur un lecteur commun à son départ, dans un souci de continuité. Parmi les documents copiés, il pourrait se trouver des photos inappropriées, des informations personnelles et des analyses de contexte susceptibles d'être jugées injurieuses par d'autres acteurs ou employés. En outre, faites attention à l'information – professionnelle et personnelle – qui se trouve sur les appareils mobiles, par exemple dans les téléphones portables, qui peuvent facilement être perdus ou volés.

Évaluez l'impact que l'information pourrait avoir si elle parvenait en de mauvaises mains – harcèlement du personnel, diffusion de photos inappropriées, accès aux courriels ou au VPN/serveur du bureau, et ainsi de suite.

Bonnes pratiques :

- Une sauvegarde de tous les fichiers est effectuée régulièrement et les copies de tous les documents et dossiers clés (accords gouvernementaux, documents juridiques, fichiers bancaires, dossiers RH) sont conservées hors site pour les préserver en cas d'incendie, d'inondation, de vol ou de tout autre événement susceptible de détruire les originaux.
- Les documents papier facilitent également les fuites d'information s'ils sont laissés dans une poubelle ou sur un bureau, permettant ainsi aux agents d'entretien, à d'autres membres du personnel ou aux visiteurs de les lire/copier/dérober. Veillez au déchiquetage de tous les fichiers qui ne sont pas gardés en lieu sûr.
- Veillez à doter tous les serveurs de bons systèmes de pare-feu de sécurité et à minimiser l'accès du personnel aux réseaux via des ordinateurs, des

tablettes ou des téléphones n'appartenant pas à l'organisation, ce afin d'éviter de propager des virus.

- Notez que Skype est tout aussi peu sécurisé contre le piratage que les autres modes de communication.
- Ne donnez jamais l'impression de collecter des « renseignements » ou de transmettre des informations militaires ou de sécurité à des gouvernements étrangers (y compris donateurs ou votre siège). De même, le cryptage de l'information peut donner une impression erronée de votre travail. Surtout si votre ONG fait valoir ses qualités d'ouverture et de redevabilité, on risque de vous interroger sur les raisons qui vous poussent à crypter des documents.
- Dans la mesure du possible, évitez les ordinateurs de bureau. Même si les ordinateurs portables sont plus faciles à voler, ils sont aussi plus transportables en cas de relocalisation du bureau ou du projet.
- Envisagez de mettre en place des processus de vérification des informations reçues par WhatsApp et d'autres applications sociales qui facilitent le partage d'informations directement entre membres du personnel. Publiez également des directives claires sur l'information qui peut ainsi être diffusée ou non.
- Veillez à disposer d'un règlement en matière de réseaux sociaux qui indique clairement au personnel ce qu'il peut et ne peut pas publier sur les réseaux sociaux.

▶ *Voir le manuel de l'EISF « Gérer le message : Gestion de la communication et des médias en cas de crise de sécurité »*

Concernant les outils techniques et directifs, « Front Line Defenders » et « Tactical Technology Collective » ont développé le guide *Security in-a-Box* consacré à la sécurité numérique des activistes et des défenseurs des droits humains. Ce guide couvre les principes fondamentaux, et fournit notamment des conseils sur l'utilisation sécurisée des plates-formes de réseaux sociaux et des téléphones portables. Il donne aussi des consignes détaillées sur l'installation et l'utilisation des logiciels et services essentiels en matière de sécurité numérique.