GUIDE DU FACILITATEUR

POUR LE NOUVEAU MANUEL DE PROTECTION POUR LES DÉFENSEURS DES DROITS HUMAINS

MAURICIO ANGEL & ENRIQUE EGUREN (ÉDITEURS)

PROTECTION international

Publié par : Protection International, Rue de la Linière 11, B-1060 Bruxelles, Belgique

ISBN : 978-2-930539-30-0

Éditeurs : Mauricio Angel & Enrique Eguren

Contributeurs : Mauricio Angel, Enrique Eguren, Sylvain Lefebvre, Nora Rehmer

Traducteurs : James Lupton (Anglais), Thomas Lecloux (Français), Valeria Luna (Espagnol)

Mise en page et graphisme : Quidam

Remerciements : Toute l'équipe PI sur le terrain et au siège, et particulièrement Balzac Buzera, Elena Caal, Gitahi Githuku, Ben Kabagambe, Ivy Kihara, Alexandra Loaiza, Luisa Pérez, Tessa de Ryck, Cahya-di Satriya, Bee Pranom Somwong, Ilaria Tosello, Kheetanat Synth Wannaboworn, Arjan Van der Waal & Xabier Zabala.

Bailleurs de fonds : American Jewish World Service ; Instrument Européen pour la Démocratie et les Droits de l'Homme (IEDDH)

Instrument Européen pour la Démocratie et les Droits de l'Homme
IEDDH

AMERICAN JEWISH WORLD SERVICE

TABLE OF CONTENTS

INTRODUCTION AU GUIDE DU FACILITATEUR

Ce Guide du facilitateur a pour but de servir d'instrument de travail aux personnes souhaitant faciliter des processus de formation destinés à développer les capacités de protection des défenseurs des droits humains (DDH), de leurs organisations et de leurs communautés. L'Unité de Politique, de Recherche et de Formation (UPRF) de Protection International (PI) a bénéficié, pour préparer ce Guide, d'un soutien important de la part de ses collègues travaillant au sein des Protection Desks établis dans les différents pays où PI est active. Les Protection Desks ont partagé leurs expériences quotidiennes aux côtés de DDH et d'organisations locales en milieu urbain et rural. Ce guide est également basé sur les concepts-clés du mouvement de l'éducation populaire. Il donne ainsi accès aux facilitateurs à des concepts qui leur permettront de stimuler l'intérêt de leurs participants et de proposer aux DDH une expérience de formation non-hiérarchique et basée sur le partage.

Ce document peut être utilisé dans le cadre du travail de formation réalisé par PI avec les organisations et communautés qu'elle accompagne. Il peut servir de ressource pour dresser un diagnostic des situations auxquelles elles sont confrontées en termes de sécurité. Il contient également des éléments qui les aideront à assurer un suivi et une évaluation de leurs progrès dans la mise en œuvre de leurs plans de sécurité.

Ce Guide du facilitateur contient en outre une série d'éléments et de conseils pouvant être utilisés pour structurer et préparer les sessions pratiques de l'atelier selon la marche à suivre décrite dans le ***Nouveau Manuel de Protection pour Défenseurs des Droits Humains*** (NMP).[1] Le Guide propose différentes façons dont les facilitateurs peuvent transmettre leur savoir en adaptant les éléments-clés du NMP à différents publics-cibles spécifiques. Il est donc conçu pour fonctionner comme une « boîte à outils » hors de laquelle les facilitateurs pourront choisir des éléments à utiliser pour préparer leurs sessions de formation.

Le Guide a au moins six objectifs :

1. **Systématiser les expériences de facilitation de processus de développement de capacités**, en reconnaissant leur complexité et la nécessité d'interventions multiples.
2. Traiter des questions liées à la **diversité des organisations et communautés de DDH partenaires** (les modèles d'apprentissage et les expériences seront différentes pour chaque cas particulier).
3. Proposer aux facilitateurs une **approche pratique, méthodologique et centrée sur les participants**, afin de favoriser l'apprentissage et la compréhension au sein des groupes.
4. Fournir aux facilitateurs les **outils nécessaires pour évaluer les besoins d'apprentissage des participants et les outils de suivi nécessaires pour mesurer les changements** résultant de la formation donnée.
5. Mettre à la disposition des facilitateurs **un matériel et une série de lectures complémentaires** leur permettant de contextualiser la formation qu'ils proposent et d'utiliser activement les expériences des organisations partenaires comme partie intégrante du processus d'apprentissage.
6. Simplifier le contenu du **Nouveau Matériel de Protection des Défenseurs des Droits Humains** rédigé par PI, et aider les facilitateurs à l'utiliser comme ressource de manière efficace.

L'équipe de l'UPRF ne cherche en aucun cas à imposer une approche unique devant être suivie à la lettre. Elle espère au contraire que ce Guide encouragera les facilitateurs à se montrer créatifs face aux principales difficultés qu'ils rencontreront dans leur travail quotidien aux côtés des DDH et des organisations locales.

1 Luis Enrique Eguren et Marie Caraj (2009). Nouveau Manuel de Protection pour Défenseurs des Droits Humains. Protection International. Bruxelles.

LE NOUVEAU MANUEL DE PROTECTION ET LE DÉVELOPPEMENT DE CAPACITÉS DE PROTECTION : FAIRE DES LIENS ET APPRENDRE ENSEMBLE

L'équipe de l'UPRF ne cherche en aucun cas à imposer une approche unique devant être suivie à la lettre. Elle espère au contraire que ce Guide encouragera les facilitateurs à se montrer créatifs face aux principales difficultés qu'ils rencontreront dans leur travail quotidien aux côtés des DDH et des organisations locales.

«La sécurité et la protection sont des domaines complexes. Elles se fondent sur des connaissances factuelles mais dépendent aussi de comportements individuels et du fonctionnement d'une organisation. L'un des messages clé de ce manuel est qu'il faut accorder à la question de la sécurité, le temps et la place qu'elle mérite, en dépit de programmes de travail surchargés, du stress extrême et de la peur qu'endurent tous les défenseurs et leurs organisations. Cela signifie qu'il est nécessaire de passer outre l'expérience individuelle de la sécurité et d'évoluer vers une culture de l'organisation dont la sécurité est inséparable».[2]

PI est bien consciente qu'il n'existe pas de formule magique qui garantisse la protection des DDH, de leurs organisations et de leurs communautés. D'autant plus que chaque DDH est immergé dans un contexte culturel, social et politique qui lui est propre et particulier. En outre, le risque est un facteur changeant. Toute tentative de formuler un plan de sécurité unique applicable à toute situation est donc vouée à l'échec, et il semble extrêmement improbable qu'un texte écrit puisse être applicable entièrement à un groupe de personnes aussi nombreux et aussi divers, regroupant des contextes culturels et politiques aussi différents.

C'est pourquoi il est important de faciliter l'interaction qui se produit au cours des ateliers et des réunions, et de créer des liens entre ce que dit le NMP et les expériences et les besoins rencontrés par les DDH dans la réalité. Cette interaction va dans deux sens, comme on peut aisément se l'imaginer : du facilitateur vers les participants et des participants vers le facilitateur. C'est une interaction qui peut et qui doit mener à un processus d'apprentissage mutuel enrichissant autant pour les facilitateurs que pour les participants.

Ceci explique pourquoi nous considérons ce Guide comme un travail en cours, sujet à des améliorations, à des changements et à des développements. Les commentaires transmis par les personnes qui l'utiliseront seront fondamentaux dans cette optique, car ils nous permettront d'enrichir ce document disponible en permanence sur internet. Nous tenterons de l'améliorer constamment en y ajoutant des éléments complémentaires dès que possible. Autrement dit, ce Guide du facilitateur se trouve entre vos mains expertes.

2 Ibid. pp. 13.

LES PROCESSUS D'APPRENTISSAGE ET LE DÉVELOPPEMENT DE CAPACITÉS

Ce chapitre est consacré aux trois fondements conceptuels du processus d'apprentissage de la gestion de sécurité pour les DDH : **l'éducation populaire**, **les méthodologies d'apprentissage pour adultes** et le **développement de capacités**. Son but est de guider les facilitateurs en leur suggérant comment favoriser au mieux la compréhension du concept de sécurité chez les participants lors des différentes réunions, rencontres et sessions de formations auxquelles ils prendront part.they will be involved in.

L'ÉDUCATION POPULAIRE

L'éducation populaire désigne une approche socio-pédagogique de l'éducation émancipatrice, ou **une éducation à la conscience critique** [1], La majeure partie du contenu de ce Guide du facilitateur s'en inspire. Bien que les méthodes et techniques d'apprentissage employées soient similaires à celles utilisées dans la méthodologie d'apprentissage pour adultes (**voir Section «Les méthodologies d'apprentissage pour adultes» ci-dessous**), l'éducation populaire cherche à construire une approche éducationnelle alternative qui soit cohérente en matière de droits, d'émancipation et de justice sociale. L'éducation populaire est dite populaire parce qu'elle travaille en priorité avec les populations pauvres en milieu rural et urbain, qui se situent majoritairement dans les pays du Sud. Il s'agit d'un effort collectif d'éducation au cours duquel les enseignants et les élèves apprennent ensemble. Le processus se divise en trois parties centrées successivement sur : (a) **les expériences concrètes des participants**, (b) **une réflexion sur ces expériences** qui mène à, (c) **l'identification d'actions visant à provoquer un changement positif.**

L'éducation populaire est née dans les années 60 avec les programmes d'alphabétisation de l'éducateur et philosophe brésilien Paulo Freire. Il apprenait à ses élèves à lire et à écrire en discutant avec eux des problèmes de base qu'ils rencontraient dans leur vie, comme par exemple le manque d'accès à des terres agraires. En voyant apparaître plus clairement les causes de leurs problèmes, les élèves analysaient et discutaient des actions conjointes qu'ils pourraient entreprendre pour changer leur situation.

Freire a forgé le terme de **« conscientisation »** pour décrire le **processus d'action-réflexion-action**, qui a permis aux participants non seulement d'apprendre à lire et à écrire, mais aussi de comprendre leur propre réalité.

L'éducation populaire suit certains principes, qui ont été appliqués dans ce Guide :

- → Le point de départ est **l'expérience concrète de l'individu DDH**.
- → **Tout le monde enseigne, tout le monde apprend**.
- → **Un degré élevé de participation** est donc nécessaire.
- → Cela mène à des **actions visant le changement**: dans ce cas-ci, la promotion d'une plus grande sécurité dans le travail de défense des droits humains.
- → C'est un **effort collectif**, qui recherche des solutions partagées plutôt qu'individuelles aux problèmes, de la même manière que l'action de défendre les droits humains est généralement collective.

1 Ce chapitre a été conçu sur base de l'ouvrage de Rick Arnold et Bev Burke, «A Popular Education Handbook» (voir **http://www.popednews.org/downloads/A_Popular_Education_Handbook.pdf**) et du site internet **http://www.practicingfreedom.org/offerings/popular-education**. Les personnes souhaitant explorer plus en profondeur le thème de l'éducation populaire peuvent lire l'ouvrage fondateur de Freire, «Pedagogy of the Oppressed».

- Cette approche privilégie la **création de connaissances nouvelles adaptées à la situation**, plutôt que l'application de connaissances existantes à de nouveaux scénarios : les plans de sécurité et leur mise en pratique doivent être créés et maîtrisés par les défenseurs, plutôt que d'être adaptés sur base de «recettes» préexistantes.
- C'est un **processus continu** qui peut être mené à n'importe quel moment et en n'importe quel endroit : ce Guide s'inspire d'une vision du développement de capacités qui considère que la sécurité et la protection des DDH supposent une notion de parcours.

QUEL EST LE RÔLE DU FACILITATEUR EN TANT QU'ÉDUCATEUR POPULAIRE EN PROTECTION ?

Le rôle du facilitateur en éducation populaire diffère radicalement en au moins quatre points de celui d'un enseignant dans le système d'éducation conventionnel:

- **L'autorité partagée :** tout le monde enseigne et tout le monde apprend.
- **La construction conjointe de connaissances :** le point de départ est l'expérience préalable des participants.
- **L'absence d'un « expert » :** elle est comblée par un respect mutuel pour les connaissances et l'expérience que tous les participants apportent au processus.
- **Le travail main dans la main :** les facilitateurs aident les participants à acquérir des idées et des compétences pour agir, tout en s'engageant eux-mêmes à agir.

Il faut cependant garder à l'esprit que les facilitateurs ne sont pas des participants et que le processus d'apprentissage est loin d'être spontané. Le rôle du facilitateur est de faire en sorte que le processus (ce qui se produit et comment cela se produit) favorise l'apprentissage et le développement de capacités de leadership dans le groupe. La manière de discuter d'une activité est importante, car la façon dont une technique est décodée est cruciale pour l'apprentissage du groupe. Les facilitateurs doivent comprendre les besoins que les participants sont susceptibles d'avoir, ainsi que leurs perceptions des problèmes de sécurité auxquels ils ont été confrontés dans le passé. Ils doivent avoir eux-mêmes une bonne connaissance de la situation, de manière à pouvoir aider les participants à la changer. La manière dont ce processus sera mené déterminera le rôle que pourront jouer les DDH dans le modelage progressif du contenu et de la forme du programme en cours de route.

THÉORIE ET PRATIQUE : PLUS QU'UNE SIMPLE MÉTHODOLOGIE !

L'éducation populaire cherche à pénétrer au cœur des questions du pouvoir et du privilège. Il arrive souvent (mais pas toujours) que les facilitateurs bénéficient d'un certain nombre d'avantages par rapport aux DDH participant aux ateliers (le fait d'être une personne extérieure, d'être un « expert », etc.). Dans ce cas, les facilitateurs doivent établir un langage et un cadre commun avec les participants, que ce soit par le biais d'un dialogue, de présentations ou d'exercices interactifs. Ils doivent créer un environnement qui permette aux participants d'être entendus et de pouvoir explorer des pistes d'action, de manière à ce que chaque membre de l'organisation (ou de la communauté) ait un rôle à jouer : en élaborant des mesures de protection, en assurant la sécurité et en prenant véritablement possession du processus.

LES MÉTHODOLOGIES D'APPRENTISSAGE : COMMENT LES ADULTES APPRENNENT

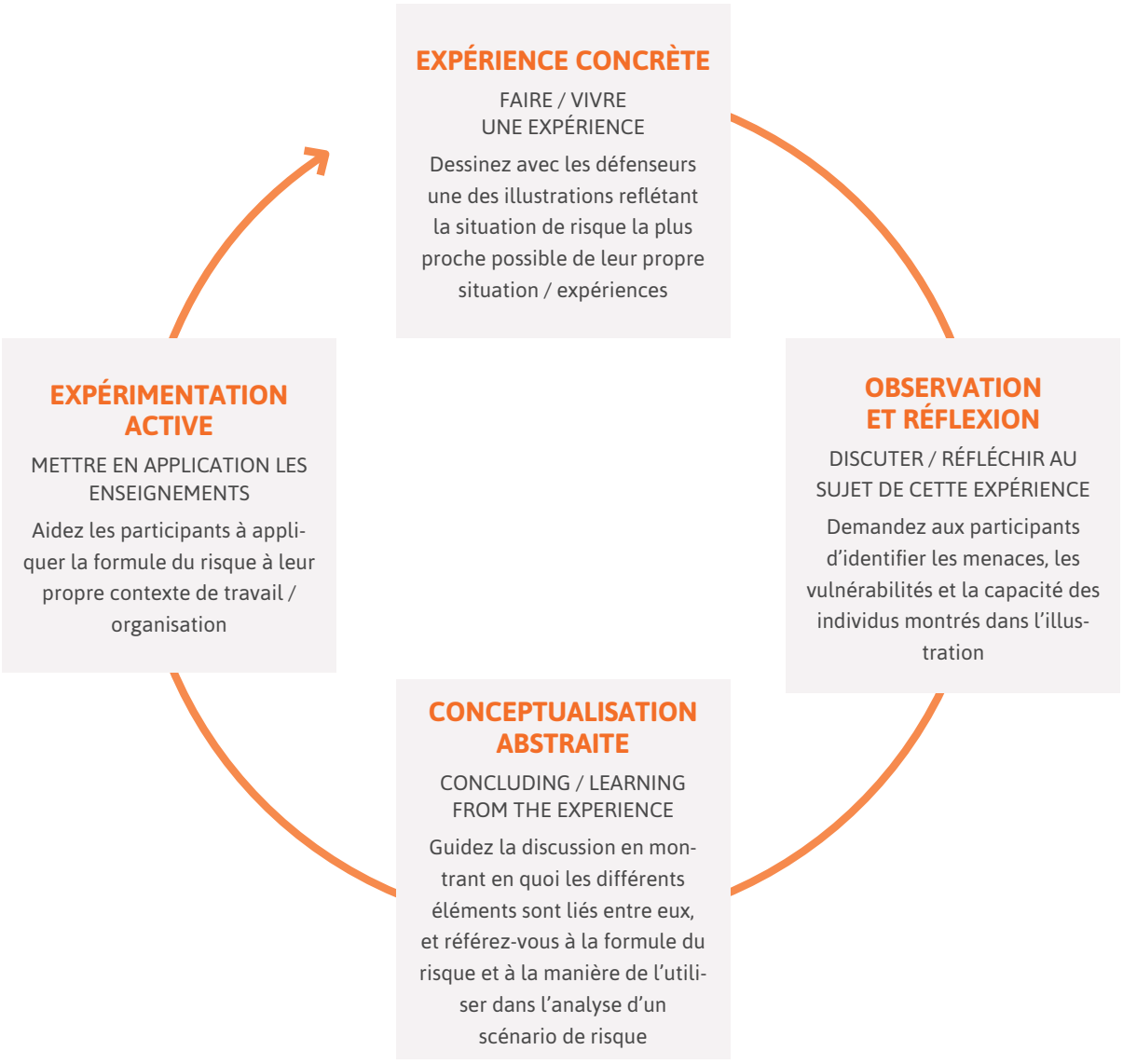
POURQUOI NOUS APPRENONS

Lors de la planification d'un processus d'apprentissage, il est essentiel pour les facilitateurs de comprendre ce qui motive les gens à apprendre. En premier lieu, c'est un **besoin** ; pour les individus, les organisations, les communautés ou les réseaux actifs dans la défense des droits humains ayant été confrontés à des incidents de sécurité graves, à des menaces, ou même à des agressions, la motiva-

tion à apprendre est évidente. Ils veulent améliorer leur niveau de sécurité et réduire les risques qu'ils encourent. Cet aspect sera examiné au cours de la **phase d'évaluation** expliquée dans le chapitre suivant. D'autres facteurs cruciaux apportant une motivation à apprendre sont la **pertinence** de l'enseignement et les **bénéfices** ressentis. En d'autres termes, les participants doivent comprendre que les outils de gestion de la sécurité sont utiles à l'amélioration de la situation actuelle. L'amélioration de la capacité à gérer les questions de sécurité sera directement bénéfique au niveau individuel et au niveau de l'organisation. S'ils veulent que leur travail ait un réel impact, les facilitateurs doivent donc stimuler activement ces facteurs et y répondre, tant pendant la durée de la phase des **ateliers** que pendant celle de **suivi**.

COMMENT NOUS APPRENONS

Les facilitateurs doivent trouver le moyen de structurer les nouvelles informations qu'ils veulent transmettre en s'appuyant le plus efficacement possible sur ce que les participants savent déjà. Pour ce faire, ils peuvent se baser sur les différentes étapes du cycle d'apprentissage par l'expérience décrit par David Kolb. [2] L'illustration suivante montre comment les facilitateurs peuvent aider les participants à acquérir un savoir nouveau à partir d'une expérience concrète.



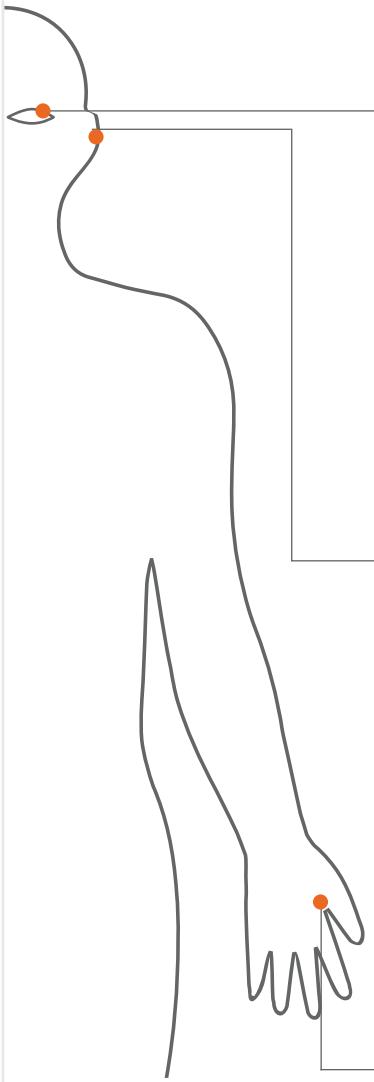
2 Kold, D & Fry. R. (1975). « Vers une théorie appliquée de l'apprentissage par l'expérience ». Dans C. Cooper (Ed.). Theories of Group Process. Londres. John Wiley. L'apprentissage par l'expérience a depuis été développé plus en profondeur et commenté largement. De nombreuses informations sur ce thème sont disponibles sur internet.

Pour renforcer les nouvelles idées et les nouvelles connaissances acquises par les participants, les facilitateurs doivent régulièrement faire référence aux autres éléments appris tout au long de la formation, en montrant comment les différents aspects sont liés entre eux et s'appuient les uns sur les autres. Il sera tout aussi utile au cours des sessions suivantes de s'appuyer sur les exercices précédents et d'utiliser les résultats des travaux, des exercices et de débats précédents.

COMMENT TOUCHER CHAQUE ÉTUDIANT

L'être humain apprend tout au long de sa vie. Les adultes en cours d'apprentissage peuvent compter sur un grand nombre de connaissances et d'expériences. En s'appuyant consciemment sur ces acquis, les facilitateurs pourront favoriser et approfondir l'apprentissage. Il est important de savoir que les gens apprennent de façons différentes. Chaque personne a sa manière la plus efficace d'absorber et d'assimiler de nouvelles informations.

Une manière simple de trouver le style d'apprentissage préféré d'une personne est d'identifier le(s) sens au(x)quel(s) cette personne fait appel pour assimiler des informations nouvelles:



STYLE D'APPRENTISSAGE & sens associé	ACTIVITÉS FAVORISANT L'APPRENTISSAGE
VISUEL la vue	• Images, graphiques, tableaux, lecture, écriture. • Les personnes qui apprennent visuellement prennent souvent des notes pendant les sessions et ont des difficultés à assimiler les informations importantes sur un thème donné rien qu'en écoutant. • Pour s'adapter efficacement à ce style d'apprentissage, les facilitateurs peuvent proposer les informations sous forme d'images ou d'illustrations, donner des instructions sur paper-board ou sur papier, dessiner les concepts et les processus, ou encore reprendre les points-clés de la discussion sur paper-board. Les personnes qui apprennent visuellement seront particulièrement réceptives aux vidéos.
AUDITIF l'ouïe	• Les personnes qui apprennent par l'audition ont souvent des difficultés à comprendre les cartes et les tableaux. • Pour travailler efficacement avec ces personnes, les facilitateurs doivent donner des explications et des instructions claires, prévoir assez de temps pour la discussion, et utiliser des enregistrements audio et/ou vidéo comme matériel d'enseignement. • Rappeler les enseignements-clés permet d'approfondir l'apprentissage
KINESTHÉSIQUE le toucher (les mouvements du corps)	• Les personnes qui apprennent de manière kinesthésique apprennent par l'expérience. • Les facilitateurs peuvent élaborer des exercices pratiques pour amener les participants à tester, appliquer ou développer eux-mêmes le savoir appris, de préférence en groupes. • L'apprentissage peut être favorisé en donnant aux participants des tâches actives, comme par exemple illustrer les enseignements-clés.

Les participants utiliseront certainement tous leurs organes sensoriels pendant une session de formation, mais un de ces sens sera généralement dominant. En outre, il est fort probable que tous les styles d'apprentissage soient représentés au sein d'un groupe de participants. La difficulté pour les facilitateurs sera de s'adresser à chacun d'entre eux et d'éviter de se concentrer sur le style qui leur est le plus proche.

Plus les sessions seront interactives, plus elles seront stimulantes pour les participants et leurs différents styles d'apprentissage.

Les principes suivants peuvent aider les facilitateurs à s'adresser de manière efficace aux trois styles d'apprentissage pendant leurs sessions[3]:

3 AI SPA 2013, Collectif Barefoot (2011). « Élaborer des activités d'apprentissage créatives et les rendre simples » : Un manuel d'accompagnement au Guide Barefoot sur les pratiques d'apprentissage dans les organisations et sur le changement social. Voir: http://www.barefootguide.org/designing-and-facilitating-creative-learning-activities.html

LE GROUPE CIBLE

Les DDH sont des personnes très engagées dont le travail repose sur des connaissances et sur des expériences personnelles. Ils évoluent au sein de réseaux complexes, et développent leur activisme en tentant de décrypter leur environnement. Ils ont une compréhension unique de la structure et du mode de fonctionnement de leur communauté, et ils sont capables de détecter et d'influencer les dynamiques politiques et sociales.

Les facilitateurs devront relever le défi (ou saisir l'opportunité) d'arriver à reconnaître et à utiliser les nombreuses ressources que chaque participant apportera à la session de formation, de manière à :

> **Favoriser et approfondir l'apprentissage au niveau individuel ;**

> **Encourager chacun à apprendre et à se nourrir des expériences des autres.**

Quand les facilitateurs reconnaissent qu'ils ne sont pas la seule source de savoir dans la formation, il se crée généralement une atmosphère d'échange où tout le monde apprend l'un de l'autre, ce qui permet d'acquérir de nouvelles connaissances et de les replacer dans le contexte de travail local des participants.[4]

→ **Il est conseillé aux facilitateurs de concevoir leurs sessions de formation d'une manière adaptée aux modes d'apprentissage naturels des adultes. La capacité d'une personne à acquérir de nouvelles connaissances et à améliorer sa pratique est déterminée notamment par son attitude face à l'apprentissage. Aidez les participants à adopter une attitude positive, et vous faciliterez le processus d'apprentissage.[5]**

→ **Prévoyez régulièrement des moments dédiés à la pratique et au partage d'expériences.**

→ **Soyez conscient de l'existence des différents styles d'apprentissage. Cela vous aidera à trouver des méthodes pour assurer la participation active de tous les participants dans leur formation.**

→ **Contextualisez les nouvelles informations : reliez-les à ce que les participants savent déjà et expliquez-en les bénéfices et la pertinence pour les participants. Cela motivera les participants.**

→ **Répéter les enseignements précédents et y faire référence régulièrement permet de renforcer l'apprentissage.**

4 Hammond, Linda-Darling, K. Austin, S. Orcutt, J. Rosso (2001). How People Learn, Introduction to Learning Theories. Stanford University School of Education. Voir: http://www.stanford.edu/class/ed269/hplintrochapter.pdf

5 Ibid.

LE DÉVELOPPEMENT DE CAPACITÉS DE PROTECTION EST TOUJOURS UN TRAVAIL À PLUSIEURS VISAGES

De nos jours, le libre exercice du droit à défendre les droits humains est reconnu internationalement. Cependant, il arrive fréquemment que ceux et celles qui travaillent comme défenseurs des droits humains (DDH) rencontrent une opposition de la part des autorités ou d'autres acteurs de la société. Et en de trop nombreuses occasions, cette opposition prend la forme d'une répression : les DDH sont menacés, stigmatisés et criminalisés. Ils subissent des agressions physiques et sont même la cible d'assassinats.

Voilà pourquoi ce Guide du Facilitateur est consacré à la question du développement des capacités des DDH à assurer eux-mêmes leur sécurité et leur protection. Ce Guide a pour objectif d'apporter une réflexion structurée sur cette question en répertoriant différentes manières dont les DDH peuvent travailler conjointement, au sein d'une organisation ou d'une communauté, afin d'améliorer leurs niveaux de protection.

QUE SONT LES CAPACITÉS DE PROTECTION ?

Le terme «capacités de protection» désigne l'aptitude des DDH, des organisations sociales et des communautés à poursuivre leur travail en faveur des droits humains de manière sécurisée et durable, même lorsqu'ils sont confrontés à des menaces ou sont cibles d'agressions en raison de leur action pour les droits humains.

Les capacités de protection sont aussi une affaire de pouvoir : «le pouvoir de…», «le pouvoir de faire…». Il s'agit en fait d'augmenter le pouvoir qu'ont les DDH de prendre des décisions lorsqu'ils se trouvent face à des choix, et le pouvoir de prendre ces décisions en toute sécurité.

EST-IL POSSIBLE DE DÉFINIR CE QUE SIGNIFIE LE DÉVELOPPEMENT DES CAPACITÉS DE PROTECTION ?

Le développement des capacités de protection se base sur la conviction que tout individu, toute organisation et toute communauté possède certaines capacités lui permettant de faire face aux menaces ou aux actes d'agression. Il est cependant souvent nécessaire de développer et d'améliorer ces capacités, particulièrement lorsque les risques encourus au quotidien sont élevés. Ces capacités peuvent être développées directement par les personnes affectées, mais un soutien externe est souvent utile pour les aider à mener à bien ce processus.

Personne ne nait «complètement formé», c'est-à-dire prêt, dans sa vie normale, à faire face à des menaces de mort ou à des agressions physiques directes. C'est pourquoi nous disons que les personnes qui défendent les droits humains sont des personnes ordinaires confrontées à des situations extraordinaires.

La construction de capacités de protection est en grande partie un processus collectif et organisationnel. C'est clairement le cas pour les organisations de la société civile, que ce soit en milieu urbain ou rural, mais c'est également vrai pour les individus, car les humains apprennent les uns des autres et au contact les uns des autres personnes.

Voilà pourquoi nous parlons du développement de capacités de protection à plusieurs niveaux :

- → **Au niveau individuel :** les capacités de protection de chacun;
- → **Au niveau organisationnel, ou communautaire :** les capacités de protection d'une organisation ou d'une communauté; et
- → **Au niveau inter-organisationnel, ou intercommunautaire :** les capacités de protection des réseaux et alliances d'organisations et ou de communautés.

Les personnes intéressées par le travail de facilitation du développement de capacités de protection doivent comprendre trois facteurs particulièrement importants, et s'assurer de les comprendre entièrement :

- → **La manière dont une organisation ou une communauté envisage son contexte et ses objectifs;**
- → **La manière dont cette organisation ou cette communauté envisage et interprète les risques auxquels elle est confrontée en raison de son action de défense des droits humains;** et
- → **La stratégie ou les stratégies de protection qu'il est possible de mettre en pratique.**

COMMENT DÉVELOPPE-T-ON DES CAPACITÉS ?

Il convient de suivre une série d'étapes logiques lors du développement des capacités de protection: elles forment un processus répétitif au cours duquel l'apprentissage se fait par la réflexion et par l'action:

- → **Réflexion :** Analyser quelles capacités sont requises pour arriver à la protection dans différents contextes et face à différents risques, et comprendre les capacités déjà existantes.
- → **Action :** Elaborer et mettre en œuvre un plan de protection et évaluer ses résultats en permanence, afin de pouvoir le modifier en fonction des besoins nouveaux et des résultats obtenus.
- → **Réflexion :** Analyser les résultats des actions menées et décider quelles capacités doivent être développées ou quelles actions sont nécessaires afin d'améliorer les niveaux de protection.

Etc.

Il est néanmoins important que le facilitateur garde toujours à l'esprit les points suivants:

- → **Un processus répétitif ne veut pas nécessairement dire un processus «ordonné» (voir plus bas);**
- → **On ne peut en aucun cas supposer que tout ce qui est fait est adéquat, ou que toute pratique est systématiquement le produit d'une réflexion. Et même lorsque la réflexion a bien lieu, elle n'est pas toujours orientée de manière correcte. En d'autres termes : la pratique peut toujours être améliorée par le biais de la réflexion.**

En résumé, l'apprentissage individuel ou collectif nécessite des moments-clés d'analyse et de réflexion, qui peuvent soit être internes soit avoir lieu avec le soutien d'autres.

C'est pourquoi ce Guide du facilitateur envisage le développement des capacités comme un processus, et pourquoi les moments d'analyse et de réflexion sont clés dans ce processus.

A quoi ressemblent ces moments d'analyse et de réflexion? Ils peuvent prendre de nombreuses formes. Pour simplifier, citons les deux formes qui nous semblent les plus importantes:

- → Les « **ateliers de protection** » , et
- → Les « **réunions** » qui, d'une manière ou d'une autre, traitent de protection.

Pour illustrer notre propos, envisageons ces moments de réflexion comme des défrichages dans une forêt de travail, de commentaires, d'échanges, de complicités, d'incertitudes, de peurs et d'activités spécifiques des DDH qui, s'ils veulent développer leurs capacités de protection, doivent faire le choix de se livrer à ces moments de réflexion.

Il arrive qu'une organisation décide d'améliorer sa capacité à se protéger en organisant un atelier de protection. Mais il arrive également qu'une communauté subisse un problème de sécurité et qu'en réponse, elle décide d'affronter le problème immédiatement, pour ensuite éventuellement organiser un atelier avec l'assistance de personnes extérieures dont elle espère qu'elles pourront améliorer ses capacités de protection. Il arrive aussi qu'une organisation soit victime d'incidents de sécurité répétés, et que ses membres organisent une réunion après chaque incident, mais restent incapables de traduire leurs réflexions en actions. En d'autres termes, une organisation peut se trouver engagée dans une séquence fragmentaire de réunions ordonnées ou désordonnées, ainsi que dans des ateliers (certains planifiés et d'autres improvisés quand le besoin ou l'opportunité se présente) pouvant avoir lieu en période calme ou en période de stress et de crainte. Voilà le contexte compliqué au cœur duquel il faut développer les capacités de protection.

L'IMPORTANCE DU POINT DE VUE ET DES CONNAISSANCES TIRÉES DE L'EXPÉRIENCE DE CHAQUE DÉFENSEUR

Le développement de capacités dépend grandement des expériences et des contextes de travail qui ont marqué le développement des individus et des groupes, car c'est en fonction de ceux-ci que chacun construit sa vision du monde. Il est important que nous comprenions que tout ce que les individus font est imprégné d'un sens qui découle de leurs expériences. C'est-à-dire que leurs actions peuvent s'expliquer en fonction de leur histoire personnelle : «voilà ce qui (m')arrive et voilà pourquoi j'agis de telle manière». Dans une situation à risque, il est impossible de séparer la gestion de la protection de la gestion de la vie quotidienne. On ne peut pas non plus espérer des individus qu'ils envisagent de manière rationnelle les risques auxquels ils sont confrontés, même s'ils sont capables d'être rationnels dans leur manière d'examiner et de comprendre toutes les informations qui leur sont disponibles.

En conséquence, il est impossible d'imposer une logique de sécurité externe à l'histoire personnelle d'un DDH. Selon ce point de vue, il ne peut pas exister d'analyse de risque **objective** (elle sera nécessairement **subjective**); il est très difficile d'arriver à une approche externe «globale» sur la question de la protection ; et ceux qui sont capables d'arriver à cette vision «holistique» de la protection ne seront pas capables d'avoir une perspective contextualisée et ancrée culturellement sur la question des DDH. Les DDH ont une compréhension partielle des choses, mais une compréhension qui est néanmoins profondément enracinée dans leur réalité. Et c'est dans cet enracinement qu'ils construisent leur protection, d'une manière fragmentaire mais cohérente.

Les facilitateurs externes doivent donc axer leur point de vue personnel subjectif dans la même direction que celui des DDH, de manière à pouvoir appréhender et comprendre leur point de vue à eux. A partir de là, il est possible de dégager les éléments communs aux deux perspectives, et de commencer à marcher ensemble sur le même chemin.

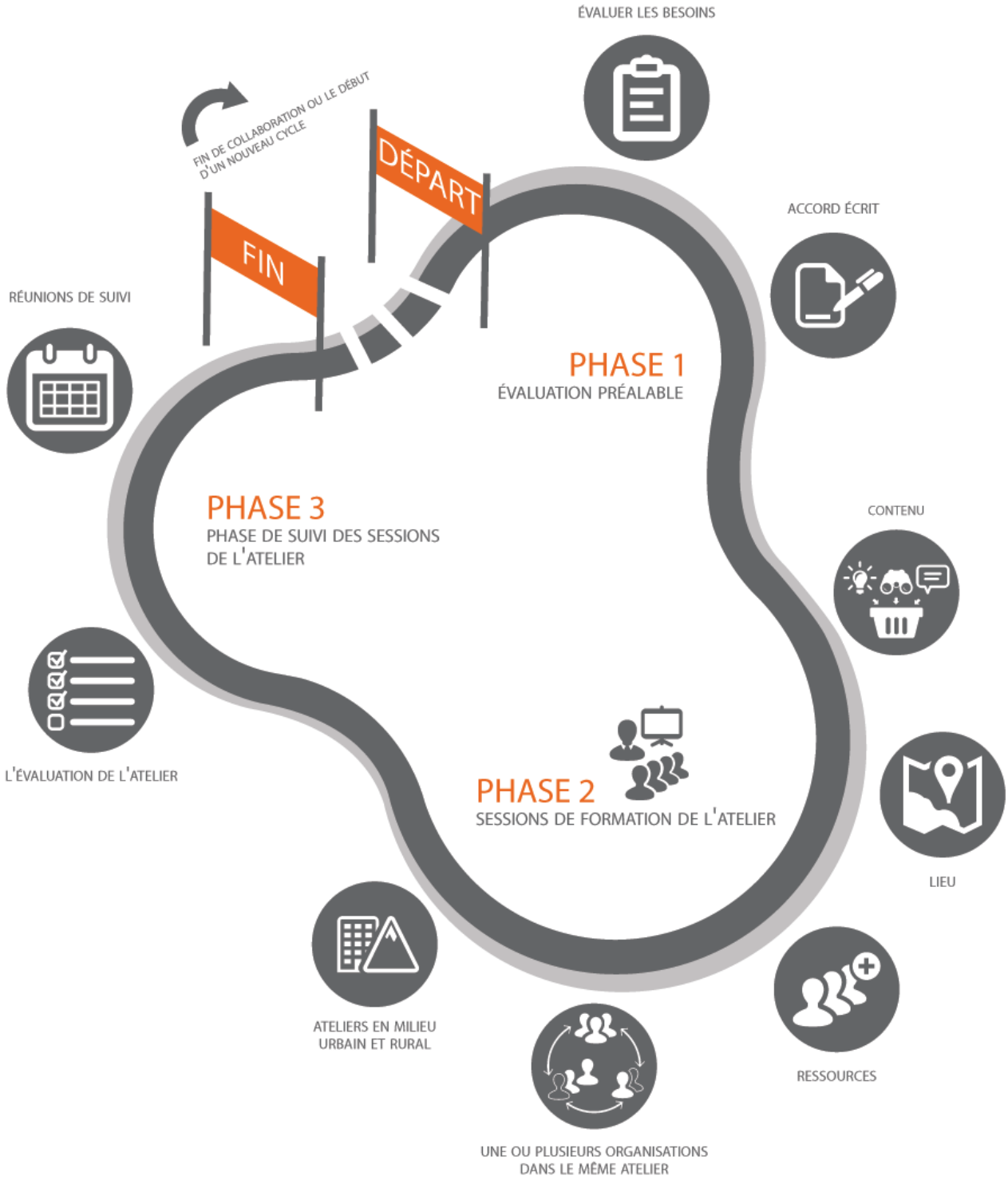
En d'autres termes, ce Guide du Facilitateur invite ses lecteurs à abandonner l'idée selon laquelle le développement de capacités de protection serait «linéaire», ou qu'il pourrait être obtenu au cours d'un ou deux ateliers dont les «leçons» seraient «applicables immédiatement». Bien au contraire, ce Guide propose une vision du développement de capacités comme étant un processus inscrit dans un contexte et dans une culture donnés, un processus qui suit une route changeante et complexe, sujette à de multiples influences et interactions. Allons donc à la rencontre les uns des autres sur ce chemin.

ALLER ENSEMBLE VERS LA PROTECTION : RÉUNIONS ET ATELIERS DE FORMATION

> NOTE : LES CHAPITRES DU NMP CORRESPONDANT À CETTE SECTION SONT LES CHAPITRES 2.1, 2.2 ET 2.3. FAMILIARISEZ-VOUS AVEC CEUX-CI AVANT DE LIRE ET D'APPLIQUER CETTE PARTIE DU GUIDE DU FACILITATEUR

Pour aider les facilitateurs à interagir de manière efficace avec les défenseurs des droits humains, leurs organisations et leurs communautés, le développement de capacités peut être conçu comme un parcours, comme l'illustre le graphique ci-dessous.

PARCOURS DU DÉVELOPPEMENT DE CAPACITÉS



Comme nous l'avons indiqué dans le chapitre précédent, le développement de capacités de protection est un processus d'apprentissage mutuel impliquant un certain nombre d'échanges avec les organisations et les communautés partenaires. Au cours de ces échanges, tant les participants que les facilitateurs vivent des « moments d'apprentissage » de réflexion et d'action. Le but est d'atteindre ensemble une série d'objectifs décidés préalablement et dont l'objectif est d'améliorer les capacités de gestion de sécurité du partenaire tout en lui permettant de continuer à travailler. Le processus (ou cycle) commence par une phase d'**évaluation**, suivie par des sessions d'**atelier** consacrées à la gestion de sécurité, puis par une phase de **suivi** comprenant l'adoption et la mise en œuvre de plans de sécurité, et enfin par une nouvelle phase d'évaluation (où en sommes nous maintenant?) lors de laquelle il sera décidé des étapes suivantes à entreprendre.

PHASE 1 - ÉVALUATION PRÉALABLE

La phase d'évaluation permet au facilitateur et à l'organisation ou la communauté de DDH partenaire de travailler ensemble pour identifier les attentes et les besoins des participants, les capacités et les compétences du facilitateur, les résultats espérés du plan d'amélioration de la sécurité, et les ressources nécessaires pour diriger l'atelier et pour mener à bien le processus général.

Cette première étape permet également au facilitateur et à l'organisation ou communauté partenaire d'établir les **objectifs** et les **priorités** pour la première partie du parcours, ainsi que de concevoir le contenu et le calendrier de l'atelier initial et des sessions consacrées au suivi.

ÉVALUER LES BESOINS

Les facilitateurs doivent réaliser une évaluation de la façon dont l'organisation/communauté partenaire traite les questions de sécurité, de manière à identifier ses besoins spécifiques et à définir le contenu et la structure de l'atelier de développement de capacités. Cette évaluation doit être faite en accord avec la direction de l'organisation ou le leader de la communauté partenaire. Il faut également évaluer les capacités et les vulnérabilités.

AVEC QUI TRAVAILLER :

Lorsque c'est possible, les facilitateurs doivent tenter d'organiser la première réunion d'évaluation avec la direction ou les leaders de l'organisation/communauté partenaire, ou avec le point de contact désigné pour les questions de sécurité. Il est important que les facilitateurs arrivent à mieux comprendre les attitudes des décideurs vis-à-vis du processus de développement de capacités. Généralement, ceux-ci auront eux-mêmes la capacité et la volonté de promouvoir un changement organisationnel. Dans certains cas, en revanche, l'initiative émanera d'autres parties de l'organisation ou de la communauté. Il sera difficile d'établir des objectifs réalistes et d'atteindre des résultats durables au terme du processus si la direction ou les leaders partenaires ne montrent que peu d'intérêt pour la gestion de la sécurité, s'ils ne participent au programme que par obligation bureaucratique, ou si le point de contact pour les questions de sécurité n'a que peu ou pas d'influence sur la prise de décision.

S'il est crucial d'obtenir l'engagement de la direction ou des leaders partenaires pour parvenir à un changement organisationnel, il est également possible que les membres du personnel soient amenés à changer leurs comportements (p.e. par rapport à l'analyse de risque, à l'évaluation des menaces et des incidents de sécurité, ou à leurs idées concernant la sécurité pendant les temps libres). Il est donc important que toutes les personnes affectées par le processus y participent. Les facilitateurs doivent rappeler aux partenaires que la sécurité est l'affaire de tous!

On ne peut trop insister sur l'importance de définir les objectifs de l'intervention de développement de capacités conjointement avec l'organisation ou communauté partenaire. A ce stade, le but premier est de s'accorder sur des objectifs réalistes qui répondent aux besoins, aux caractéristiques et aux ressources (financières et humaines) de l'organisation/communauté partenaire et des DDH qui constituent ses membres. Les sessions de formation de l'atelier doivent être adaptées à la culture, à la mémoire et aux caractéristiques du partenaire, ainsi qu'au contexte dans lequel il évolue. C'est pourquoi il est important d'identifier les raisons pour lesquelles l'organisation/communauté a demandé à participer à un atelier.

Plusieurs raisons peuvent motiver une organisation ou une communauté à participer à un atelier de sécurité : le souhait de réaliser une évaluation de ses capacités de gestion de sécurité ; la volonté d'apprendre comment évaluer et gérer la sécurité ; ou la volonté d'apprendre comment faire face aux problèmes de sécurité dans son travail quotidien (les évaluer et en assurer un suivi). L'expérience nous montre que **cette volonté est souvent liée à une situation concrète ou à des incidents de sécurité réels touchant l'organisation**. Ces situations, qu'elles concernent des menaces directes ou indirectes, des e-mails ou un site internet piratés, ou le simple fait d'être confronté à des risques, amènent souvent les organisations à repenser les questions de sécurité et la manière dont elles les gèrent. Un des principaux objectifs de l'intervention de développement de capacités est donc de faire face à ces situations concrètes de sécurité.

Il est également crucial d'identifier les besoins de l'organisation ou de la communauté au niveau des problèmes et des pratiques de sécurité, car ce sont ces besoins qui détermineront les objectifs spécifiques du processus. Cette analyse doit être réalisée avec les directeurs/leaders. Il est cependant possible - mais peu probable - que ces personnes ne soient pas au courant de la réalité et du travail quotidien des membres du personnel. Dans ce cas, les facilitateurs pourront décider d'intégrer une partie dédiée à l'évaluation dans le cycle de l'atelier. Ceci présentera l'avantage d'inclure les visions de tous les membres du personnel, et non pas uniquement celles de la direction, dès le début du processus. Une telle approche peut en outre renforcer la motivation et le degré d'engagement de tous les participants vis-à-vis des objectifs de l'atelier. De nombreuses organisations insistent sur l'importance d'établir des relations de travail horizontales pour favoriser la confiance et la cohésion. Il faut cependant être conscient que cela prend du temps. Au bout du compte, la méthode choisie dépendra de l'objectif global de l'atelier et du temps disponible. Chacune des deux approches possibles pour l'identification initiale des objectifs présente des avantages et des inconvénients.

Reportez-vous au formulaire «**RÉvaluation des risques et gestion de sécurité pour défenseurs des droits humains**» en **Annexe 1 de ce chapitre**. Ce document donne aux facilitateurs des recommandations de base qui les aideront à diriger la réunion d'évaluation avec les organisations et communautés partenaires. Les réponses aux questions du formulaire peuvent donner une idée du large spectre de risques auxquels sont confrontés les organisations et communautés partenaires. Les facilitateurs ont pour tâche de les aider à développer leur capacité à gérer ces risques.

ACCORD ÉCRIT

Comme nous l'avons déjà indiqué, le développement de capacités de protection et de sécurité est un processus nécessitant un engagement sérieux de la part de l'organisation/communauté partenaire en vue d'amener les changements nécessaires à l'amélioration de la protection des DDH. De leur côté, les facilitateurs doivent partager leurs connaissances et leur expérience en matière de sécurité et de protection, et accompagner les partenaires dans l'élaboration de plans de sécurité et pendant la phase de suivi de leur application.

Ces engagements doivent être inscrits dans un accord écrit (ou mémorandum d'entente) signé par les deux parties. Cet accord sert de point de départ pour le processus de contrôle et d'évaluation, et servira au bout du compte à juger du succès du processus. Voir le formulaire « **Accord sur le développement de capacités de gestion de sécurité** » en **Annexe 2 de ce chapitre**.

PHASE 2 - SESSIONS DE FORMATION DE L'ATELIER

Les sessions de l'atelier sont des réunions structurées pour le développement de capacités. Leur but de sensibiliser les DDH participant à l'atelier aux questions de sécurité et de protection, et de leur transmettre des connaissances et des compétences. D'autre part, les ateliers sont basés sur les principes de l'éducation populaire, ce qui permet aux facilitateurs d'apprendre de l'expérience des participants.

CONTENU

Le succès d'un atelier de développement de capacités de sécurité et de protection est proportionnel à la mesure dans laquelle il répond aux besoins des participants. Par exemple, si une organisation possède d'excellentes compétences d'analyse de contexte, le facilitateur pourra décider de sauter la section consacrée à l'évaluation de l'environnement pour passer directement à l'équation du risque. Le facilitateur a également la liberté de modifier l'ordre dans lequel sont traités les différents thèmes dans le **Nouveau Manuel de Protection** et dans le Guide du facilitateur pour mieux s'adapter aux besoins des organisations et communautés avec lesquelles il travaille. Le facilitateur doit cependant veiller à ce que chaque session s'appuie sur ce qui a été vu précédemment, de manière à préserver la pertinence et la cohérence de l'atelier.

CONSEILS POUR LES SESSIONS DE L'ATELIER

- → **Durée estimée:** l'expérience nous montre que les sessions de sensibilisation peuvent durer entre 2 et 6 heures, et les sessions de formation entre 2 et 3 jours. Mais en fin de compte la durée des ateliers dépendra des objectifs conclus et du contenu à traiter.
- → **Composition du groupe de participants:** encore une fois, il n'y a pas de critères fixes. Mais les facilitateurs doivent encourager les organisations/communautés à trouver un équilibre entre le nombre de directeurs/leaders et le nombre de membres du personnel. Ceci s'applique également aux sessions de formation comprenant plusieurs organisations ou communautés.

LIEU

Une fois le contenu défini, il faut trouver un accord sur le lieu où sera organisé l'atelier. Deux éléments doivent être pris en compte pour le choix du lieu: l'**espace disponible** et la **ssécurité des participants**. Le local doit être assez spacieux pour que les participants se sentent à l'aise et puissent réaliser les activités d'apprentissage, notamment les travaux de groupes et les jeux de rôles. Le lieu de l'atelier doit se trouver dans un endroit où les participants et les facilitateurs se sentent en sécurité, pour que l'atelier puisse se dérouler dans aucune inquiétude et dans une atmosphère de confiance.

Les ateliers en milieu rural peuvent avoir lieu dans des bâtiments communautaires utilisés habituellement pour organiser des réunions. Pour les organisations en milieux urbains, en revanche, il sera plus pratique d'organiser l'atelier dans leurs bureaux. L'avantage du bureau est d'être un endroit familier où les gens se sentent habituellement en sécurité. De plus, cela n'entraîne aucun coût financier supplémentaire. Ce choix comporte toutefois certains inconvénients, particulièrement quand les bureaux sont réduits, quand les participants sont distraits par leurs ordinateurs et continuent de s'occuper de leur travail, ou quand il n'y a pas d'endroit sûr et discret pour organiser les sessions (par exemple si les bureaux sont partagés entre plusieurs organisations ou s'ils reçoivent fréquemment des visiteurs). Dans ces cas-là, il sera préférable d'organiser l'atelier dans un lieu extérieur, comme une salle de conférence ou le bureau d'une autre organisation de confiance. Il est à noter qu'un changement de lieu peut contribuer à créer une nouvelle dynamique en brisant la routine quotidienne associée au lieu de travail. Les facilitateurs doivent bien entendu tenir compte des risques spécifiques liés au fait d'organiser un atelier dans un local externe.

RESSOURCES

Idéalement, les sessions ne doivent pas compter plus de 20 participants. S'il y a plus de 30 participants, les facilitateurs peuvent suggérer aux organisations/communautés partenaires de travailler en groupes plus restreints, et réunir ensuite toute l'assemblée pour des comptes-rendus et des discussions.

Un seul facilitateur peut mener les sessions, mais il peut être avantageux de travailler à deux pour améliorer la dynamique de l'atelier. Deux facilitateurs travaillant ensemble peuvent partager les responsabilités (mener différentes sessions, prendre des notes, etc.) et amener une diversité de points de vue et d'expériences à l'atelier. S'ils travaillent avec un collègue, les facilitateurs doivent préparer et répéter à l'avance le contenu des sessions et des activités d'apprentissage.

Les activités et les exercices de l'atelier doivent être adaptés à la réalité et au contexte culturel des participants. Ceci est également valable pour les objectifs, la structure et le calendrier. Pour cette raison, les facilitateurs doivent se renseigner à l'avance sur le domaine des droits humains dans lequel les participants travaillent, sur leur niveau d'éducation, sur leur âge, sur leur sexe et sur leurs origines (si cela se justifie). Les facilitateurs doivent donc éviter d'utiliser les mêmes méthodes d'apprentissage partout : un groupe de DDH composé d'avocats et d'assistants juridiques sera peut-être réceptif à des concepts abstraits et à une approche académique avec des présentations sur PowerPoint, tandis qu'un groupe composé de paysans ayant un faible niveau d'éducation scolaire sera plus sensible à une méthode visuelle et ancrée dans un contexte (voir le chapitre 2 sur l'apprentissage des adultes). Quel que soit leur milieu d'origine, les participants ne démarrent jamais de zéro. Même s'ils n'utilisent pas les concepts du manuel de sécurité, ils doivent avoir des idées concernant la sécurité et la protection. **La difficulté pour les facilitateurs est de relier ces expériences concrètes aux concepts de sécurité et de protection**.

UNE OU PLUSIEURS ORGANISATIONS DANS LE MÊME ATELIER

Les méthodes et outils utilisés pour réaliser les ateliers diffèrent selon que les facilitateurs travaillent avec une ou plusieurs organisations. Les objectifs du processus de formation peuvent être affectés par un certain nombre de problèmes liés aux différentes identités des organisations partenaires et aux contextes dans lesquels elles travaillent.

Quand tous les participants sont issus d'une même organisation ou communauté, le facilitateur peut tirer parti du fait de travailler avec un **groupe homogène** dont les attentes et les intérêts en matière de sécurité sont communs, et qui partage les mêmes menaces, les mêmes vulnérabilités et les mêmes capacités. Le facilitateur peut alors choisir des exemples et des exercices tirés de leur propre expérience. Les activités et les exercices réalisés formeront alors la base du plan de sécurité que l'organisation ou la communauté devra élaborer, ce qui permettra d'accélérer le processus de développement de capacités.

Quand le **groupe est hétérogène** c'est-à-dire que les participants sont issus d'organisations différentes, d'autres difficultés se présentent pour le facilitateur, notamment celles de définir des objectifs communs, de gérer les différentes attentes des participants, etc. Les participants peuvent également avoir des inquiétudes différentes par rapport à leur sécurité, ils peuvent être confrontés à des menaces différentes et ne pas avoir les mêmes vulnérabilités et capacités. La confidentialité des informations peut également former une difficulté. Certaines organisations ne souhaitent pas partager des informations internes, ce qui peut ralentir le processus. Les facilitateurs devront dans ce cas générer une dynamique de groupe qui favorise la compréhension commune, tout en canalisant la diversité. Il sera tout aussi important d'installer la confiance dès le début du processus. Vous trouverez dans les annexes de ce Guide une série d'idées d'activités pouvant servir à bâtir cette confiance. Ces activités peuvent être adaptées en fonction des différents contextes.

Malgré ces difficultés, les ateliers regroupant plusieurs organisations différentes peuvent aussi présenter des avantages. La diversité des participants et l'opportunité pour eux de partager leurs expériences enrichissent et dynamisent souvent le processus. Chaque organisation évoluant dans un contexte différent amènera sa propre identité, sa propre culture et ses propres idées sur les questions de sécurité. Cette diversité permet aux participants de partager leur expérience. Chaque organisation bénéficiera à son tour de cette diversité, ce qui créera un processus d'apprentissage mutuel. Il est même possible que ces processus donnent naissance à des réseaux ou à des accord de solidarité et de soutien mutuel.

MOTIVATION DES PARTICIPANTS

Tant au niveau individuel qu'au niveau de l'organisation, et quels que soient les objectifs de l'atelier, le processus est voué à l'échec si les participants n'ont pas la motivation nécessaire pour prendre les questions de sécurité au sérieux. Ce facteur dépend en partie de la capacité du facilitateur à mobiliser les participants autour d'objectifs communs et à encourager leur participation active. Il est tout aussi important que les facilitateurs puissent détecter les éventuels signes précoces de désengagement ou de manque de motivation, et qu'ils en discutent avec la direction, les leaders ou la personne de contact désignée afin que des mesures correctives puissent être prises. Les facilitateurs peuvent utiliser le « Cahier de bord personnel » proposé en **Annexe 3 de ce chapitre** comme un guide pour aider les participants à tirer le maximum de chaque session de formation.

ATELIERS EN MILIEU URBAIN ET RURAL

Les besoins en termes de technologie diffèrent entre milieux urbains ou ruraux, de la même manière que les environnements de travail des organisations ou communautés partenaires. Dans les zones rurales reculées en particulier, les facilitateurs doivent essayer d'être auto-suffisants, c'est-à-dire d'utiliser un paper-board, des marqueurs et d'autres outils similaires plutôt qu'un ordinateur portable et un projecteur [1]. Mais les facilitateurs doivent surtout se montrer créatifs et utiliser le matériel qu'ils trouvent autour d'eux. Ils doivent également imprimer les informations données et les résultats d'ateliers précédents pour en distribuer des copies aux organisations et communautés partenaires.

Dans les milieux urbains et dans les zones rurales disposant d'infrastructures et de services publics appropriés, les facilitateurs pourront recourir davantage à la technologie (ordinateurs portables, projecteurs, connexions internet). Ils doivent cependant être préparés à organiser l'atelier sans l'aide de ces outils, au cas où ceux-ci ne fonctionneraient pas ou au cas où les facilitateurs penseraient que les participants seraient plus réceptifs à une manière plus traditionnelle d'organiser les sessions. Les facilitateurs peuvent également fournir des copies électroniques des résultats de l'atelier.

Dans tous les cas, les facilitateurs doivent se renseigner préalablement sur les moyens technologiques disponibles dans le local où est donné l'atelier, et se préparer en conséquence. Il faut cependant garder à l'esprit que ce sont avant tout les échanges face-à-face et les activités conjointes qui donnent toute leur utilité aux ateliers.

1 Facilitators can use a laptop for note-taking purposes if it has enough battery power or there are adequate power sources; care should be taken to ensure data protection and encryption when travelling to remote areas.

La distinction entre contexte urbain et rural est bien prise en compte dans ce Guide et dans les activités d'apprentissage qu'il propose. Lorsque c'est nécessaire, ces activités sont donc adaptées à l'un ou l'autre de ces contextes. Ce qui est applicable à des organisations urbaines ne le sera peut-être pas pour des communautés rurales, et vice-versa. Il peut par exemple sembler inadapté de concevoir un plan de sécurité formel pour une communauté paysanne. Au lieu de cela, les facilitateurs préféreront se concentrer sur l'élaboration de mesures et de stratégies de protection concrètes qui pourront ensuite être mises en pratique dans les activités quotidiennes de la communauté. Les méthodes employées peuvent aussi être différentes. Les sections du Guide concernées par cette question précisent si les activités d'apprentissage sont destinées à être appliquées aux deux contextes ou à un seul.

La distinction entre ateliers ruraux et urbains a aussi d'autres implications au niveau du contenu. Il est bien plus important pour les organisations et les communautés rurales d'agir de manière conjointe et collective, et c'est la raison pour laquelle ce Guide met l'accent sur les ateliers des **réseaux de protection destinés aux communautés rurales**. Cette décision a été prise sur base de plusieurs années d'expérience de terrain auprès de communautés et d'organisations locales en zones rurales. Ces groupes sont confrontés à d'énormes difficultés pour assurer leur protection collective face aux menaces et aux risques résultant de leur travail pour la défense de leurs droits économiques, sociaux et culturels, y compris le droit au territoire où ils vivent et travaillent.[2]

Les DDH opèrent en effet au sein de contextes socio-institutionnels relativement complexes. Ils interagissent avec d'autres organisations locales, des ONG, des acteurs non-étatiques et des institutions publiques. Tous ces acteurs peuvent opérer simultanément au niveau local, régional, national et/ou international. Ce réseau de relations entre acteurs internes et externes peut donc contribuer à générer une capacité d'action collective (c'est-à-dire la protection des membres de la communauté et la défense du territoire).

PENDANT LES SESSIONS CONSACRÉES AUX RÉSEAUX DE PROTECTION, LES FACILITATEURS DOIVENT :

- → **Informer les communautés quant aux avantages qu'offre un réseau, notamment pour les aider à avoir accès ou à mobiliser des ressources (internes et externes) et pour générer une protection (pour les membres individuels et pour la collectivité).**
- → **Proposer des outils qui aident les communautés à mieux comprendre la question du territoire et la manière dont elles fonctionnent en tant que groupe.**
- → **Améliorer les capacités de la communauté à défendre son territoire.**
- → **Renforcer la capacité du mouvement de DDH à poursuivre son travail de défense des droits humains.**

Les facilitateurs trouveront des informations supplémentaires sur les réseaux de protection pour les communautés rurales dans le chapitre 5.8 de ce Guide.

2 PI réalise en ce moment une étude sur les réseaux de protection communautaires. Ce travail se base sur les expériences en cours avec des communautés rurales du Guatemala et d'autres pays où PI possède des bureaux de protection locaux. Les résultats de ce projet sont attendus pour la fin de l'année 2014 et sont destinés à servir de base d'informations pour améliorer les pratiques actuelles et les stratégies de protection des DDH opérant au sein de communautés.

CE QUI FAIT LE SUCCÈS D'UN ATELIER :

- L'engagement de la direction de l'organisation et/ou des leaders de la communauté.
- Une préparation faite conjointement avec l'organisation participante.
- Une connaissance des questions liées à sécurité, tant au niveau de l'institution qu'au niveau de l'individu.
- La qualité, la diversité et le dynamisme de la méthodologie (vidéos, cartes, jeux de rôles, etc.) et le partage de l'expérience du facilitateur pour favoriser la compréhension des situations.
- Un contenu adapté aux attentes et aux expériences des participants.
- La présence, si possible, de deux facilitateurs pour diriger l'atelier.
- Des activités et des exercices adaptés au contexte.
- Un plan de sécurité contenant des objectifs clairs et réalistes. (Il est préférable d'avoir un plan de sécurité simple adapté aux besoins plutôt qu'un plan ambitieux qui ne sera pas appliqué).
- Des résultats concrets pour les participants.
- Un lieu approprié.

PHASE 3 - PHASE DE SUIVI DES SESSIONS DE L'ATELIER

Pour des thèmes complexes comme la gestion de la sécurité d'une organisation ou d'une communauté, des ateliers de formation uniques sont rarement utiles. Pour que le processus de développement de capacités contribue de manière efficace à créer un changement et obtienne des résultats durables, il faut assurer un suivi des sessions de formation de l'atelier, une fois celles-ci terminées. Au cours de cette troisième phase, les facilitateurs et les partenaires doivent se rencontrer plusieurs fois, et éventuellement même organiser une suite à la formation si le besoin s'en fait sentir. Comme au cours des phases précédentes, la période de suivi doit être organisée conjointement avec la direction de l'organisation ou les leaders de la communauté ayant reçu la formation. C'est pourquoi **il est important d'inclure dans l'accord écrit conclu au début du processus un engagement de l'organisation à réaliser les activités de suivi**. Ceci étant dit, il n'y a aucune restriction à organiser des rencontres en-dehors de l'accord initial si le partenaire en fait la demande ou si une opportunité se présente. Par exemple, si l'organisation partenaire appelle le facilitateur pour lui demander conseil à la suite d'un incident de sécurité récent.

Il n'y a pas de limite au nombre de réunions de suivi que les organisations et les facilitateurs peuvent organiser, mais leur nombre dépendra principalement de contraintes horaires et budgétaires. D'autre part, il est important de trouver le bon équilibre entre le besoin de guidance de la part du facilitateur et la capacité à gérer son propre plan de sécurité. Malgré ces considérations, l'expérience nous montre qu'une phase de suivi réussie doit se dérouler en trois étapes.

La première étape est **l'évaluation de l'atelier** par l'organisation partenaire, qui est chargée de donner une appréciation de la qualité de la formation et de la performance des facilitateurs en regard de ses propres attentes. Cette étape doit avoir lieu immédiatement après l'atelier ou dans les quelques jours suivants, pour que les détails soient toujours frais dans l'esprit des participants. L'évaluation doit aussi aider les facilitateurs à parfaire la pertinence des ateliers. Le «**Formulaire d'évaluation de l'atelier**» figurant en Annexe 4 de ce chapitre peut servir de modèle pour cette évaluation.

La seconde étape concerne les **réunions de suivi**. TCes réunions doivent être organisées régulièrement (tous les mois ou tous les deux mois) pendant une période donnée (de six mois à deux ans selon les circonstances) et doivent permettre d'évaluer la mise en pratique du plan et des mesures de sécurité élaborées pendant les sessions de l'atelier. Elles donnent l'opportunité aux facilitateurs de

résoudre les problèmes et d'aider les partenaires à surmonter les obstacles qu'ils peuvent rencontrer en cours de route. Dans les **Annexes 5 de ce chapitre**, les facilitateurs trouveront un tableau intitulé « **Réunions mensuelles de suivi** » conçu pour les aider à structurer leur dialogue avec la direction de l'organisation ou les leaders de la communauté partenaire. Il est très important que les partenaires comprennent que cette étape n'est pas une évaluation de leurs progrès ou de leur manque de progrès dans l'application du plan de sécurité, mais qu'elle concerne en premier lieu les besoins et les barrières qu'ils peuvent rencontrer. Les réunions constituent aussi des occasions d'apprendre de l'expérience des facilitateurs (p.e. « ceci est arrivé à d'autres organisations, est-ce arrivé à la vôtre ? », etc.). Sur ce thème, voyez également le chapitre 2.3 du NMP au sujet des barrières et des processus organisationnels. L'expérience nous montre que trop souvent, le travail d'élaboration d'un plan de sécurité est perçu comme onéreux et intimidant par les membres des organisations ou communautés partenaires, alors qu'en réalité ce n'est pas le cas. Les facilitateurs doivent être clairs sur ce point, tout en rappelant cependant aux organisations et communautés qu'il n'y a pas de recette miracle, et certainement pas de plan de sécurité prêt-à-l'emploi qu'elles pourraient utiliser.

La troisième et dernière étape concerne la **fin de la collaboration ou le début d'un nouveau cycle**. L'étape précédente fournit la base pour évaluer ce qui doit être fait ensuite. En fonction du stade atteint par l'organisation/communauté concernant l'adoption du plan et le niveau d'engagement interne, les facilitateurs pourront décider de mettre un terme à la collaboration, de commencer un nouveau cycle, ou de creuser plus en détail sur des thèmes particuliers. Le «**Formulaire d'évaluation final**» figurant en **Annexe 6 de ce chapitre** peut être utilisé comme guide à cet effet.

ANNEXE 1

ÉVALUATION PRÉALABLE

> ÉVALUATION DE RISQUES ET GESTION DE SÉCURITÉ POUR DÉFENSEURS DES DROITS HUMAINS

A COMPLÉTER PAR LE FACILITATEUR EN CONSULTANTATION AVEC LE DDH/L'ORGANISATION/LA COMMUNAUTÉ PARTENAIRE

NOM DE LA PERSONNE EN CHARGE DE L'ÉVALUATION:

DATE ET LIEU:

PERSONNE INTERROGÉE (ET POSITION DANS SON ORGANISATION):

Note pour les facilitateurs: veuillez prendre en compte que certaines organisations ne souhaiteront pas consigner par écrit toutes les informations demandées dans ce formulaire pour des raisons de sécurité. Si tel est le cas, il faudra leur donner l'assurance que les données communiquées seront conservées en sécurité.

A. PROFIL

1. Nom du DDH, de l'organisation ou du réseau ; coordonnées et adresse.

2. Pour les organisations et les réseaux, indiquez le type d'organisation :

- ☐ ONG locale / organisation basée dans une communauté
- ☐ ONG nationale
- ☐ ONG internationale
- ☐ Institution nationale (p.e. Commission nationale des droits humains, Bureau de l'ombudsman)
- ☐ Institution académique ou de recherche
- ☐ Gouvernement
- ☐ Indépendant (attaché à aucune institution ou organisation)
- ☐ Autre (spécifiez)

3. Le participant a-t-il un (ou plusieurs) bureau(x) ?

- ☐ Oui
- ☐ Non

4. Nombre de bureaux (y compris les branches), lieu (pays et ville) et nombre de personnes employées.

5. Veuillez indiquer les principaux groupes-cibles avec/pour lesquels travaille le défenseur, l'organisation ou le réseau :

- ☐ Défenseurs des droits humains
- ☐ Populations indigènes
- ☐ Médias
- ☐ Travailleurs migrants
- ☐ Décideurs politiques
- ☐ Police, armée ou forces de sécurité
- ☐ Déplacés internes, réfugiés, immigrés
- ☐ Femmes
- ☐ Prisonniers
- ☐ Minorités sexuelles
- ☐ Autres (spécifiez)

6. Veuillez indiquer les principaux thèmes liés aux droits humains traités actuellement par le défenseur, l'organisation ou le réseau :

- ☐ Liberté d'information/d'expression
- ☐ Liberté de vivre à l'abri de la torture
- ☐ Droits liés au travail
- ☐ Accès à la Justice (procès équitables, arrestations arbitraires, etc.)
- ☐ Droits des minorités: ☐ Religieuses ☐ Ethniques ☐ Autres
- ☐ Droits des réfugiés
- ☐ Droits des défenseurs des droits humains
- ☐ Droits des femmes
- ☐ Droits de l'enfant
- ☐ Bonne gouvernance
- ☐ Droits économiques, sociaux et culturels
- ☐ Autres (spécifiez)

7. Indiquez les principales activités réalisées (maximum 3) :

- ☐ Recherche
- ☐ Formation
- ☐ Publications
- ☐ Développement communautaire
- ☐ Résolution de conflits
- ☐ Éducation aux droits humains
- ☐ Campagnes anti-corruption
- ☐ Journalisme
- ☐ Plaidoyer
- ☐ Surveillance
- ☐ Aide juridique
- ☐ Autres

B. INFORMATIONS CONTEXTUELLES

1. Quelles sont les principales violations des droits humains commises dans la zone/communauté concernée?

2. Quels sont les principaux facteurs contribuant à ces violations ?

3. Qui sont les principaux auteurs de violations des droits humains dans la zone/communauté concernée ?

4. En quoi le travail du défenseur affecte-t-il ces personnes ?

5. Comment les participants ont-ils réagi au travail des DDH ?

6. Votre travail a-t-il des implications différentes pour les femmes et les hommes ? Si oui, en quoi ?

C. PRATIQUES ACTUELLES DU DDH, DE L'ORGANISATION OU DU RÉSEAU EN MATIÈRE DE GESTION DE LA SÉCURITÉ

1. Quels sont les risques qu'ils encourent en raison de leur travail en faveur des droits humains (pensez également à l'information et la communication) ? Pourquoi ?

2. Les participants ont-ils connu des incidents de sécurité liés à leur travail qui ont mis en péril leur sécurité ? Si oui, veuillez décrire ces incidents (Quand est-ce arrivé ? Qu'est-ce qui est arrivé ? Qui était impliqué ?)

3. Le DDH, l'organisation ou la communauté analyse-t-elle les incidents individuellement ou (dans le cas des organisations et des réseaux) conjointement ?

4. Quelles sont les mesures de sécurité appliquées actuellement ? A quels risques ces mesures répondent-elles ?

5. L'organisation planifie-t-elle activement sa sécurité ? Si oui, comment ?

D. GESTION DES OPÉRATIONS INFORMATIQUES PAR L'ORGANISATION/RÉSEAU/DÉFENSEUR.

1. Comment les ordinateurs sont-ils utilisés ? (ordinateurs fixes, ordinateurs portables, tablettes, etc.)

2. Des incidents de sécurité informatiques ont-ils eu lieu (e-mails ou site internet piratés, vols d'ordinateurs ciblés, etc.) ?

3. Le défenseur, l'organisation ou la communauté peut-elle compter sur un soutien en matière de technologies de l'information ? Si oui, de la part de qui ?

4. Que font les participants actuellement pour protéger les données informatiques ?

5. Comment les téléphones sont-ils utilisés pour des tâches liées au travail (e-mails professionnels lus par téléphone, etc.).

E. ASPECTS DE BIEN-ÊTRE À PRENDRE EN COMPTE PAR LE FACILITATEUR PENDANT L'ÉVALUATION

1. Sur base des informations fournies ci-dessus, pourrait-il y avoir des cas de traumatismes résultant d'événements ou d'expériences qui auraient eu un impact important sur le bien-être des membres du personnel ? (p.e. une attaque physique subie en raison du travail comme DDH, avoir été témoin d'actes violents commis contre d'autres personnes, etc.)

2. Les DDH ont-ils parlé d'incidents de sécurité ou d'attaques subies dans le passé ayant entraîné un niveau de risque élevé susceptible de créer un état de nervosité parmi le personnel ?

3. Y a-t-il des indications d'une charge de travail élevée pouvant avoir un impact sur le bien-être physique et émotionnel en termes de stress et de fatigue ?

4. La politique et la pratique de l'organisation prennent-elles en compte le bien-être des employés (vacances annuelles, congés pour récupérer des heures supplémentaires ou du travail fait le week-end, services de soutien tels qu'une aide psychologique (obligatoire ou sur demande), etc.) ?

5. Quelle est l'atmosphère générale parmi les membres du personnel ? Permettrait-elle une discussion ouverte sur le stress et la peur au sein du personnel ?

6. La direction soutient-elle l'idée d'inclure la question du bien-être dans le processus de développement de capacités ?

F. MOTIVATION ET ENGAGEMENT

1. Quelle est votre motivation à participer à un processus de développement de capacités centré sur la gestion de la sécurité ?

2. Réfléchissez aux éventuelles initiatives de développement de capacités auxquelles vous auriez déjà participé. Considérant uniquement celles qui ont eu du succès : quels sont les facteurs qui ont contribué à la réussite du processus de changement organisationnel ?

3. Quel changement souhaitez-vous voir comme résultat de votre participation à ce processus de développement de capacités - tant au niveau individuel qu'au niveau de l'organisation ?

4. Qui doit être impliqué pour que ce changement ait lieu ?

G. QUI DOIT ÊTRE IMPLIQUÉ POUR QUE CE CHANGEMENT AIT LIEU ?

1. Combien de personnes participeront-elles à l'atelier ?

2. Quelle est la composition du groupe de participants ? (direction/leaders, personnel/membres)

3. Combien de jours l'atelier va-t-il durer ?

4. Où va-t-il avoir lieu ? Quel est le matériel technique disponible ?

5. Quels doivent être les objectifs de l'atelier ?

H. AUTRES

Veuillez indiquer ici tout autre commentaire, remarque ou question :

ANNEXE 2

MÉMORANDUM D'ENTENTE

> OU ACCORD POUR LE DÉVELOPPEMENT DE CAPACITÉS DE GESTION DE LA SÉCURITÉ

TO BE COMPLETED BY THE FACILITATOR IN CONSULTATION WITH THE HRD/ORGANISATION/COMMUNITY

ACCORDS CONCLUS AVEC LE PARTENAIRE

NOM DU RÉSEAU, DE L'ORGANISATION OU DE LA COMMUNAUTÉ:

DATE:

FACILITATEUR:

PERSONNEL DE COORDINATION OU DE DIRECTION:

POINT DE CONTACT POUR LES QUESTIONS DE SÉCURITÉ:

PERSONNE(S) DE CONTACT:

ACCORDS:

RESPONSABILITÉS PRISES POUR ASSURER LE RESPECT DES ACCORDS (DÉTAILS CI-DESSOUS):

DÉLAIS D'APPLICATION:

EXEMPLES D'INDICATEURS DE PROGRÈS

(Il doit s'agir ici d'étapes concrètes correspondant à la profondeur et à la complexité du changement souhaité. Elles doivent répondre aux questions «Qui fait quoi comment?»)

Note : ces exemples sont appropriés à un hypothétique atelier en milieu urbain et n'ont ici qu'une valeur d'exemple.

1. Les résultats suivants sont attendus: il s'agit d'actions facilement réalisables, comme par exemple participer à un atelier. (Entre 4 et 8 indicateurs)

1. Tous les membres de l'organisation participent aux ateliers d'analyse de risques et de plan de sécurité.
2. La direction et les points de contact pour les questions de sécurité participeront aux réunions de suivi.
3. Toute personne devant utiliser des outils de sécurité informatiques participera aux sessions qui y sont consacrées.
4. Tous les membres de l'organisation participent à l'évaluation globale de la performance de l'organisation en matière de sécurité.
5. Les personnes ayant besoin de conseils concernant un cas spécifique ont participé à une réunion au cours de laquelle elles ont pu être conseillées.
6. Les membres de l'organisation participent à l'analyse du contexte institutionnel.

...

2. Les résultats suivants sont souhaités: il s'agit ici d'actions indiquant un apprentissage plus actif ou un engagement plus important. (Entre 8 et 12 indicateurs).

1. Les membres de l'organisation sont conscients de la nécessité de se doter d'un plan de sécurité et des mesures qu'il contient.
2. Tous les membres de l'organisation rapportent les incidents de sécurité au bon endroit (le cahier des incidents ou le point de contact pour les questions de sécurité).
3. Les membres de l'organisation formulent des propositions pour améliorer le plan et corriger ses points faibles.
4. Les membres de l'organisation appliquent en moyenne 50 % du plan de sécurité et des mesures qu'il contient.
5. Les membres de la direction de l'organisation et le point de contact pour les questions de sécurité analysent les incidents de sécurité et évaluent les menaces, les vulnérabilités et les capacités qui y sont associées.
6. Les membres de la direction de l'organisation (ou le point de contact pour les questions se sécurité) informent le reste de l'organisation des résultats de l'analyse des incidents et recueillent les impressions et les contributions de chacun.
7. Les membres de la direction de l'organisation et les points de contact pour les questions de sécurité préparent des protocoles établissant les actions à entreprendre en cas de situation d'urgence.

...

3. Les résultats suivants sont idéaux: ces actions indiquent une réelle transformation et une réalisation maximale des objectifs. Il est possible qu'elles prennent plus de temps que qui est prévu dans le programme pour se mettre en place. (Entre 3 et 6 indicateurs)

1. L'ensemble du plan de sécurité est appliqué entièrement par tous les membres de l'organisation.
2. Les membres de la direction de l'organisation et les points de contact pour les questions de sécurité possèdent toutes les informations nécessaires sur les risques ; ils les analysent, créent des protocoles ou des mesures pour y réagir, et les présentent au reste de l'organisation pour accord ; ils s'assurent également que les analyses de contexte et de risque sont bien réalisées et que les plans de sécurité sont bien préparés régulièrement.
3. L'organisation gère le risque de manière autonome, elle n'a besoin de conseils ou de formation qu'en résultat de ses propres analyses.

...

EXAMPLES OF PROGRESS INDICATORS

1. **Les résultats suivants sont attendus:** il s'agit d'actions facilement réalisables, comme par exemple participer à un atelier. (Entre 4 et 8 indicateurs)

2. **Les résultats suivants sont souhaités:** il s'agit ici d'actions indiquant un apprentissage plus actif ou un engagement plus important. (Entre 8 et 12 indicateurs).

3. Les résultats suivants sont idéaux: ces actions indiquent une réelle transformation et une réalisation maximale des objectifs. Il est possible qu'elles prennent plus de temps que qui est prévu dans le programme pour se mettre en place. (Entre 3 et 6 indicateurs)

SUIVI

Le facilitateur et le partenaire s'accordent sur la date et la forme des activités de suivi et des réunions à venir.

Signature de la personne responsable (approuvé).

ANNEXE 3

CAHIER DE BORD PERSONNEL

> TIRER LE MAXIMUM D'UN PROCESSUS DE FORMATION:

UN CAHIER DE BORD PERSONNEL EST UN OUTIL PERMETTANT AUX PARTICIPANTS D'AVOIR UNE RÉFLEXION (INDIVIDUELLE OU COLLECTIVE) SUR UN PROCESSUS D'APPRENTISSAGE OU DE DÉVELOPPEMENT DE CAPACITÉS

Vous trouverez le cahier de bord sur la page suivante. Imprimez-en une copie pour chaque participant, avec un nombre de pages égal au nombre de jours de la formation. Expliquez la fonction du cahier de bord aux participants dès le premier jour de la formation. Prévoyez du temps à la fin de chaque journée ou pendant la matinée suivante pour que les participants puissent le compléter. Les informations contenues dans les cahiers de bord restent en possession des participants.

Il arrive souvent lors d'un processus ou d'un atelier de formation que les participants aient de nombreuses expériences d'apprentissage différentes. Celles-ci ont tendance à se mélanger et donc à s'effacer. Cela peut se produire assez rapidement. Nous avons constaté qu'à mi-parcours d'une formation, la plupart des personnes ont des difficultés à se souvenir exactement de ce qu'elles ont appris au cours des premiers jours.

Ce cahier de bord personnel vous aidera à bénéficier au maximum de l'expérience de formation. Vous pourrez y noter les messages les plus importants de chaque journée. Au terme de chaque journée de formation (ou le matin suivant), vous disposerez de 10 à 15 minutes pour réfléchir aux activités du jour (ou du jour précédent) et pour noter les enseignements que vous avez jugé les plus importants.

A la fin de la formation, ce document vous servira de résumé de ce que vous avez appris et ce dont vous avez fait l'expérience. Ce résumé vous aidera à choisir des enseignements que vous souhaitez utiliser dans votre travail quotidien.

→ **Dans le premier encart** (voir page suivante), vous pouvez noter les **observations** que vous avez faites pendant la journée. Qu'avez-vous entendu ? Qu'avez-vous vu ? Il n'y a pas de mauvaises réponses, n'hésitez donc pas à écrire tout ce qui vous vient à l'esprit.

→ **La seconde question** concerne le sentiment que ces observations ont suscité en vous. Les impressions sensorielles sont essentielles à l'apprentissage, c'est pourquoi nous nous efforcerons de faire appel à tous les sens pendant le processus de formation, afin d'approfondir l'apprentissage. Dans vos réflexions, citez les événements que vous avez trouvés **marquants** tout au long de la journée : ceux qui vous ont enthousiasmé, ceux qui vous ont surpris, étonné, ennuyé, etc. ?

→ **La troisième question** concerne la **signification de vos sentiments**. Pourquoi avez-vous été étonné? Pourquoi tel événement était-il marquant ? Pourquoi n'étiez-vous pas d'accord avec ce qui était dit ou fait ? Qu'est-ce que cela vous apprend sur vos expériences par rapport au thème de l'atelier jusqu'à présent?

→ **La dernière question** question concerne l'avenir et l'impact de l'atelier sur votre travail. **Qu'avez-vous appris** sur vous-même ? Qu'est-ce que cela implique pour vous ? Qu'allez-vous faire pour **changer ou pour améliorer** vos compétences et votre comportement ? Qu'est-ce que cela implique pour votre travail ou vos activités futures ?

CAHIER DE BORD PERSONNEL

JOUR .....

1. Qu'ai-je observé aujourd'hui ? Quels ont été les thèmes abordés ? Quels exercices avons-nous réalisés ?

2. Quels ont été les éléments marquants dans les sessions d'aujourd'hui ? Qu'est-ce qui a suscité mon enthousiasme ? Avec quoi n'étais-je pas d'accord ?

3. Pourquoi étais-je enthousiaste ? Pourquoi n'étais-je pas d'accord ?

4. Qu'ai-je appris sur moi-même ? Qu'est-ce que cela implique pour mon travail ? Que vais-je changer ou ajouter dans ma manière de travailler ?

ANNEXE 4

PREMIÈRE ÉTAPE DU SUIVI

> FORMULAIRE D'ÉVALUATION DE L'ATELIER

1. L'atelier de formation a-t-il répondu à vos attentes ? Si non, pourquoi ?

2. Vos connaissances et votre expérience ont-elles été appréciées et incorporées activement dans la formation ? Si non, comment pourrait-on améliorer ce point ?

3. Le contenu de la formation était-il bien préparé ? Si non, qu'est-ce qui pourrait être fait différemment ?

4. L'atelier était-il facile à comprendre ? Si non, comment pourrait-on améliorer ce point ?

5. Vous sentez-vous désormais en mesure de travailler activement à la gestion de votre sécurité ? Si non, de quel type de soutien supplémentaire auriez-vous besoin ?

6. Vous sentez-vous désormais en mesure de partager vos connaissances avec d'autres personnes ? Si non, de quel type de soutien supplémentaire auriez-vous besoin ?

7. Pour améliorer nos compétences de formateurs, nous accordons beaucoup d'importance à vos commentaires. N'hésitez pas à nous dire quels sont nos points forts et quels sont les points à améliorer.

NOM DU FACILITATEUR :

Points forts :

Points à améliorer :

NOM DU FACILITATEUR :

Points forts :

Points à améliorer :

NOM DU FACILITATEUR :

Points forts :

Points à améliorer :

8. La logistique de la formation était-elle adéquate (le lieu, les trajets, etc.) ?

MERCI BEAUCOUP !

ANNEXE 5

DEUXIÈME ÉTAPE DU SUIVI

> RÉUNIONS MENSUELLES DE SUIVI

ORGANISATION OU COMMUNAUTÉ :

DATE & LIEU :

PERSONNE RESPONSABLE DU SUIVI :

1. INCIDENTS DE SÉCURITÉ.

1. Notez-vous et analysez-vous les incidents de sécurité ?

2. Agressions subies :

2. PLAN DE SÉCURITÉ.

1. Quelles ont été les mesures de sécurité les plus efficaces de votre plan de sécurité ?

2. Vos vulnérabilités ont-elles diminué ?

3. Vos capacités ont-elles augmenté ?

4. En quelle proportion les membres de l'organisation ont-ils appliqué les mesures de sécurité ?

5. Y a-t-il eu une résistance à l'application des règles de sécurité de la part de certains membres de l'organisation ?

6. A quelles difficultés institutionnelles avez-vous dû faire face pour mettre en avant le plan de sécurité ?

7. En quelle proportion le plan de sécurité a-t-il été appliqué ?

8. Quand prévoyez-vous de réévaluer vos risques et de revoir votre plan de sécurité ?

3. AUTRES FACTEURS.

1. Éléments liés au contexte :

2. Observations Générales :

ANNEXE 6

TROISIÈME ÉTAPE DU SUIVI

> ÉVALUATION FINALE

Les éléments présentés dans le formulaire ci-dessous doivent servir à rapporter les réalisations d'un DDH, d'une organisation ou d'une communauté à la suite du processus de développement de capacités. Le tableau contient une liste de contrôle et un espace réservé pour expliquer brièvement la décision qui a été prise : soit de finaliser le processus, soit de modifier ses termes, soit d'initier un nouveau cycle. Un espace est également prévu pour donner des notes sur le processus de soutien qui a été fourni.

Pour assurer une approche participative, l'organisation partenaire doit être associée à l'évaluation, de préférence en participant à une session d'évaluation pendant laquelle les DDH ont la possibilité de discuter du processus, des progrès réalisés et des enseignements tirés. Cette session contribuera à fournir les informations nécessaires pour apporter les réponses aux questions ci-dessous.

1. Raisons pour lesquelles une des entités ou les deux entités ont décidé de mettre un terme à la collaboration :

2. Évaluation générale de la situation au moment où la collaboration a cessé :

3. Soutien supplémentaire du facilitateur pouvant encore être nécessaire sur base de la liste présentée dans le tableau ci-dessous :

4. Évaluation générale du processus de soutien :

5. Aspects de la gestion de sécurité : connaissances - attitude - comportement :		
COPIER LA LISTE D'ACTIONS DE LA FICHE DE CONTRÔLE	**PERSONNE RESPONSABLE**	**DESCRIPTION DE LA SITUATION APRÈS INTERVENTION**

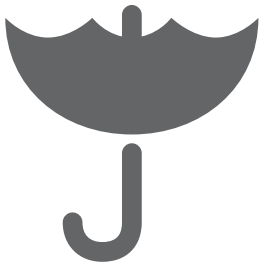
CONTRÔLER LES PROGRÈS

> LES CHAPITRES DU NMP CORRESPONDANT À CETTE SECTION SONT LES CHAPITRES 2.1, 2.2 ET 2.3
FAMILIARISEZ-VOUS AVEC CEUX-CI AVANT DE LIRE ET D'APPLIQUER CETTE PARTIE DU GUIDE DU FACILITATEUR

Le changement ou l'action (lorsque c'est nécessaire) représente l'objectif ultime pour qui soutient des DDH pendant un processus de développement de capacités destiné à renforcer leur gestion de la sécurité. Pour arriver à un changement ou une action réussie, il faut parvenir à transformer les attitudes et les comportements au niveau individuel autant qu'au niveau de l'organisation. L'illustration ci-dessous explique les différents niveaux de changement durable que les DDH doivent atteindre s'ils veulent arriver à une gestion efficace de la sécurité.

Changements réalisables immédiatement

- Le personnel de l'organisation ou les membres de la communauté acquièrent des connaissances en matière de gestion de la sécurité.
- Certaines nouvelles pratiques de sécurité sont mises en place



Changements plus profonds

- Une augmentation des connaissances, mais surtout un changement dans les attitudes au sein des membres de l'organisation ou de la communauté
- Mise en place de pratiques plus structurées en matière de sécurité

Changements fondamentaux

- Développement et application de politiques et de changements culturels en matière de gestion de la sécurité au sein de l'organisation ou de la communauté.

Ceci pose cependant certaines questions : comment les facilitateurs savent-ils qu'ils font ce qui est juste et que des progrès sont faits au niveau des pratiques de sécurité? Comment s'assurent-ils que leur travail vise bien la réalisation des objectifs déterminés par les DDH? Comment savent-ils ce qui fonctionne ou pas? Comment justifient-ils leurs efforts?

Des méthodes de contrôle et d'évaluation peuvent aider à trouver les réponses à ces questions. Les facilitateurs doivent appliquer ces méthodes d'une manière participative (c'est-à-dire en y associant les DDH de sorte que ceux-ci prennent réellement possession du processus de contrôle), s'ils veulent comprendre les points de vue des personnes responsables du processus de changement.

L'objectif essentiel du contrôle est de recueillir des informations tout au long du processus de développement de capacités, de les analyser et de fournir des commentaires destinés à améliorer ce processus. **Recueillir les donnée** pertinentes aidera à :

- → **Préparation :** Trouver la meilleure manière dont les facilitateurs peuvent soutenir les DDH pendant une période donnée, mais aussi assister les DDH dans leur propre planification de sécurité, en s'assurant qu'elle soit réaliste, réalisable et pertinente, et que les participants sentent qu'ils la maîtrisent.
- → **Améliorer la mise en pratique :** en voyant ce qui fonctionne bien et ce qui nécessite un changement (p.e. un soutien technique spécifique pour les DDH ou un changement du format du processus de formation).
- → **Adapter la stratégie:** aider les DDH à revoir leur stratégie et s'assurer qu'elle réponde bien à leurs besoins.
- → **Apprendre :** comprendre pourquoi un changement a eu lieu et comprendre ce que signifie pour les facilitateurs et les DDH de travailler pour améliorer la gestion de leur sécurité.
- → **Assurer la transparence:** recueillir des données sur l'impact des efforts des facilitateurs afin de justifier les ressources utilisées par ceux-ci et par les organisations et communautés partenaires.

Les processus d'apprentissage et de changement ne sont pas linéaires, mais sont plutôt le résultat d'influences mutuelles entre de nombreux facteurs et acteurs, tant internes qu'externes à l'organisation ou à la communauté avec laquelle les facilitateurs travaillent. Donc, si les facilitateurs ne s'intéressent qu'à la manière dont leur aide contribue à amener le changement, ils risquent d'ignorer en quoi d'autres facteurs et acteurs y contribuent également. Comprendre cela permettra aussi aux facilitateurs d'apprendre au sujet de leur propre travail.

Mais de quelles données a-t-on besoin, et en quelle quantité? Pour éviter que le processus de contrôle ne devienne un but en soi, les facilitateurs doivent se demander quelles informations ils doivent réellement avoir pour remplir de façon efficace leurs rôles multiples d'évaluateur, de formateur, de coach, de guide, de partenaire, d'interlocuteur-test, etc. Il est donc essentiel de faire des choix entre ce que l'on doit savoir et ce que l'on voudrait savoir.

L'illustration suivante montre le type d'informations pouvant être utile aux facilitateurs tout au long du processus de développement de capacités. Elle fait référence à certains outils fournis dans ce Guide pouvant être utilisés pour recueillir et analyser ces informations. Les facilitateurs sont encouragés à adapter ces outils à leurs propres besoins et à ceux des DDH avec qui ils travaillent.

	ÉLÉMENTS	INFORMATIONS PERTINENTES OBTENUES	OUTILS UTILES /APPROCHES EFFICACES
ÉVALUATION	• Contexte politique (acteurs et dynamiques) • Profil de risque • Structure et dynamique de l'organisation • Pratiques actuelles en matière de gestion de sécurité • Réflexion des DDH sur les pratiques actuelles de gestion de sécurité et sur les changements souhaités	• Situation de base au niveau des pratiques de gestion de sécurité • Besoins de formation (p.e. identifier les zones de connaissance et les transferts de compétences pour améliorer le contenu de la formation) • Structures et dynamiques de l'organisation à prendre en compte dans le processus de changement	• Formulaire d'évaluation • Roue de la sécurité • Plan de la session de formation
FORMATION	• Cahier de bord personnel des participants • Évaluation quotidienne de la réalisation des objectifs d'apprentissage et de la qualité du travail du facilitateur • Fin de l'évaluation de la formation : réalisation des objectifs d'apprentissage et bonne qualité du travail du facilitateur • Compte rendu fait par le facilitateur pour tirer des enseignements	• Situation de risque • Enseignements-clés pour les membres du personnel • Capacités du personnel et dynamiques internes utiles pour identifier les facteurs favorisant ou empêchant le changement • Méthodes de facilitation efficaces/inefficaces • Points à améliorer pour les facilitateurs • Leçons apprises par le facilitateur/l'institution	• Cahiers de bord personnels des participants • Exercices d'évaluation quotidiens • Fin de l'évaluation de la formation • Compte rendu fait par le facilitateur
PRÉPARATION DES SESSIONS	• Vision : quel changement voulons-nous voir dans notre gestion de sécurité? • Formuler des plans d'action • Agenda de réunions/actions de suivi avec le facilitateur	• Où l'organisation veut-elle aller? • Qui fera quoi à quel moment? • Quel soutien est attendu de la part du facilitateur?	• Plan d'action
SUIVI (MULTIPLE)	• Soutien technique personnalisé • Processus de contrôle en regard du plan d'action • Si nécessaire, faciliter la révision des objectifs et des actions	• Quelles actions ont été entreprises, par qui, et avec quel effet? Qu'est-ce qui a fonctionné, qu'est-ce qui n'a pas fonctionné, et pourquoi? Comment cela va-t-il influencer notre travail futur? • Quels ajustements sont nécessaires pour rendre/maintenir les objectifs/actions adaptés aux besoins de l'organisation?	• Modèle de contrôle
CONTRÔLE	• Description des pratiques actuelles en matière de gestion de sécurité • Preuves de changement de comportements (anecdotes, observations, descriptions d'événements) • Comparaison par rapport à la situation de base • Mettre en évidence les points d'apprentissage	• Qu'est-ce qui a changé? • Changement intentionné ou non-intentionné? • Comment le changement est-il arrivé? Quels acteurs y ont contribué ou l'ont limité? • Changement individuel et institutionnel • Leçons apprises • Bonnes/mauvaises pratiques	• Situation de base (dans le formulaire d'évaluation) • Modèle de contrôle • Modèle d'évaluation

SOUTENIR LES DDH DANS LEUR PROCESSUS DE PLANIFICATION

Les formations en gestion de sécurité sont souvent organisées suite à une évaluation initiale lors de laquelle les DDH travaillent avec un facilitateur en vue d'identifier les outils dont ils pourraient avoir besoin pour être capables d'analyser leur situation de sécurité et de développer des stratégies de réduction des risques. Le processus de formation constitue donc un moyen de transférer des connaissances et des compétences aux DDH de la manière la plus utile possible pour eux.

La formation ne représente qu'une partie du processus de changement et ne constitue pas un objectif en soi, mais elle agit souvent comme un événement révélateur pour les DDH qui travaillent avec les facilitateurs. Une fois que les défenseurs comprennent qu'il est possible d'influencer les risques et qu'ils ont une idée des outils à leur disposition pour les influencer, c'est à eux qu'il revient de décider de façon beaucoup plus concrète ce qu'ils veulent changer dans leur gestion de la sécurité et la manière précise dont ils souhaitent le faire.

Une des responsabilités-clés des facilitateurs sera d'aider les défenseurs à faire des plans adaptés, réalistes et réalisables. Concevoir de grands projets qui ne peuvent pas être mis en pratique ne sert à rien ni à personne. Les facilitateurs doivent guider les DDH pour qu'ils adoptent une approche étape-par-étape qui tienne compte de la suite logique des actions, des délais d'exécution et des responsabilités, et qui anticipe les difficultés possibles en avançant des solutions potentielles. Cela rendra l'expérience d'apprentissage responsabilisante et donnera aux facilitateurs un instrument pour contrôler les progrès réalisés.

Un **plan de sécurité** est comme une **carte routière** menant les DDH à la destination qu'ils souhaitent, mais ceux-ci doivent savoir ce dont ils ont besoin pour être sûrs d'arriver à bon port. En premier lieu, les défenseurs doivent dire clairement où ils veulent aller. Cela peut sembler simple, mais les défenseurs ont souvent des difficultés à articuler exactement le changement qu'ils veulent provoquer. Après avoir pris part à un processus de formation en gestion de sécurité, les défenseurs comprennent généralement mieux leurs risques, leurs vulnérabilités et leurs capacités, et ils ont une vision plus critique de leurs pratiques au niveau de la gestion de leur sécurité. Pour aider les DDH à articuler un objectif, les facilitateurs doivent leur demander d'expliquer quelle serait pour eux la manière idéale de gérer leur sécurité. Les facilitateurs doivent souligner l'importance de prendre en considération les éléments suivants : les comportements, les attitudes, le changement institutionnel et les différents rôles de la direction, du point de contact ou du groupe de travail désigné pour les questions de sécurité, et des autres membres du personnel.
Si le facilitateur travail avec une organisation entière, voilà à quoi pourrait ressembler le résultat :

Le programme est destiné à faire de la gestion de la sécurité une priorité de la direction, en attribuant des rôles et des responsabilités clairement définis à tous les membres du personnel. Les points de contact pour les questions de sécurité sont qualifiés en matière de gestion de sécurité et transmettent leurs connaissances à leurs collègues. Ils réalisent des évaluations des risques et sont principalement responsables de dresser un plan clair des mesures, des protocoles et des politiques de sécurité établies à la suite de l'évaluation des risques, du contrôle de la mise en pratique et des révisions régulières.

La direction crée et maintient une culture de travail soucieuse de la sécurité au sein de l'organisation, et elle montre l'exemple en la respectant. Elle s'assure que plan et les mesures de sécurité sont bien appliqués et respectés par le personnel, et elle soutient un processus d'apprentissage interne mené sur base des pratiques de l'organisation en matière de gestion de sécurité. La direction identifie les ressources nécessaires pour intégrer pleinement la gestion de la sécurité et sensibilise les partenaires-clés aux questions de gestion de sécurité, de manière à améliorer le réseau de protection de l'organisation. L'ensemble du personnel partage une conception commune de la gestion de la sécurité et de son application, et contribue au changement organisationnel en se conformant aux pratiques de gestion de la sécurité.

Quand une organisation commence à planifier la façon dont elle veut atteindre son objectif de sécurité, **il est essentiel pour les facilitateurs de pouvoir reconnaître autant les structures et les dynamiques de l'organisation que les rôles et les capacités des individus**. Cela peut se passer lors de la phase d'évaluation et pendant l'atelier. Au sein des organisations, la plupart des employés ont des responsabilités clairement attribuées. La direction, les chargés de programme et les assistants ont des rôles complémentaires. Les positions des personnes sont aussi souvent des indicateurs de leur niveau d'influence sur la prise de décisions, autant dans le travail quotidien qu'au niveau de l'institution. Cependant, les réseaux, communautés et organisations locales en milieu rural peuvent avoir des structures hiérarchiques différentes. Les facilitateurs doivent donc être sensibles aux relations interpersonnelles et aux profils individuels des employés pour les aider à comprendre les cercles informels d'influence. S'ils sont conscients de ces facteurs, les facilitateurs pourront activement en faire usage pendant leur travail de soutien du processus de changement. Cela s'avérera particulièrement important lors de l'attribution des rôles et des responsabilités pendant la phase de planification, pour que le processus général de changement puisse vraiment aboutir.

Une fois que l'organisation a formulé son objectif idéal de gestion de sécurité, les facilitateurs doivent l'aider à définir les étapes nécessaires pour y parvenir. **A ce stade, un des rôles fondamentaux du facilitateur sera d'encourager les participants à diviser ces étapes en plus petites unités plus facilement réalisables**. Au lieu de définir des tâches complexes dont le succès dépend de multiples interventions faites par de nombreuses personnes différentes, le fait de fragmenter les choses en petites unités de comportements, d'actions ou de relations permettra de rendre les actions plus claires et facilitera l'identification des ressources nécessaires pour les accomplir (en termes de temps, de capacités, de matériel, etc.).

EXEMPLE:

Plutôt que d'établir un objectif général **Tableau A, «mauvaises pratiques»**, le facilitateur doit aider le groupe à diviser la tâche en plusieurs étapes gérables, avec des responsabilités clairement attribuées et des délais clairement définis **Tableau B, "bonnes pratiques"**). Ce format peut aider à obtenir toutes les informations nécessaires en obligeant les défenseurs à bien réfléchir aux réponses aux questions suivantes :

→ En **quoi** cette action contribue-t-elle à la réalisation de notre objectif général?

→ **Qui** est responsable de cette action?

→ **Quel** est le délai d'exécution cette action?

MAUVAISES PRATIQUES : TABLEAU A

Action	Personne responsable	Délai d'exécution
Améliorer la gestion de sécurité de l'organisation	Le point de contact pour les questions de sécurité (PCS)	Trois mois

BONNES PRATIQUES: TABLEAU B

Action	Personne responsable	Délai d'exécution
Définir clairement le rôle du point de contact pour les questions de sécurité (PCS) et s'assurer que ce rôle est bien compris par tous les membres du personnel	La direction	Immédiat

Créer un espace pour discuter des incidents de sécurité et pour analyser conjointement la situation de sécurité	La direction	Immédiat
Les membres du personnel rapportent, analysent et réagissent aux incidents de sécurité.	Tous les employés	Immédiat
Identifier les pratiques existantes en matière de gestion de sécurité	Le PCS	Deux semaines
Prévoir un budget pour les consultations du personnel au sujet de la gestion de sécurité (p.e. prévoir des rafraîchissements lors des réunions)	La direction	Une semaine
Organiser un exercice d'évaluation des risques de l'organisation avec tous les membres du personnel et décider conjointement des zones prioritaires	Le PCS et l'ensemble du personnel	Un mois
Tracer l'ébauche d'un plan des pratiques quotidiennes nécessaires pour réduire les risques identifiés	Le PCS	Deux mois
Séance de réflexion avec l'ensemble du personnel au sujet de l'ébauche de plan de sécurité ; assigner des responsabilités pour sa future application	La direction et l'ensemble du personnel Facilité par le PCS	Trois
Contrôler la bonne application du plan de sécurité	Le PCS et la direction	Pendant les deux mois suivants
Révision des pratiques de sécurité en consultation avec l'ensemble du personnel et en présence du facilitateur, révision du plan d'action pour l'étape suivante du processus	Le PCS et la direction	Après six mois
Version finale du plan de sécurité	Le PCS	Dans les deux semaines suivant la révision des pratiques de sécurité

Les facilitateurs peuvent se renseigner pour savoir dans quels domaines l'organisation pense avoir besoin d'un soutien supplémentaire lors de la rédaction de son propre plan de travail. Ils doivent également s'accorder avec l'organisation pour déterminer quand et comment les progrès seront contrôlés (visite personnelle, appel téléphonique, courrier électronique, etc.). Le facilitateur et l'organisation ou communauté partenaire doivent tous deux conserver une copie du plan d'action et l'utiliser pour contrôler les progrès réalisés lors de la phase de suivi.

Si l'ensemble du personnel de l'organisation n'assiste pas à la réunion de planification, les facilitateurs doivent encourager les participants à réfléchir à la façon dont ils vont tenir leurs collègues absents informés des questions de gestion de sécurité. Ce partage d'informations est essentiel pour faire en sorte que le processus d'amélioration des pratiques de sécurité engagé par l'organisation soit inclusif et que tous les membres en prennent véritablement possession.

RECUEILLIR LES INFORMATIONS NÉCESSAIRES PAR LE CONTRÔLE

Le facilitateur peut utiliser une version étendue du tableau ci-dessus pendant ses rencontres ultérieures avec l'organisation dans le cadre de la phase de suivi, lorsqu'il s'agira de contrôler les progrès réalisés dans l'application du plan.

Action	Personne responsable	Délai d'exécution	Changement observé	Facteurs aidant/ limitant le changement	Action de suivi à entreprendre (et par qui)
Définir clairement le rôle du point de contact pour les questions de sécurité (PCS) et s'assurer que ce rôle est bien compris par tous les membres du personnel	La direction	Immédiat	Le PCS est désigné, le mandat développé, approuvé par le Conseil et annoncé à l'ensemble du personnel		Aucun
Créer un espace pour discuter des incidents de sécurité et pour analyser conjointement la situation de sécurité	La direction	Immédiat	Les incidents de sécurité figurent à l'agenda des réunions hebdomadaires du personnel	Conscience de l'importance des incidents de sécurité	Prendre en compte les absences régulières des employés de terrain pendant ces réunions : comment vont-ils participer aux discussions sur les incidents de sécurité?
Les membres du personnel rapportent, analysent et réagissent aux incidents de sécurité.	Tous les employés	Immédiat	Les informations sur les incidents de sécurité sont partagées pendant les réunions hebdomadaires du personnel	Une atmosphère de confiance et de respect au sein de l'équipe	Idem Créer un format standard pour consigner par écrit les incidents de sécurité (PCS, dans un délai d'une semaine - lui montrer le modèle) Le PCS dispose désormais de l'autorité requise pour agir sur l'analyse des incidents de sécurité - nécessité de décider des responsabilités de prise de décisions (direction)
Identifier les pratiques existantes en matière de gestion de sécurité	Le PCS	Deux semaines	Pas encore réalisé	Le PCS est occupé par d'autres tâches	La direction doit faire des ajustements dans la charge de travail du PCS pour préserver son efficacité

Il est peut-être trop ambitieux de penser que toute organisation sera capable d'appliquer des changements fondamentaux dans son approche institutionnelle de la gestion de sécurité immédiatement après avoir pris part à un processus de formation. C'est pourquoi il est peut-être préférable de «**commencer petit**», c'est-à-dire de laisser l'organisation choisir deux risques prioritaires et d'établir ensuite un plan d'action visant à améliorer leurs capacités à les gérer. Une fois que des progrès auront été faits et que l'engagement aura augmenté au niveau de toute l'organisation, le facilitateur pourra apporter son soutien pour aider l'organisation à planifier un changement plus profond et plus fondamental, étalé sur une période plus longue, en utilisant le même format.

Tout au long de leur engagement aux côtés des DDH, les facilitateurs sont encouragés à rester en contact avec eux, que ce soit par des rencontres face-à-face, quand c'est possible et nécessaire, ou par d'autres moyens de communication sécurisés. Si les facilitateurs encouragent les consultations régulières et qu'ils sont réceptifs aux demandes des partenaires, ils renforceront leur relation avec les DDH et les motiveront dans leur engagement. Donner des conseils par téléphone ou par e-mail, partager des informations ou discuter via Skype sont autant d'actions de suivi que les facilitateurs

doivent entreprendre dans le cadre de leur contribution à la réalisation des objectifs de l'organisation ou communauté partenaire. Pendant les séances de suivi réalisées en personne, les facilitateurs doivent: **(a) évaluer les progrès** faits par rapport au plan d'action et **noter les informations** (sur les raisons pour lesquelles les progrès ont eu lieu ou non) sur la fiche de contrôle ; et **(b) apporter toute aide technique pouvant être nécessaire** pour faire en sorte que les étapes établies dans le plan soient respectées et que l'objectif global soit atteint.

En insérant des aspects de contrôle dans leurs interactions avec les DDH, les facilitateurs peuvent aider les organisations à se pencher à nouveau sur leurs objectifs et leurs stratégies, et à faire des ajustements si nécessaire. Le fait de saisir les points-clés de ce processus peut fournir aux facilitateurs des enseignements essentiels et améliorer ainsi les processus à venir.

A la fin du processus - déterminée idéalement selon un calendrier prédéfini - le facilitateur et les DDH doivent évaluer si les objectifs ont été atteints ou non, et synthétiser l'expérience d'apprentissage d'une manière qui améliorera leurs futures méthodes de travail.

COMMENT LES FACILITATEURS PEUVENT-ILS APPRENDRE DU PROCESSUS?

La transparence est souvent le premier facteur qui vient à l'esprit quand on parle de contrôle, mais ce sont les opportunités d'apprentissage qui constituent le facteur le plus précieux pour les facilitateurs dans leurs efforts pour améliorer constamment leur manière de travailler. Comme cela a été dit plus haut, si les facilitateurs veulent tirer des enseignements du processus de contrôle, ils doivent prévoir du temps et utiliser les ressources et les outils qui pourront leur permettre d'obtenir et d'analyser les informations.

Les facilitateurs doivent faire en sorte que les DDH issus des organisations et des communautés partenaires soient au centre du processus, c'est-à-dire qu'ils jouent un rôle-clé dans la planification et l'application du processus, et qu'ils donnent leur opinion sur les progrès et sur les facteurs qui contribuent au succès ou qui rendent le succès plus difficile à atteindre.

BIBLIOGRAPHIE

- David A. Kolb & Ronald Fry (1975). « Toward an Applied Theory of Experiential Learning ». Dans C. Cooper (Ed.). Theories of Group Process. John Wiley. Londres.
- AI SPA 2013, Collectif Barefoot (2011). Designing and Facilitating Creative Learning Activities, A Companion Booklet to the Barefoot Guide on Learning Practices in organisations and social change. Voir : http://www.barefootguide.org/designing-and-facilitating-creative-learning-activities.html
- Linda-Darling Hammond, Kim Austin, Suzanne Orcutt & Jim Rosso (2001). How People Learn, Introduction to Learning Theories. Stanford University School of Education. Stanford. Voir : http://www.stanford.edu/class/ed269/hplintrochapter.pdf
- Carol Dweck (2006). Mindset: The new psychology of success. New York. Random House.
- SSarah Earl, Fred Carden & Terry Smutylo (2001). Outcome Mapping. Building Learning and Reflection into Development Programs. IDRC. Voir : http://web.idrc.ca/openebooks/959-3/
- Kaia Ambrose & Huib Huyse (2009). « Considerations for learning-oriented Monitoring and Evaluation with Outcome Mapping. OM Ideas ». Outcome Mapping Learning Community. Voir : http://www.outcomemapping.ca

PRÉPARER LES SESSIONS DE L'ATELIER

Ce chapitre est consacré à la préparation et à la mise en pratique des différentes sessions de l'atelier, qui visent à développer les capacités de protection des organisations de DDH et des communautés partenaires. Il est conçu pour aider les facilitateurs à préparer ces sessions en utilisant comme ressource principale le **Nouveau Manuel de Protection** (NMP). Les facilitateurs doivent lire attentivement cette introduction avant de se pencher sur les différentes sections.

STRUCTURE

Chaque session doit s'appuyer sur les précédentes. Toutefois, en fonction des besoins spécifiques des organisations/communautés partenaires et des accords que les facilitateurs auront conclus préalablement avec elles, les facilitateurs ne seront pas toujours tenus de suivre l'ordre exact du Guide. Si tel est le cas, ils doivent garder à l'esprit que certaines activités devront être adaptées.

RÉFÉRENCE AUX CHAPITRES DU NMP

Chacun des chapitres de ce Guide se réfère à un ou à plusieurs chapitre(s) correspondant(s) dans le **NMP**.

> **CHAPITRE X.X** DU NPM
> TITRE DE CHAPITRE

OBJECTIFS D'APPRENTISSAGE

Les facilitateurs trouveront dans cette section les objectifs-clés de chaque session : les principaux concepts et méthodes de protection à présenter.

OBJECTIFS D'APPRENTISSAGE

> Objectif d'Apprentissage 1
> Objectif d'Apprentissage 2

MESSAGES-CLÉS

Ces messages soulignent les éléments les plus importants à retenir lors de chaque session. Ils sont développés tout au long des activités d'apprentissage et sont ensuite repris dans la section Conseil aux facilitateurs.

MESSAGES-CLÉS

> Message-clé 1
> Message-clé 2

LA SESSION

Cette section propose des activités d'apprentissages, ainsi qu'un guide étape-par-étape pour mener chaque session. Les facilitateurs doivent considérer l'horaire donné comme une indication approximative. Le but est de leur proposer des idées dont ils peuvent s'inspirer pour construire eux-mêmes leur session. Cette section contient également une liste de matériel pouvant aider les facilitateurs à préparer les sessions, mais ceux-ci doivent aussi faire preuve de créativité et utiliser leurs propres idées. Enfin, cette section indique les difficultés principales que les facilitateurs sont susceptibles de rencontrer au cours de la session (p.e. des questions posées par les participants, des concepts difficiles à appréhender, etc.). Ceci devrait les aider à anticiper les difficultés et à s'y préparer.

LA SESSION

DIFFICULTÉS POUVANT SURVENIR LORS DE CETTE SESSION :

→ Difficulté 1
→ Difficulté 2

LA SESSION ÉTAPE PAR ÉTAPE :

ACTIVITÉS D'APPRENTISSAGE

C'est ici que les facilitateurs trouveront des exemples d'activités aidant à l'apprentissage (p.e. des discussions de groupe, des jeux de rôles, etc.). Les activités ont été conçues autant que possible pour être réalisées avec des groupes homogènes (dont tous les participants sont issus d'une même organisation) autant qu'avec des groupes mixtes. Les exemples fournis sont applicables autant à des organisations urbaines que rurales.

ACTIVITÉS D'APPRENTISSAGE

ACTIVITÉ 1

ACTIVITÉ 2

CONSEILS AUX FACILITATEURS

Ces suggestions ont pour but d'aider les facilitateurs à comprendre comment diriger les activités et comment expliquer les points-clés de la session aux participants.

→ Conseil 1
→ Conseil 2
→ Conseil 3

RESSOURCES COMPLÉMENTAIRES

A la fin de chaque section, les facilitateurs trouveront une liste de ressources complémentaires qu'ils pourront consulter s'ils le souhaitent. Ces ressources leur permettront d'en savoir plus sur les thèmes traités dans le **NMP**, et leur fourniront des idées supplémentaires pour créer leur propre atelier.

> Koenraad Van Brabant (2000). Operational Security Management in Violent Environments. A Field Manual for Aid Agencies. Overseas Development Institute. Londres.

> Front Line Defenders (FLD) (2011). Workbook on Security: Practical Steps for Human Rights Defenders at Risk. Front Line. Dublin.

> Comité Cerezo Mexico, Fray Francisco de Vitoria O.P., A.C. et al. (2010). Manual de Introducción. La Seguridad en las Organizaciones Civiles y Sociales. Mexico.

> *Colectivo ANSUR (2012). Tejidos de Protección.*

> Protection International & Udefegua (2009). Cuidándonos: Guía de protección para defensores y defensoras de derechos humanos en áreas rurales. Guatemala.

RESSOURCES COMPLÉMENTAIRES

> Van Brabant. Op. Cit. Ch (pp. 22-38).

> FLD. Op. Cit. Chapter 6.

> Comité Cerezo Mexico e Cit. Chapter 2. (pp. 31-3

APERÇU DE L'ATELIER

Les différentes sessions présentées dans ce chapitre suivent une logique commune. Elles ont toutes la même structure, qui tente de présenter le contenu de ce que pourrait être l'atelier de sécurité idéal. Les facilitateurs ont cependant toute la liberté d'omettre les sessions qui ne seraient pas nécessaires dans certaines circonstances, par exemple celles consacrées à l'analyse du contexte ou à la sécurité informatique. Ainsi, la session consacrée aux réseaux de sécurité s'adresse principalement au milieu rural, car nous avons constaté que la création d'un plan de sécurité formel constitue un objectif qui n'est pas toujours approprié au travail avec des communautés ou des organisations de DDH actives dans des régions isolées.

APPROCHE GLOBALE

En matière de protection et de sécurité, il est important d'avoir une approche globale qui tienne compte tous les niveaux entrant en ligne de compte (physique, informatique et psychosocial). Souvenez-vous ainsi que la sécurité informatique comprend les questions du stockage, de la communication et de la gestion de l'information, et que ces trois aspects sont liés entre eux. Cela ne signifie toutefois pas que l'on doive s'occuper de tous ces aspects en même temps. Les facilitateurs doivent donc toujours garder à l'esprit le caractère global de la formation qu'ils proposent, ils doivent savoir quels aspects ils peuvent inclure à tout moment, et ils doivent décider conjointement avec les participants s'il y a lieu de les inclure ou non.

LA PERSPECTIVE DE GENRE ET AUTRES FACTEURS SOCIAUX

Dans le domaine de la protection et de la sécurité, comme dans d'autres domaines, il est important de garder une perspective de genre et d'être conscient des autres facteurs sociaux qui amènent un risque d'exclusion (l'appartenance ethnique, l'âge, la préférence sexuelle, etc.). Il est important, dans le même temps, d'avoir une approche intégrante et différentielle de l'identité. Cet aspect est mis en évidence dans chaque session. Les facilitateurs doivent conserver cette perspective avec un œil critique tout au long du processus de formation.

1. EVALUER SON ENVIRONNEMENT

> **CHAPITRE 1.1.** NMP
PRENDRE DES DÉCISIONS FONDÉES EN MATIÈRE DE SÉCURITÉ ET DE PROTECTION

OBJECTIFS D'APPRENTISSAGE

> Comprendre pourquoi il est important d'analyser les implications de l'environnement de travail en matière de sécurité.

> Utiliser différentes méthodes pour réaliser l'analyse du contexte et des parties prenantes.

MESSAGES CLÉS

> Tous les DDH peuvent être confrontés à des risques, mais tous les DDH ne sont pas confrontés aux mêmes risques.

> Les risques encourus par les DDH dépendent du contexte politique (menaces) et de leurs propres vulnérabilités et capacités.

> Le contexte politique, les menaces, les vulnérabilités et les capacités sont des facteurs dynamiques. Le risques est donc lui aussi un facteur dynamique, il peut changer à tout moment.

LA SESSION

DIFFICULTÉS POUVANT SURVENIR LORS DE CETTE SESSION :

→ Les méthodes présentées au cours de cette session ont pour but de capturer la complexité de l'environnement au sein duquel travaillent les DDH. Elles doivent donc être adaptées en fonction de ce contexte. Notez que vous devrez vous familiariser avec ces méthodes de travail avant le début de l'atelier. Il n'est en effet pas simple de les comprendre à la première lecture.

→ Pour cette session, le facilitateur devra avoir une compréhension de base du contexte de travail des participants, afin que ceux-ci puissent entamer la discussion par des exemples concrets. Il obtiendra les informations nécessaires lors de l'évaluation préliminaire (voir **Chapitre 3** de ce Manuel **Annexe 1 – Formulaire d'évaluation préliminaire**).

→ Pour favoriser la compréhension, soyez aussi concret que possible et restez le plus proche possible des expériences personnelles des participants.

→ Prenez en compte les besoins spécifiques des femmes DDH en matière de protection (menaces, vulnérabilités, capacités, incidents fréquents, etc.).

→ Lors de l'évaluation des risques, le facilitateur devra prendre en compte les particularités de toute autre groupe social pouvant le justifier (par exemple : les populations indigènes, les défenseurs LGBTI, les défenseurs handicapés, etc.).

→ La composition du groupe est importante :

- Pour les groupes homogènes, les exemples et les exercices devront autant que possible être tirés de leur contexte de travail
- Pour les groupes hétérogènes (comprenant des participants issus de différentes organisations), les exemples devront avoir trait aux expériences particulières de chacun des groupes. Il faudra éventuellement concevoir des exercices de groupe pour explorer les exemples théoriques, afin d'assurer une compréhension commune des questions abordées. La difficulté pour le facilitateur sera ici de fournir aux participants suffisamment d'informations contextuelles pour qu'ils puissent réaliser les exercices.

LA SESSION ÉTAPE PAR ÉTAPE :

Durée	Durée totale	Activité	Outil / méthode / matériel
5´		**Introduction :** • Accueillez les participants et faites un tour de présentations ; • Présentez les objectifs et la structure de l'atelier ; • Expliquez pourquoi il est important d'analyser le contexte de travail.	Préparez à l'avance les points abordés sur un paper-board ou dans une présentation PowerPoint
15´	20'	**Activité :** • Discutez de l'affirmation suivante : «Tous les DDH sont confrontés à des risques, mais tous les DDH ne sont pas confrontés aux mêmes risques». • Activité facultative en fonction du temps disponible : visualiser le contexte (si cette activité est ajoutée, les facilitateurs devront adapter l'horaire).	Paper-board Cartons blancs Marqueurs
15´	35'	**Activité :** poser des questions	Liste de questions pertinentes dans le NMP Paper-board
10´	45'	Explication de l'analyse des forces en présence	Diagramme des forces en présence Paper-board Cartons Ruban adhésif
30´	75'	**Activité :** analyse des forces en présence	
15´	90'	Explication de l'analyse des acteurs / des parties prenantes	Paper-boards Matrice pour l'analyse des parties-prenantes
60´	15'	**Activité :** analyse des acteurs / des parties prenantes	
10´	160'	**Conclusions**	
		DURÉE : COMPTER 180 MINUTES (3 HEURES), DONT UNE PAUSE DE 20 MINUTES.	

ACTIVITÉS D'APPRENTISSAGE

DISCUTEZ DE L'AFFIRMATION : «TOUS LES DDH SONT CONFRONTÉS À DES RISQUES, MAIS TOUS LES DDH NE SONT PAS CONFRONTÉS AUX MÊMES RISQUES».

Présentez l'affirmation au groupe et écrivez-la sur votre paper-board. Invitez les participants à répondre à l'affirmation et demandez-leur d'expliquer leur raisonnement. Mettez en évidence les éléments-clés de leurs contributions sur le paper-board (p.e. l'importance du profil du défenseur, son emplacement géographique, son sexe, ses ressources pour gérer les risques, ses organisations partenaires, etc.). Ces éléments seront utiles pour d'autres parties de la session.

- → Cette activité produit généralement de bons résultats et augmente le niveau d'activité de l'assemblée. Les participants discutent de l'affirmation proposée et donnent des exemples issus de leur propre expérience.
- → Le résultat de la discussion offre un point de départ pour explorer les raisons pour lesquelles il est important d'analyser son contexte de travail. Il est essentiel que les participants comprennent qu'ils font partie d'un réseau complexe d'acteurs influencé par des décisions politiques, et qu'ils réalisent qu'ils ne sont pas isolés dans leur travail pour des droits humains.
- → Les discussions menées tout au long de cette session ont pour objectif d'aider les participants à arriver à une meilleure compréhension des problèmes et des acteurs qui ont un impact sur leur travail et sur qui leur travail a un impact. Cette compréhension augmente la capacité des DDH à prendre des décisions éclairées concernant les mesures et les procédures de sécurité à appliquer.
- → Lorsque vous guiderez la discussion, il sera essentiel de ne pas seulement réfléchir d'un point de vue national ou régional, mais de comprendre également la dynamique du contexte local particulier au sein duquel travaillent les participants.

VISUALISER LE CONTEXTE (ACTIVITÉ FACULTATIVE)

Tous les participants ont pour tâche de répertorier par écrit sur des cartons les éléments du contexte politique, économique et social qui ont un impact sur la sécurité de leur organisation ou de leur communauté. Deux ou trois cartons par participant suffisent. Chacun des participants doit ensuite lire à voix haute ce qu'il a écrit et expliquer pourquoi il l'a écrit

En tant que facilitateur, vous devrez regrouper les cartons sous différents thèmes sur votre paper-board ou sur le mur. Vous devrez identifier les thèmes qui se dégagent durant la session (p.e. contexte politique, économique, social, ou tout autre thème). Enfin, vous devrez résumer les résultats de la session. Les cartons seront laissés en place pour que les participants puissent s'y référer pendant les sessions suivantes de l'atelier.

MÉTHODE 1 - POSER DES QUESTIONS

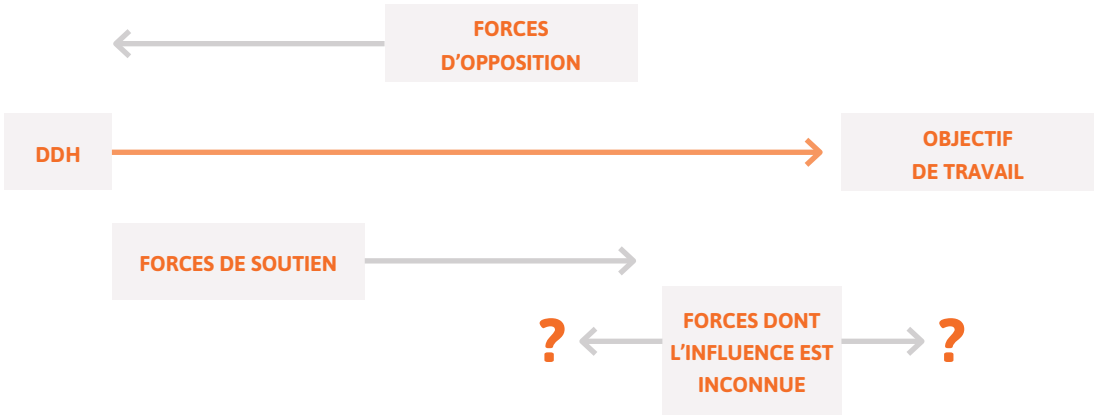
C'est l'un des outils qui aident les défenseurs à mieux comprendre et à mieux analyser leur environnement de travail. Il est important de poser des questions qui vous permettront de comprendre l'environnement de travail des participants. **Posez** donc **des questions ouvertes** qui encouragent les participants à trouver des solutions, et évitez les questions qui n'appellent que des réponses par oui ou par non. Si vous y parvenez, vous verrez que la conversation coulera très naturellement. Les questions posées se baseront les unes sur les autres : les réponses mèneront à d'autres questions.

Pour vous aider, vous pouvez utiliser la liste de questions utiles renseignée dans le chapitre du NMP qui y est consacré (Chapitre 1.1). Lorsque c'est possible, développez vos questions en faisant référence au contexte qui est familier aux participants.

MÉTHODE 2 - ANALYSE DES FORCES EN PRÉSENCE

Cet outil peut aider les participants à visualiser les forces qui soutiennent ou entravent le travail des DDH. Il part sur l'hypothèse selon laquelle les problèmes de sécurité proviennent des «forces d'opposition», et que la stratégie de sécurité doit tirer avantage de la force et de l'influence des «forces de soutien» qui permettent aux DDH de poursuivre plus facilement leurs objectifs.

Pour expliquer cet outil, montrez l'illustration suivante sur votre paper-board:



Pour faciliter la compréhension, utilisez des exemples d'objectifs de travail et de parties prenantes familiers à l'environnement de travail des participants.

Distribuez trois cartons à chaque participant et demandez-lui de dresser une liste des forces opérant dans son environnement de travail. Afin de visualiser l'analyse, demandez aux participants de venir un par un devant l'assemblée et de ranger les cartons sur le paper-board en trois catégories : les forces de résistance, les forces de soutien et les forces aux intentions inconnues. Ils devront expliquer leurs choix. Utilisez du ruban adhésif pour maintenir les cartons en place. N'ayez pas peur de questionner les participants plus en détail concernant leurs choix si vous estimez qu'ils sont trop superficiels (p.e. si un participant travaillant sur des évictions forcées range l'Eglise dans les forces de soutien sans considérer qu'elle possède de nombreuses terres, ou si un participant place la police dans les forces de soutien malgré le fait qu'elle puisse avoir des liens avec des acteurs illégaux).

Ceci génèrera une discussion et mènera probablement à une plus grande différentiation entre les parties-prenantes, et à l'identification de sous-catégories occupant différentes positions par rapport aux objectifs de travail des DDF (par exemple, s'ils représentent différentes positions, les médias peuvent être divisés selon qu'ils appartiennent à l'Etat ou à un groupe privé).

Les participants vous poseront probablement des questions au sujet des forces aux intentions inconnues. Au cas-par-cas, soit les participants considéreront ces acteurs comme des forces de soutien, sur la base du fait qu'ils ne présentent pas un risque concret d'entrave au travail des DDH, soit ils décideront de les surveiller régulièrement afin d'évaluer s'ils changent de position et deviennent une force de soutien ou de résistance. Dans certaines circonstances, il peut être utile d'essayer de transformer des forces inconnues en forces de soutien, par exemple en les éduquant sur les objectifs poursuivis par les DDH. Cela s'apparentera à des activités de plaidoyer et de campagne.

MÉTHODE 3 - ANALYSE DES PARTIES PRENANTES

Voilà le plus complexe des trois outils. Il ajoute une nouvelle couche à l'analyse : les intérêts des différentes parties prenantes par rapport à un certain problème, et les relations entre les parties prenantes avec lesquelles les DDH ont des contacts. C'est un outil permettant d'augmenter de manière significative la quantité d'informations disponibles à l'heure de prendre des décisions en matière de protection.

Demandez aux participants d'expliquer ce qu'ils comprennent par le terme «partie prenante», et de s'accorder sur une définition. Ensuite, détaillez-leur les différentes catégories de parties prenantes, telles qu'elles sont décrites dans le **NMP (p. 20)**, en résumant leurs engagements et leurs devoirs en matière de protection des DDH. Pour contextualiser, demandez aux participants de citer, pour chacune des trois catégories, des parties prenantes issues de leur propre environnement de travail.

Soyez conscient qu'il est fréquent de confondre les stratégies et les actions des parties prenantes. Il y a souvent un écart considérable entre les devoirs d'une partie prenante et ses pratiques. Cet exercice a pour but d'illustrer et d'analyser la complexité du contexte.

Expliquez aux participants les quatre étapes de l'analyse des parties prenantes, telles qu'elles sont décrites dans le **NMP (p. 25)** et faites appel à des exemples locaux pour faciliter la compréhension.

Créez une matrice pour l'analyse des parties prenantes, afin de faciliter la classification des nombreuses informations que va générer l'analyse du contexte. Cet exercice requiert beaucoup d'espace. Utilisez donc une grande partie d'un mur ou du sol (couvrez cet espace avec des feuilles de votre paper-board ou divisez-le en utilisant des cartons ou d'autres repères). Demandez aux participants de choisir un certain nombre de parties prenantes parmi la liste créée pendant l'analyse des forces en présence, et aidez-les à les placer dans la matrice, comme expliqué dans le NMP.

Dans chaque case se trouvant à l'intersection entre la colonne et la ligne correspondant à la même partie prenante, les participants devront indiquer :

- → les objectifs et les intérêts de cette partie prenante à protéger (ou à attaquer) les DDH.
- → ses stratégies en matière de protection (ou d'agression) des DDH.
- → sa capacité à attaquer les DDH, ou la vulnérabilité de la protection qu'il offre.
- → sa volonté d'attaquer ou de protéger les DDH (faible / moyenne / élevée).

Dans les autres cases, c'est-à-dire celles se situant à l'intersection entre deux parties prenantes différentes, les participants devront réfléchir aux relations qui existent entre ces deux parties au niveau des problèmes et des stratégies de protection.

En fonction du nombre de participants à l'atelier et de leurs rôles, cet exercice pourra soit être réalisé par le groupe entier (pour les ateliers plus réduits), soit par des groupes de deux, auquel cas chaque groupe se verra attribuer deux parties prenantes et devra décrire leurs caractéristiques et leurs relations par rapport aux autres parties prenantes indiquées dans la matrice. A la fin de l'exercice, les résultats seront rassemblés, et les descriptions concordantes ou absentes seront débattues entre tous les participants.

Pour terminer, demandez aux participants de citer des implications concrètes de cet exercice pour leur travail, et conservez leurs réponses. Ces réponses pourront notamment identifier un manque de contact avec les parties prenantes favorables à la protection des DDH, ou l'existence de certaines parties prenantes pouvant avoir un intérêt à nuire aux DDH mais pouvant aussi être sensibles à l'influence des forces de soutien, et la nécessité de développer une stratégie pour exploiter cette possibilité.

- → C'est l'un des outils les plus complexes du manuel et les participants ont généralement du mal à le mettre en pratique. Pour arriver à des résultats concrets, il sera nécessaire de fournir de bonnes explications et d'accompagner de près les participants dans le processus d'analyse. Il est préférable de préparer des questions à l'avance pour nourrir la discussion et l'analyse.
- → Pour les activités relevant de l'analyse des acteurs, si vous avez un nombre réduit de participants (jusqu'à huit), il n'est pas nécessaire de les diviser en plus petits groupes. Si le groupe est plus important, il est par contre recommandé de le faire. L'atelier durera alors peut-être plus longtemps, étant donné que tous les groupes réaliseront chacune des activités. Vous devrez adapter l'horaire de la session en conséquence..

COMMENTAIRE GÉNÉRAL

→ Veuillez noter que l'horaire proposé dans le guide de session étape-par-étape n'inclut qu'un seul exercice par méthode d'analyse. Il ne prévoit pas de temps pour réaliser toutes les activités d'apprentissage au cours d'une seule et même session. Si vous souhaitez réaliser toutes les activités, vous devrez adapter l'horaire. En outre, les différentes activités d'apprentissage proposées dans ce chapitre se basent les unes sur les autres, et il est donc recommandé de les utiliser de manière consécutive.

→ Pour favoriser la compréhension, soyez aussi concret que possible et restez le plus près possible des expériences personnelles des participants. Parlez aux participants des connexions qui existent entre différentes parties prenantes et de la façon dont cela peut influencer les risques qu'ils encourent.

CONCLUSION

Demandez aux participants d'identifier les enseignements-clés. Ce point fait également figure de résumé de la session et aide ainsi les participants à traiter et à structurer les informations reçues. En tant que facilitateur, vous devrez faire le lien entre cette étape et les objectifs d'apprentissage établis précédemment, en utilisant l'exercice comme une manière d'évaluer si ces objectifs ont été atteints ou non.

Demandez aux participants avec quelle méthode ils se sont sentis le plus à l'aise, et pourquoi. Leurs réponses vous aideront à savoir quels points n'ont pas été compris pleinement, ou n'ont pas été assez clairs, et à y revenir.

Conservez les travaux les plus intéressants produits lors des exercices de groupe et des séances de réflexion, surtout si ces exercices se basaient sur les contextes de travail réels des participants. Si vous disposez d'un espace suffisant et d'un environnement sécurisé, vous pouvez afficher ces documents au mur de la salle de travail. Ils serviront de référence et de ressource pour les sessions à venir.

A la fin de la session, vous devriez avoir une meilleure compréhension du contexte de travail des participants. Ces connaissances constitueront pour vous une mine d'informations pour les sessions suivantes.

RESSOURCES COMPLÉMENTAIRES

> Van Brabant. Op. Cit. Chapitre 3.2. (pp. 22-38).

> FLD. Op. Cit. Chapitre 6.

> Comité Cerezo Mexico et al. Op. Cit. Chapitre 2. (pp. 31-35).

> Collectif ANSUR. Op. Cit. (pp. 33-35).

2. ANALYSE DES RISQUES

> **CHAPITRE 1.2** NMP
EVALUER LE RISQUE : MENACES, VULNÉRABILITÉS ET CAPACITÉS

OBJECTIFS D'APPRENTISSAGE

- Définir les concepts de menace, vulnérabilité capacité.
- Réaliser une analyse de risques.
- Maîtriser le concept de risque.

MESSAGES CLÉS

- Le risque est un concept dynamique, qui varie avec le temps et qui doit être réévalué périodiquement.
- Le risque est un concept subjectif qui dépend toujours du contexte, des capacités et des vulnérabilités du défenseur et de l'organisation. La perception et la tolérance du risque peuvent également varier d'une personne à une autre et d'une organisation à une autre.
- Le risque est directement proportionnel à la menace. En principe, s'il n'y a pas de menace, il n'y a pas de risque (il est cependant important d'être prêt au cas où une menace surviendrait).

LA SESSION

DIFFICULTÉS POUVANT SURVENIR LORS DE CETTE SESSION :

- → Les participants ont parfois des difficultés à faire la distinction entre les menaces et les risques.
- → Les participants confondent parfois des éléments du contexte avec des vulnérabilités.
- → Prenez en compte les besoins spécifiques des femmes DDH en matière de protection (menaces, vulnérabilités, capacités, incidents, etc.).
- → Lors de l'évaluation des risques, prenez en compte les particularités de toute autre catégorie sociale pouvant le justifier (par exemple : les populations indigènes, les défenseurs LGBTI, les défenseurs handicapés, etc.).

LA SESSION ÉTAPE PAR ÉTAPE :

Durée	Durée totale	Activité	Outil / méthode / matériel
5´		**Introduction :** • Objectifs et structure de la session ;	Préparez à l'avance les points abordés sur un paper-board ou dans une présentation Power-Point
15'	20'	**Définir menace / vulnérabilité / risque** (équation du risque et balance des risques). Présentation orale ou projection de la vidéo sur l'analyse du risque. Ecrivez les définitions sur votre paper-board et laissez-les bien visibles.	Laptop / projecteur / hauts-parleurs ext. pour **la vidéo sur l'analyse du risque** Dessin de l'équation du risque et/ou de la balance des risques sur le paper-board
20'	40'	**Appréhender les concepts de risque, de menace, vulnérabilité capacité.** • Activité d'apprentissage 1 : Représenter les risques, les menaces, les vulnérabilités et les capacités	Paper-board Cartons Feutres Illustration de l'analyse des risques
75´	115'	**Appliquer les concepts :** • Explication de l'exercice : Appliquez l'analyse de risques à votre propre organisation / communauté. • Activité d'apprentissage 2 : Recenser les menaces, les vulnérabilités et les capacités. • Activité d'apprentissage 3 : Evaluation conjointe du risque	Tableau 3 : «Informations nécessaires pour évaluer les vulnérabilités et les capacités d'un groupe» (NMP, pp. 34-37)
10´	125'	**Conclusion**	
		DURÉE : COMPTER 145 MINUTES (2 HEURES 25 MINUTES), **DONT UNE PAUSE DE 20 MINUTES.**	

ACTIVITÉS D'APPRENTISSAGE

DÉFINIR MENACE / VULNÉRABILITÉ / CAPACITÉ / RISQUE

Sur la base du dessin de l'équation du risque (ou de la balance des risques), définissez risque, menace, capacité et vulnérabilité. En fonction du niveau de compréhension affiché par les participants, vous pouvez choisir soit de leur présenter les définitions fournies dans le manuel, soit de laisser le groupe échanger ses idées pour trouver les définitions collectivement. Si vous choisissez cette dernière option, assurez-vous que les éléments-clés suivants soient au centre des définitions :

→ **Risque :** un événement possible, quoique incertain, pouvant porter préjudice.

→ **Menace :** une déclaration ou une indication de l'intention d'infliger du tort ou des dommages.

→ **Capacité :** forces ou ressources qui améliorent la sécurité.

→ **Vulnérabilité :** tout facteur qui rend plus probable la matérialisation des préjudices ou qui augmente l'exposition aux risques.

Vous pouvez également choisir de montrer la vidéo expliquant l'équation du risque en utilisant un ordinateur portable, des hauts-parleurs et un projecteur. A la fin de la vidéo, demandez aux participants de relever les caractéristiques-clés de chaque concept, afin de vous assurer de leur compréhension.

Quand les participants n'auront plus de questions à poser, poursuivez par l'illustration des concepts.

→ Comprendre les risques est essentiel pour une gestion efficace de la sécurité. C'est pourquoi cette session constitue le cœur-même de l'atelier, et pourquoi il est essentiel que les participants en assimilent bien les concepts avant d'entamer les sessions suivantes.

→ Expliquez aux participants que le concept de risque doit être décortiqué. Sans quoi, certains DDH pourront peut-être le percevoir comme un danger trop écrasant pour eux. Quand le risque est subdivisé, les participants réalisent qu'il est composé de nombreux éléments sur lesquels ils peuvent travailler séparément afin de minimiser le risque.

COMPRENDRE LES CONCEPTS DE RISQUE, DE MENACE, DE VULNÉRABILITÉ ET DE CAPACITÉ

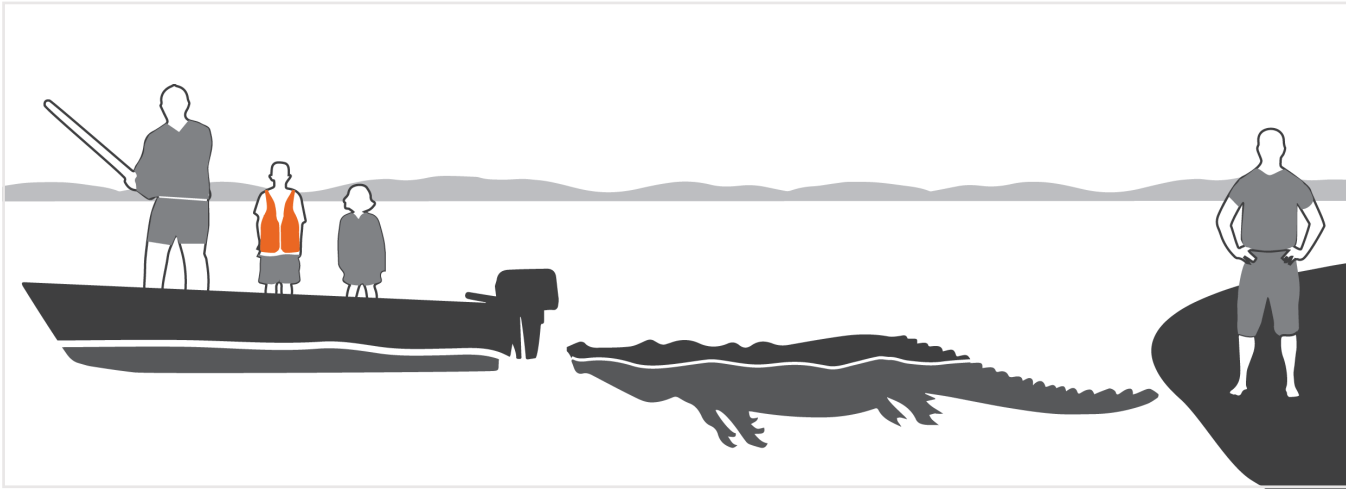
REPRÉSENTER LES CONCEPTS DE RISQUE, DE MENACE, DE VULNÉRABILITÉ ET DE CAPACITÉ.

Choisissez la représentation que vous préférez et qui est la plus proche de l'expérience et du contexte de travail de vos participants :

→ **ILLUSTRATION N°1 :**

Deux enfants sont dans un petit bateau sur une rivière, en compagnie d'un adulte. L'adulte est bien plus grand qu'eux et il porte un grand bâton en bois. L'un des enfants porte un gilet de sauvetage et sait nager, tandis que l'autre n'a pas de gilet et ne sait pas nager. Le père des enfants les observe depuis la rive de la rivière, dans laquelle nagent des crocodiles.

Instructions : pendant que vous racontez l'histoire aux participants, dessinez la scène sur votre paper-board (ou affichez-en une grande version imprimée au mur). Ensuite, demandez aux participants d'identifier les menaces présentes dans la scène, ainsi que les vulnérabilités et les capacités des deux enfants.



- **Menaces :** l'adulte menaçant de blesser les enfants ; la rivière ; les crocodiles qui pourraient tuer les enfants.
- **Risques :** les enfants peuvent se noyer ; se faire manger par les crocodiles ; ou être battus par l'adulte s'ils restent dans le bateau.
- **Vulnérabilités :** ne pas porter de gilet de sauvetage ; ne pas savoir nager : ne pas avoir assez de force physique pour repousser l'homme au bâton.
- **Capacités :** porter un gilet de sauvetage ; savoir nager ; le père des enfants qui observe (s'il a la possibilité d'agir).

→ **ILLUSTRATION N°2 :**

Dessinez un nuage menaçant sur votre paper-board. Demandez aux participants quels sont les risques résultant de cette menace et quelles seraient leurs vulnérabilités et capacités. Vous pouvez illustrer de cette manière:

MENACE
(PLUIE)

RISQUE
(ÊTRE MOUILLÉ)

VULNÉRABILITÉ
(SANDALES, PAS DE MANTEAU)

CAPACITÉ
(BOTTES, PARAPLUIE, MANTEAU)

→ **ILLUSTRATION N°3 :**

Copiez l'illustration ci-dessous sur une feuille de votre paper-board et affichez-là au mur (ou utilisez un ordinateur portable et un projecteur). Commencez par demander aux participants ce qu'ils voient dans le dessin, puis demandez-leur d'identifier les risques, les menaces, les vulnérabilités et les capacités (ils auront peut-être déjà commencé en répondant à la première question, auquel cas vous n'avez pas à poser de question).

- **Menace :** les deux personnes menaçant de pousser le rocher.
- **Risque :** être blessé ou tué par la chute du rocher.
- **Vulnérabilités :** être seule ; ne pas savoir que des personnes la menacent;
- **Capacités :** les personnes représentent une communauté ; elles sont moins exposées au risque que la femme car elles se trouvent de l'autre côté de la rivière, elles sont à l'abri dans la forêt et elles peuvent voir le rocher ; elles pourraient avertir la femme seule du risque qu'elle encourt ; la maison représente également une capacité (elle peut constituer un abri).

Retournez à l'équation du risque (ou à la balance des risques) sur le paper-board et montrez une fois de plus les différentes composantes interdépendantes : pour réduire les risques, les DDH doivent réduire délibérément leurs vulnérabilités, augmenter leurs capacités et tenter de réduire la menace (ou mieux encore, l'acteur menaçant peut cesse de menacer). Insistez sur le fait que les vulnérabilités et les capacités sont des variables internes, des éléments sur lesquels les défenseurs peuvent agir.

→ Le manuel vous suggère de choisir une des trois illustrations pour expliquer plus en détail les composantes du risque. Si vous préférez en présenter deux, vous devrez adapter l'horaire de la session.

→ Quelle que soit l'illustration que vous utilisez, aidez les participants à identifier les risques, les menaces, les vulnérabilités et les capacités en vous référant aux définitions de ces concepts que vous avez élaborées précédemment. Conservez les illustrations et les définitions bien visibles, comme références.

→ Gardez à l'esprit que pour le premier et pour le troisième cas, au moins une des menaces principales est intentionnelle. C'est-à-dire que la personne qui exerce la menace a la possibilité de se raviser et de supprimer cette menace. Dans le second cas, en revanche, la pluie est un danger naturel que l'on ne peut pas arrêter.

APPLIQUER CES CONCEPTS

Si tous les participants font partie de la même organisation ou du même réseau, vous pouvez réaliser l'activité d'apprentissage suivante. Si les participants proviennent de différentes organisations et n'ont pas la même expérience ou les mêmes connaissances, utilisez l'exemple renseigné plus bas dans la section «travailler avec plusieurs groupes».

RECENSER LES MENACES, LES VULNÉRABILITÉS ET LES CAPACITÉS

Une fois qu'ils ont assimilé les concepts de risque, de menace, de capacité et de vulnérabilité, aidez les participants à appliquer ces concepts à leur propre situation.

Si vous avez suffisamment de participants (au moins douze), formez trois groupes. Distribuez des cartons jaunes (vulnérabilités) au premier groupe, de cartons bleus (capacités) au deuxième, et des cartons rouges (menaces) au troisième. Si vous n'avez pas de cartons de couleur, écrivez les lettres V, C et M clairement sur un coin de chaque carton, pour marquer à quel groupe il appartient. Demandez aux participants de réfléchir au travail réalisé par leur organisation.

Chaque groupe se penchera sur chacun des trois concepts en divisant ses activités comme suit : 15 minutes pour le premier tour, 10 minutes pour le deuxième et 5 minutes pour le troisième. Une personne de chaque groupe jouera le rôle de «centre d'intérêt» et ne changera donc pas de groupe. Les centres d'intérêt sont responsables de faire en sorte que le groupe écrive sur les cartons les vulnérabilités, les capacités et les menaces de son organisation. En tant que guide, vous pouvez distribuer aux participants (ou projeter sur un écran) le tableau 3 du (**NPM, pp. 32-35**).

Pour les groupes de moins de douze personnes, tous les participants travaillent sur les trois concepts (vulnérabilités, capacités et menaces) en même temps, pendant environ 30 minutes en tout.

Prenez en compte qu'une idée identifiée comme capacité au terme d'une réflexion collective peut se révéler être aussi une vulnérabilité (ou vice-versa), en fonction de l'approche utilisée et du contexte. Par exemple, considérons une organisation devant se rendre dans une zone rurale reculée et ayant pour cela besoin un véhicule. Le fait de disposer d'un nouveau véhicule tout-terrain peut être considéré comme une capacité, parce que ce sera plus sûr en termes de fiabilité et de sécurité, mais cela peut aussi constituer une vulnérabilité, si dans cette zone des petits criminels ou des acteurs armés sont susceptibles d'être attirés par les nouveaux véhicules. D'un autre côté, le fait de dépendre des transports publics peut faire qu'il soit plus compliqué d'atteindre sa destination à temps, mais cette solution peut aussi être plus sûre, car il est probable que rien n'arrivera à un DDH sans que ce ne soit vu par d'autres passagers. Assurez-vous donc que les vulnérabilités et les capacités décrites au cours de la session soient assez détaillées (deux cartons peuvent par exemple être utilisés pour le même facteur, un comme vulnérabilité et un comme capacité, tout en expliquant pourquoi ce facteur constitue à la fois une vulnérabilité et une capacité).

RELIER LES MENACES AUX VULNÉRABILITÉS ET AUX CAPACITÉS

Prenez deux minutes pour placer les cartes où elles doivent se trouver sur l'équation du risque (ou la balance des risques), qui doit être affichée au mur. Demandez aux participants d'observer l'équation du risque (ou la balance des risques) et engagez une discussion. Ceci devrait aider les participants à visualiser les résultats de l'activité.

Ensuite, demandez aux participants de choisir les menaces les plus concrètes et d'identifier les vulnérabilités et les capacités qui y sont associées. Si certaines vulnérabilités et capacités sont liées à plus d'une menace (ce qui est probable), utilisez de nouveaux cartons pour créer plusieurs copies des mêmes vulnérabilités et capacités, en nommant le risque associé à chacune. Vous pouvez utiliser le tableau suivant :

Menaces	Vulnérabilités	Capacités	Risque
Citez une menace	Citez les vulnérabilités liées à cette menace	Citez les capacités liées à cette menace	Citez le risque associé à cette menace
...	...	...	...
...	...	...	...
...	...	...	...

S'il y a confusion entre risque et menace, retournez à l'illustration que vous avez choisie au début de la session pour aider les participants dans leurs choix. Encouragez le débat entre tous les participants (maximum 15 minutes).

TRAVAILLER AVEC PLUSIEURS GROUPES

Si vous avez un groupe de participants issus de différentes organisations, avec des expériences et des domaines de travail divers, élaborez de préférence un exercice générique pour que les participants puissent s'entraîner à appliquer les concepts. Cet exercice peut par exemple être une étude de cas telle que celle-ci, que vous pourrez adapter autant que possible au contexte de travail des participants :

Deux journalistes travaillent dans un pays déchiré par une guerre civile. L'un d'eux est un professionnel aguerri, tandis que l'autre est assez jeune (mais il a suivi une formation en sécurité et protection). Ils roulent en voiture sur une route secondaire, dans une zone où l'on rapporte des affrontements militaires. La voiture n'est pas à l'épreuve des balles. La surface de la route est en très mauvais état et susceptible de s'affaisser. Il n'y a pas de présence policière ou militaire le long de la route. Les deux journalistes ont parlé de leur voyage à leur réseau de soutien. Ils sont en étroite relation avec Reporters Sans Frontières et font partie d'un média national important. Ils se dirigent vers une communauté dont les membres ont reçu des menaces de mort de la part de groupes paramilitaires et de la part de groupes de guérilla. Pour atteindre

cette communauté, ils doivent traverser une zone contrôlée par les paramilitaires, qui ont des liens avec le gouvernement. Lorsqu'ils arrivent à l'un des checkpoints paramilitaires, un des gardes leur dit de manière très ambiguë : «c'est bon, continuez, mais faites attention à vous»".

Suivez ensuite les étapes décrites plus haut (citer les menaces, vulnérabilités et capacités ; et relier les menaces et les vulnérabilités aux capacités).

- → Créez des études de cas adaptées aux contextes de travail de vos participants et préparez des questions pour stimuler la discussion.
- → Si les participants confondent des éléments du contexte avec des vulnérabilités, utilisez des exemples concrets ou des images pour illustrer la différence. Insistez également sur le fait que les vulnérabilités sont internes à l'organisation. Si les participants confondent des éléments du contexte avec des vulnérabilités, posez-leur cette question : «Dans tel et tel contexte, quelles sont vos vulnérabilités?»
- → Si les participants ont des difficultés à distinguer les menaces des risques, utilisez des exemples concrets ou des images pour illustrer ces concepts. Il est utile de rappeler aux participants la définition de ces concepts. Le risque concerne des événements possibles, mais incertains, pouvant provoquer des torts. Une menace est la possibilité que quelqu'un porte atteinte à l'intégrité physique ou morale ou à la propriété d'autrui par une action délibérée et souvent violente. Donc, un risque est le tort potentiel associé à une menace, considérant les vulnérabilités et les capacités de l'organisation ou de la communauté concernée (d'où l'utilisé de l'analyse du risque).
- → La différence entre menace et vulnérabilité : une erreur fréquente consiste à désigner «la pauvreté», «l'absence de fonds» ou «des informations erronées» comme des menaces. Il peut être préférable de reformuler ces éléments comme des vulnérabilités : «le manque d'accès à des fonds», «le manque d'accès à des revenus de base» ou «le manque d'accès à des informations fiables». La raison de cette reformulation en vulnérabilités est que cela amène à réfléchir à la manière de les transformer en capacités. En fin de compte, l'analyse du risque n'est autre qu'un outil servant à élaborer un plan de sécurité sur mesure, et nous avons besoin de points d'entrée pour entamer l'élaboration de ce plan.
- → Les agressions vont plus loin que les menaces, car les torts ont déjà été causés. Il peut exister un risque de devenir la cible d'une agression. L'agression proprement dite peut avoir été précédée de menaces (p.e. «mêlez-vous de vos affaires, ou nous nous occuperons de vous»), mais la menace diffère tant du risque que de l'agression.
- → Les participants se sentiront peut-être abattus et vous demanderont que faire des résultats de l'analyse du risque. Ils voudront peut-être déterminer leur niveau de risque et tomber d'accord sur la façon d'y réagir. Soyez toutefois prévenus que cela pourra parfois mener à des discussions sans fin. Dites-leur plutôt que la gestion du risque, c'est agir en réaction aux menaces, aux vulnérabilités et aux capacités, et que ces questions seront traitées plus concrètement dans les chapitres suivants, plus spécifiquement dans les chapitres **5.6**, **5.7** et **5.8**. Les activités réalisées au cours de cette session seront utilisées dans des sessions à venir. Conservez donc bien les résultats de cette session!

CONCLUSION

Travaillez en assemblée avec le groupe pour résumer ce qui a été appris durant les discussions. Les éléments-clés à dégager sont les suivants:

- → Le risque varie en fonction du niveau de menace, mais aussi des capacités et vulnérabilités de la personne.
- → Le risque peut être différent pour plusieurs acteurs se trouvant dans la même situation, en raison des différences de capacités et de vulnérabilités («Tous les DDH sont confrontés à des risques, mais tous les DDH ne sont pas égaux face aux risques») ;
- → Le risque est un facteur dynamique et influencé par le contexte, il doit donc être réévalué périodiquement ;
- → Les menaces sont des variables externes sur lesquelles les défenseurs ont un pouvoir limité, mais la probabilité de les voir se matérialiser ou avoir un impact négatif sur les DDH peut être réduite en augmentant les capacités et en réduisant les vulnérabilités.

RESSOURCES COMPLÉMENTAIRES

- > Van Brabant. Op. Cit. Chapitre 4.2. (pp. 43-55).
- > FLD. Op. Cit. Chapitre 2.
- > Comité Cerezo Mexico et al. Op. Cit. Chapitre 3. (pp. 35-45)
- > Collectif ANSUR. Op. Cit.
- > Protection International & Udefegua. Op. Cit.

3. COMPRENDRE ET ÉVALUER LES MENACES

> **CHAPITRE 1.3.** NMP
COMPRENDRE ET ÉVALUER LES MENACES

OBJECTIFS D'APPRENTISSAGE

- Identifier les menaces auxquelles sont confrontés les DDH.
- Evaluer la probabilité de l'exécution des menaces en utilisant les cinq étapes décrites dans le NMP.

MESSAGES CLÉS

- Il est important de distinguer les menaces directes (ciblées et inhérentes à la situation de conflit) des menaces indirectes.
- Les DDH doivent être capables d'identifier les modèles, les sources et les objectifs des menaces.
- Il est essentiel de comprendre le concept de «constituer» une menace
- Les menaces ont toujours un effet psychologique.

LA SESSION

DIFFICULTÉS POUVANT SURVENIR DURANT LA SESSION :

- → Une analyse de menaces fiable n'est possible que lorsque les éléments du contexte ont clairement été identifiés.
- → Les participants pourront rencontrer des difficultés à identifier des mesures de sécurité devant être prises sur base de cas de figure hypothétiques (p.e. lors des conclusions de l'analyse des menaces).
- → Les participants jugeront peut-être qu'ils n'ont pas suffisamment d'informations pour évaluer les menaces.
- → Les participants pourront confondre des menaces et des incidents de sécurité.
- → Les participants parleront peut-être de menaces potentielles en voulant faire référence à des risques. Vous devrez faire une distinction claire entre menace et risque (voir Conseils aux facilitateurs, chapitre 5.2).
- → Prenez en compte les besoins spécifiques des femmes DDH en matière de protection (menaces, vulnérabilités, capacités, incidents fréquents, etc.).
- → Lors de l'évaluation des risques, prenez en compte les particularités de toute autre catégorie sociale pouvant le justifier (par exemple : les populations indigènes, les défenseurs LGBTI, les défenseurs handicapés, etc.).

LA SESSION ÉTAPE PAR ÉTAPE :

Durée	Durée totale	Activité	Outil / méthode / matériel
05´		**Introduction :** • Objectifs et structure de la session	Préparez les points à l'avance sur un paper-board ou dans une présentation PowerPoint.
40'	45'	**Qu'est-ce qu'une menace ?** • Expliquez différents types de menaces. • Identifiez des menaces. • Expliquez la différence entre «émettre» et «constituer» une menace.	Paper-board ou présentation PowerPoint avec affirmations sur le thème "émettre vs. constituer une menace". Paper-board vierge. Marqueurs. Cartons. Ruban adhésif.
60´	105'	**Comment évaluer une menace ?** • Expliquez les cinq étapes de l'évaluation d'une menace. • Activité d'apprentissage : analyse de menaces.	Flipchart (or slide) with the five steps Print-outs of cases to distribute among participants.
15´	120'	**Conclusion**	
		DURÉE : COMPTER 140 MINUTES (2 HEURES 20 MINUTES), DONT UNE PAUSE DE 20 MINUTES.	

ACTIVITÉS D'APPRENTISSAGE

QU'EST-CE QU'UNE MENACE ?

EXPLIQUEZ LES DIFFÉRENTS TYPES DE MENACES (VOIR NPM, PP. 41-43) :

→ Menace directe (ciblée) : «Arrêtez de faire l'idiot ou vous finirez comme votre collègue».

→ Menace indirecte (liée au travail du DDH) : une organisation partenaire vient de recevoir une menace de mort ; au cours d'une conférence de presse un représentant haut placé du gouvernement a accusé mon organisation de n'être qu'une bande de collaborateurs de la guérilla.

→ Les menaces contingentes, dues à la présence de la personne dans une zone de conflit.

IDENTIFIER LES MENACES

Demandez aux participants d'écrire sur un carton une menace qu'ils ont reçue ou entendue dans le passé. Sur votre paper-board ou sur un tableau, dessinez deux colonnes, l'une intitulée «menaces directes» et l'autre «menaces indirectes». Demandez aux participants de déterminer si leur menace est directe ou indirecte et de coller le carton dans la colonne correspondante en utilisant du ruban adhésif. Demandez aux participants pourquoi ils ont placé leur carton dans une colonne plutôt que l'autre, et engagez avec eux une discussion sur la nature de la menace figurant sur chaque carton. Ceci vous aidera à mettre en évidence la distinction entre menace directe et indirecte.

Introduisez brièvement le concept d'incident de sécurité si vous vous apercevez que les participants confondent ce concept avec celui de menace (voir ci-dessous, Conseils aux facilitateurs).

→ Les participants pourront confondre des menaces et des incidents de sécurité. Il est important de souligner que «toutes les menaces sont des incidents de sécurité, mais tous les incidents de sécurité ne sont pas des menaces». Les menaces et les incidents de sécurité peuvent avoir des objectifs différents. Au minimum, un incident de sécurité provoqué intentionnellement a pour but d'obtenir des informations sur les défenseurs. Les menaces ont pour but de faire peur aux défenseurs et de les mettre sous pression pour qu'ils abandonnent leur travail.

→ Les participants parleront peut-être de menaces potentielles. Mais la plupart du temps, ils voudront par là faire référence à des risques. Vous devrez leur indiquer la différence entre les risques et les menaces et insister sur le fait qu'une menace doit être quelque chose de réel et de concret. Ils parleront par exemple de la menace d'être attaqué. Vous devrez leur expliquer qu'il s'agit là d'un risque (cela pourrait arriver), ce qui est différent d'une menace («vous finirez comme votre collègue si vous continuez comme ça»). Notez que dans ce cas-ci, l'auteur a clairement fait savoir que le DDH pourrait subir le même sort que son collègue qui a été attaqué ou tué.

EMETTRE ET CONSTITUER UNE MENACE

Ecrivez les affirmations suivantes sur votre paper-board (ou projetez-les), et discutez-en avec le groupe :

→ Certaines personnes **émettant** des menaces finissent **constituer** une menace.

→ De nombreuses personnes **émettant** des menaces **ne constituent pas** une menace.

→ Certaines personnes **n'émettant jamais** de menace **constituent** une menace.

Extrayez de la discussion les éléments-clés suivants (certains exemples sont fournis dans le **NMP**) :

→ Une menace n'est crédible que si elle indique que l'on peut (raisonnablement) penser que la personne qui l'émet a la capacité de nuire. Parfois, les auteurs tentent de dissimuler leur manque de capacité d'action en insufflant la peur chez les DDH. Mais dans d'autres cas, des menaces proférées par des auteurs potentiellement capables de nuire ont une composante psychologique plus effective.

→ Pour réagir de manière appropriée, vous devez savoir si la menace peut ou non être exécutée.

→ Il est important de jauger la capacité de l'auteur et exécuteur potentiel de la menace pour comprendre si la personne constitue réellement une menace. Lorsqu'ils émettent des menaces à l'encontre des DDH, seuls quelques individus ont réellement l'intention ou la capacité de commettre un acte violent. A l'inverse, certaines personnes peuvent représenter une menace sérieuse sans jamais l'articuler.

→ Attirez l'attention sur le fait que l'impact d'une menace, ainsi que la réaction d'un individu à cette menace, seront différents si a) la victime est raisonnablement certaine qu'il est improbable que la menace soit mise à exécution, ou si b), elle pense que la menace peut être réelle. Il est très important pour le bien-être psychologique des DDH d'être capable d'évaluer la faisabilité d'une menace.

COMMENT ÉVALUER UNE MENACE ?

EXPLIQUEZ LES CINQ ÉTAPES DE L'ÉVALUATION D'UNE MENACE

Suivez les indications fournies dans le **NMP (pp. 43-44)**. Ecrivez les étapes sur votre paper-board, ou projetez-les.

→ Les cinq étapes ont pour but de guider cette analyse et de faire en sorte que les conclusions sont basées sur une interprétation crédible.

→ Pour qu'un DDH soit capable de conduire une bonne analyse, il est important qu'il identifie clairement

les éléments qui entourent les menaces. Indiquez que le processus est composé de deux phases. La phase 1 (qui comprend les étapes 1 et 2) consiste à reconnaître et à classer plus ou moins chronologiquement les faits et les schémas d'actions (ou modèles) qui entourent les menaces. Lors de cette première étape, il est préférable de ne pas interpréter les faits, car ils pourraient se rapporter à plusieurs causes différentes. L'analyse et l'interprétation des faits à proprement parler sont réalisées au cours de la phase 2 (comprenant les étapes 3 à 5).

→ Pour l'étape 2, qui consiste à reconnaître le modèle, expliquez aux participants les éléments de fréquence (à quelle fréquence les menaces ont-elles été émises?, ont-elles été plus fréquentes dernièrement?, etc.), d'intensité (les menaces sont-elles devenues plus fortes?) et de moyens employés.

→ L'analyse évolue au fil du temps. Elle commence par des faits concrets, qui sont ensuite interprétés, avant qu'un jugement ne soit formulé. C'est-à-dire qu'une conclusion raisonnable est tirée concernant la probabilité de l'exécution de la menace, sur la base d'une identification claire et d'une interprétation des faits. D'où l'importance de suivre chacune des étapes dans le bon ordre. Les conclusions tirées (étape 5) restent cependant presque toujours des hypothèses. Il n'y aura en effet jamais à disposition toutes les informations nécessaires pour parvenir à une interprétation non contestable. Malgré cela, insistez sur le fait que lorsqu'il s'agit d'élaborer des mesures de sécurité, les DDH doivent toujours agir en se basant sur le pire scénario possible selon la conclusion à laquelle ils sont arrivés. Le but de cette méthode n'est pas de «supputer ce qui pourrait arriver», mais de prendre des décisions fondées sur ce qu'il convient de faire face à des menaces directes.

LES FAITS	→	**1** • Etablissez les faits qui entourent la menace. **2** • Déterminez s'il existe un modèle de menaces qui se répète dans le temps. → Fréquence → Intensité → Moyens
INTERPRÉTATION	→	**3** • Déterminez l'objectif de la menace. **4** • Déterminez la source de la menace. **5** • Dressez une conclusion raisonnée et raisonnable déterminant s'il est possible ou non que la menace soit mise à exécution.

ANALYSE DES MENACES

Demandez aux participants d'appliquer les cinq étapes en utilisant deux ou trois exemples de cas fictifs basés sur des situations réelles. Imprimez les exemples ci-dessous et distribuez-en des copies aux participants. Vous pouvez également utiliser des exemples réels tirés de l'expérience et du contexte de travail des participants. Si vous choisissez cette option, tenez compte du fait que l'exercice pourra avoir un aspect émotionnel plus fort. Si le nombre de participants l'autorise, divisez-les en groupes plus réduits (le nombre idéal est de quatre ou cinq personnes par groupe).

Les participants devront ensuite appliquer les cinq étapes de l'évaluation des menaces à deux cas différents. Une autre option consiste à demander à chaque groupe d'évaluer un cas et de présenter son analyse à l'assemblée.

→ Les participants jugeront peut-être qu'ils n'ont pas suffisamment d'informations et qu'il est difficile de prendre des mesures concrètes sur la base d'exemples de cas hypothétiques. Cela dit, le simple fait de ne pas avoir assez d'informations constitue une information en soi. On sait que l'on ne sait pas. Il faudra donc élaborer les mesures de sécurité en se basant sur ce manque d'informations et en fonction d'une analyse du pire scénario possible.

→ Lorsque vous discuterez du résultat du travail du groupe sur l'analyse de la menace, guidez les participants pour vous assurez que tous les éléments soient bien envisagés et que toutes les interprétations possibles ont bien été prises en compte. Cet exercice peut se révéler assez complexe et chronophage, mais il est utile. Vous trouverez plus bas quelques conseils pour faciliter la discussion.

→ **CAS N°1 : UNE MENACE CONTRE UNE AVOCATE**

Une jeune avocate ayant très peu d'expérience est engagée par la famille de la victime dans une affaire de meurtre où l'accusé est un officier de l'armée. Pendant une semaine entière, après la première audience de l'affaire, l'avocate reçoit des appels téléphoniques pendant la nuit. Son interlocuteur ne dit rien puis raccroche après un moment. Plusieurs mois passent et, en raison de la nature sensible de l'affaire, l'avocate, bien qu'elle continue à travailler de façon indépendante, décide de demander le soutien d'une ONG de défense des droits humains. Ensemble, l'avocate et l'ONG organisent une conférence de presse pour expliquer l'affaire et les progrès qui ont été faits. La nuit suivante, les appels téléphoniques reprennent, mais cette fois l'interlocuteur insulte l'avocate («salope», «pute», «truie», etc.) pendant quelques secondes puis raccroche. Quelques mois plus tard a lieu une nouvelle audience publique, précédée pendant plusieurs jours par une couverture médiatique. L'avocate répond aux questions des médias à l'intérieur du bâtiment du tribunal. Un des soirs précédant l'annonce du jugement, l'avocate reçoit un coup de téléphone de la part d'une femme qui lui dit : «Je me suis trouvée à côté de vous au tribunal aujourd'hui. La prochaine fois que nous serons si proches, vous aurez moins de chance». L'avocate a tellement peur que le jour suivant, elle demande une réunion d'urgence avec l'ONG qui la soutient, afin d'analyser les menaces.

→ **Faits** : un officier de l'armée est accusé de meurtre ; première audience publique de l'affaire ; pas de tribunal militaire ; l'avocate de la victime reçoit les premiers appels téléphoniques une semaine après la première audience publique, l'interlocuteur ne dit rien ; une conférence de presse a lieu ; nouveaux coups de téléphone nocturnes avec cette fois des insultes envers l'avocate ; seconde audience publique; déclarations publiques de l'avocate à la télévision ; dernier appel téléphonique de menaces.

→ **Modèles** : appels téléphoniques ; menaces proférées après des apparitions publiques ; les menaces augmentent en «intensité» d'une manière graduelle mais claire (intensité n'est cependant pas synonyme de capacité d'agir).

→ **Objectif** : il n'est affirmé à aucun moment ! Mais il semble que l'objectif soit que l'avocate cesse de travailler sur l'affaire.

→ **Source** : les informations dont nous disposons indiquent que les menaces pourraient provenir d'une personne liée d'une manière ou d'une autre à l'affaire, mais qui n'a pas accès aux informations de la procédure judiciaire. Les menaces peuvent émaner soit d'acteurs au sein des forces de sécurité qui ne veulent pas que l'officier de l'armée soit condamné mais qui ne peuvent pas prendre le risque de d'affirmer publiquement, soit de la famille de l'officier. En observant le modèle des menaces, on peut raisonnablement supposer que la personne qui les émet n'a pas accès aux informations confidentielles sur l'affaire. L'auteur des menaces semble puiser ses informations uniquement des médias et des apparitions publiques de l'avocate.

→ **Conclusion** : cette menace peut être considérée comme n'étant pas réelle. L'auteur ne constitue pas une menace, car il/elle n'a démontré aucune capacité de mettre ses menaces à exécution.

→ **CAS N°2 : UNE MENACE CONTRE UNE ACTIVISTE RURALE**

Une femme activiste ayant une grande expérience des organisations va vivre avec sa famille dans une zone rurale. Après quelques mois, elle commence à aider ses voisins à renforcer l'organisation interne de la communauté, afin de les aider dans leur lutte pour le droit à la terre. La communauté souhaite occuper des terres au sujet desquelles elle est en discorde avec un éleveur de bétail. Quelques semaines plus tard, un officier de police rencontre le mari de l'activiste et le prévient : «Si vous ne pouvez pas garder votre femme à la maison, faites alors en sorte de la contrôler.» Quelques jours plus tard, l'activiste trouve devant la porte de sa maison une invitation à ses propres funérailles. Peu de temps après, lorsqu'elle rentre chez elle avec son mari, elle constate que la porte d'entrée est ouverte et que les meubles à l'intérieur sont cassés. Lorsqu'ils se réveillent le matin suivant, ils constatent que toutes leurs poules ont été tuées et que quelqu'un a laissé un mot écrit à la main disant : «Vous devriez quitter votre maison après avoir lu ce mot. Ne prenez pas la peine de vous plaindre auprès de vos amis de la capitale. Si vous décidez de rester, vous finirez comme vos poules. Signé : L'Armée du Peuple. Dieu, Ordre, Patrie.».

- → **Faits** : une activiste part vivre dans une région rurale avec sa famille et aide les gens à défendre leur terre ; l'officier de police donne-t-il un conseil spontané au mari, ou émet-il une menace? ; première menace émise (invitation à ses funérailles) ; effraction dans la maison de l'activiste ; poules assassinés ; propriété saccagée et menaces de mort.
- → **Modèles** : il y a une augmentation claire de l'intensité de la menace dans ce cas-ci, en partant d'actions verbales pour arriver à des actions physiques pouvant exposer la DDH à une attaque perpétrée par les auteurs. Notez également l'utilisation de symboles et les références à la mort, qui sont destinées à effrayer la victime et à accompagner l'augmentation d'intensité des menaces.
- → **Objectif** : que la femme mette un terme à ses activités et quitte la région.
- → **Source** : dans ce cas-ci, plusieurs auteurs possibles peuvent être envisagés. Ce sont soit des voyous armés liés aux éleveurs de bétail, soit les éleveurs eux-mêmes, soit des officiels de l'Etat voulant utiliser les terres. Bien que l'on ne sache pas qui se cache derrière les menaces, les auteurs ont clairement démontré qu'ils ont la capacité d'agir. Notez qu'il n'est pas possible de savoir avec certitude si l'officier de police menace le mari ou s'il tente de lui rendre un service. Dans une société sexiste, il est possible que le policier veuille l'avertir du fait que les activités de sa femme pourraient leur attirer des ennuis, soit parce qu'il a entendu quelque chose, soit parce qu'il est lié aux auteurs des menaces. L'intervention du policier est très ambiguë, et c'est pourquoi il est important de ne pas croire que les choses sont ce qu'elles semblent être à première vue.
- → **Conclusion** : la menace est réelle et la prochaine étape sera probablement une atteinte à l'intégrité physique de l'activiste ou de sa famille.

→ **CAS N°3 : UNE MENACE CIBLANT UN MEMBRE DE LA FAMILLE D'UN DDH**

Deux DDH se rendent dans une petite ville lors d'une des visites régulières qu'ils font tous les deux mois pour recueillir des informations sur des violations des droits humains. Des déplacés internes viennent généralement depuis leur camp à la rencontre des DDH à une date convenue précédemment. Ces visites durent généralement plus ou moins trois jours. Le premier jour de la visite, un déplacé interne dit aux DDH : «Des gens posent des questions sur vous». Les DDH décident de poursuivre leur travail. L'un d'eux reçoit un appel sur son portable de la part de sa fille, Léa. La jeune fille est inquiète car elle a reçu un coup de téléphone anonyme disant que son père a été retrouvé empoisonné.

Au même moment, un déplacé interne s'approche des DDH et leur tend une feuille sur laquelle est écrit:

«8h30 : Léa à l'école ;

13h00 : Léa à la maison ;

15h00 : Léa au volley-ball ;

17h00 : Léa ???????».

- → **Faits** : des DDH recueillent des informations sur des violations des droits humains ; des déplacés internes disent aux défenseurs que «des gens posent des questions sur eux» ; appel téléphonique de Léa (fille d'un des DDH) très inquiète après avoir reçu de mauvaises nouvelles au sujet de son père ; un des DDH (le père) reçoit un message écrit décrivant le quotidien de sa fille.
- → **Modèles** : il apparaît que les DDH et leurs familles sont surveillés depuis un moment, tant dans le village, qui est proche du camp de déplacés, qu'à leur domicile. Léa et les DDH ont reçu le même type de message.
- → **Objectif** : que les DDH cessent de recueillir des informations sur des violations des droits humains concernant les déplacés internes.
- → **Source** : la source est clairement liée aux personnes dont les intérêts sont touchés par les activités des DDH. Avec les informations disponibles, il est difficile de dire qui ces personnes sont réellement. Ce pourrait être des membres de milices impliquées dans des violations des droits humains. Les auteurs ont démontré une capacité et une volonté d'agir (ils ont réussi à trouver où les DDH vivent, leurs numéros de téléphone et leur emplacement), et ils semblent pouvoir faire en sorte que les DDH reçoivent leurs messages.
- → **Conclusion** : cette menace peut être considérée comme un avertissement ; il va falloir agir pour réduire les vulnérabilités et augmenter les capacités.

CONCLUSION

Clôturez la session en demandant aux participants d'identifier les enseignements-clés.

Replacez cette session dans le processus général de gestion de la sécurité en rappelant aux participants l'importance de comprendre le contexte lors d'une analyse de menaces (référez-vous aux concepts abordés dans le **chapitre 5.1**).

Rappelez aux participants l'importance d'analyser les menaces s'ils veulent pouvoir faire un bon usage de l'équation du risque (**Chapitre 5.2.**)

RESSOURCES COMPLÉMENTAIRES

- > Van Brabant. Op. Cit. Chapitre 4.2. (pp. 44-49).
- > FLD. Op. Cit. Chapitre 3.
- > Comité Cerezo Mexico et al. Op. Cit. Chapitre 5. (pp. 56-60).

4. INCIDENTS DE SÉCURITÉ

> **CHAPITRE 1.4.** NMP
INCIDENTS DE SÉCURITÉ : DÉFINITION ET ANALYSE

OBJECTIFS D'APPRENTISSAGE

- Apprendre à repérer, à identifier et à évaluer les incidents de sécurité.
- Apprendre à réagir aux incidents de sécurité.

MESSAGES CLÉS

- Toutes les menaces sont des incidents de sécurité, mais tous les incidents de sécurité ne sont pas des menaces.
- Les incidents de sécurité représentent l'unité de base de mesure de la sécurité. Ils indiquent une résistance ou une pression à l'encontre du travail des DDH. On pourrait les considérer comme une sorte de «feed-back» pouvant aider à l'amélioration de la gestion de la sécurité des DDH.
- Les incidents de sécurité doivent être consignés par écrit, signalés aux collègues, puis analysés. Si l'incident s'avère sérieux, il faut agir en conséquence.

LA SESSION

DIFFICULTÉS POUVANT SURVENIR DURANT LA SESSION

- → Les participants pourront confondre des menaces et des incidents de sécurité.
- → Les participants pourront trouver compliqué de réagir à des incidents de sécurité quand ils n'auront que quelques éléments pour les évaluer.
- → Prenez en compte les besoins spécifiques des femmes DDH en matière de protection (menaces, vulnérabilités, capacités, incidents, etc.).
- → Lors de l'évaluation des risques, prenez en compte les particularités de toute autre catégorie sociale pouvant le justifier (par exemple : les populations indigènes, les défenseurs LGBTI, les défenseurs handicapés, etc.).

LA SESSION ÉTAPE PAR ÉTAPE :

Durée	Durée totale	Activité	Outil / méthode / matériel
10´		**Introduction :** • Objectifs et structure de la session.	Préparez les points à l'avance sur un paper-board ou dans une présentation PowerPoint.
50'	60'	**Reconnaître les incidents de sécurité.** • Expliquez la distinction entre menaces et incidents de sécurité (NPM, pp. 47-48). • Analyse de cas • Reconnaître les incidents de sécurité dans son propre environnement (activité facultative : adaptez l'horaire si vous la faites).	Impressions de cas particuliers à distribuer aux participants. Paper-board. Marqueurs.
50´	110'	**Évaluer et réagir aux incidents de sécurité.** • Expliquez les trois étapes de la gestion d'incidents de sécurité. • Jeu de rôle.	Les trois étapes présentées en impressions papier, sur paper-board ou via PowerPoint. Exemples d'incidents de sécurité pour le jeu de rôle.
10´	120'	**Conclusion**	
		DURÉE : COMPTER 140 MINUTES (2 HEURES 20 MINUTES), DONT UNE PAUSE DE 20 MINUTES	

ACTIVITÉS D'APPRENTISSAGE

RECONNAÎTRE LES INCIDENTS DE SÉCURITÉ

ANALYSE DE CAS

Choisissez une des activités suivantes (analyse de cas n°1 ou n°2). Si vous réalisez les deux activités, il n'est pas nécessaire de voir chacun des cinq exemples de l'analyse de cas n°1.

→ Les participants pourront confondre des menaces et des incidents de sécurité. Voir Conseils aux facilitateurs - Identifier les menaces (chapitre 5.3).

→ Cet exercice ne sera utile que dans des contextes de grande insécurité où les DDH sont clairement en danger et acceptent de partager certaines informations sur le sujet (avec l'accord des participants, il pourra même être utile de recueillir des informations sur des incidents réels dans le but de les dénoncer). Dans le cas contraire, il n'y aura probablement pas suffisamment d'incidents à rapporter, et la ligne du temps ne sera pas utile à illustrer la question. Si vous ne travaillez pas dans un contexte semblable à celui-là, vous pouvez sauter cet exercice et passer au suivant.

→ **ANALYSE DE CAS N°1**

Les participants travaillent en groupe. Chaque groupe reçoit une feuille où figurent les situations suivantes à analyser. Discutez ensuite des résultats avec toute l'assemblée.

Choisissez la réponse correcte pour chaque situation et expliquez votre réponse :

A. C'est un incident de sécurité.

B. C'est une menace.

C. Ce n'est qu'un vol (les vols de téléphones portables sont fréquents).

1.1 *Je me trouve à l'arrêt de bus, j'attends le bus en parlant au téléphone. Un homme s'approche de moi par derrière, s'empare de mon portable et s'enfuit à travers la foule. Je me souviens l'avoir vu me regarder quelques minutes plus tôt. J'ai aussi remarqué que plusieurs personnes utilisaient leur portable, mais qu'il m'a choisi moi. Maintenant, je suis inquiet parce que j'ai enregistré des numéros dans ce portable.*

1.2 *Je marche en direction de mon bureau. A un moment donné, je regarde de l'autre côté de la rue et constate que quelqu'un m'observe fixement. Soudainement, l'homme tend sa main vers moi en forme de revolver et fait mine de me tirer dessus. Je continue de marcher et j'atteins mon bureau sans qu'aucun problème n'arrive.*

1.3 *Je suis sur le point d'entrer dans mon bureau quand je me rends compte que la porte est ouverte et qu'une effraction a été commise pendant la nuit. Le bureau est sens dessus dessous. Quelques ordinateurs ont été volés, mais plusieurs dossiers concernant des affaires sensibles se trouvent toujours sur le bureau.*

1.4 *Une effraction a été commise dans mon bureau. Au milieu du désordre, je trouve une feuille où est écrit : «La prochaine fois, nous passerons à la vitesse supérieure.».*
Je marche dans la rue. Je traverse au carrefour. Une moto roulant très vite manque de me renverser. Deux hommes se trouvent sur la moto. Celui assis à l'arrière semble très fâché. Il me dit de faire attention avant de traverser, et que la prochaine fois ils ne s'arrêteront pas.

→ Pour vous aider à faire en sorte que les discussions restent centrées sur des éléments-clés aidant à comprendre la différence entre menace et incident de sécurité, examinez les réponses-types suivantes pour le cas n°1. Vous pouvez vous servir de celles-ci pour les quatre autres situations :

- Si un groupe choisit la réponse a) : Sur base des informations disponibles, ne peut-on pas considérer qu'il s'agit d'un simple vol ? En vérité, on ne peut pas savoir avec certitude s'il s'agit d'un vol ou d'un incident de sécurité. Mais étant donné qu'il pourrait s'agir d'une action ciblée, le vol doit être classé comme incident de sécurité. Vous devez prendre toutes les mesures nécessaires pour réduire les risques causés par le vol de numéros de téléphone privés et par la possibilité d'un usage malveillant du téléphone (si le voleur le revend au marché noir ou s'il imite votre voix à des fins illégales). S'il s'agit d'un simple vol, il n'arrivera vraisemblablement rien de sérieux. Mais en cas de doute vous devez réagir sur base du pire scénario possible, car cela vous permettra de prendre de meilleures mesures de sécurité pour faire face aux éventuelles conséquences du vol. La réponse est donc correcte, mais pour des raisons différentes.
- Si un groupe choisit la réponse b) : Voir ci-dessus : Reconnaître les incidents de sécurité et les menaces.
- Si un groupe choisit la réponse c) : Encore une fois, la question est de savoir s'il s'agit d'un simple vol ou d'un incident de sécurité. On peut considérer cet événement comme un simple vol, mais comment être certain que, même si le téléphone a été volé sans violence et sans dommages physiques, ce n'était pas un vol ciblé lié au travail de la victime comme DDH ? Comme vous ne pouvez pas en être sûr (et notez qu'aucune autre personne utilisant de portable n'a été agressée autour de vous), il pourrait très bien s'agir d'une action ciblée. C'est pourquoi le vol doit être considéré comme un incident de sécurité ciblé. Il est ainsi important de prendre toutes les mesures de sécurité nécessaires pour réduire les risques causés par le vol de numéros de téléphones privés et par la possibilité d'un usage malveillant du téléphone (voir aussi la fin de la réponse a).

→ **ANALYSE DE CAS N°2**

Lisez le cas suivant avec les participants et discutez-en tous ensemble :

A, B, C et D travaillent au sein de la même ONG de défense des droits humains. Ils écrivent un rapport sur la violence policière et prévoient de le publier dans deux semaines. Lundi, A rentre chez elle après le travail et voit un individu posté en face du bureau qui lui sourit. Elle ne tient pas compte de l'incident et suppose que la personne se montrait simplement aimable.

Le jour suivant, B déjeune dans un café à côté du bureau. Un homme entre après lui et s'assied à une table très proche de la sienne, alors que le café est vide de clients. B ne tient pas compte de l'incident.

Mercredi soir, C quitte le bureau pour rentrer chez elle. Un homme l'arrête devant le bureau pour demander son chemin. L'homme lui demande aussi si elle travaille là et quel type de travail elle fait. C répond à l'homme de manière évasive et rentre chez elle. Elle ne tient pas compte de l'incident et n'y pense plus.

Vendredi, D, qui aime bien aller boire un verre, se rend directement dans un bar du quartier en quittant le bureau. Après cinq bières, il entame une longue conversation avec un sympathique inconnu rencontré dans le bar. A un moment donné, D demande à l'inconnu de surveiller son sac pendant qu'il se rend aux toilettes. Quand D revient, l'inconnu est parti. Son sac est toujours là, près du barman, donc D se dit qu'il n'y a pas de problème. Quand il rentre chez lui quelques heures plus tard, D se rend compte que ses clés de bureau ne sont pas dans son sac. Il se demande s'il les a peut-être laissées au bureau, mais étant un peu ivre, il décide de s'en préoccuper le lendemain. Le lendemain matin il reçoit un coup de téléphone l'avertissant qu'une effraction a été commise dans son bureau la nuit précédente.

Si vous voulez ajouter un peu d'humour à la session, donnez la réponse suivante comme étant la bonne: « Non, la morale de l'histoire est qu'il ne faut pas boire ! » Ensuite, expliquez aux participants que bien que ce ne soit pas aux autres de dire aux gens de ne pas boire, il est néanmoins important, quand on s'occupe de questions de sécurité, d'être conscient du fait que la consommation d'alcool ou de drogue peut augmenter les risques, car elle diminue le niveau de vigilance et rend les gens insouciants. La leçon est bien entendu que les incidents de sécurité doivent être signalés et analysés. Dans ce cas-ci, de nombreux incidents de sécurité s'étaient produits mais n'avaient pas été l'objet d'une discussion, donc D n'était pas conscient d'être vulnérable et exposé à un risque quand il s'est rendu au bar, même si son comportement dans ce bar était irréfléchi.

→ Évaluer et réagir aux incidents de sécurité (le jeu de rôle)

- L'idée est de faire suivre aux participants les trois étapes de la gestion d'incidents de sécurité. Ne guidez le jeu de rôle que lorsque c'est nécessaire. La première étape formelle consiste à consigner l'incident par écrit (les participants sauteront peut-être cette étape). Ensuite, l'analyse doit permettre d'identifier les faits qui entourent l'incident de sécurité, ainsi que les auteurs et sources possibles (quel aspect du travail de l'organisation ou du DDH est lié à cet incident?), et les objectifs de l'incident (obtenir des informations, mais dans quel but?). Enfin, les participants doivent décider de la manière dont il convient de réagir : les mesures de sécurité à adopter, les implications pour le plan de sécurité, les actions à entreprendre, etc.
- Si nécessaire, rappelez aux participants qu'ils doivent également s'occuper de la victime de l'incident.
- Clôturez le jeu de rôle en demandant aux participants d'en identifier les enseignements-clés.

RECONNAÎTRE LES INCIDENTS DE SÉCURITÉ DANS SON PROPRE ENVIRONNEMENT :

Après l'exercice traitant du cas n°1 ou n°2, demandez aux participants de réfléchir à des incidents qui ont pu arriver dans leur propre environnement de travail sans être remarqués ou sans qu'ils n'y attachent trop d'importance. Insistez sur l'importance de prendre en compte tous les incidents sans exception, même ceux qui semblent les plus insignifiants. Les incidents de sécurité mineurs sont souvent reliés entre eux et peuvent ouvrir la voie à des agressions ou à des incidents de sécurité plus sérieux. Prenez garde à bien gérer les émotions qui peuvent surgir de cet exercice et assurez-vous qu'il ne soit reproché à personne de ne pas avoir réagi à un incident ou une menace, ou de ne pas l'avoir signalé.

Ensuite, distribuez des cartons (rouge, jaune et vert) et demandez aux participants d'y écrire tout incident de sécurité ayant pu se produire au cours de l'année écoulée (un incident par carton). Les incidents sérieux (qui ne sont pas forcément des menaces) doivent être écrits sur les cartons rouges, les incidents d'intensité moyenne sur les cartons jaunes, et les incidents d'intensité faible sur les cartons verts. Dites aux participants qu'ils doivent rester concis. Ils auront plus de temps pour expliquer les incidents plus en détails pendant la discussion de groupe.

Utilisez plusieurs feuilles de paper-board pour dessiner une ligne du temps représentant l'année, et affichez-la au mur. Écrivez chaque mois de l'année sur la ligne. Demandez aux participants de placer les cartons reprenant leurs incidents de sécurité sur la ligne du temps, selon leurs souvenirs. Pendant que les participants expliquent les détails de leurs incidents de sécurité, le facilitateur doit essayer de les guider dans l'identification et la classification qu'ils ont attribuées à chaque incident.

A la fin de l'exercice, aidez le groupe à résumer les enseignements tirés concernant les liens existant entre différents incidents, les informations recueillies sur les intérêts et les intentions de l'agresseur potentiel, et l'importance de consigner par écrit et d'analyser les incidents de sécurité.

ÉVALUER ET RÉAGIR AUX INCIDENTS DE SÉCURITÉ

Expliquez aux participants les trois étapes à suivre pour évaluer les incidents de sécurité et pour y réagir, comme indiqué dans le **NPM (Chapter 1.4, pp. 49)** Vous pouvez préparer une présentation à l'avance ou écrire les étapes sur votre paper-board. Ensuite, travaillez sur ce thème en faisant un jeu de rôle.

→ **JEU DE RÔLE (30 MINUTES)**

SCÉNARIO:

Une des membres de votre organisation marche dans la rue et remarque qu'elle est suivie. Elle change de trottoir et continue son chemin. L'homme qui la suit fait la même chose. Elle tourne ensuite à gauche et accélère le pas. Elle ne voit plus l'homme et décide d'aller au bureau pour y déposer quelques documents. Elle n'est pas certaine d'avoir réellement été suivie, donc elle ne dit rien à ses collègues. Quand elle quitte le bureau pour rentrer chez elle, après quelques dizaines de mètres elle repère le même homme, cette fois assis dans une camionnette sans plaques d'immatriculation. Elle décide de retourner immédiatement au bureau et d'informer ses collègues. Tous les membres du personnel présents se rassemblent pour discuter de l'incident et décider de la manière de réagir.

Actions :

Demandez aux participants de faire une simulation d'une réunion et d'appliquer les trois étapes de la gestion d'incidents de sécurité.

Rôles :

Une personne joue le rôle du témoin de l'incident de sécurité. Les autres participants jouent les rôles des autres membres de l'organisation.

CONCLUSION

Clôturez la session en demandant aux participants de rappeler les enseignements-clés de la session.

Insistez sur les messages-clés en revenant à des exemples ou à des problèmes qui se sont présentés pendant la session.

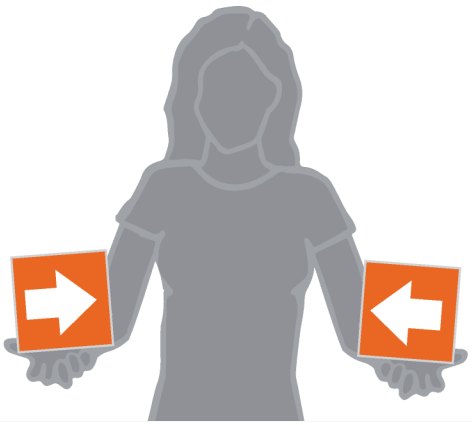
Replacez la session dans le contexte du processus de gestion de la sécurité. Rappelez aux participants l'importance des incidents de sécurité (voir les messages-clés).

Bien que les incidents de sécurité ne soient pas nécessairement intégrés dans l'équation du risque, ils doivent néanmoins être considérés comme des indicateurs de l'impact du travail des défenseurs et de leur sécurité. Des mesures de sécurité doivent donc être adaptées aux incidents de sécurité subis par l'organisation.

RESSOURCES COMPLÉMENTAIRES

- Van Brabant. Op. Cit. Chapitre 16. (pp. 240-250).
- FLD. Op. Cit. Chapitre 3.
- Comité Cerezo Mexico et al. Op. Cit. Chapitre 5. (pp. 53-56).

5. PRÉVENIR LES AGRESSIONS ET Y RÉAGIR



> **CHAPITRE 1.5** NMP
PRÉVENIR LES AGRESSIONS ET Y RÉAGIR

OBJECTIFS D'APPRENTISSAGE

> Évaluer la probabilité que différents types d'agression se produisent.

> Réfléchir de manière critique à la manière de prévenir les agressions et y réagir.

MESSAGES CLÉS

> Une agression est le point culminant d'un processus incluant souvent des incidents de sécurité et parfois des menaces. Ce n'est donc généralement pas un événement inattendu. Une agression est le produit de trois facteurs interactifs :

- Une partie qui recourt à des actions violentes et à des moyens violents pour parvenir à ses fins ;
- Des circonstances et des éléments déclencheurs qui amènent l'agresseur à envisager la violence comme option ;
- Un cadre favorable.

> Pour être mises à exécution, les agressions requièrent des ressources et des capacités adéquates et un environnement favorable. C'est pourquoi le travail de prévention des agressions doit s'intéresser au coût politique éventuel des agressions, et s'efforcer de réduire l'exposition physique des DDH aux agressions.

> Préparer une agression nécessite du temps et des ressources. Il est donc essentiel pour les défenseurs de détecter et d'analyser tout signe pouvant indiquer une éventuelle agression. Pour ce faire il faut :

- Évaluer les risques (NMP, chapitre 1.2).
- Évaluer la probabilité de l'exécution d'une menace (NMP, chapitre 1.3).
- Analyser les incidents de sécurité et y réagir (NMP, chapitre 1.4).

LA SESSION

DIFFICULTÉS POUVANT SURVENIR DURANT LA SESSION :

→ La session pourra avoir une forte charge émotionnelle si elle est basée sur des cas réels.

→ Les participants pourront avoir des difficultés à séparer clairement les trois facteurs interactifs menant aux agressions.

→ Lors de l'analyse des risques, il faudra prendre en compte les besoins spécifiques des femmes DDH en matière de protection (menaces, vulnérabilités, capacités, incidents, etc.), ainsi que les particularités de toute autre catégorie sociale pouvant le justifier (par exemple : les populations indigènes, les défen-

LA SESSION ÉTAPE PAR ÉTAPE :

Durée	Durée totale	Activité	Outil / méthode / matériel
10´		**Introduction :** • Objectifs et structure de la session	Préparez les points à l'avance sur un paper-board ou dans une présentation PowerPoint.
20'	30'	**Explication du concept d'agression** • L'agression comme produit de trois facteurs interactifs. • Qui se cache derrière les agressions?	Écrivez les trois facteurs sur un paper-board ou projetez-les via PowerPoint.
45´	75'	**Déterminer la faisabilité d'une agression** • Activité d'apprentissage : évaluer la probabilité d'une agression	Tableaux aidant à déterminer la faisabilité d'une agression (NMP, chapitre 1.5). Vidéo sur l'assassinat de Marisela Escobed (http://www.youtube.com/watch?v=QNvgrEKedsw).
30'	105'	**Prévenir une agression directe / indirecte.** • Analyse de cas : vous pouvez utiliser soit un exemple basé sur des faits réels, choisi par les participants, soit l'exemple proposé ci-dessous • Exercice : planifier en tant qu'agresseur	Impressions sur papier des cas proposés. Informations contextuelles sur l'analyse de cas.
10'	115'	**Conclusion**	
		DURÉE : COMPTER 135 MINUTES (2 HEURES 15 MINUTES), DONT UNE PAUSE DE 20 MINUTES.	

ACTIVITÉS D'APPRENTISSAGE

EXPLICATION DU CONCEPT D'AGRESSION

Référez vous au Chapitre 1.5. du NMP pour expliquer pourquoi et comment les agressions ont lieu. Voir également la partie «Conseils aux facilitateurs» ci-dessous. Deux points principaux guideront votre explication :

→ L'agression comme produit de trois facteurs interactifs **(p.53)**.

→ Qui se cache derrière les agressions? **(NMP, pp.55-57)**

→ Les agressions violentes commises contre les DDH ont pour objectif de les pousser à abandonner leur travail en leur causant un préjudice direct ou indirect (p.e. en s'en prenant à des membres de leur famille). Il y a là non seulement une composante physique, mais également une dimension émotionnelle qu'il faut reconnaître.

→ Lorsque vous présentez le concept d'agression, soulignez le fait que la violence n'est pas seulement un acte, mais aussi un processus. Une agression violente commise contre un défenseur ne surgit pas de nulle part. L'analyse minutieuse des agressions montre souvent qu'elles constituent le point culminant de conflits, de différends, de menaces et d'incidents de sécurité dont les origines peuvent être retracées. Le point positif, c'est qu'en observant, en analysant et en réagissant aux incidents de sécurité, et en mettant en place des mesures de sécurité, les défenseurs peuvent réduire de manière significative le risque d'agression violente. Ils ne doivent donc pas croire qu'ils sont impuissants.

→ Expliquez les trois facteurs interactifs qui amènent une agression et donnez des exemples pour aider les participants à les assimiler. Si c'est possible, choisissez un exemple tiré de l'expérience personnelle des participants. Sinon, vous pouvez utiliser les exemples suivants :

→ **Exemple** : le travail d'une femme DDH affecte les intérêts d'un riche homme d'affaires actif dans l'élevage à grande échelle et ayant exproprié illégalement des paysans de leurs terres. La DDH possède des preuves de ces faits. Pour la faire taire, l'agresseur potentiel a besoin d'obtenir des informations sur ses agissements, ses habitudes et ses vulnérabilités. Cela nécessite un investissement en termes de temps et de ressources. L'agresseur potentiel doit prendre une décision consciente en évaluant si une agression visant à mettre un terme au travail de la DDH est plus avantageuse pour lui que les possibles répercussions que cet acte pourrait avoir devant la justice. Il est moins coûteux pour un agresseur potentiel de mettre une menace à exécution dans un environnement où le niveau d'impunité est élevé, car les risques de répercussions seront limités ou inexistants. L'agresseur doit également trouver un cadre propice pour commettre l'agression en encourant le moins de risques possibles d'être découvert ou arrêté. Il doit donc passer du temps à préparer l'agression afin de limiter les éventuelles conséquences négatives pour lui.

DÉTERMINER LA FAISABILITÉ D'UNE AGRESSION

ÉVALUER LA PROBABILITÉ D'UNE AGRESSION

Divisez les participants en trois groupes, un groupe pour chaque thème. Demandez-leur d'appliquer les trois tableaux proposés dans le **NMP (pp.58-60)**, «Évaluer la probabilité d'une agression», soit à leur propre environnement de travail, soit à un autre cadre qui leur est familier.

Discutez des résultats avec l'ensemble des participants (soyez conscients de tout facteur sensible dans le cas où il y aurait des problèmes de confiance entre les participants).

→ Pour empêcher une agression, il est nécessaire d'être capable d'analyser la probabilité qu'elle se produise. Pour aider les participants à acquérir cette capacité, utilisez les tableaux fournis dans le NMP (pp. 58-60). Ces tableaux aideront les participants à identifier les différents facteurs qui interagissent dans le développement d'une agression, et à jauger leur importance relative lors de l'évaluation de la probabilité de différents types d'agressions (crimes de droit commun, agressions liées à la situation et agressions directes).

PRÉVENIR UNE AGRESSION DIRECTE / INDIRECTE

Rappelez aux participants que pour prévenir une agression il est essentiel de:

→ Persuader l'agresseur potentiel ou la personne émettant les menaces qu'une agression impliquera pour lui un coût et des conséquences inacceptables ;

→ Réduire la probabilité que des agressions ne surviennent.

Choisissez un des exercices ci-dessous (utiles à l'évaluation de la probabilité d'une agression) :

Pour chacun des deux exercices, divisez les participants en petits groupes (quatre à cinq personnes) pendant environ une demi-heure, après quoi chaque groupe devra présenter le résultat de ses discussions. Ensuite, engagez une discussion générale entre tous les participants pendant environ 15 minutes.

EXERCICE N°1 - ANALYSE DE CAS : L'ASSASSINAT DE MARISELA ESCOBEDO (DDH MEXICAINE)

(Cette vidéo ne peut être visionnée que si le facilitateur a accès à internet ou si le fichier a été téléchargé préalablement.)

Après la disparition de sa fille Rubi Fayre en août 2008 (elle a été retrouvée morte en juin 2009), Marisela Escobedo a consacré son existence à essayer d'obtenir justice pour la mort de son enfant. En décembre 2010, un homme armé s'est approché de Marisela et lui a tiré dessus pendant qu'elle participait à une manifestation pacifique devant le Palais du gouvernement dans la ville de Chihuahua. Une caméra de sécurité placée au sommet du bâtiment a enregistré la scène de l'assassinat. Cet enregistrement est devenu un témoignage douloureux mais d'une valeur unique. Bien que la vidéo soit en langue espagnole et qu'il n'y ait pas de sous-titres disponibles, elle constitue une ressource visuelle utile et facile à comprendre. Quelques éléments de base sur la scène : pendant les protestations, Marisela campait dans le parc ; au moment de l'attaque elle était assise à une table sur le trottoir avec un ami (sur la partie droite de l'écran), en face de l'entrée principale du bâtiment du gouvernement. Une voiture blanche approche, un tireur en sort et attaque Marisela et la personne qui l'accompagne. Marisela tente de s'échapper et court de l'autre côté de la rue vers le bâtiment du gouvernement (de droite à gauche de l'écran), mais l'homme lui tire dessus quand elle atteint le trottoir (sur la gauche de l'écran). Il retourne ensuite en courant vers la voiture et quitte la scène.

Demandez aux participants de lire les informations contextuelles sur ce cas (vous les aurez imprimées), ensuite montrez-leur la vidéo. Pour l'analyse, demandez aux participants de suivre les trois conditions nécessaires pour mener à bien une attaque, et demandez-leur comment chacune de ces conditions aurait pu être influencée pour prévenir l'attaque :

A. Les modèles de pensée et de comportement utilisés par l'individu ou les individus qui ont commis l'acte.

B. Pourquoi l'agresseur a-t-il pensé qu'il pouvait «atteindre un objectif» ou «résoudre un problème» en commettant l'acte? (Quel est le mobile probable de l'attaque, quelle est la nature du problème, comment a-t-elle été commise, etc.).

C. Quel contexte ou quelles circonstances ont rendu l'attaque possible (décrire l'endroit où elle a eu lieu, la manière dont elle a été commise, etc.).

→ Le présent exemple est basé sur un cas réel, mais le facilitateur peut aussi choisir un autre cas (sous forme écrite) si celui-ci est pertinent et adéquat.

→ Rappelez qu'il est essentiel, pour prévenir une agression, de persuader l'agresseur potentiel ou la personne émettant les menaces qu'une agression impliquera pour lui un coût et des conséquences inacceptables, et de réduire la probabilité qu'une agression se produise.

EXERCICE N°2 - PLANIFIER EN TANT QU'AGRESSEUR

Demandez aux participants de mettre au point un plan d'attaque visant un DDH. Savoir comment les agresseurs pensent est l'une des meilleures manières de prévenir une attaque. Les facilitateurs peuvent également lire la section «Surveillance et contre-surveillance» du **(NPM, pp.62-64)** pour les guider dans cet exercice):

A. Imaginez une situation dans laquelle un DDH voyage tous les jours entre son domicile et bureau. Le DDH a déjà reçu une menace de mort précédemment. Les assaillants comptent déguiser leur attaque en une agression commune, passer le DDH à tabac et tenter ainsi de le pousser à arrêter son travail de défenseur. Les assaillants, deux individus payés par un officier de police local, ne veulent pas être identifiés au cas où ils se feraient arrêter. (Dessinez si possible un plan de la route, etc.)

B. Imaginez le reste des informations contextuelles vous-même, notamment la maison où vit le DDH, la distance entre la maison et le bureau, l'utilisation éventuelle d'une forme de transport, le moment auquel l'attaque doit avoir lieu (dans son temps libre ou pas), etc.

C. Imaginez ce vous devriez faire afin de prévenir une telle attaque, sans avoir aucune information préalable. En d'autres termes, quelles mesures de sécurité faudrait-il adopter pour permettre au DDH de diminuer ou d'éliminer le risque d'une telle attaque?

- → Ce second cas peut se révéler très stimulant, car il demande aux participants d'adopter le point de vue des assaillants. Cet exercice doit cependant être réalisé avec une grande précaution, car le fait de demander aux participants de jouer ce rôle peut provoquer des tensions ou amener certains participants à surjouer leur rôle. Évitez cet exercice si vous n'êtes pas à l'aise avec le groupe.
- → Pour prévenir les agressions directes et mieux comprendre leur logique, il peut s'avérer utile de se mettre à la place des agresseurs. Cet exercice devrait aider les participants à obtenir une meilleure compréhension de la pensée, des comportements et des stratégies adoptées par les agresseurs. Les agressions commises contre les défenseurs sont souvent le produit d'un processus de pensée et de comportement qu'il est possible de comprendre et dont il est possible de tirer enseignement, même s'il s'agit de processus illégitimes. La plupart des personnes qui s'en prennent aux défenseurs considèrent la violence comme un moyen «utile» d'atteindre un objectif ou de «résoudre un problème».

CONCLUSION

Clôturez cette session en demandant aux participants de rappeler les enseignements-clés.

RESSOURCES COMPLÉMENTAIRES

> Van Brabant. Op. Cit. Chapitres 7-12.

6. ÉLABORER UNE STRATÉGIE DE SÉCURITÉ GLOBALE

> **CHAPITRE 1.6** NMP
ÉLABORER UNE STRATÉGIE DE SÉCURITÉ GLOBALE

OBJECTIFS D'APPRENTISSAGE

> Reconnaître et analyser les stratégies et les tactiques de protection utilisées par les DDH.

> Définir une stratégie globale pour protéger l'espace de travail des DDH.

MESSAGES CLÉS

> Les DDH et leurs organisations ne partent pas de zéro en ce qui concerne les questions de sécurité. Ils ont inévitablement déjà appliqué des stratégies de dissuasion et de protection ad-hoc pour gérer les risques et les menaces.

> Toutes les stratégies ne sont pas en mesure de couvrir toutes les éventualités, elles comportent inévitablement des failles. Toutes les stratégies sans exception (ad-hoc ou formelles) doivent au minimum satisfaire aux critères RADER : Réactivité, Adaptabilité, Durabilité, Efficacité et Réversibilité.

> Une stratégie de sécurité globale a pour but d'élargir et de préserver l'espace de travail des DDH en agissant sur deux axes : l'acceptation et la tolérance envers le travail réalisé par les DDH ; et la dissuasion et la persuasion des agresseurs potentiels.

LA SESSION

DIFFICULTÉS POUVANT SURVENIR DURANT LA SESSION :

→ Ce module est très théorique, très conceptuel, dans le style occidental. Si vous travaillez avec des DDH actifs au niveau local, qui ont une expérience directe mais peu de connaissances formelles ou conventionnelles, il sera peut-être préférable de sauter cette session et de passer directement au Chapitre 5.8.

→ Reconnaître et analyser les stratégies et les tactiques de dissuasion ad hoc déjà existantes.

→ Respecter les stratégies ad hoc liées aux croyances religieuses ou culturelles tout en insistant sur la nécessité d'adopter des mesures de sécurité et de protection plus ciblées.

→ Amener les participants à comprendre clairement le concept d'»espace de travail du DDH».

→ Prendre en compte les besoins spécifiques de protection que peuvent avoir les femmes DDH ou tout autre groupe social particulier (populations indigènes, défenseurs LGBTI, défenseurs handicapés, etc.) en termes de stratégies, de normes de sécurité, etc., tant au niveau des protocoles de routine qu'au niveau des procédures d'urgence.

LA SESSION ÉTAPE PAR ÉTAPE :

Durée	Durée totale	Activité	Outil / méthode / matériel
10´		**Introduction** • Objectifs et structure de la session.	Préparez les points abordés à l'avance sur un paper-board ou dans une présentation PowerPoint. Utilisez les vidéos de PI "Stratégies de protection" et "Objectifs de sécurité et de protection" comme informations contextuelles.
30'	40'	**Stratégies et tactiques de dissuasion ad hoc** • Identifier les stratégies et les tactiques de sécurité • Gérer le risque après avoir réalisé une évaluation	Paper-board présentant les critères RADER pour une stratégie de sécurité efficace.
30´	70'	**L'espace de travail sociopolitique des DDH** • Définition de l'espace de travail socio-politique des DDH • La sécurité et l'espace de travail des DDH	Paper-board illustrant les deux axes de l'espace de travail des DDH **(NPM, p.72)**
40'	110'	**Élargir l'espace de travail des DDH** (stratégie de sécurité globale)	Marqueurs Cartons
10'	120'	**Conclusion**	
		DURÉE : COMPTER 140 MINUTES (2 HEURES 20 MINUTES), DONT UNE PAUSE DE 20 MINUTES.	

ACTIVITÉS D'APPRENTISSAGE

STRATÉGIES ET TACTIQUES DE DISSUASION AD HOC ; FAIRE FACE AU RISQUE

Après avoir introduit les concepts principaux (voir ci-dessous, Conseils aux facilitateurs), aidez les participants à identifier les stratégies et les tactiques de dissuasion ad hoc qu'ils utilisent dans leur vie quotidienne.

Après avoir fait la liste des stratégies ad hoc sur votre paper-board, introduisez les six manières de faire face au risque (l'accepter, le réduire, le partager, etc. ; **NMP, p.69**) afin de catégoriser les stratégies ad hoc des participants.

En fonction du temps disponible, vous pourrez choisir d'analyser soit une soit plusieurs de ces stratégies selon les critères RADER (voir les critères RADER pour l'analyse des stratégies de dissuasion, NMP p.68). Insistez auprès des participants sur le préjudice potentiel pouvant découler de n'importe laquelle des stratégies s'il lui manque un ou plusieurs critères.

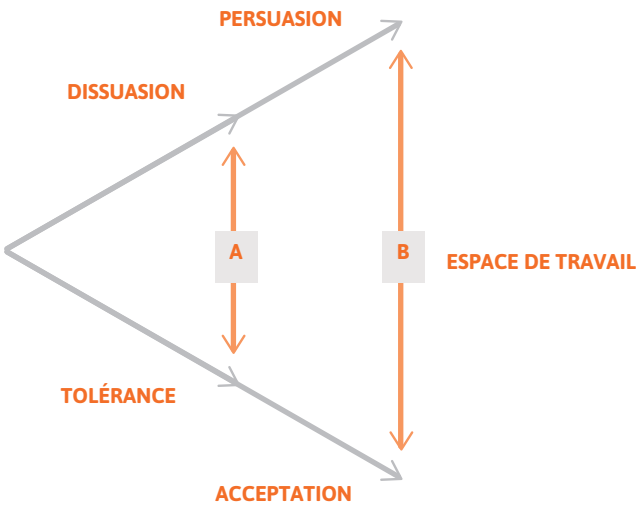
Clôturez l'activité en indiquant que lorsque des DDH sont menacés, leur niveau de stress augmente et ils ressentent le besoin d'agir rapidement. Cependant, le fait d'analyser les stratégies selon les cinq critères les aidera à choisir des stratégies efficaces basées sur une perspective à long terme.

- → Basez votre introduction à cette question sur les idées décrites dans le NMP. Les vidéos de PI «Stratégies de protection» et «Objectifs de sécurité et de protection» peuvent être utiles pour la préparation de l'introduction.
- → Les individus DDH, les organisations et les communautés confrontés à des menaces font appel à différentes stratégies ad hoc pour faire face aux risques qu'ils perçoivent. Ces stratégies varieront en fonction de plusieurs facteurs : l'environnement (rural ou urbain) ; le type de menace ; les ressources sociales, financières et légales à disposition ; les expériences précédentes ; les perceptions individuelles subjectives du risque, etc. Pour obtenir une liste de stratégies ad hoc adoptées par des DDH, avec des exemples, reportez-vous au **NMP (pp.67-68)**.
- → Rappelez aux participants que la plupart des stratégies ad hoc sont applicables immédiatement et sont destinées à atteindre un objectif à court terme. Elles s'apparentent donc davantage à des tactiques qu'à des stratégies de réponse globales.
- → Comme les stratégies ad hoc sont éminemment subjectives, il est possible qu'elles ne répondent pas à des besoins réels au niveau de l'individu ou de l'organisation. En conséquence, les DDH doivent s'assurer de faire en sorte qu'elles ne soient pas nuisibles au groupe de manière plus générale, surtout si les stratégies utilisées ne sont pas réversibles. Soulignez qu'il est nécessaire d'acquérir une perspective à long terme concernant les stratégies de sécurité. Et plus particulièrement, qu'il faut qu'une stratégie de sécurité réponde aux critères RADER pour être efficace.
- → En résumé, dans leur réflexion sur la sécurité et la protection, les DDH doivent tenir compte autant de leurs propres stratégies de sécurité ad hoc que de celles des autres personnes qui les entourent. Il est cependant d'une importance-clé de renforcer celles qui sont efficaces tout en limitant l'impact de celles qui peuvent nuire à d'autres collègues DDH.

L'ESPACE DE TRAVAIL SOCIOPOLITIQUE DES DDH

Introduisez le concept d'»espace de travail sociopolitique des DDH» **(NMP, pp.61-73)**. Basez votre présentation plus particulièrement sur la définition fournie dans le **NMP (p.71)**: «toute activité que le défenseur peut mener sans dépasser son seuil personnel de tolérance au risque». En d'autres termes, les limites de l'espace de travail sociopolitique sont définies par ce que le DDH estime être des conséquences acceptables ou inacceptables à son travail. Pour expliquer cette idée, vous pouvez utiliser ou adapter l'exemple fourni dans le NMP.

Poursuivez en expliquant la stratégie de sécurité global **(NMP, pp.73-75)**. Pour ce faire, dessinez sur votre paper-board l'illustration fournie dans le NMP pour expliquer les deux axes de l'espace de travail des DDH (tolérance/acceptation et dissuasion/persuasion) .



Clôturez cette section en expliquant aux participants qu'une stratégie de sécurité globale doit comprendre une dimension de plaidoyer : les actions entreprises dans le cadre d'une telle stratégie doivent contribuer à augmenter le coût politique des attaques commises contre les DDH et à réduire les niveaux d'impunité des agresseurs potentiels.

- → Les activités quotidiennes des DDH peuvent avoir un impact négatif sur les intérêts d'acteurs puissants (le gouvernement, les forces de sécurité, des groupes armés d'opposition, des entreprises multinationales, etc.). Il faut cependant garder à l'esprit que les acteurs puissants hostiles sont des entités complexes : ils ne forment pas un bloc homogène dans leur hostilité envers les DDH. Certains éléments parmi les forces de sécurité peuvent en effet être dévoués à la protection des défenseurs alors que d'autres sont à la source de menaces et d'agressions.
- → Si les participants vous demandent comment mesurer l'acceptabilité d'un risque, vous devrez leur rappeler que cela varie grandement en fonction des individus et des organisations. Par exemple, une personne X arrivera à son seuil d'acceptabilité après avoir reçu un coup de téléphone de menaces, mais une personne Y n'atteindra ce seuil qu'après l'assassinat de son fils. Le seuil d'acceptabilité peut aussi évoluer avec le temps (p.e., il y a deux ans je me fichais d'aller en prison, mais aujourd'hui plus). Les stratégies de sécurité doivent donc élargir et préserver l'espace de travail des DDH afin que ceux-ci puissent continuer à opérer.
- → L'illustration de l'espace de travail sociopolitique (NMP) devrait vous aider à expliquer que les DDH peuvent travailler dans un espace très réduit (représenté par l'intersection A) ou dans un espace plus large (intersection B). Idéalement, la stratégie de sécurité globale doit viser à faire passer les DDH de la situation A à la situation B en augmentant les niveaux de tolérance, d'acceptation, de dissuasion et de persuasion.
- → Concernant la dimension de plaidoyer de la stratégie de sécurité globale : il est essentiel pour les DDH de comprendre leur position (leur espace de travail) et de comprendre comment la renforcer (occuper l'espace de travail) en influençant les parties prenantes et les acteurs hostiles.

ACTIVITÉ : ÉLARGIR L'ESPACE DE TRAVAIL DES DDH (STRATÉGIE DE SÉCURITÉ GLOBALE)

L'objectif de la stratégie de sécurité globale est d'élargir l'espace de travail en augmentant chacun de ses quatre paramètres : la tolérance, l'acceptation, la dissuasion et la persuasion.

Divisez les participants en quatre groupes (ou faites l'activité avec tous les participants s'ils sont moins de huit). Chaque groupe devra proposer une série d'actions (min. 1, max. 3) visant à augmenter un des paramètres. Demandez aux groupes d'écrire une action par carton.

Si l'ensemble du groupe des participants est homogène, encouragez-les à réaliser l'exercice pour leur propre organisation / communauté. Si le groupe est hétérogène ou s'il y a des réticences à utiliser un cas réel, proposez un exemple fictif (voir ci-dessous, Conseils aux facilitateurs). Remédiez aux problèmes de compréhension de l'exercice s'il y en a.

Après 20 minutes de discussions en petits groupes, rassemblez tous les participants et utilisez les 20 minutes restantes pour demander aux groupes de venir coller les cartons où sont écrites leurs actions sur le mur, en les regroupant autour de chacun des paramètres. Demandez aux groupes d'expliquer brièvement les raisons pour lesquelles ils pensent que ces actions peuvent aider à obtenir plus de tolérance et d'acceptation de la part des agresseurs potentiels, ou peuvent dissuader et persuader ces agresseurs. Encouragez la discussion entre les différents groupes.

→ **Exemple fictif** : vous travaillez pour une ONG environnementale qui dénonce la pollution des réserves d'eau d'un village par une usine de production de papier détenue par une multinationale. La direction de l'usine, qui entretient des rapports avec de puissantes figures politiques locales, est ouvertement hostile aux rapports publiés par l'ONG. Lors d'une visite de terrain il y a deux jours, les leaders du village vous ont parlé d'une rumeur selon laquelle un politicien local prévoit d'engager des hommes de main pour «apprendre une bonne leçon» à cette bande d'écologistes «qui mettent en danger des emplois locaux avec leurs accusations infondées».

→ Si vous avez à éclaircir d'éventuelles incompréhensions pendant l'exercice, référez vous aux indications données dans le NMP pour chaque paramètre de l'espace de travail **NMP (pp.73-75)**.

CONCLUSION

Demandez aux participants de rappeler les éléments-clés de la session et répondez aux éventuelles questions ou inquiétudes. Rappelez aux participants qu'une stratégie de sécurité globale n'invalide pas les éventuelles stratégies et tactiques de dissuasion ad hoc déjà mises en place. L'idée est de renforcer celles qui sont efficaces tout en essayant de limiter celles qui sont potentiellement nuisibles.

Faites le lien entre cette session et les sessions 5.1 à 5.5, et expliquez en quoi cette session se nourrit des précédentes. Insistez sur le fait que les DDH ne seront capables d'élargir efficacement leur espace de travail que s'ils ont une compréhension claire de leur environnement de travail, de l'identité des agresseurs, et de leurs propres capacités et vulnérabilités.

Clôturez en rappelant aux participants qu'une stratégie de sécurité globale a pour but d'élargir et de préserver l'espace de travail des DDH (en travaillant sur les axes de la tolérance / acceptation et de la dissuasion / persuasion). Étayez vos remarques en montrant à nouveau l'illustration des deux axes de l'espace de travail **(NMP, p.72)**.

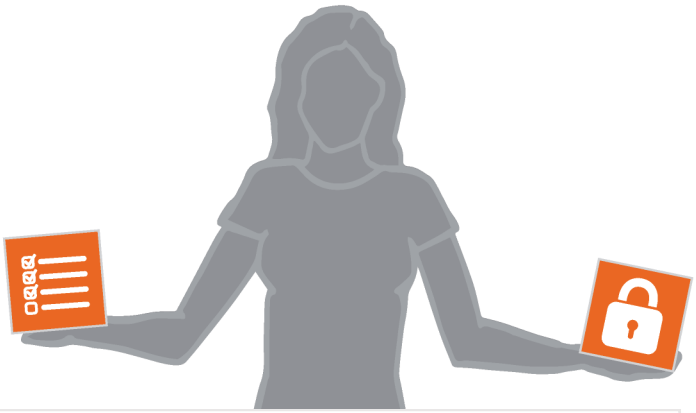
RESSOURCES COMPLÉMENTAIRES

> Van Brabant. Op. Cit. Chapitres 2 et 5.

> FLD. Op. Cit. Chapitre 5.

7. PRÉPARER UN PLAN DE SÉCURITÉ

> **CHAPITRE 1.7** NMP
PRÉPARER UN PLAN DE SÉCURITÉ



OBJECTIFS D'APPRENTISSAGE

> Les participants devront pouvoir identifier leurs propres objectifs de sécurité et de protection.

> Les participants devront pouvoir élaborer un plan de sécurité.

MESSAGES CLÉS

> Un plan de sécurité aide à réduire les vulnérabilités et à augmenter les capacités de manière à pouvoir faire face aux menaces ou à en diminuer la probabilité, réduisant ainsi les risques. Il est préférable d'avoir un plan de sécurité simple que les défenseurs pourront appliquer plutôt qu'un plan complexe qu'ils n'appliqueront probablement pas.

> Une bonne analyse de risques permet l'identification des principales menaces, vulnérabilités et capacités, en vue de mettre l'accent sur les choses les plus importantes dans le plan de sécurité. Dans le cas où les DDH ne disposent pas de beaucoup de temps ou de beaucoup de ressources, ceci leur permettra de faire en sorte que les ressources disponibles soient consacrées aux problèmes de sécurité prioritaires.

LA SESSION

DIFFICULTÉS POUVANT SURVENIR DURANT LA SESSION :

→ Élaborer un plan de sécurité simple et réaliste mettant l'accent sur les problèmes prioritaires.

→ Amener les participants à accepter le plan et leur indiquer comment commencer à l'appliquer à court et à moyen terme. Prendre en compte les besoins spécifiques de protection que peuvent avoir les femmes DDH ou tout autre groupe social particulier (populations indigènes, défenseurs LGBTI, défenseurs handicapés, etc.) en termes de stratégies, de normes de sécurité, etc., tant au niveau des protocoles de routine qu'au niveau des procédures d'urgence.

LA SESSION ÉTAPE PAR ÉTAPE :

Durée	Durée totale	Activité	Outil / méthode / matériel
20´		**Introduction**: • Objectifs et structure de la session. • Objectifs des mesures de sécurité.	Préparez les points à l'avance sur un paper-board ou dans une présentation PowerPoint.
90'	110'	**Élaborer un plan de sécurité.**	Résultats de l'analyse de risque réalisée au cours de la session 5.2. Feuilles de paper-board de la session 5.2. Paper-board Marqueurs Modèles de tableaux pour l'élaboration d'un plan de sécurité (à projeter via un ordinateur portable ou à préparer sur paper-board)
10'	120'	**Conclusion**	
		DURÉE : COMPTER 140 MINUTES (2 HEURES 20 MINUTES), DONT UNE PAUSE DE 20 MINUTES.	

ACTIVITÉS D'APPRENTISSAGE

OBJECTIF DES MESURES DE SÉCURITÉ

Pour introduire cette session, citez les trois objectifs généraux devant être inclus dans un plan de sécurité:

→ Faire en sorte qu'une personne cesse de faire quelque chose (p.e. qu'un agresseur cesse de menacer ou d'attaquer les DDH).

→ Faire en sorte qu'une personne fasse ce qu'elle doit faire (p.e. qu'une autorité légitime empêche des agresseurs de nuire aux DDH).

→ Faire en sorte que les DDH soient moins vulnérables et augmentent leurs capacités de protection.

Utilisez des exemples tirés des expériences personnelles des participants pour illustrer ces trois objectifs. Rappelez ensuite aux participants l'équation du risque (voir NMP et Chapitre 5.2. de ce Guide). Indiquez que les deux premiers objectifs concernent les menaces et que le dernier concerne les vulnérabilités et les capacités. Soulignez également le fait que les deux premiers objectifs sont liés à leurs capacités. Les mesures qu'ils prennent augmenteront en effet leur capacité à dissuader les agresseurs potentiels.

ÉLABORER UN PLAN DE SÉCURITÉ

L'élaboration d'un plan de sécurité complet est une tâche complexe qui requiert un temps considérable. Dans cet exercice, vous vous concentrerez uniquement sur la manière de concevoir un plan de sécurité simple basé sur les priorités établies par l'analyse de risques d'une organisation.

COMMENT TRAVAILLER:

Ce travail se base sur l'analyse de risques réalisée précédemment. Si vous travaillez avec un groupe homogène, référez-vous aux résultats de l'exercice d'évaluation de risques figurant dans le Chapitre 5.2. (Si vous travaillez avec un groupe hétérogène, voyez les Conseils aux facilitateurs.) Ayez à votre disposition les feuilles de paper-board de cet exercice, afin de faciliter le processus.

1. **Sélectionner les menaces les plus spécifiques:** Les participants devront choisir les menaces les plus sérieuses ou celles qui se rapportent le plus à leurs principales vulnérabilités, car ce sont ces menaces-là qui leur font encourir les plus grands risques (voir **NMP, chapitre 1.2.** fpour trouver des conseils et des indications). (10 minutes)
2. **Réévaluer les vulnérabilités :** Donnez aux participants quelques minutes pour réévaluer les vulnérabilités qu'ils ont associées précédemment aux menaces sélectionnées. Faites des ajustements là où vous pensez que c'est nécessaire. Focalisez-vous plus particulièrement sur ces vulnérabilités-là quand vous planifierez des actions visant à réduire les risques engendrés par les menaces sélectionnées. Souvenez-vous : toutes les vulnérabilités ne sont pas associées à toutes les menaces. (10 minutes)
3. **Réévaluer les capacités :** Demandez aux participants de réaliser le même exercice pour la liste des capacités qu'ils ont associées aux menaces sélectionnées. (10 minutes)
4. **Transformer les vulnérabilités en «objectifs» dans le plan de sécurité :** Aidez-vous du tableau ci-dessous (l'exemple n'est pas exhaustif). (30 minutes)

Menace	Objectif	Vulnérabilité (associée à la menace)	Objectif
«Effraction - Des effractions ont eu lieu dans d'autres bureaux.»	«Réduire la possibilité d'une effraction dans notre bureau.» «Réduire l'impact négatif d'une effraction dans nos bureaux si elle devait se produire.»	«Nous possédons des informations sensibles stockées dans les ordinateurs du bureau.»	«Même si une effraction a lieu, nous prévenons : • la perte d'informations stockées dans nos ordinateurs ; • l'accès à ces informations pour des personnes non-autorisées.»

5. **Développer chaque objectif :** Écrivez les actions pouvant être réalisées pour atteindre l'objectif. Attirez l'attention des participants sur le fait que des mesures de sécurité doivent inclure des actions préventives et des mesures réactives. Ces objectifs et ces actions constitueront la trame du plan de sécurité (30 minutes). Exemple :

Objectifs	Actions
«Réduire la possibilité d'une effraction dans notre bureau.»	• Conjointement avec d'autres organisations, faire une déclaration publique dénonçant le nombre d'effractions commises dans des organisations, et exigeant que des mesures soient mises en place par le gouvernement pour arrêter le phénomène. • - Exercer une pression sur les autorités concernées (la police et le pouvoir législatif) pour qu'elles enquêtent sur les intentions qui se cachent derrière la vague d'effractions et qu'elles traduisent les auteurs en justice.
«Même si une effraction se produit, nous ne perdrons pas les informations stockées sur les ordinateurs et des personnes non-autorisées ne pourront pas y avoir accès.» Note : cet objectif suppose que l'organisation possède dans son réseau de soutien des équipes de spécialistes en technologies de l'information.	• - Mettre en place un réseau informatique doté d'un serveur central. • - Effectuer des back-ups réguliers du disque dur du serveur central et conserver les copies dans un coffre ou dans un endroit protégé en dehors du bureau. • - Installer un programme de cryptage simple et sécurisé pour le serveur central, de manière à empêcher l'utilisation des informations en cas de vol du matériel.

6. **Faire la liste de toutes les actions à entreprendre, sous la forme d'un plan:** Pour cela, projetez sur un écran le tableau ci-dessous. Utilisez soit l'exemple fourni, soit un exemple tiré de l'expérience personnelle du groupe. Vous pouvez également choisir d'écrire les éléments-clés sur votre paper-board pour guider les participants dans leur travail de groupe, plus tard. Demandez aux participants de former des groupes de 4 à 5 personnes et attribuez un nombre égal de menaces à chaque groupe. Chaque groupe devra élaborer des mesures de sécurité pour chaque menace qui lui aura été attribuée. Pour rendre ce plan réaliste/opérationnel, soulignez qu'il est important d'attribuer un délai à chaque action et d'assigner des responsabilités. Chaque groupe devra ensuite présenter les résultats à l'ensemble de l'assemblée, et les actions proposées devront être débattues entre tous les participants. A la fin de l'exercice, ils auront la trame générale de leur plan de sécurité. Plus vous avez de temps à consacrer à cet exercice, plus le plan sera concret. L'organisation pourra commencer à travailler sur le plan immédiatement après la formation.

   Le tableau suivant illustre plus en détail l'élaboration du plan en utilisant les mêmes exemples :

Objectifs		Mesures de sécurité	Responsabilités	Coûts	Délai
Généraux (liés aux menaces)	**Spécifiques (liés aux vulnérabilités)**				
«Réduire les possibilités d'une effraction dans notre bureau».	«Même si une effraction a lieu, nous prévenons : • la perte d'informations stockées dans nos ordinateurs ; • l'accès à ces informations pour des personnes non-autorisées.»	Déterminer quelles informations sont sensibles afin de prendre des mesures complémentaires pour empêcher l'accès non-autorisé	**Chargés de programmes et membres de la direction**	**$0**	**Dans les trois mois**
		Mettre en place un réseau informatique avec un serveur central au bureau. Le serveur ne doit pas être facilement accessible aux personnes extérieures	**Chargé des technologies de l'information / Consultant externe en technologies de l'information**	**$0**	**Dans les trois mois**
		Acheter un disque dur externe	**Chargé des finances**	**$200**	**Dans les deux semaines**
		Faire un back-up (une copie) du disque dur du serveur central chaque semaine	**Chargé de l'information et de la communication**	**$0**	**Tous les mois**
		Conserver une copie du back-up dans un coffre ou dans un endroit sûr (à l'extérieur du bureau)	**Chargé de programmes**	**$0** (si on utilise un logiciel libre)	**Tous les six mois**
		Trouver, apprendre à utiliser, et utiliser un programme de cryptage	**Chargé de l'information et de la communication**	**$0** (si on utilise un logiciel libre)	**Dans les deux mois**

	Formation interne sur le programme de cryptage et sur les mots de passe sécurisés	**Tout le monde**	**$0**	**Dans le mois**
	Installer un programme de cryptage pour le serveur central et les back-ups, de manière à empêcher l'accès aux informations en cas de vol	**Chargé de l'information et de la communication**	**$0** (si on utilise un logiciel libre)	**Dans les deux semaines**
	Conjointement avec d'autres organisations, faire une déclaration publique dénonçant le nombre d'effractions commises dans des organisations, et exigeant que des mesures soient mises en place par le gouvernement pour arrêter le phénomène	**Chargé de l'information et de la communication**	**$0**	**Dans le mois**
	Exercer une pression sur les autorités concernées (la police et le pouvoir législatif) pour qu'elles enquêtent sur les intentions qui se cachent derrière la vague d'effractions et qu'elles traduisent les auteurs en justice	**Chargé de plaidoyer**	**$0**	**Immédiat**

→ **Communiquez aux participants les informations suivantes sur le lancement d'un processus de préparation d'un plan de sécurité:**

- **Un plan de sécurité n'est utile que s'il est mis en application :** disposer d'un plan de sécurité ne réduit pas automatiquement les risques. Les plans doivent être partagés, expliqués et appliqués pour avoir un impact sur la sécurité des DDH.
- **La gestion de la sécurité est un processus dynamique qui évolue avec le temps et qui requiert une réévaluation régulière:** Le risque est en effet un concept dynamique, car il dépend d'un environnement en perpétuel changement. Un plan qui est bon aujourd'hui sera peut-être inapproprié dans six mois. Si la situation évolue, les défenseurs doivent revoir leur analyse et leur plan en conséquence. Il faut penser la gestion de la sécurité comme un processus permanent, basé sur l'analyse de menaces, de vulnérabilités et de capacités changeantes, ainsi que sur le contexte sociopolitique.
- **Pour être efficaces, les plans de sécurité doivent être réalistes :** An effective security plan must take into account a realistic timeframe and the organisation's capacities. If the plan is too ambitious or demanding, it runs the risk of being shelved. Your role as facilitator is to ask questions that help defenders to assess whether their planned actions are realistic and achievable.
- **Les plans de sécurité doivent comprendre une dimension réactive et une dimension préventive.**

→ **Difficultés pouvant survenir lors de l'activité d'élaboration d'un plan de sécurité :**

- Vous travaillerez peut-être avec une longue liste de menaces et de vulnérabilités, ce qui pourra engendrer des difficultés. Une fois que vous aurez sélectionné les menaces, il ne faudra sélectionner

que les vulnérabilités qui y sont liées. Cela rendra l'exercice plus facile, et cela permettra au plan de cibler les problèmes de sécurité prioritaires. Voir **NMP, chapitre 1.7.** pour des exemples concrets

- Si vous travaillez avec un groupe hétérogène, vous devrez inventer un exemple ou diviser les participants en plusieurs groupes (chacun correspondant à une organisation). Une manière simple de procéder serait de se servir de l'activité réalisée dans le chapitre 5.2 de ce Guide. Gardez à l'esprit que s'il y a un manque de confiance entre les participants, il sera peut-être difficile d'échanger des détails ayant trait à des analyses de risques et à des plans de sécurité réels (d'où l'intérêt de travailler sur des exemples fictifs). Chaque organisation devra cependant réaliser les exercices, de manière à pouvoir définir son propre plan de sécurité au terme de l'atelier.
- Les participants confondront peut-être objectifs et actions. Cela ne devrait pas poser de problème tant qu'ils parviennent à définir des mesures de sécurité pertinentes et concrètes. Ne perdez donc pas trop de temps à des éclaircissements purement conceptuels. Consacrer plutôt vos efforts à obtenir des résultats concrets.

CONCLUSION

> Demandez aux participants de rappeler les enseignements-clés.

> Rappelez-leur l'importance d'intégrer dans la conception du plan de sécurité les analyses effectuées dans les sessions précédentes en matière de gestion de la sécurité (analyse du contexte, évaluation des risques, analyse des menaces et des incidents de sécurité).

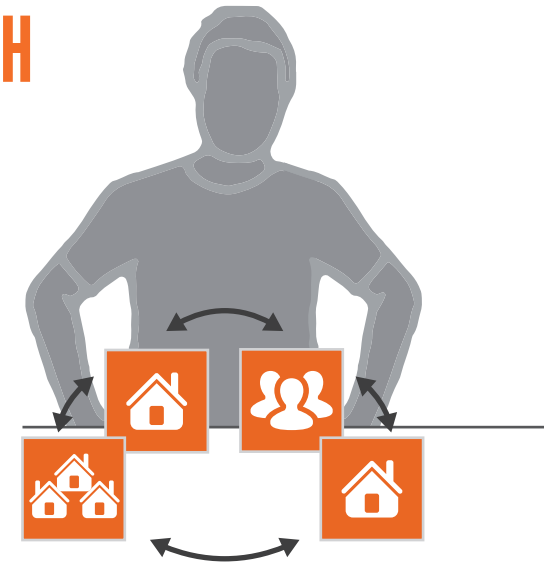
> Indiquez aux participants que pour le travail à suivre il leur sera utile de lire le chapitre du NMP consacré à ce thème.

RESSOURCES COMPLÉMENTAIRES

> Van Brabant. Op. Cit. Chapitre 5. (pp. 56-72) et chapitre 21. (pp. 310-322).

> FLD. Op. Cit. Chapitre 5

8. RÉSEAUX DE PROTECTION POUR DDH BASÉS DANS DES COMMUNAUTÉS RURALES



> PI & UDEFEGUA (2009). CUIDÁNDONOS: GUÍA DE PROTECCIÓN PARA DEFENSORES Y DEFENSORAS DE DERECHOS HUMANOS EN ÁREAS RURALES. GUATEMALA. PP. 89-113

CETTE SESSION S'ADRESSE UNIQUEMENT AUX COMMUNAUTÉS ET ORGANISATIONS RURALES ACTIVES AU NIVEAU LOCAL. ELLE S'APPUIE SUR LES CHAPITRES 5.1 À 5.5 ET PRÉSENTE UNE INTRODUCTION À LA SÉCURITÉ COLLECTIVE ET À LA GESTION DE SÉCURITÉ POUR CES GROUPES PARTICULIERS DE DDH.

OBJECTIFS D'APPRENTISSAGE

> Renforcer la capacité collective à faire face aux risques auxquels sont confrontés les DDH qui travaillent avec des communautés rurales.

> Comprendre la dynamique des réseaux de sécurité.

MESSAGES CLÉS

> La gestion collective de la sécurité dans des zones rurales où les habitants sont éparpillés sur de vastes territoires nécessite de l'organisation et de la coordination.

> Il est plus aisé de partager les risques si des liens forts unissent la communauté.

LA SESSION

DIFFICULTÉS POUVANT SURVENIR DURANT LA SESSION :

→ Parvenir à s'appuyer sur le travail réalisé lors des sessions précédentes, et plus particulièrement celles comprises dans les Chapitres 5.2. and 5.6. de ce Guide.

→ Trouver un espace suffisant pour mener à bien la session. Faites en sorte d'avoir à votre disposition un local spacieux où il vous sera possible d'afficher aux murs de nombreux cartons, feuilles de paper-board et autres documents utiles.

→ Adapter les stratégies de protection en zones rurales à l'approche de la protection en réseau.

→ Rendre le contenu et les concepts de la session accessibles à des participants ayant un faible niveau d'éducation scolaire, voire analphabètes.

→ Prendre en compte les besoins spécifiques de protection que peuvent avoir les femmes DDH ou tout autre groupe social particulier (populations indigènes, défenseurs LGBTI, défenseurs handicapés, etc.) en termes de stratégies, de normes de sécurité, etc., tant au niveau des protocoles de routine qu'au niveau des procédures d'urgence.

LA SESSION ÉTAPE PAR ÉTAPE :

Durée	Durée totale	Activité	Outil / méthode / matériel
10´		**Introduction:** • Objectifs et structure de la session	Préparez à l'avance les points abordés sur un paper-board*
60'	70'	**Stratégies de sécurité et mesures de sécurité** • Examen d'une analyse de risques (15') • Qu'est-ce qu'une mesure de sécurité? Qu'est-ce qu'une stratégie de sécurité? (15') • Activité n°1 : Élaborer des stratégies de sécurité (30')	Représentation sur paper-board de la balance des risques Représentation sur paper-board des critères RADER pour une stratégie de sécurité efficace ; Représentation sur paper-board du tableau des mesures de sécurité (voir ci-dessous) ; Feuilles de paper-board vierges et marqueurs. Utilisez les vidéos de PI "Stratégies de protection" et "Objectifs de sécurité et de protection" comme informations contextuelles.
140	210'	**Réseaux de protection.** • Activité n°2 : Exercice : marcher ensemble (30') • Explication du concept de réseaux de protection (30') • Première réflexion collective sur les réseaux de protection (10') • Activité n°3 : Réseaux sociaux et filets de pêche (20') • Activité n°4 : Récit(s) concernant des communautés (15') et réflexion collective finale sur le(s) récit(s) (35')	Téléphone ; Tableau ; Image agrandie d'un réseau de protection ; Autocollants ou cartons représentant les différents éléments d'un réseau de protection (flèches ; Objectif ; Comité du réseau de protection ; Commission d'analyse et d'alerte anticipée ; Notre communauté ; Autre communauté ; Institutions nationales des droits humains ; Organisations de soutien nationales / internationales ; Institutions internationales) ; Image agrandie d'un filet de pêche ; Impressions sur papier des récits
10'	220'	**Conclusion**	
		DURÉE : COMPTER 240 MINUTES (4 HEURES), DONT UNE PAUSE DE 20 MINUTES.	

** Vous pouvez également utiliser un ordinateur portable, un projecteur et des hauts-parleurs. Il se peut cependant que si vous ayez difficilement accès à l'électricité dans certaines zones reculées.*

ACTIVITÉS D'APPRENTISSAGE

RISQUES, MESURES DE SÉCURITÉ ET STRATÉGIES DE SÉCURITÉ

EXAMEN D'UNE ANALYSE DE RISQUES

Cette partie de la session se base sur l'analyse de risques réalisée précédemment par les participants (voir chapitre 5.2 de ce Guide). Rappelez aux participants les résultats de l'analyse de risques en affichant au mur la balance des risques et les résultats de leurs travaux précédents sur ce thème. Expliquez que les mesures de sécurité doivent être élaborées en fonction des résultats de la balance des risques.

QU'EST-CE QU'UNE MESURE DE SÉCURITÉ? QU'EST-CE QU'UNE STRATÉGIE DE SÉCURITÉ?

L'idée est de présenter aux participants quelques exemples de stratégies et de mesures de sécurité adaptés aux besoins d'une communauté et à ceux d'un individu. Votre intervention devra donc se baser sur les méthodes et les activités décrites dans le chapitre 5.6. de ce Guide. Soulignez plus particulièrement la nécessité de concevoir des stratégies de sécurité permettant aux DDH de gérer les risques tout en continuant à faire leur travail et à vivre leur vie dans un environnement sûr. Poursuivez en présentant les six stratégies de sécurité pour gérer le risque (**NMP, p. 69, et guide Cuidándonos [non disponible en français], pp. 15-22**).

- → Pour vous assurer d'obtenir une discussion utile quand vous expliquez les six stratégies de gestion du risque, une bonne façon de faire consiste à demander aux participants s'ils ont déjà eux-mêmes utilisé une de ces stratégies. Ils ne les auront peut-être pas identifiées comme stratégies à l'époque, et réaliseront seulement maintenant que leur réaction à une situation qu'ils devaient affronter relevait d'une des stratégies examinées au cours de cette session. En fonction du temps disponible, vous pourrez choisir une ou plusieurs de ces stratégies ad hoc et les analyser selon les critères RADER.
- → Vous pouvez également donner des exemples concrets de stratégies de sécurité fournis dans le guide Cuidándonos (pp. 104-111).
- → Clôturez l'activité en indiquant que lorsque des DDH sont menacés, leur niveau de stress augmente et ils ressentent le besoin d'agir rapidement. Cependant, le fait d'analyser les stratégies selon les cinq critères les aidera à choisir des stratégies efficaces basées sur une perspective à long terme.

ACTIVITÉ : ÉLABORER DES STRATÉGIES DE SÉCURITÉ

Formez autant de groupes que nécessaire pour analyser les menaces et les incidents de sécurité qui ont été identifiés précédemment (habituellement entre deux et quatre). Le nombre de personnes par groupe doit être plus ou moins égal.

Chaque groupe doit analyser une menace ou un incident de sécurité (pour simplifier, vous pouvez regrouper les menaces ou les incidents de sécurité qui présentent les mêmes modèles), puis tenter de concevoir des stratégies de sécurité pour y faire face. Donnez une feuille de paper-board vierge à chaque groupe et demandez aux participants d'y recopier le tableau des mesures de sécurité ci-dessous, puis de le remplir pour le cas qui leur a été attribué.

Menace/incident de sécurité spécifique ou modèle	Vulnérabilités	Capacités	Mesures	Responsabilités	Délai
...	...	...	...	...	...
...	...	...	...	...	...

Quand les groupes auront fini de remplir leur tableau, rassemblez tous les participants et demandez à un représentant de chaque groupe d'afficher son tableau au mur et de présenter son travail. Encouragez les autres groupes à poser des questions et à commenter les résultats. Sur base de la discussion, les participants devront soit accepter les mesures de sécurité, soit en proposer de nouvelles. Insistez sur la nécessité de définir des priorités, d'attribuer des responsabilités et de s'accorder sur un délai d'action réaliste.

RÉSEAUX DE PROTECTION

Avant d'introduire le concept de réseau de protection, proposez l'exercice suivant :

ACTIVITÉ N°2 : MARCHER ENSEMBLE

Cette activité permet aux participants de se rendre compte à quel point il est difficile de marcher ensemble. Pour arriver à une bonne coordination, il est fondamental d'être organisé et d'établir un leadership.

Placez un téléphone sur une table au centre de la pièce et demandez aux participants de former deux groupes (de taille égale).

Chaque groupe se rassemble séparément à 10 mètres l'un de l'autre et à 10 mètres du téléphone. Expliquez aux deux groupes que chaque participant doit tenir l'oreille d'un second participant et le genou d'un troisième, de manière à former un grand nœud humain. Ensuite, dites aux deux groupes de se mouvoir en direction du téléphone, sans se dénouer, pour aller faire un appel téléphonique d'urgence.

Si les groupes se détachent avant d'avoir atteint le téléphone, demandez-leur d'essayer une nouvelle fois. Dites-leur de réfléchir pour trouver comment ils pourraient atteindre le téléphone sans défaire le nœud. L'activité se termine si l'un des groupes atteint le téléphone ou si les deux groupes se disloquent une deuxième fois. Observez les difficultés qui surviennent lorsque les participants essaient de bouger en groupe.

Pour résumer l'exercice, demandez au groupe de se livrer à une réflexion collective : demandez aux participants comment ils se sont sentis pendant l'activité et pourquoi ils ont réussi ou n'ont pas réussi à atteindre le téléphone. Si les groupes ne le disent pas eux-mêmes, expliquez que le nœud symbolise un réseau. Le nœud fait qu'il est difficile de marcher ensemble (citez quelques unes des difficultés que vous avez pu noter). Mais si les éléments emmêlés dans ce nœud s'organisent et créent un modèle de leadership qui les rassemble, ils parviendront à avancer ensemble et à atteindre le téléphone pour appeler à l'aide.

→ Considérez cette activité comme une dynamique de groupe, mais reliez-là aussi à la question de la sécurité. Soulignez l'importance de la cohésion de la communauté pour la gestion de la sécurité.

EXPLIQUEZ COMMENT FONCTIONNENT LES RÉSEAUX DE PROTECTION (GUIDE CUIDÁNDONOS, P. 89-113).

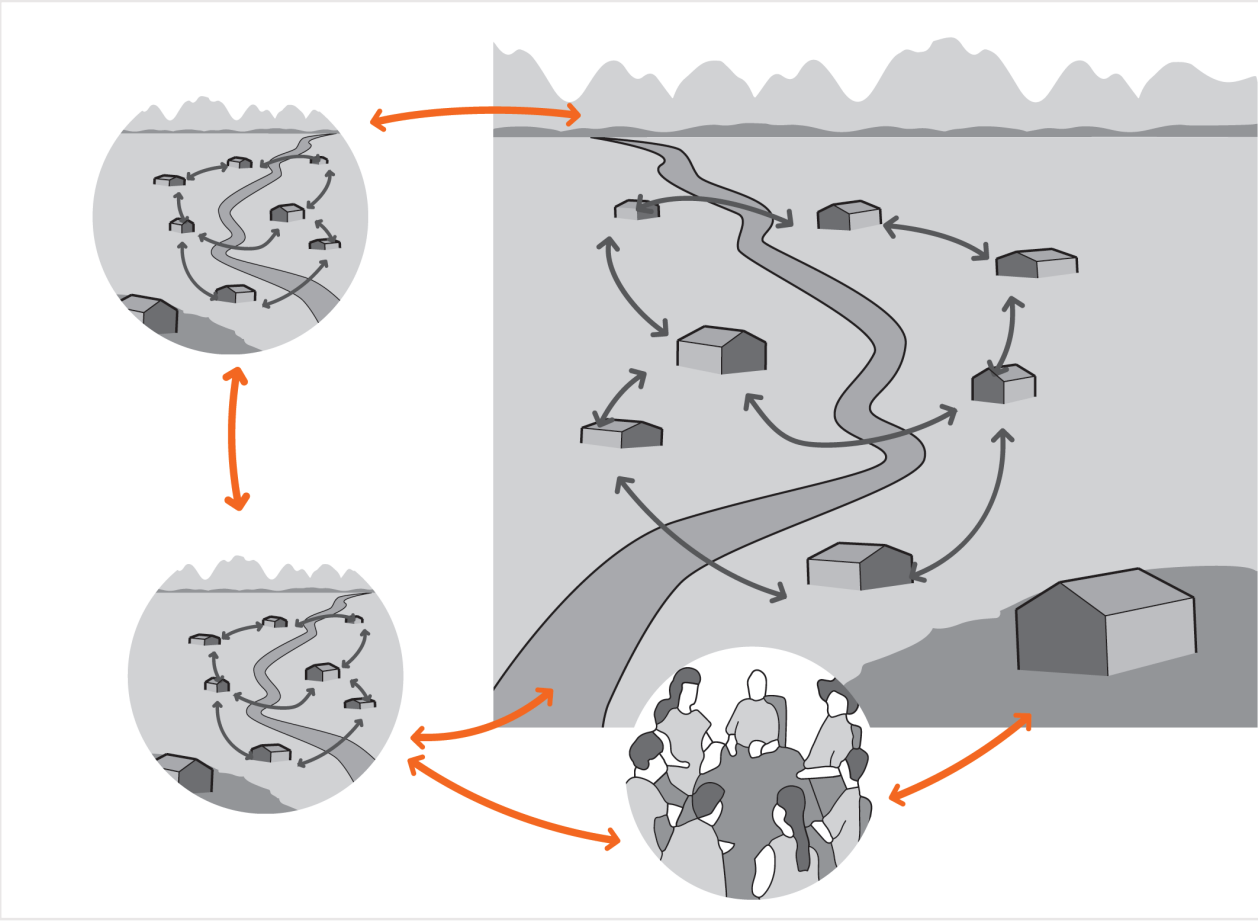
Affichez au mur l'image ci-dessous agrandie pour illustrer le concept de réseau de protection.

Utilisez l'image pour décrire le réseau de protection idéal. Placez sur l'image les cartons/autocollants où sont écrits les différents éléments composant un réseau de protection, tout en les lisant (utilisez l'illustration dans le **guide Cuidándonos, p.97**, pour plus d'indications).

Expliquez ce qu'est un réseau de protection (voir les Conseils aux facilitateurs pour plus d'indications). L'**objectif** des réseaux de protection est de protéger les DDH qui travaillent avec des communautés et avec des organisations actives localement, et de défendre leurs territoires (placez l'autocollant consacré à l'objectif des réseaux de protection sur l'image).

Toute communauté doit créer son propre **comité de réseau de protection** (placez l'autocollant corres-

pondant à côté de la grande maison dans le coin inférieur droit de la grande zone verte). Le comité est en charge de la coordination et de la prise de décisions en matière de sécurité et de protection. Il s'assure du respect des mesures de sécurité et guette les problèmes de sécurité et de protection.



Pour assurer la protection de la communauté, il est essentiel de mettre en place et de maintenir une communication de haute qualité sur base régulière avec d'autres organisations. Ceci inclut les autres communautés, les institutions nationales des droits humains, les organisations nationales et internationales, et les organes internationaux (placez les autocollants correspondants sur l'image : les autres communautés sont représentées par les petites zones vertes à gauche de la communauté principale, les autres organisations doivent être placées au bout des flèches rouges).

Certains membres du comité du réseau de protection doivent être désignés comme officiers de liaison chargés de la communication avec ces autres organisations. Une fois que le réseau de protection a été étendu à d'autres organisations, il doit être possible de créer un second comité de coordination rassemblant tous les acteurs qui soutiennent la communauté. On l'appellera la **Commission d'analyse et d'alerte précoce** (placez l'autocollant correspondant à côté du cercle représentant des personnes en réunion). Cette commission se compose d'un représentant de la communauté (qui est également membre du comité du réseau de protection) et de représentants d'autres communautés et organisations. Ces personnes doivent avoir de bonnes facultés d'analyse et doivent bénéficier de la confiance de la communauté.

Le processus de gestion de la sécurité des réseaux de protection consiste en **trois étapes** : **a)** l'information, **b)** l'analyse, **c)** la prise de décision. Ces étapes doivent être suivies aux trois niveaux de la gestion de la sécurité : **1)** au niveau de l'individu, **2)** au niveau de la communauté, **3)** en coordination externe avec d'autres organisations ou communautés.

→ **A. INFORMATION:**

La communauté doit s'efforcer de recueillir des informations sur ce qui se passe sur son territoire, puis partager ces informations au sein de la communauté en utilisant des canaux de communication efficaces (les flèches bleues dans l'illustration).

→ **B. ANALYSE :**

Sur base de ces informations, la communauté devra parvenir à ses propres conclusions concernant les risques encourus. Cette étape est celle de l'analyse de risques. Rappelez aux participants les méthodes d'analyse du contexte et des risques vues au cours des sessions du chapitre 5.1 et 5.2 de ce Guide.

→ **C. PRISE DE DÉCISION:**

Les décisions en matière de mesures de sécurité doivent être prises sur la base de l'analyse des risques. Au niveau **individuel**, chaque membre de la communauté doit être attentif à son environnement (rappelez aux participants la session du **Chapitre 5.4.**) et doit analyser les risques qu'il encourt. Toutes les informations recueillies doivent être transmises au comité du réseau de protection. Au niveau de la **communauté** , chaque membre a la responsabilité de rassembler des informations concernant les menaces et les incidents de sécurité subis par la communauté. Le niveau de la communauté est crucial, car c'est à ce niveau que le contrôle du territoire est affirmé. Encore une fois, les informations recueillies doivent être communiquées au comité du réseau de protection, qui les analysera et qui prendra les mesures collectives nécessaires pour protéger la communauté et pour organiser une réaction si c'est nécessaire. Enfin, au niveau **externe** , les informations obtenues doivent être transmises à la Commission d'analyse et d'alerte anticipée. Cet organe se charge de l'analyse globale et décide des mesures de sécurité à prendre et des éventuelles actions à mener. Le représentant de la communauté auprès de la Commission est chargé de communiquer l'analyse, les informations et les alertes à la communauté.

→ L'objectif des réseaux de protection est de protéger les DDH travaillant dans des communautés rurales et de sécuriser leur espace de travail. Le concept se base sur le principe selon lequel toute protection, si elle se veut efficace, doit émaner de la communauté et/ou de l'organisation locale elle-même, de manière à faire en sorte que toutes les activités et tous les efforts réalisés soient bien mis en commun. Les stratégies et les mesures de protection destinées à assurer la sécurité des habitants ou des membres d'une organisation sont donc intimement liées à la défense de leur territoire, un enjeu qui se définit en termes politiques et géographiques.

→ On pourrait décrire les réseaux de protection comme des réponses ou des efforts collectifs menés au sein d'une communauté, ou partagés entre une communauté et des organisations externes, destinés à répondre aux risques encourus et à la répression subie en raison de leurs actions de défense des droits humains.

→ Une organisation efficace constitue le cœur-même d'un réseau de protection

PREMIÈRE RÉFLEXION COLLECTIVE SUR LES RÉSEAUX DE PROTECTION

Après cette section assez théorique sur les réseaux de protection, encouragez les participants à discuter et à réfléchir au sujet de ces réseaux. Réexpliquez les concepts si nécessaire. Les facilitateurs peuvent utiliser des exemples réels pour illustrer leurs explications (le **guide Cuidándonos** propose une série d'exemples rapportés d'Amérique latine).

La discussion pourra aboutir aux conclusions suivantes :

Les réseaux de protection sont utiles pour :

→ Connaître et analyser les informations dont les communautés ont besoin pour protéger leur territoire.

→ Partager ces informations.

→ Être capable d'élaborer des jugements et de prendre des décisions pour protéger la communauté.

→ Rechercher des alliances avec d'autres acteurs partageant les mêmes buts.

→ Mener des actions conjointes.

→ Résister.

Quand la discussion vous semblera terminée, passez aux activités suivantes, qui vous aideront à illustrer plus en profondeur le concept de réseau de protection:

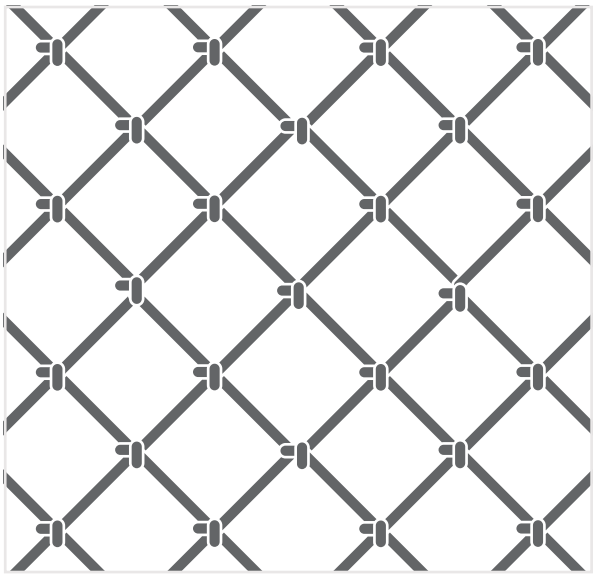
ACTIVITÉ N°3 : COMPARAISON ENTRE LES RÉSEAUX SOCIAUX ET DES FILETS DE PÊCHE

Il n'est pas toujours facile d'expliquer ce qu'on entend précisément par réseau. La compréhension de la notion de réseau est largement intuitive. Ce caractère intuitif aide à expliquer le concept, mais il rend également plus difficile la tâche de creuser la question plus en profondeur. Pour simplifier cette tâche, il peut être utile de comparer les réseaux avec des filets de pêche.

→ **PRÉSENTEZ L'ACTIVITÉ DE CETTE MANIÈRE:**

Nous avons vu que les réseaux de protection sont composés d'individus et d'organisations qui entretiennent des contacts réguliers pour échanger des informations, prendre des décisions et agir sur des questions de protection qui concernent leurs membres. Les réseaux ne se présentent pas toujours eux-mêmes comme tels. Quand nous parlons de réseaux, nous faisons référence à toutes les interactions entre des individus et des organisations pouvant avoir lieu sous de nombreuses formes différentes et à différents niveaux.

→ **ENCOURAGEZ LES PARTICIPANTS À ENGAGER LA DISCUSSION:**



Affichez au mur une grande image d'un filet de pêche. Demandez aux participants ce qui est le plus important : les **cordes** ou les **nœuds**? Écoutez leurs réponses et notez-les sans faire de commentaire. Ensuite, dressez une comparaison entre les filets de pêche et les réseaux sociaux. Demandez aux participants si ce qu'ils ont dit au sujet des filets de pêche s'applique aussi aux réseaux sociaux. A ce stade, vous pouvez faire remarquer d'autres aspects que les participants auront omis (voir Conseils aux facilitateurs).

→ La réponse logique à la question de savoir ce qui est le plus important entre les cordes et les nœuds, est : les deux. Sans nœuds, les cordes ne sont que des cordes, il n'y a pas de filet. D'un autre côté, il est impossible de faire des nœuds sans cordes. On pourrait aussi dire que les filets ne sont pas tous les mêmes, qu'ils diffèrent selon l'espacement plus ou moins grand des nœuds, c'est-à-dire selon la largeur des mailles. Si les nœuds sont trop éloignés les uns des autres, le filet sera inutilisable, puisque tous les poissons pourront passer entre ses mailles. Au niveau de la sphère sociale, on pourrait dire de la même manière que s'il n'y a que quelques personnes ou quelques organisations dans un réseau (peu de cordes) et que celles-ci n'entretiennent pas beaucoup de contacts (peu de nœuds), alors le réseau social ne sera pas très fort.

→ Ces éléments aideront à tirer des conclusions de la discussion : de la même manière qu'un filet solide permettra de faire une meilleure pêche, un réseau fort et bien structuré permettra une meilleure collaboration. Si vous voulez attraper de gros poissons, vous aurez besoin d'un filet solide. Un filet fragile se cassera facilement. La même chose vaut pour les communautés : une communauté fragile ne sera pas capable d'affronter un ennemi grand et fort, elle se brisera avant d'avoir atteint ses objectifs. Mais de la même façon que différentes communautés peuvent se réunir pour se renforcer, le pêcheur qui veut rendre son filet plus efficace pour attraper de plus gros poissons pourra utiliser différentes cordes ou augmenter le nombre de nœuds de son filet.

ACTIVITÉ N°4: RÉCIT(S) CONCERNANT DES COMMUNAUTÉS

TCette activité a pour but d'aider les participants à comprendre **1)** les faiblesses et les forces des réseaux de protection, et **2)** comment les réseaux de protection contribuent au renforcement des communautés. Un récit fictif d'une situation souvent rencontrée par les communautés vous est proposé ci-dessous (voir l'**Annexe de ce chapitre**). Les facilitateurs sont cependant encouragés à se montrer créatifs et à inventer leur propre récit en l'adaptant aux expériences et aux contextes locaux. Mais il leur est également conseillé d'être très prudents, afin d'éviter que des participants ne ressentent certains éléments comme des allusions pouvant interférer avec le bon déroulement de l'atelier.

Si vous décidez de n'utiliser qu'une seule histoire, distribuez-en une copie à chaque participant et demandez à l'un d'entre eux de la lire à voix haute. Si vous utilisez deux histoires, divisez les participants en deux groupes. Les membres de chaque groupe doivent se rassembler et l'un d'entre eux doit lire à voix haute une des histoires. Ensuite, les groupes doivent discuter au sujet d'une série de questions posées par le facilitateur. Quand le travail de groupe est terminé, chaque groupe doit lire son histoire à voix haute devant tous les participants et rendre compte de la discussion qu'il vient d'avoir. Cela permettra aux membres de l'autre groupe d'exprimer leur avis sur le sujet. La session se termine quand les participants sont arrivés au bout des deux discussions.

Utilisez les questions suivantes pour guider les réflexions (voir Conseils aux facilitateurs) :

→ Quels aspects d'un réseau de protection cette histoire concerne-t-elle ?

→ Comment un réseau de protection aurait-il pu être utile à la communauté dans cette histoire ?

→ Quels aspects d'un réseau de protection cette histoire concerne-t-elle ? Parmi d'autres éléments, vous pouvez mentionner ceux-ci : la communauté n'avait pas accès aux informations sur les plans de construction d'une autoroute ; elle n'avait pas de contacts dans la ville à qui exprimer son opposition ; elle pensait qu'il serait suffisant d'envoyer une simple communication écrite ; quand les membres de la communauté se sont réunis après l'arrivée des pelleteuses ils n'ont pas collaboré ; les quelques personnes qui ont agi ont été arrêtées ; la communauté ne s'est pas préparée pour le retour des pelleteuses ; elle ne disposait pas de système d'alerte anticipée ; elle n'avait pas de contact à prévenir en cas de retour des pelleteuses, etc.

→ Comment un réseau de protection aurait-il pu être utile à la communauté dans cette histoire? Il aurait pu se renseigner sur le projet de construction ; analyser la situation ; définir des mesures de protection ; désigner des représentants chargés de s'occuper du problème ; coordonner les actions ; établir un système d'alerte anticipée ; établir des contacts préliminaires avec des personnes ou des communautés susceptibles d'être des alliées (par exemple le prêtre de la communauté voisine, etc

CONCLUSION

> Demandez aux participants de rappeler les éléments-clés de la session et répondez aux éventuelles questions ou inquiétudes.

> Montrez aux participants qu'une stratégie de sécurité globale doit s'appuyer sur les enseignements tirés lors des sessions et des étapes précédentes du processus de gestion de la sécurité.

> Demandez aux participants s'ils pensent que les réseaux de protection peuvent être utiles pour les aider à gérer les risques auxquels ils sont confrontés.

RESSOURCES COMPLÉMENTAIRES

> Van Brabant. Op. Cit. Chapitres 2 et 5.

> FLD. Op. Cit. Chapitre 5

ANNEXE À CE CHAPITRE

LA COMMUNAUTÉ CONTRE L'AUTOROUTE

Voici l'histoire d'une petite communauté d'environ 200 familles qui vivait dans une région montagneuse, à l'entrée d'une vallée située à quelques kilomètres de la ville. Dans le passé, cette zone avait été traversée par les routes qui reliaient les régions montagneuses à la vallée, comme en témoigne un ancien chemin de terre.

Un jour, le maire de la communauté a été informé des plans du gouvernement régional de construire une autoroute passant en plein milieu de la communauté. Cela impliquait l'achat obligatoire des terres situées en plein centre de la communauté, ce qui représentait environ la moitié de son territoire. La nouvelle a plongé les habitants de la communauté dans une grande inquiétude. Ils allaient perdre leurs terres en sachant que l'argent qu'ils recevraient en compensation ne leur suffirait pas pour refaire leurs vies ailleurs. Ils n'avaient en outre aucune envie de quitter un endroit qui appartenait à leurs familles depuis des générations. Les personnes habitant plus haut dans la montagne ont réalisé que l'autoroute affecterait la communauté de nombreuses façons, et que leurs vies ne seraient plus jamais les mêmes. La communauté a donc décidé de s'opposer à la construction de la route. Il faut savoir qu'il était également possible de tracer une trajectoire de route alternative, contournant les montagnes pour traverser une vallée inhabitée. Mais cette solution aurait été plus chère et aurait pris plus de temps à construire, ce qui aurait réduit les profits pour l'entreprise de construction.

Le maire, qui était en poste depuis de nombreuses années, a commencé à représenter les intérêts de la communauté et a organisé une réunion avec plusieurs habitants pour discuter de ce qu'il fallait faire. Tous étaient très en colère, et ont donc décidé de d'écrire une lettre de protestation au gouvernement régional. Après six mois, aucun progrès n'avait été fait. A ce stade, certaines familles avaient reçu une lettre officielle les informant qu'elles devaient quitter leur propriété en l'échange d'une compensation financière non-spécifiée.

Un jour, les habitants ont vu arriver deux grandes pelleteuses et cinq camions, protégés par un groupe de gardes travaillant pour une entreprise de sécurité privée. C'est ainsi qu'ils ont compris que les travaux étaient sur le point de commencer et que leur lettre avait été ignorée. L'ensemble de la communauté s'est réuni en urgence et une dizaine de personnes parmi les plus en colère ont proposé de s'opposer aux travaux et de les forcer les ouvriers à s'en aller. Le reste de la communauté hésitait, en partie par peur des gardes de sécurité et en partie parce que c'était la première fois qu'ils étaient confrontés à une telle situation. Le groupe d'hommes en colère, jugeant qu'il n'y avait plus de temps à perdre, a alors décidé de se mettre en travers du passage des machines. Une bagarre a éclaté avec les gardes de sécurité, faisant trois blessés parmi les habitants et deux parmi les gardes. Après cet événement, les machines et les gardes ont quitté la communauté, à la grande joie des habitants. Après deux semaines durant lesquelles rien n'est arrivé, la communauté a commencé à retrouver son calme habituel.

Puis, un jour, les machines sont revenues, tôt le matin, cette fois escortées par 40 gardes de sécurité armés de pistolets et accompagnés de chiens. Les pelleteuses se sont mises au travail immédiatement. La communauté n'avait pas envisagé comment elle devrait réagir face à une telle situation. Le maire et quelques uns des individus qui avaient mené l'action la première fois n'étaient pas présents, car ils se trouvaient en ville pour traiter les affaires de la petite coopérative dont ils étaient membres. Pendant que les machines commençaient à travailler, les gardes de sécurité faisaient le tour de la communauté pour arrêter ceux qui les avaient attaqués la fois précédente. Un des gardes qui avaient été blessés à cette occasion désignait les personnes à arrêter. Quand un groupe de femmes s'est approché des gardes et leur a demandé où ils emmenaient les hommes, les gardes ont simplement répondu qu'ils allaient leur apprendre une bonne leçon. Personne ne savait quoi faire, jusqu'à ce que quelqu'un pense à avertir le prêtre qu'ils avaient vu le jour précédent en chemin vers une autre communauté située à une quinzaine de kilomètres. Mais personne ne savait si le prêtre n'était pas déjà parti vers une autre communauté plus au nord. Au crépuscule, les pelleteuses sont parties, en même temps que les gardes. Le même soir, les membres de la communauté ont formé un petit comité qui s'est rendu à la ville la plus proche avec l'intention de parler à la police et d'apprendre où leurs voisins avaient été emmenés. Le maire est rentré à la nuit tombante, et après avoir appris ce qui s'était produit, a convoqué une réunion à la première heure le lendemain matin.

9. LA SÉCURITÉ DE L'ORGANISATION

> NMP **CHAPITRE 1.8**
AMÉLIORER LA SÉCURITÉ AU TRAVAIL ET AU DOMICILE

> NMP **CHAPITRE 2.1.**
ÉVALUER LA PERFORMANCE DE SÉCURITÉ DE L'ORGANISATION : LA ROUE DE LA SÉCURITÉ

> NMP **CHAPITRE 2.2**
S'ASSURER DU RESPECT DES RÈGLES ET PROCÉDURES DE SÉCURITÉ

> NMP **CHAPITRE 3.1.**
COMMENT RÉDUIRE LES RISQUES LIÉS À LA PERQUISITION ET / OU AU CAMBRIOLAGE D'UN BUREAU

OBJECTIFS D'APPRENTISSAGE

> Pouvoir évaluer la gestion globale de la sécurité d'une organisation (ou d'une communauté).

> Parvenir à améliorer le respect des règles de sécurité au sein d'une organisation.

MESSAGES CLÉS

> Pour évaluer votre sécurité, il vous faut respecter une double approche : d'une part l'autoévaluation, et d'autre part l'évaluation de la manière dont les autres vous perçoivent.

> La sécurité est l'affaire de tous.

> Pour veiller au respect des règles et des protocoles de sécurité, il est fondamental de construire une culture de la sécurité au niveau de l'organisation.

> Les règles ne sont observées que si elles sont pleinement comprises par tout le monde.

> Une bonne gestion de la sécurité demande du temps et des ressources.

LA SESSION

DIFFICULTÉS POUVANT SURVENIR DURANT LA SESSION :

→ Des difficultés et des sensibilités liées à la dynamique de l'organisation peuvent apparaître.

→ Les informations et les concepts proposés sont complexes.

→ Il faut prendre en compte les besoins spécifiques de protection que peuvent avoir les femmes DDH ou tout autre groupe social particulier (populations indigènes, défenseurs LGBTI, défenseurs handicapés, etc.) en termes de stratégies, de normes de sécurité, etc., tant au niveau des protocoles de routine qu'au niveau des procédures d'urgence.

→ Cette session ne s'adresse qu'aux organisations actives en milieu urbain. Si vous travaillez avec des communautés ou des organisations actives localement en milieu rural, nous vous recommandons de vous focaliser uniquement sur la partie **Observation des règles et des protocoles de sécurité** et d'ignorer l'analyse de cas. La discussion autour d'une affirmation fonctionne bien pour cette session, mais vous devrez tenir compte des caractéristiques et des besoins spécifiques de ces organisations (voir **chapitre 5.8 de ce Guide** ainsi que le **guide Cuidándonos**).

LA SESSION ÉTAPE PAR ÉTAPE :

Durée	Durée totale	Activité	Outil / méthode / matériel
15´		**Introduction:** • Le parcours d'apprentissage.	Préparez les points à l'avance sur un paper-board ou dans une présentation PowerPoint. Image agrandie du processus de construction de capacités en matière de protection (chapitre 3)
65'	80'	**Roue de la sécurité** • Explication • Activité n°1 : remplir la roue de la sécurité	Illustration agrandie de la roue de la sécurité (ou présentation PowerPoint)
60'	140'	**Observation des règles et des protocoles de sécurité** • Discussion autour d'une affirmation • Explication du concept de règles de sécurité • Activité n°2 : Analyse de cas	Impressions sur papier des cas présentés ci-dessous Paper-board Marqueurs
75	215'	**Améliorer la sécurité au domicile et au bureau** • Explication • Activité n°3 : Analyser la sécurité des participants à leur domicile et à leur bureau • Activité n°4 : Jeu de rôle	Tableau "Liste de contrôle : Révision de la sécurité du bureau (NMP chapitre 1.8). Exemple de mandat de perquisition (peut être fictif mais doit être réaliste). Lois locales concernant les perquisitions légales (si possible). Paper-board Marqueurs
15	230´	**Conclusion**	
		DURÉE : COMPTER 270 MINUTES (4 HEURES 30 MINUTES), DONT DEUX PAUSES DE 20 MINUTES.	

ACTIVITÉS D'APPRENTISSAGE

INTRODUCTION : LE PARCOURS D'APPRENTISSAGE

Montrez aux participants une carte de leur parcours d'apprentissage jusqu'à présent. Pour ce faire, imprimez l'illustration du parcours de construction de capacités en matière de protection (chapitre 3 de ce Guide) et affichez-la au mur ou projetez-la. Les outils présentés au cours des sessions de formation sont représentés par des symboles qui apparaissent le long du parcours. Assurez-vous que tout le monde soit capable d'utiliser les outils, et prévoyez un peu de temps pour d'éventuels éclaircissements.

Ensuite, recentrez la discussion sur les aspects organisationnels de la gestion de la sécurité, c'est-à-dire à la façon dont les organisations fonctionnent, dont les décisions sont prises et dont les changements ont lieu. Rappelez aux participants qu'une bonne gestion de la sécurité a pour but de changer les attitudes et les comportements. La formation aura peut-être déjà engendré chez les participants un certain degré de changement d'attitude, mais il s'agit maintenant de travailler consciemment sur leurs comportements en tant qu'individus et sur la manière d'opérer de leurs organisations au quotidien.

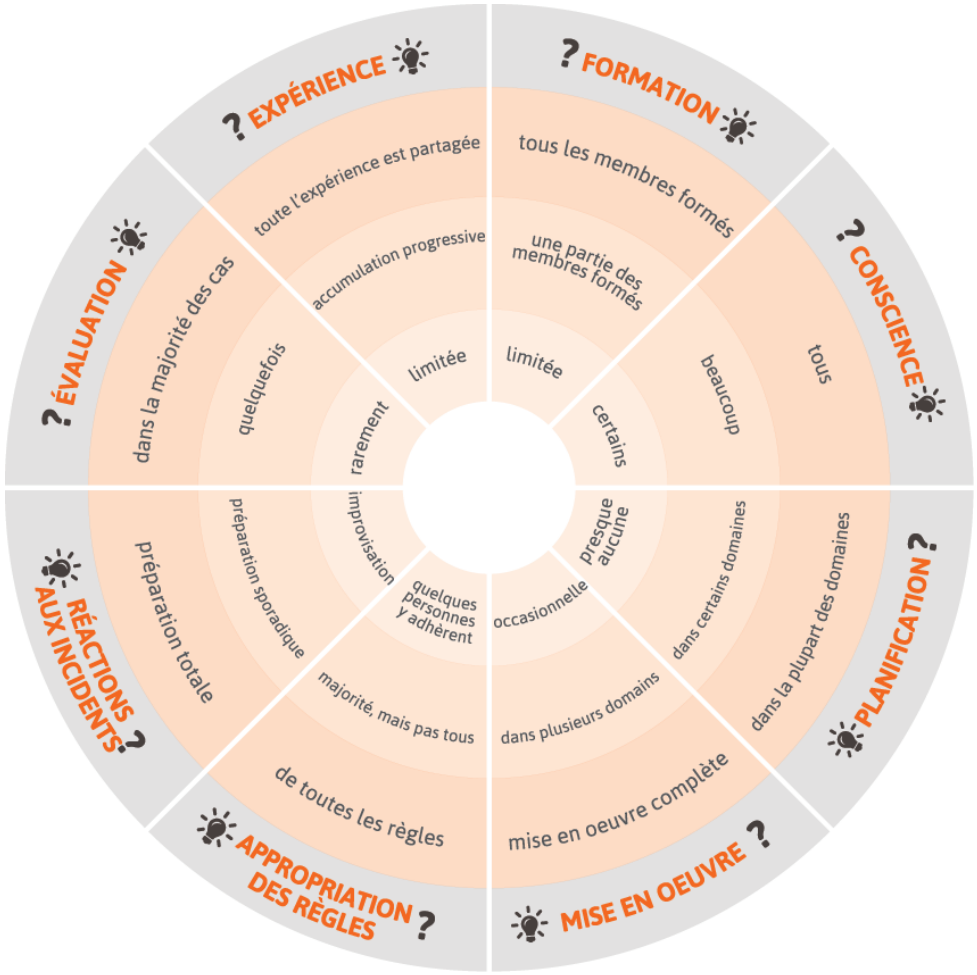
Remind participants that the existence of a security plan does not automatically ensure security or protection. Invite participants to express their views on this, as it will help you steer the discussion in the right direction. Faci-

litators should point out that security requires ownership of the whole process, starting with an assessment of the current levels of organisational security, identifying where improvements could be made, implementing security plans, and eventually conducting a regular monitoring and evaluation process.

LA ROUE DE LA SÉCURITÉ

EXPLICATION

Présentez la roue de la sécurité sur votre paper-board ou projetez-la sur un écran. Expliquez les six composantes, ou six dimensions, de la roue (NMP, chapitre 2.1, pp. 140-141). Quand les participants auront appréhendé l'outil, expliquez-leur l'analyse étape par étape de la roue de la sécurité, c'est-à-dire les questions qu'il faut poser pour déterminer à quel point les besoins en sécurité sont actuellement rencontrés et pour identifier les améliorations qui pourraient être nécessaires ou conseillées (NMP, chapitre 2.1, pp. 142-146). Le principe de la roue de la sécurité est qu'elle doit être aussi ronde que possible, pour qu'elle puisse rouler facilement si elle était une vraie roue. En termes de gestion de la sécurité, cela veut dire qu'il n'est pas intéressant d'être très fort dans une zone mais faible dans d'autres. Toutes les zones doivent être égales.



ACTIVITÉ N°1 : REMPLIR LA ROUE DE LA SÉCURITÉ

Demandez aux participants d'appliquer l'analyse à leur propre organisation. Divisez les participants en groupes, si nécessaire, auquel cas plusieurs roues de la sécurité seront produites pour une même organisation. Quand tous les groupes ont terminé, ils doivent comparer les différentes roues produites. Clôturez l'activité en engageant une discussion avec tous les participants sur les résultats de l'exercice.

→ Si vous travaillez avec un groupe homogène (et que vous n'avez donc pas divisé les participants en plusieurs groupes pour cet exercice), discutez avec l'ensemble de l'assemblée de la signification de chacune des dimensions de la roue, représentées par les rayons (**NMP** chapitre 2.1). Dans le cas contraire, donnez des instructions avant le début du travail de groupe. Il faut colorer un certain pourcentage de chaque rayon, l'un après l'autre, pour représenter le statut actuel de la pratique de l'organisation. Cela suscitera vraisemblablement quelques désaccords et discussions au sujet du pourcentage devant être attribué à chaque section. Aidez le groupe à arriver à un consensus en expliquant que la roue est un outil servant à illustrer le statut actuel de l'organisation, qu'elle est un point de départ pour réaliser des changements au sein de l'organisation. Pour terminer, recommandez aux participants de revoir la roue dans six mois pour évaluer leurs progrès.

→ Si les participants ont été divisés en groupes, demandez à ceux qui travaillent au sein de la même organisation de travailler ensemble. Affichez ensuite tous les résultats au mur et discutez des éléments généraux ci-dessous. Le groupe obtiendra probablement une roue dont les rayons sont colorés différemment. Ceci permet de déterminer quel type d'actions doit être prioritaire pour améliorer la protection et la sécurité de l'organisation.

OBSERVATION DES RÈGLES ET DES PROTOCOLES DE SÉCURITÉ

DISCUTEZ DE L'AFFIRMATION SUIVANTE

→ **«La sécurité de notre organisation n'est équivalente qu'à celle de notre élément le plus faible.»**

Lisez cette phrase à voix haute devant les participants, écrivez-là sur votre paper-board, et engagez la discussion avec l'ensemble du groupe. Cette phrase se base sur le principe selon lequel un agresseur potentiel voulant obtenir des informations sur des DDH, ou leur porter préjudice, tentera probablement de trouver le maillon le plus faible pour arriver à ses fins. Par exemple, il tentera de se rapprocher d'une personne qui a l'habitude d'être ivre le samedi soir. De la même manière, une personne voulant faire peur au personnel d'une organisation ciblera probablement quelqu'un qui a l'habitude de négliger sa sécurité. De même qu'une personne prudente pourra subir une attaque parce qu'une personne négligente a laissé la porte ouverte. En résumé : une seule personne négligente peut mettre en danger toute l'organisation.

EXPLICATION DU CONCEPT DE RÈGLES DE SÉCURITÉ

Présentez brièvement comment il convient de définir et de superviser des règles de sécurité (**NMP, chapitre 2.2**). Cela donnera aux participants une base pour l'analyse de cas.

ACTIVITÉ N°2 : ANALYSE DE CAS : DÉTERMINER LA QUALITÉ DES RÈGLES?

Lors de cette activité, les participants doivent analyser trois règles de sécurité d'une organisation fictive. Vous pouvez choisir de travailler avec le groupe entier ou de diviser les participants en trois groupes. Distribuez une règle de sécurité (ci-dessous) à chaque participant du groupe et demandez-leur de les analyser en fonction des critères suivants : est-elle pratique, est-elle durable, est-elle inclusive, est-elle efficace ? Notez que la formulation des règles est intentionnellement alambiquée, le but étant de provoquer une discussion entre les participants sur l'adéquation des règles et sur les éventuelles améliorations à leur apporter.

Accordez aux participants 10 minutes pour faire ce travail, puis demandez à l'assemblée (ou à chacun des groupes si les participants ont été divisés) de présenter son analyse des règles. Encouragez ensuite la discussion entre tous les participants (voir Conseils aux facilitateurs). Si vous le souhaitez, vous pouvez utiliser des exemples de règles de sécurité issus de l'organisation des participants (mais soyez conscient que cela peut créer des tensions).

→ **RÈGLE N°1 :**

Avant d'entamer la vérification d'une violation présumée des droits humains, consultez les parties consacrées à la question dans le manuel de sécurité afin d'être sûr que tout est réalisé dans le respect des règles. Si vous n'avez pas connaissance du manuel de sécurité parce que vous venez d'entrer en poste, demandez l'aide de vos collègues ou de votre superviseur direct.

→ **Aspects positifs :**

- La règle fait référence à un manuel de sécurité, ce qui veut dire qu'au moins l'organisation en a un. Une règle devrait stipuler que tous les employés doivent connaître l'existence de ce manuel.
- Il est dit implicitement que quelqu'un est responsable des questions de sécurité : le superviseur direct, à qui les nouveaux membres du personnel peuvent poser leurs questions en matière de sécurité. Le fait de devoir demander peut toutefois constituer une barrière. Si l'organisation a une culture d'ouverture et de consultation (c'est-à-dire si le personnel, et en particulier la direction, se montre disposé à aider), cela ne devrait cependant pas poser de problème.

→ **Aspects négatifs :**

- Les nouveaux employés ne devraient pas avoir à accomplir de telles tâches. S'ils ont à le faire, ils doivent être formés et supervisés correctement.
- Le manuel de sécurité doit être facilement accessible, ce qui ne semble pas être le cas ici.
- Le personnel devrait savoir quelles parties du manuel de sécurité il doit consulter. S'il faut du temps pour trouver les sections que l'on cherche, les employés se décourageront probablement et ne suivront pas la règle.
- La règle implique un travail additionnel, ce qui peut amener certaines personnes à l'ignorer.
- Deux questions plus générales peuvent se poser : la règle a-t-elle du sens dans le contexte de travail de l'organisation ? Tous les membres du personnel ont-ils participé à l'élaboration de la règle (ce qui les encouragerait à y adhérer) ?
- Enfin, il ne faut pas oublier l'aspect humain du travail. La règle pourrait donner lieu à une approche bureaucratique vis-à-vis des personnes venant demander de l'aide à l'organisation.

→ **RÈGLE N°2:**

Les bureaux de terrain nationaux sont responsables devant le siège international de Genève de la sécurité de leur personnel local. Selon la situation dans le pays, les visites de terrain dans des zones reculées et à hauts risques comptent parmi les moments de plus grande vulnérabilité en termes de sécurité. Pour cette raison, les normes de sécurité internationales de l'organisation, qui doivent être appliquées dans chaque pays, exigent que le personnel :

- Prépare minutieusement et au moins sept jours à l'avance toute visite de terrain en zone de haut risque. Avant de se rendre sur le terrain, les employés doivent se rencontrer pour revoir les protocoles concernant la préparation de visites de terrain (voir le manuel de sécurité). La visite de terrain ne pourra en aucun cas avoir lieu si toutes les conditions nécessaires ne sont pas respectées.

→ **Aspects positifs :**

- La référence faite à des normes internationales suggère clairement l'importance de la règle.

→ **Aspects négatifs :**

- La règle des sept jours peut constituer un obstacle. Par ailleurs, dans des régions où la situation de sécurité est instable et fragile, la règle pourrait s'avérer insuffisante, car une analyse réalisée un certain jour pourrait ne plus être valide le lendemain.
- Il n'est potentiellement pas réaliste de supposer que tous les membres d'une équipe pourront

toujours se réunir avant d'entamer une visite de terrain. Cela pourrait avoir un impact sur l'application de la règle (certains membres pourraient la contourner de temps à autres) ou sur le travail de l'organisation en lui-même (il y aurait un risque que des visites de terrain soient annulées à cause de la règle).

- La bonne manière d'inclure les nouvelles recrues dans l'élaboration des règles de sécurité et d'encourager ces recrues à y adhérer est de les associer à l'analyse et à l'évaluation périodique des règles. Dans les organisations dont le processus de prise de décisions est hiérarchique, le personnel devrait au moins pouvoir faire part de ses éventuelles remarques sur la viabilité réelle, l'efficacité et l'adéquation des règles. Dans les organisations au processus de prise de décisions plus inclusif, le personnel peut participer à l'évaluation et à l'adoption de règles de sécurité. Il peut s'avérer compliqué de trouver le bon équilibre entre la participation et l'utilisation efficace des ressources. Les règles doivent être revues périodiquement, mais il faut également veiller à éviter les changements trop fréquents, sans quoi le personnel pourra en venir à ignorer les règles. Malgré cela, les situations d'urgence peuvent parfois obliger les organisations à remodeler une règle rapidement.

→ **RÈGLE N°3 :**

Pendant les missions de terrain en dehors de la ville, les aspects de sécurité doivent inclure les temps libres, c'est-à-dire les soirées et les week-ends. Tous les employés de l'organisation doivent suivre les règles suivantes pendant leur temps libre:

- Vous ne devez pas vous trouver dans la rue après 21h. Passée cette heure, vous devez vous trouver à votre résidence habituelle, et si vous logez dans une autre maison ou à l'hôtel vous devez avertir la personne responsable. Si vous avez un téléphone portable, il doit être opérationnel à tout moment.
- Les employés régionaux détermineront quels endroits ne peuvent pas être visités après 21h pour des raisons de sécurité.
- Il est interdit de consommer de l'alcool ou d'autres drogues.
- Toute action personnelle pouvant compromettre la sécurité d'autres personnes ou l'image de l'organisation est interdite.

→ **Aspects positifs :**

- De manière générale, il est positif qu'une règle traite de la sécurité dans les temps libres, et qu'elle prenne en compte les moments où les employés ne sont pas officiellement en train de travailler.
- La règle définit des zones de danger, ce qui rend plus facile de les éviter.
- La règle traite également de la consommation d'alcool et de drogue, ce qui peut être difficile à aborder dans certains contextes culturels.

→ **Aspects négatifs :**

- Les problèmes de sécurité liés à la consommation d'alcool et de drogue devraient être mieux expliqués. Une organisation devrait éviter de parler de valeurs morales, elle devrait plutôt traiter la question sous l'angle de la sécurité. L'accent devrait être mis sur la vulnérabilité et la responsabilité. La règle devrait dire clairement qu'en cas d'événement, les employés doivent être préparés à réagir. Dans certains cas, tolérer une faible consommation d'alcool tout en interdisant l'usage de toute substance illicite permet d'arriver plus facilement au respect de la règle.
- De manière générale, la règle n'explique pas le raisonnement qui la sous-tend. Une approche réglementaire de ce type peut parfois se révéler plus compliquée à faire appliquer. Il est souhaitable d'expliquer plus en détail les raisons pour lesquelles les règles doivent être respectées. Le problème majeur étant que le meilleur moyen de faire faire une chose à quelqu'un est de la lui interdire.

- Les critères et les conditions nécessaires pour d'obtenir l'autorisation de se déplacer ne sont pas clairs, et le membre du personnel responsable de donner l'autorisation n'est pas précisé. La règle devrait également faire une référence claire à la section concernée dans le manuel.
- On pourrait dire, pour terminer, que le dernier point concernant les actions personnelles susceptibles de compromettre la sécurité des collègues est plutôt vague. Les actions dont il s'agit et les situations dans lesquelles elles pourraient avoir lieu sont loin d'être évidentes et mériteraient d'être précisées.

AMÉLIORER LA SÉCURITÉ AU DOMICILE ET AU BUREAU

EXPLICATION

Basez votre explication sur le **NMP (Chapitre 1.8)**. L'objectif de sécurité principal doit être d'empêcher l'accès non-autorisé aux lieux de travail ou aux domiciles des DDH. Évaluer la sécurité d'un bureau s'apparente à réaliser une analyse de risques. Le processus fait appel aux mêmes concepts de menace, vulnérabilité et capacité. Soulignez le fait que les vulnérabilités d'un bureau doivent être évaluées à la lumière des menaces qu'il subit. Rappelez également ce qui a été dit dans la discussion sur le respect des règles de sécurité : la sécurité d'un bureau n'est équivalente qu'à celle de son élément le plus faible.

ACTIVITÉ N°3 : ANALYSER LA SÉCURITÉ DES PARTICIPANTS À LEUR DOMICILE ET À LEUR BUREAU

Demandez aux participants d'analyser la sécurité de leur bureau en utilisant le tableau fourni dans le **NMP (Liste de contrôle : Révision de la sécurité du bureau, p. 97)**. Si nécessaire, divisez les participants en plusieurs groupes. Encouragez-les à discuter de leurs analyses pour conclure l'exercice. Si vous travaillez avec des groupes hétérogènes, demandez aux participants issus d'une même organisation de travailler ensemble.

ACTIVITÉ N°4 : JEU DE RÔLE : UNE PERQUISITION LÉGALE

Quatre participants se voient attribuer les rôles suivants (ces rôles doivent être adaptés au contexte et aux lois du pays concerné):

→ Le juge, qui dispose d'un mandat de perquisition (adapté au contexte).

→ Deux policiers, qui réalisent la perquisition.

→ Un individu, sans papiers d'identité, qui cache un sac en plastique rempli de cocaïne puis feint de le trouver.

Les autres participants sont les membres de l'organisation. Leur rôle est de décider de la réaction à donner à la perquisition.

Une fois le jeu de rôle terminé, il faut l'évaluer. Donnez aux participants vos remarques sur base des concepts et des éléments figurant dans le **chapitre 3.1 du NMP**.

→ Renseignez-vous sur le cadre légal dont relèvent les perquisitions légales dans le pays où vous travaillez. Imprimez les informations et distribuez-les aux participants à la fin du jeu de rôle.

→ Pendant l'analyse du jeu de rôle, demandez aux participants comment ils se sont sentis pendant le jeu de rôle. Insistez sur le fait qu'ils se sentiront plus en sécurité en ayant connaissance du cadre légal et en étant au fait de leurs droits.

→ Divisez le processus d'évaluation en trois phases (ceci devra être adapté en fonction des termes exacts de la loi):

- Les actions à mener avant la perquisition : se renseigner sur ses droits ; revoir les protocoles de sécurité et plus particulièrement la gestion sécurisée d'informations (**NMP chapitre 3.1**); former les membres de l'organisation à la manière de réagir face à un mandat de perquisitiont;
- Les actions à mener pendant la perquisition : appeler un avocat (ou une personne qui répondra à coup sûr et qui pourra appeler un avocat et d'autres personnes utiles) ; lire attentivement le mandat de perquisition pour s'assurer de sa légalité ; ne pas laisser les policiers entrer dans le bâtiment non-accompagnés (ceci dépendra de votre droit légal à refuser de quitter les lieux sur ordre de la police) ; être attentif à toute action illégale que pourraient commettre les officiers d'application de la loi.
- Les actions à mener après la perquisition : s'assurer que tout le monde va bien ; évaluer le résultat de la perquisition ; élaborer un plan pour y réagir et pour limiter son impact négatif.

CONCLUSION

> Demandez aux participants de rappeler les enseignements-clés de la session. Insistez sur les messages-clés en revenant à des exemples ou à des problèmes cités pendant la journée.

RESSOURCES COMPLÉMENTAIRES

> Van Brabant. Op. Cit. Chapitres 18-21.

> Comité Cerezo México. Op. Cit. Chapitre 7.

> Collectif ANSUR. Op. Cit.

10. GESTION DE L'INFORMATION ET SÉCURITÉ INFORMATIQUE

> **CHAPITRE 1.11** NMP
LA SÉCURITÉ, LA COMMUNICATION ET LES TECHNOLOGIES DE L'INFORMATION

> **CHAPITRE 3.3** NMP
LA SÉCURITÉ DE LA GESTION DE L'INFORMATION

Ce chapitre sera utile aux facilitateurs si des risques pour la sécurité des données informatiques conservées par les défenseurs ont été décelés pendant l'évaluation préalable à la formation ou pendant la formation en elle-même. Mais plus généralement, cette session est principalement destinée à sensibiliser les participants à un aspect spécifique de la sécurité des technologies de l'information (TI) (voir les objectifs ci-dessous). En fonction du profil de risque informatique de l'organisation, de ses besoins de formation et de la configuration du processus de développement de capacités, ce thème peut être traité soit comme une partie d'une session de formation consacrée à la fois aux dimensions physique et informatique de la sécurité (qui sont liées), soit comme une introduction à un module de formation séparé et plus détaillé consacré à la sécurité informatique. **Les facilitateurs doivent toutefois s'assurer que l'analyse de risques réalisée par les DDH couvre bien les deux dimensions et que les plans de développement de capacités tiennent compte des liens qui les unissent. Dans le cas contraire, les sessions ne seront pas pertinentes ou ne répondront pas aux risques encourus par les DDH.**

OBJECTIFS D'APPRENTISSAGE

> Sensibiliser les participants à l'importance de la sécurité des technologies de l'information, en mettant en évidence les risques associés à la perte ou au vol de données informatiques.

> Indiquer des ressources qui aideront les DDH à améliorer la sécurité de leurs données.

MESSAGES CLÉS

> Les risques pour la sécurité des informations détenues par les DDH ne proviennent pas seulement de défaillances techniques et d'attaques ciblées commises pour avoir accès ou pour détruire ces informations, ils proviennent aussi de pratiques de communication négligentes.

> En protégeant l'accès aux informations et en faisant régulièrement des sauvegardes (back-ups) des informations, il est possible de réduire le risque de perte ou de vol de ces données.

LA SESSION

DIFFICULTÉS POUVANT SURVENIR DURANT LA SESSION :

→ Les facilitateurs doivent avoir une connaissance de base des outils de sécurité informatique (au niveau de l'utilisateur), et en particulier de ceux qui peuvent aider à minimiser les risques de perte de données et d'accès non-autorisé aux données.

→ Même s'ils utilisent des ordinateurs et d'autres appareils informatiques régulièrement, certains défenseurs n'ont qu'une compréhension très basique de leur fonctionnement. Faites en sorte que les discussions soient les plus simples possibles et évitez les termes techniques qui peuvent être déroutants ou être mal compris. Si ces termes ne peuvent pas être évités, expliquez-les avec un vocabulaire simple, non-technique, et pensez à utiliser des illustrations. Faites en sorte que ces explications restent visibles pendant toute la session, pour pouvoir y faire référence ultérieurement.

LA SESSION ÉTAPE PAR ÉTAPE :

Durée	Durée totale	Activité	Outil / méthode / matériel
05´	5´	**Introduction:** • Objectifs et structure de la session.	Préparez les points à l'avance sur un paper-board ou dans une présentation PowerPoint.
10´	15´	**Risques pour la sécurité des communications**	Paper-board
45´	60´	**Activité** : back-up de données et protection face à un accès non-autorisé	Paper-board Post-it autocollants
		Montrer aux participants comment utiliser les outils de sécurité informatique (activité facultative)	Ordinateur portable Clé USB avec la dernière version d'installation des outils « Security in a Box »
		DURÉE : COMPTER 60 MINUTES (1 HEURE) PLUS UNE PAUSE DE 20 MINUTES.	

ACTIVITÉS D'APPRENTISSAGE

Cette session s'intéresse principalement au risque de perte de données (due à l'absence de sauvegardes et au vol d'informations), et aide les participants à identifier leurs vulnérabilités existantes liées à leur façon de gérer les informations stockées sur des outils informatiques. Ces informations sont appelées « données entreposées ». La session parlera de procédures simples mais fondamentales et présentera des outils et des mesures informatiques et non-informatiques pouvant améliorer la capacité des DDH à gérer le risque.

Les facilitateurs trouveront dans les **chapitres 1.11 et 3.3 du NMP** du matériel d'enseignement pouvant les aider à préparer cette session. Comme les menaces et les technologies de protection des données informatiques évoluent très rapidement, nous encourageons les facilitateurs à se familiariser également avec d'autres sources d'informations sur ce thème. Une liste non-exhaustive de ressources complémentaires pour vous documenter plus en profondeur est indiquée à la fin de cette section.

RISQUES POUR LA SÉCURITÉ DES COMMUNICATIONS

Pour introduire ce thème, le facilitateur peut commencer par demander aux participants quels moyens ils utilisent pour communiquer avec leurs collègues et avec d'autres personnes extérieures à l'organisation ou à la communauté. Ecrivez la liste des moyens de communication cités sur votre paper-board. S'ils ne l'ont pas mentionné, rappelez aux participants que le fait de parler face-à-face est peut-être la manière la plus fréquente de communiquer (parfois par inadvertance) des informations sensibles sur leur travail. La sécurité et la protection des informations n'est donc pas qu'une question de technologies de communication sophistiquées.

Ensuite, lancez une réflexion collective avec les participants sur les différentes façons d'accéder légalement à des informations ou à des communications, mais aussi de les manipuler. Par exemple : dans une conversation face-à-face, par téléphone, ou en tirant profit du cadre de sécurité physique du bureau. Inspirez-vous des informations figurant dans le **chapitre 1.11 du NMP**.

Si les participants considèrent que leurs conversations face-à-face ou par téléphone portable risquent d'être écoutées, recommandez-leur d'inclure dans leurs plans de sécurité des protocoles pour la transmission d'informations sensibles par des communications de ce type. Vous pouvez renseigner le chapitre 1.11 du NMP comme aide-guidance.

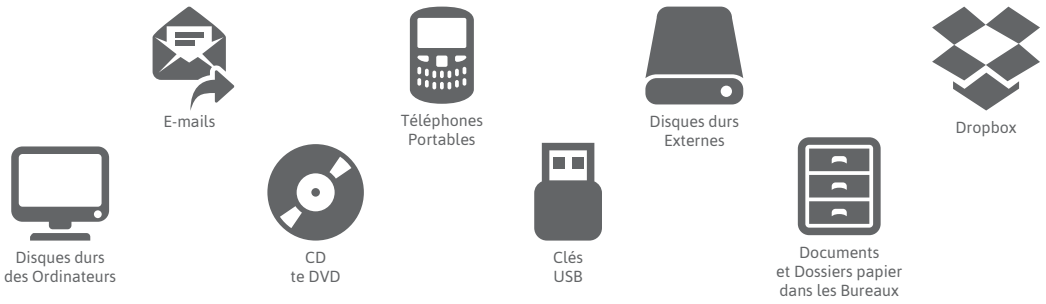
Passez ensuite à un aspect différent de la sécurité des informations en demandant aux participants le degré d'importance des informations qu'ils conservent sous format numérique (e-mails, rapports, coordonnées de partenaires et de bénéficiaires de services, etc.) Si les participants attribuent une grande importance à ces informations, demandez-leur de citer (ou indiquez-leur, s'ils n'y parviennent pas seuls) plusieurs façons dont ils risquent de perdre ces informations (p.e. suite à une erreur technique, suite à une perte ou un vol de matériel, ou suite à un accès non-autorisé).

ACTIVITÉ : BACK-UP DE DONNÉES ET PROTECTION FACE À UN ACCÈS NON-AUTORISÉ [1]

En fonction de ce qui a été vu lors des sessions précédentes réalisées avec les participants et des discussions sur les risques liés à la sécurité des informations, faites un lien avec le risque de perte de données et ce qu'il peut signifier pour les DDH et les personnes avec et pour qui elles travaillent. Demandez aux participants quelles mesures stratégiques ad hoc ils appliquent actuellement pour éviter la perte de leurs données.

Dessinez une matrice (voir ci-dessous) sur deux feuilles de paper-board collées ensemble, et affichez-la de manière bien visible sur un mur. Expliquez aux participants qu'il s'agit d'un exercice de localisation des informations dont le but est de visualiser le type d'informations qu'ils possèdent et l'endroit où elles sont stockées. Cet exercice constituera une base pour élaborer une stratégie de réduction des risques de perte de données.

Commencez par demander aux participants de faire la liste des différents endroits où sont stockées leurs informations. Si aucune suggestion n'est avancée, vous pouvez citer les éléments suivants :



Ajoutez les endroits cités par les participants dans la ligne supérieure de la matrice. Demandez ensuite aux participants quel type d'informations ou de données ils stockent dans chacun de ces endroits.

Exemple :

Écrivez un exemple sur un carton ou un post-it et placez-le dans la bonne partie de la matrice (p.e. des rapports stockés sur les disques durs des ordinateurs).

Demandez-leur s'il existe d'autres copies de ces données quelque part. Si oui, utilisez un post-it de couleur différente et placez-le à l'endroit où est stockée la copie. Profitez-en pour faire la différence entre le document original et les copies sauvegardées (ou back-ups). (Dans l'exemple ci-dessous, le rouge indique le document original et le jaune indique la sauvegarde.)

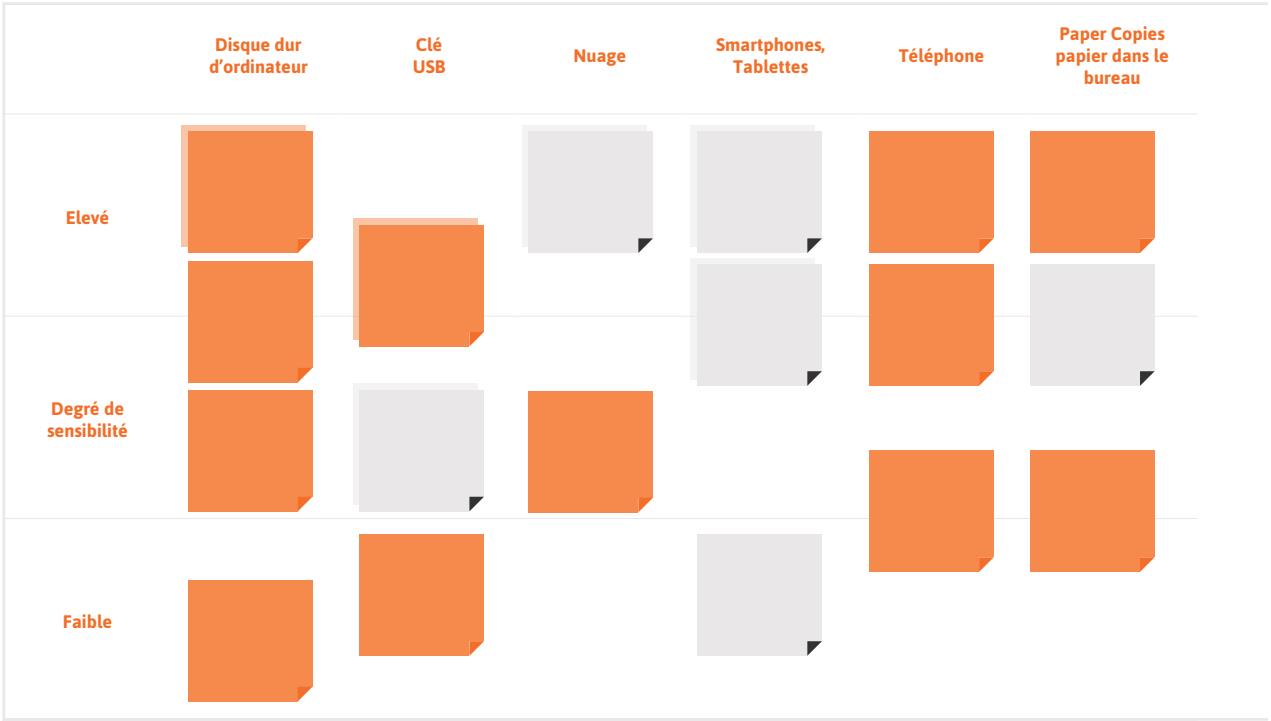
1 Cette activité est adaptée des travaux de Samir Nassar, Daniel Ó Clunaigh et Ali Ravi, du Collectif Tactical Technology, pour le projet LevelUp. Nous conseillons également aux facilitateurs de lire le **chapitre 3.3 du NMP** pour plus d'informations.

Répétez ce processus en y ajoutant une dimension supplémentaire : la sensibilité des données (c'est-à-dire les données qui en cas de perte ou d'utilisation abusive risquent de causer des dommages considérables soit aux DDH soit aux personnes avec qui ils travaillent, comme par exemple des victimes de violences de genre). Ajoutez donc un second axe (vertical) représentant la sensibilité. Plus haut un carton sera placé sur le tableau, plus les données représentées seront sensibles. Placez les deux cartons ou post-it sur l'axe représentant leur degré de sensibilité. Si le temps disponible est limité, vous pouvez réduire cette partie de l'exercice à un ou deux exemples.

Formez ensuite des petits groupes : un groupe par organisation quand les participants sont issus de différentes organisations, un groupe par thème quand les participants sont issus d'une seule organisation. Cette activité peut aussi être réalisée sous forme de séance de réflexion collective avec l'ensemble du groupe si tous les participants viennent de la même organisation.

Allow 5-10 minutes for this exercise. It is advisable for the facilitator to observe each group and identify interesting characteristics (e.g. where there is a particularly large dependence on one device or copies/back-ups are few, etc.). By the end of the exercise each team should have completed a matrix.

Voilà à quoi pourrait ressembler le résultat :



Expliquez que cette matrice donne une idée d'où sont situées les données. Demandez aux participants si ce sont là toutes les données que leur organisation ou communauté produit. La réponse est non, bien entendu, ce n'est qu'un faible pourcentage.

Expliquez que cette matrice donne une idée d'où sont situées les données. Demandez aux participants si ce sont là toutes les données que leur organisation ou communauté produit. La réponse est non, bien entendu, ce n'est qu'un faible pourcentage.

Pour montrer la vulnérabilité qu'entraîne cette situation, demandez aux participants ce qui peut faire en sorte qu'un ordinateur cesse de fonctionner.

- → Les virus et les programmes malveillants peuvent détruire les données stockées sur un ordinateur.
- → Les ordinateurs peuvent être volés ou confisqués.
- → Les problèmes d'infrastructures comme les pannes de courant peuvent endommager les ordinateurs.

Vous pouvez demander aux participants qui ont déjà été affectés par un de ces problèmes de lever la main.

Demandez-leur ensuite ce qui arriverait aux données si un des événements cités ci-dessus devait arriver. Pour rendre les choses plus marquantes, vous pouvez arracher brutalement chacun des post-it figurant dans cette colonne et les jeter au sol. Les post-it restants représentent alors toutes les informations qui leur restent.

Demandez aux participants de réfléchir à ce qui pourrait être fait pour éviter une telle situation. Ils répondront probablement qu'ils doivent conserver plus de copies dans des endroits différents. Expliquez que c'est ce qu'on appelle faire une sauvegarde, ou un back-up.

Si vous avez assez de temps, penchez vous maintenant sur le thème de la sensibilité des données. Si possible, prenez la matrice d'un autre groupe comme exemple. Si tous les participants ont réalisé l'exercice ensemble, choisissez une autre colonne de la matrice. Demandez aux participants quel serait l'impact si leur téléphone, leur disque dur ou leur clé USB était volé(e). Prenez les post-it collés dans la colonne concernée, mais gardez-les en main et lisez-les à voix haute. Ceci illustre le fait que quelqu'un d'autre est désormais en possession des informations contenues sur l'appareil. Demandez aux participants ce que cette personne pourrait faire avec les données et dans quelle situation les DDH se retrouveraient dans ce cas.

Sur base de l'activité précédente consacrée à la sauvegarde des données, demandez aux participants de citer au moins trois des cinq actions qu'ils doivent entreprendre pour réduire les vulnérabilités qu'ils ont identifiées. Ces actions peuvent être informatiques (citez le programme Cobian Backup) ou non-informatiques (collecter des fonds pour acheter des supports de sauvegarde, créer des protocoles de sauvegarde, etc.). En fonction de la composition du groupe, demandez aux participants d'entreprendre ces actions au niveau organisationnel (pour les groupes homogènes) ou au niveau individuel (pour les groupes hétérogènes).

- → Cette activité est essentiellement une analyse de risques concernant les données que les DDH possèdent et sont susceptibles de perdre. Elle aide à identifier les vulnérabilités existantes.
- → Pour faire cet exercice, il faudra idéalement un niveau élevé de confiance au sein du groupe de participants, ou un groupe pouvant aisément être divisé en plus petits groupes relativement homogènes. Pour les groupes où le niveau de confiance est faible et pour les groupes hétérogènes dont les participants ne se connaissent pas bien et ne souhaitent peut-être pas dévoiler aux autres quelles informations ils possèdent et comment elles sont stockées, il faudra modifier l'exercice pour le rendre plus général, tout en maintenant les mêmes enseignements.

MONTRER AUX PARTICIPANTS COMMENT UTILISER LES OUTILS DE SÉCURITÉ NUMÉRIQUE ACTIVITÉ FA

CULTATIVE)

Si elle est réalisée, cette partie de la session a pour but de remédier aux vulnérabilités qui ont été identifiées et de renforcer les capacités des participants à faire face au risque de perte ou d'accès non-autorisé aux « **"données entreposées "** (c'est-à-dire les données stockées sur des appareils, voir plus haut) et aux **"données en mouvement "**.

On qualifie de **"données en mouvement "** les échanges d'informations via internet, e-mail, téléphone portable ou médias sociaux qui ont fréquemment lieu entre les DDH dans le cadre de leur travail et de leur communication avec des parties prenantes. Un des principaux risques est que des adversaires parviennent à accéder à des informations sensibles sans autorisation, que ce soit en piratant des comptes d'utilisateurs, en épiant les DDH ou en interceptant les informations par d'autres moyens techniques. En aidant les DDH à identifier les vulnérabilités existantes dans ce domaine, vous les encouragerez à établir des procédures pour créer et conserver des mots de passe forts, utiliser des canaux de communication plus sûrs (cryptés), et s'assurer que les informations échangées soient elles-mêmes sécurisées (en les cryptant).

Pour remédier aux vulnérabilités identifiées pendant ces exercices, les facilitateurs devront se familiariser avec les concepts suivants :

- → La création de mots de passe forts (pour les comptes de courrier électronique, les ordinateurs, les fichiers, etc.)
- → Le cryptage des données entreposées et des données en mouvement
- → La protection de la vie privée dans la communication via internet
- → La sauvegarde d'informations
  Nous encourageons les facilitateurs à présenter ces outils de sécurité informatique aux participants en utilisant les ressources proposées sur le site Security in a Box **https://securityinabox.org** Voyez également la section Conseils aux facilitateurs, ci-dessous.

Pour travailler avec les ressources proposées par le site Security in a Box, les facilitateurs doivent prendre note des conseils suivants : **https://securityinabox.org**, les facilitateurs doivent prendre note des conseils suivants

Be conversant with the use of the tools yourself by making it a part of your own security strategy: strong password practices, encrypting information stored on devices or sent via the internet or mobile networks, and regular data back up.[2]

- → Maîtrisez vous-mêmes l'utilisation des outils en les incluant dans votre propre stratégie de sécurité : choisissez des mots de passe forts, cryptez vos informations stockées sur des appareils ou envoyées par internet ou par réseau de téléphonie mobile, faites des back-ups réguliers
- → Lisez attentivement la section correspondante du « Livret pratique » que vous trouverez sur la page **https://securityinabox.org/en/howtobooklet.** Ce livret indique à quelles vulnérabilités s'adresse chaque outil et illustre ces explications par des études de cas que vous pourrez à votre tour adapter au contexte de travail de vos participants.
- → Soyez conscient que les outils offrent différentes fonctions, et ne présentez que celles qui correspondent aux risques identifiés par les participants, afin de ne pas surcharger ceux-ci d'informations qu'ils n'auront peut-être jamais l'occasion d'utiliser.

2 Etant donné la rapidité de l'évolution dans ce domaine, tenez-vous au courant des derniers développements en termes de sécurité numérique et de protection des données privées en visitant régulièrement les sites Security in a Box, AccessNow (**www.accessnow.org**), Ono (**https://onorobot.org**) a), et d'autres sites de référence. Si vous en avez l'occasion, suivez une formation consacrée à la sécurité numérique. Cela vous permettra d'améliorer vos capacités d'utilisation des outils, d'en découvrir d'autres, et d'améliorer vos compétences de facilitateur dans ce domaine.

- → Lors du choix du local de la formation, vérifiez qu'il y ait bien un accès constant à l'électricité et des solutions de dépannage (comme des générateurs) pour vous assurer que la formation ne sera pas interrompue par des pannes de courant.
- → Téléchargez la dernière version des outils que vous voulez présenter sur le site Security in a Box avant la session de formation, et enregistrez-les sur votre ordinateur ou sur un espace de stockage portable pour les utiliser au cours de vos présentations et pour que les participants puissent les copier. Cette précaution permettra d'éviter les retards si la connexion internet ne permet pas aux participants de télécharger le logiciel rapidement pendant la session de formation.
- → Avant la session, testez les installations et tous les éléments que vous prévoyez de présenter, pour être certain qu'ils fonctionnent correctement sur votre ordinateur. Ceci est essentiel pour que vous soyez en mesure d'expliquer le processus d'installation et les différentes fonctions aux participants avec l'aide d'un projecteur.
- → Pour éviter la propagation de virus informatiques, demandez aux participants s'ils ont un programme antivirus et demandez-leur de vérifier qu'il est bien à jour. Vous pouvez également prévoir une copie de l'antivirus gratuit Avast pour les participants qui n'ont pas d'antivirus ou dont le programme n'est pas à jour.
- → Si les participants utilisent leur ordinateur personnel ou professionnel pendant la session de formation (plutôt que de louer des ordinateurs qui ont fait l'objet d'un entretien et d'un nettoyage pour éliminer les éventuels logiciels malveillants ou superflus), il sera probablement plus compliqué pour eux d'installer les outils ou d'effectuer certaines tâches, en raison des paramètres différents de leurs ordinateurs. Comme vous n'êtes pas technicien et que le temps disponible est limité, n'essayez pas de résoudre ces problèmes pendant la session. Demandez plutôt aux participants qui rencontrent un problème de travailler avec un de leurs collègues, de manière à faire en sorte que les objectifs de la session puissent être atteints pour l'ensemble du groupe.
- → Il est souhaitable d'avoir au moins un ordinateur pour deux participants, pour que ceux-ci puissent suivre vos instructions et s'essayer eux-mêmes aux outils.
- → Utilisez la section correspondante des « Guides pratiques » pour vous préparer à faire la démonstration des outils (**https://securityinabox.org/en/handsonguides**). Entraînez-vous à l'avance et anticipez les questions. Utilisez un vocabulaire simple et illustrez la pertinence des outils pour répondre aux risques identifiés par les défenseurs .[3]
- → Quand vous présenterez les outils, demandez aux participants de fermer toutes les autres applications et de suivre votre première démonstration sur l'écran de projecteur. Demandez-leur ensuite de faire la même chose sur leur ordinateur en suivant la manœuvre que vous montrez à l'écran. Enfin, demandez leur de répéter la même procédure sans guidance. Plus ils auront d'opportunités de s'exercer à l'utilisation des outils, plus l'expérience d'apprentissage sera fructueuse.
- → L'utilisation d'outils de sécurité numérique peut se révéler compliquée pour de nombreux DDH. Expliquez-leur les bénéfices qu'ils tireront de l'utilisation de ces outils en réponse aux risques auxquels ils sont confrontés. Dites-leur que plus ils utiliseront les applications, plus ils se sentiront à l'aise avec elles.
- → Renvoyez les participants aux ressources proposées sur le site Security in a Box **https://securityinabox.org** pour découvrir d'autres outils et obtenir d'autres conseils. Tous ces outils sont gratuits, et la boîte à outils est mise à jour régulièrement..
- → Le Kit d'aide d'urgence en sécurité numérique pour les défenseurs des droits humains présente des scénarios de risque spécifiques et propose des conseils de mesures immédiates pour remédier à la situation. Il propose également des liens vers des ressources complémentaires comme Security in a Box et d'autres initiatives (**https://www.apc.org/en/irhr/digital-security-first-aid-kit**).

3 Level Up! est une ressource en cours d'élaboration pour les formateurs en sécurité numérique. Elle proposera des informations aidant à préparer et à donner des sessions de formation à la sécurité numérique. Consultez le site **http://level-up.cc** pour obtenir des idées et des conseils.

CONCLUSION

> Rappelez aux participants que l'activité consacrée à la sauvegarde et à la perte ou au vol de données a pour but de les éclairer quant aux endroits où sont stockées leurs données, et à la partie de ces données qui sont sensibles et qui doivent donc être protégées d'un éventuel accès non-autorisé et sauvegardées en back-up pour éviter qu'elles n'existent qu'en un seul endroit. Demandez-leur de rappeler les enseignements-clés et les lectures complémentaires nécessaires, qu'ils doivent inclure dans leurs plans d'action.

> Si vous avez parlé d'outils spécifiques de sécurité informatique, demandez aux participants de rappeler à quels risques ces outils répondent et pourquoi ils pensent qu'il y a lieu de les utiliser. Pour vous assurer de la bonne application des outils, pensez à donner aux participants des travaux pratiques, pour qu'ils puissent s'entraîner et se familiariser à leur usage.

RESSOURCES COMPLÉMENTAIRES

> Association for Progressive Communication (2013), « Digital Security First-Aid Kit for Human Rights Defenders. Voir : **https://www.apc.org/en/irhr/digital-security-first-aid-kit**

> Front Line Defenders (2009), « Digital Security and Privacy for Human Rights Defenders. Voir: **http://www.frontlinedefenders.org/files/en/esecman.en_.pdf**

> Tactical Tech Collective, «Me and My Shadow»Voir: **https://myshadow.org/**. Ressources et outils destinés à limiter les informations laissées derrière soi en utilisant internet.

> Level Up! Une boîte à outils pour les formateurs en sécurité informatique. Voir : **http://www.level-up.cc**.

> Le collectif Technical Tech et Front Line ont développé la boîte à outils de référence Security in a Box **http://securityinabox.org** disponible en ligne et sous forme de livre ou de DVD. Nous vous recommandons d'utiliser la version en ligne du logiciel, qui est la plus à jour. Securityinabox.org traite les questions suivantes:

- **Protéger votre ordinateur contre les logiciels malveillants et les pirates**
- **Assurer la sécurité physique de vos données**
- **Créer et sauvegarder des mots de passe sûrs**
- **Protéger les données sensibles stockées sur votre ordinateur**
- **Récupérer des données perdues**
- **Détruire définitivement des données sensibles**
- **Préserver la confidentialité de vos communications sur Internet**
- **Préserver votre anonymat et contourner la censure sur Internet**
- **Préserver votre anonymat et contourner la censure sur Internet**
- **Utiliser votre téléphone mobile en sécurité (autant que possible…)**
- **Utiliser votre smartphone en sécurité (autant que possible…)**

Protection International AISBL
11 Rue de la Linière
1060 Bruxelles – Belgique
+32 2 609 44 05
http://protectioninternational.org