



GUIDE

GESTION DES RISQUES ET DES NOUVELLES MENACES



**MENACES
RISQUES**

Ce document et ses supports sont la propriété exclusive de FRANCOPOP – Réseau international francophone de formation policière. Ils ne peuvent être reproduits ou utilisés sans l'autorisation préalable et écrite de FRANCOPOP.

Les exemples et les cas pratiques cités dans ce guide ont pour seul objectif d'illustrer des pratiques inspirantes ou des approches en matière de gestion des risques et des nouvelles menaces. Aucun jugement n'est porté sur les organisations ou les personnes concernées quant à la qualité des services offerts à leur population.

Cet ouvrage est le fruit d'une collaboration entre des professionnels issus de la sécurité publique, des spécialistes et des chercheurs universitaires pour mettre en commun l'expérience et la connaissance utiles au développement de réponses adéquates face aux nouvelles menaces et aux risques y étant liés. Nos remerciements les plus sincères vont aux personnes qui ont contribué à ce guide ainsi qu'à l'Organisation internationale de la Francophonie pour son soutien financier.

Le genre masculin est utilisé sans aucune discrimination et uniquement pour alléger le texte.

Produit par FRANCOPOL – Réseau international francophone de formation policière

Sous la direction de **Thierry Dierick**, responsable de projet, Police fédérale/Académie nationale de police – Belgique
| Coordination et rédaction : **Leila Oujjan**, coordonnatrice de la rédaction, secrétaire de direction, Police fédérale/
Académie nationale de police – Belgique

Collaborateurs à la rédaction : **Sophie Hatt**, Police nationale, Direction de la coopération internationale au ministère de l'Intérieur français – France | **Thierry Dierick**, Police fédérale/Académie nationale de police – Belgique | **Éric Denécé**, directeur du Centre Français de Recherche sur le Renseignement – France | **Ousman Ramadan Zacharia**, Centre tchadien des études stratégiques et d'analyse prospective – Tchad | **Amin Boutaghane**, Unité de coordination de la lutte antiterroriste – France | **Jean-Luc Gonzales**, attaché de sécurité intérieure près de l'ambassade de France – Sénégal | **Cécile Oyono**, École internationale des forces de sécurité (EIFORCES) | **André Duvillard**, Réseau national de sécurité – Suisse | **Grégory Gomez del Prado**, Service de renseignement et de la protection de l'État, Sûreté du Québec – Canada | Professeur **Amadou Sall**, Cellule régionale de la radicalisation et de l'extrémisme violent au Sahel – Mauritanie | **Pascal Bastide**, École nationale supérieure de police – France | **Raoul Jaccard**, Service psychologique de la police neuchâteloise – Suisse | **Claude Passchier**, Police fédérale/Académie nationale de police – Belgique | **André Etter**, Conseil cantonal de sécurité – Suisse | **Alain Gorka**, Gendarmerie vaudoise – Suisse | **Bart Cappaert**, Police fédérale – Belgique | **Grégory Briche**, Institut de recherche criminelle de la Gendarmerie nationale – France | **Pierre-Henri Machet**, Direction centrale du recrutement et de la formation de la Police nationale – France | **Augustin Ochogni**, Direction de l'informatique et des traces technologiques – Côte d'Ivoire | **Jean Lafrenière**, Sûreté du Québec – Canada | **Serge Houtain**, Police judiciaire fédérale – Belgique | **Dr Papa Gueye**, Police nationale – Sénégal | **Dr Babacar Ndaw**, Commission Nationale de Cryptologie – Sénégal | **Florent Bouvier**, École nationale à vocation régionale – France | **France Thibodeau**, Collège canadien de police – Canada | **Sébastien Jaquier**, Institut suisse de police de Neufchâtel – Suisse | **Professeure Ndioro Ndiaye**, Réseau francophone pour l'égalité femme-homme/Alliance pour la migration, le leadership et le développement – Sénégal | **Ahmadou Tidjani Abdou Ali**, École Nationale de Police et de la Formation Permanente – Niger | **Abdou Wahabou Sall**, Police aux frontières – Sénégal | **Fady Dagher**, Service de police de Longueuil – Canada | **Marie Diallo**, Caisse de Sécurité Sociale – Sénégal | **Yves Guay**, École nationale de police du Québec – Canada | **Freya Oosterlinck**, Police fédérale – Belgique | **Pierre St-Antoine**, École nationale de police du Québec – Canada | **Roger Ouédraogo**, commissaire divisionnaire de police, chargé de mission au Cabinet du ministre de la Sécurité – Burkina Faso | **Andrée-Ann Deschênes**, Université du Québec à Rimouski – Canada | **Annie Gendron**, École nationale de police du Québec – Canada | **Josée Bergeron**, École nationale de police du Québec – Canada | **Manon Beaumier**, Université du Québec à Trois-Rivières – Canada | **Dorlie Kabieni Amboyi**, doctorante en droit international public à la Faculté d'Angers – France

Avec l'aide de **Suzanne Roy**, technicienne en affaires institutionnelles, École nationale de police du Québec – Canada

Conception graphique : **Erick Marshall**, designer graphique – Canada

Révision linguistique : **RévisArt** – Canada

FRANCOPOL, Bruxelles, septembre 2019

ISBN 978-2-9815673-4-5 (Format PDF)

ISBN 978-2-9815673-3-8 (Format imprimé)

Sous la direction du Secrétariat général de FRANCOPOL



Photo par Daniel Tatford sur Unsplash

Extrait du site Web de l'Organisation internationale de la Francophonie (OIF) au sujet du 5^{ème} Congrès international de FRANCOPOL :

Avec le soutien de l'OIF, le réseau international francophone de formation policière (FRANCOPOL) a organisé son cinquième congrès international à Dakar (Sénégal) du 17 au 19 octobre 2018. [Celui-ci portait sur la gestion des risques et des nouvelles menaces.]

Ce grand rassemblement, qui a coïncidé avec le 10^e anniversaire de FRANCOPOL, s'est tenu pour la première fois en Afrique et réunissait environ 160 participants en provenance d'une vingtaine de pays de l'espace francophone, particulièrement d'Afrique, d'Amérique du Nord et d'Europe. Il avait pour thème la « Gestion des risques et des nouvelles menaces ». Cette session a également été marquée par l'adhésion de la Macédoine et du Cambodge – premier pays du continent asiatique à intégrer cette organisation policière francophone. [...]

La cérémonie d'ouverture du Congrès était présidée par le représentant du ministre de l'Intérieur du Sénégal, son directeur de cabinet Mamadou Diop, en présence des hautes autorités des Forces de sécurité (Police et Gendarmerie) du Sénégal et de représentants diplomatiques.

La présidente de FRANCOPOL, [Mme] Sophie Hatt [directrice de la Direction de la coopération internationale de la Police nationale française], a rappelé le parcours de ce réseau aujourd'hui dans « une phase d'expansion ininterrompue », confirmant son statut de « première organisation internationale policière francophone qui rassemble, à ce jour, une soixantaine d'institutions en provenance d'une vingtaine de pays d'Amérique, d'Europe et d'Afrique, et aujourd'hui d'Asie et d'Europe centrale ».

Le représentant de l'OIF, [M.] Dominique Delpuech, directeur adjoint « Affaires politiques et gouvernance démocratique », a saisi l'occasion de la cérémonie d'ouverture pour « rendre un hommage appuyé aux forces de sécurité publique de l'espace francophone qui, par leur engagement et leur dévouement, consacrent leur vie – très souvent au péril de celle-ci – au maintien de l'ordre et donc à la stabilité et à la paix à

l'intérieur de leur pays, mais aussi aux niveaux régional et international », avant de « réitérer le plein soutien de l'OIF à FRANCOPOL, un des 16 réseaux institutionnels sur lesquels s'appuie la Francophonie pour incarner les engagements de ses États et gouvernements membres ».

M. Delpuech a également rappelé la contribution de son organisation dans la « lutte contre le terrorisme », la gestion de la « cybercriminalité » et des « flux migratoires », ainsi que sur la question des « risques psychosociaux », ces enjeux d'actualité au cœur de son action. En effet, le XVII^e Sommet de la Francophonie (Erevan, 11-12 octobre 2018) a permis de « réaffirmer la mobilisation de la Francophonie dans la lutte contre le fléau terroriste, et sa détermination en faveur de la prévention de la radicalisation et de l'extrémisme violents pouvant conduire au terrorisme », a-t-il souligné. En témoigne la création récente de FrancoPrev, le Réseau francophone de prévention de la radicalisation et de l'extrémisme violents. Avant d'ajouter que sur la cybercriminalité, l'OIF s'employait, depuis le lancement d'une Stratégie numérique lors du Sommet de Kinshasa en 2012, à « accompagner ses membres dans leur volonté d'instaurer un environnement de confiance numérique ». Cela a abouti à la publication, en février 2017, du *Guide pratique de la cybersécurité et de la cyberdéfense*. S'agissant de la gestion des flux migratoires, l'OIF a partagé « son approche humaniste, respectueuse de la dignité et des droits fondamentaux de tous les migrants, qui valorise également le parcours et la contribution de ces personnes au développement de nos sociétés », a rappelé le représentant de l'OIF.

Source : Organisation internationale de la Francophonie, 2018 (www.francophonie.org/5e-congres-francopol-49304.html).

Les membres du réseau international FRANCOPOL remercient l'Organisation internationale de la Francophonie pour le soutien apporté à l'organisation de ce congrès international ainsi qu'à l'élaboration du présent guide.

TABLE DES MATIÈRES

MOT DE LA PRÉSIDENTE	7
1 DISCOURS D’OUVERTURE	8
2 TERRORISME	12
2.1 INTRODUCTION - IMAGE DU PHÉNOMÈNE	12
2.2 LUTTE CONTRE LE TERRORISME	15
2.2.1 <i>Pratiques inspirantes</i>	15
2.2.1.1 Prise en charge des femmes radicalisées dans les pays du bassin du lac Tchad	15
2.2.1.2 Détection de la radicalisation et de l’extrémisme violent : quel rôle pour la police?	16
2.2.1.3 Formation en ligne sur les menaces extrémistes et l’extrémisme violent	19
2.2.1.4 Problématiques de la radicalisation des jeunes d’Afrique de l’Ouest : quelles pistes de solution?	20
2.2.1.5 Lutte contre la radicalisation	23
2.2.1.6 Gestion des menaces et prévention de la violence (MPV)	25
2.2.2 <i>Échanges</i>	28
2.3 GESTION D’INCIDENTS LIÉS AU TERRORISME	31
2.3.1 <i>Pratiques inspirantes</i>	31
2.3.1.1 Exercice de simultanéité d’attentats terroristes en mai et en octobre 2018 au Burkina Faso, en Côte d’Ivoire, en Guinée-Conakry, au Mali, en Mauritanie, au Niger et au Sénégal	31
2.3.1.2 Détection des comportements suspects (Behavior Detection Officer)	33
2.3.1.3 Riposte à un accrochage	36
2.3.1.4 Riposte en deuxième échelon – Concept ÉGIDE	38
2.3.1.5 Gestion opérationnelle d’une tuerie de masse	40
2.3.1.6 Équipe multidisciplinaire d’extraction des blessés (Formation Casualty Extraction Team)	42
2.3.1.7 Gestion de scènes de crime complexes par la Gendarmerie nationale : les capacités opérationnelles de l’Institut de recherche criminelle de la Gendarmerie nationale	45
2.3.1.8 Entraînement au tir « vidéo assisté »	48
2.3.2 <i>Échanges</i>	50

3	CYBERCRIMINALITÉ	54
3.1	INTRODUCTION	54
3.2	PRATIQUES INSPIRANTES	55
3.2.1	<i>Présentation des travaux du comité technique sur la cybercriminalité de FRANCOPOL</i>	55
3.2.2	<i>Présentation de la Division spéciale de cybersécurité</i>	58
3.2.3	<i>Présentation de l'École nationale à vocation régionale</i>	60
3.2.4	<i>Primo-intervenants en cybercriminalité</i>	62
3.2.5	<i>Enquêtes sur des cybercrimes</i>	63
3.2.6	<i>Nouvelles technologies et préservation des preuves, genèse d'un projet national de formation de base pour les policiers</i>	65
3.3	ÉCHANGES	69
4	GESTION DES FLUX MIGRATOIRES	71
4.1	INTRODUCTION – IMAGE DU PHÉNOMÈNE	71
4.2	PRÉSENTATION DE L'ÉQUIPE CONJOINTE D'INVESTIGATION	73
4.3	ÉCHANGES	74
5	GESTION DES RISQUES PSYCHOSOCIAUX	77
5.1	SANTÉ MENTALE DANS L'UNIVERS POLICIER	77
5.2	PRATIQUES INSPIRANTES	80
5.2.1	<i>SOLVE, une approche intégrée de la gestion des risques psychosociaux dans une organisation</i>	80
5.2.2	<i>Prévention des répercussions psychologiques dans la pratique des métiers d'urgence : présentation d'une formation en ligne pour les policiers, les techniciens ambulanciers paramédicaux et les pompiers</i>	83
5.2.3	<i>Analyse de risque intégrée dans le cadre de la préparation, de la gestion et de l'évaluation des événements d'ordre public, tant sur le plan opérationnel que sur celui du bien-être et de la sécurité</i>	85
5.2.4	<i>Nouvelle approche de formation en désescalade à l'École nationale de police du Québec</i>	89
5.2.5	<i>Gestion de la santé mentale psychologique au travail des policiers : les six principes incontournables pour une meilleure pratique organisationnelle</i>	92
5.2.6	<i>Échanges</i>	95
6	CONCLUSION	96
7	UN REGARD EXTÉRIEUR	97



Photo par EV sur Unsplash

MOT DE LA PRÉSIDENTE

L'année 2018 a été exceptionnelle pour FRANCOPOL. Le Réseau international francophone de formation policière fêtait en effet 10 années d'existence. À l'occasion de cet anniversaire, et pour la première fois sur le continent africain, FRANCOPOL organisait, en 2018, son 5^e Congrès international à Dakar du 17 au 19 octobre sur la thématique générale de la gestion des risques et des nouvelles menaces. Ces 10 ans ont été marqués par le développement de liens forts entre nos pays au travers de discussions et d'actions de coopération au sein de la communauté policière francophone. Aujourd'hui, notre réseau rayonne à travers le monde et poursuit la promotion de sa marque distinctive reconnue sur tous les continents.

L'événement, placé sous le haut patronage du ministère de l'Intérieur sénégalais, a rassemblé des hauts responsables et des experts d'une vingtaine de pays de l'espace francophone dans les domaines de la lutte contre le terrorisme, de la cybercriminalité et des flux migratoires. Sur ces vastes sujets, le congrès proposait des conférences et des débats permettant de présenter les bonnes pratiques déployées à l'échelle internationale. Devant les nombreuses menaces qui compromettent la sécurité globale, FRANCOPOL s'engage, depuis sa création, dans une coopération accrue de manière à lutter efficacement contre la criminalité transnationale ainsi que contre toute forme de violence. Enjeu majeur pour nos États, notre mobilisation est essentielle et la coopération internationale est indispensable. Les menaces actuelles auxquelles sont confrontés l'ensemble des pays membres de son réseau imposent une réflexion commune sur la manière de les gérer. Réseau institutionnel de la Francophonie et partenaire privilégié de l'Organisation internationale de la Francophonie, FRANCOPOL se fixe comme objectif d'offrir un lieu d'échange, de collaboration et de diffusion afin de faire progresser les pratiques.

C'est dans cette optique que le réseau FRANCOPOL reste persuadé que le partage des informations et des formations élaborées à l'occasion de son 5^e Congrès international a permis de conforter et de redoubler notre engagement. Je remercie tout particulièrement les autorités sénégalaises de nous avoir fait l'honneur d'accueillir cet événement à Dakar, l'ensemble des intervenants et des participants pour leur engagement, le Comité des écoles qui a coordonné avec brio une programmation riche, de même que nos partenaires privés et institutionnels pour leur soutien.

Sophie Hatt, présidente de FRANCOPOL

1. DISCOURS D'OUVERTURE

Quelles sont les nouvelles menaces auxquelles nos sociétés sont confrontées et les réponses apportées par les services de police?

Depuis le début des années 1990, sous le double effet de la révolution technologique et géopolitique, l'environnement international a connu de profonds bouleversements. Si l'opinion publique est généralement consciente et au fait des grands conflits qui ensanglantent ou déstabilisent le monde, elle ne perçoit pas les autres risques qui menacent l'équilibre de notre monde.

Nos États, nos sociétés et nos entreprises sont aujourd'hui confrontés à cinq nouveaux types de risques qu'il est indispensable de prendre en considération afin qu'ils ne perturbent pas leur stabilité, leur devenir et le développement de leurs activités.

— **Les risques géopolitiques** résultent de l'accroissement du terrorisme, de l'insécurité internationale et de la multiplication des zones à risque. Les phénomènes qui en découlent (instabilité politique, attentats, guérillas, enlèvements d'expatriés, piraterie maritime, etc.) perturbent considérablement l'internationalisation des activités. Les organisations non gouvernementales (ONG) et les entreprises qui exportent ou s'implantent à l'étranger se retrouvent de plus en plus fréquemment dans des situations où elles n'ont plus d'interlocuteurs locaux permettant d'assurer la sécurité de leur environnement, voire de leur territoire. Cela leur impose un accroissement du coût de leur fonctionnement ou l'obligation de quitter certains marchés ou certaines zones d'intervention. De même, aujourd'hui, deux fois plus de pays qu'il y a vingt ans sont quasiment « interdits » aux touristes, illustration d'une dégradation généralisée de la sécurité intérieure de nombreux pays.

Les « zones grises » sont des régions qui ne sont pas ou plus contrôlées par les États, étant passées sous le contrôle d'entités terroristes ou criminelles. Le manque

de contrôle aux frontières étatiques permet la libre circulation de bandes armées à l'origine de violence, de crimes et de pillages. Aujourd'hui, des « zones grises » existent dans presque tous les pays africains, au Moyen-Orient (Syrie, Irak, Yémen, Afghanistan) et en Amérique latine (Mexique, Colombie, etc.). Dans ces espaces, chefs de guerre, de clans ou de mouvements religieux radicaux assurent le contrôle d'une partie du territoire. Les interventions militaires effectuées en vue de rétablir un semblant d'ordre sont confrontées à d'innombrables difficultés, à l'exemple de la Somalie ou de l'Afghanistan. Toutefois, force est de reconnaître que les « zones grises » ne sont pas une particularité des régions en guerre : certaines banlieues des métropoles européennes en présentent également toutes les caractéristiques (insécurité, trafics, violence, etc.).

— **Les risques criminels** illustrent l'irruption d'organisations criminelles (mafias, cartels, etc.) dans l'économie légale. Les acteurs illicites s'infiltrent dans les États comme dans les activités traditionnelles des entreprises par de multiples moyens (placements immobiliers, participations financières, rachats de PME, contrefaçon, extorsion, blanchiment, fraude, corruption, cybercriminalité, etc.) afin de développer leurs affaires ou de « recycler » leurs fonds; ce phénomène affecte de plus en plus le fonctionnement de l'économie internationale.

En effet, la mondialisation n'a pas profité qu'aux seuls acteurs économiques classiques. De nombreux réseaux criminels ont su saisir cette occasion de se développer et d'étendre leurs activités, tirant principalement parti de l'accélération des flux transfrontaliers, des politiques de dérégulation et de la généralisation du capitalisme libéral à l'échelle planétaire. Les criminels, les mafias et les cartels ont su, beaucoup plus rapidement que les entreprises et les États, tirer parti de la mondialisation. Ils utilisent mieux les technologies, les transferts bancaires, l'ouverture des marchés.

Depuis une vingtaine d'années, INTERPOL observe avec inquiétude l'accroissement considérable et la diversification des activités illicites. Ce développement de la criminalité organisée profite du fait que les systèmes policiers et judiciaires ont toujours de grandes difficultés à unifier leurs actions.

- **Les risques sociétaux** sont l'expression des comportements déviants qui caractérisent les sociétés du XXI^e siècle marquées par la perte des repères religieux, philosophiques et idéologiques, ainsi que par la recherche de sens et la montée du fondamentalisme.

Il existe deux types de risques sociétaux : les **dérives sectaires** et les **phénomènes contestataires**. Tous deux relèvent d'une même volonté de remettre en cause les sociétés libérales et de déstabiliser les entreprises au nom d'une croyance que les uns cherchent à imposer (islam radical, scientologie, autres sectes, etc.) ou d'une « cause » que les autres défendent avec une très grande violence (mouvements anticapitalistes, antimarques, écologistes radicaux, défenseurs des « droits » des animaux, etc.). Au-delà de la classique contestation sociale, ces phénomènes se répercutent de plus en plus durement sur la cohésion des nations, l'ordre public et l'activité des entreprises.

Nous sommes ainsi confrontés à la multiplication des contestations de toute nature. Nos sociétés sont de plus en plus travaillées par des mouvements d'opinion – légitimes ou non – qui veulent absolument se faire entendre et imposer leurs idées ou le changement. Ces mouvements d'opinion tirent pleinement profit de l'hypermédiatisation de nos sociétés modernes, constamment à la recherche de la nouveauté et de la primeur au détriment d'une information équilibrée.

Si les mouvements contestataires sont loin de constituer un risque nouveau, ils se singularisent néanmoins par une double évolution survenue à partir des années 1990 : d'une part, ils ont changé d'objet en

s'en prenant désormais prioritairement à des cibles économiques (grandes entreprises et « pouvoir de l'argent »), et non plus uniquement aux symboles de l'État; d'autre part, ils se caractérisent par une violence accrue, pouvant aller parfois jusqu'au terrorisme.

En effet, certains mouvements contestataires ont de plus en plus fréquemment recours à la violence pour tenter d'atteindre rapidement leurs objectifs. Sous leur impulsion, à Seattle (États-Unis, 1999) et à Gènes (Italie, 2001), la protestation lors des sommets du G8 a pris la forme d'une guérilla urbaine instaurée par le mouvement des Black Blocs. Pour ces derniers, « frapper un flic, ce n'est pas de la violence, mais de la vengeance » contre des institutions illégitimes. Certains de ces groupes extrémistes n'ont pas d'autre raison d'être que ces manifestations brutales et ponctuelles; ils sont à l'origine de pillages et de dégradations en marge des manifestations, et ils recherchent délibérément l'affrontement avec les forces de l'ordre.

- **Les risques anticoncurrentiels** sont la conséquence du durcissement de la concurrence économique (accroissement de l'intensité concurrentielle, course effrénée à l'innovation et à la conquête des marchés), lequel conduit de nombreux acteurs à recourir à des pratiques hostiles, déloyales ou illégales pour acquérir des informations (espionnage), contourner les règles d'accès aux marchés (corruption, influence, pressions politiques) ou venir à bout de la concurrence (déstabilisation, sabotage).

Si la victoire du libéralisme sur le communisme a permis à l'économie de marché de s'imposer, ce succès a paradoxalement entraîné le retour du rôle de l'économie comme domaine principal de concurrence entre les nations. La guerre pour le contrôle des marchés mondiaux que se livrent les États et les entreprises est d'une intensité sans cesse croissante.

La recherche tous azimuts de l'information ne cesse de s'élargir, et de nouvelles méthodes de captation de

l'information se généralisent. Pour certains acteurs particulièrement agressifs, l'objectif prioritaire n'est plus de satisfaire les besoins du marché, mais de détruire psychologiquement les offres et la réputation des concurrents dans l'esprit des clients. De tels procédés prennent manifestement leurs distances avec l'éthique traditionnelle – comme avec la légalité – et s'inspirent largement de savoirs provenant du monde du renseignement et des opérations clandestines, même si la filiation avec ceux-ci est rarement évoquée.

Ces méthodes font courir des risques énormes aux pays et aux entreprises qui en sont victimes, pouvant aller jusqu'à remettre en cause leur existence. Certains États développés contribuent objectivement à pervertir la loi de l'offre et de la demande par des interventions clandestines (emploi des services de renseignement) et des pressions politiques afin de s'assurer que leurs entreprises remportent les marchés contre leurs concurrents, même s'ils prônent officiellement le respect des lois du commerce mondial.

- **Les risques pénaux extrajudiciaires** sont la résultante de l'application extraterritoriale du droit américain en matière de règles d'exportation (embargos), de normes anticorruption et de lutte contre le terrorisme (*renditions*).

Depuis la fin de la guerre froide, les États-Unis ont en effet développé une redoutable stratégie afin d'assurer leur suprématie politique et économique. Cette stratégie se fonde principalement sur l'imposition de leurs règles juridiques à tous leurs rivaux. En trois décennies, les États-Unis sont quasiment parvenus à transformer le reste de la planète en un nouvel État américain. En effet, les lois édictées à Washington s'imposent aujourd'hui au reste du monde, au détriment des droits et des intérêts des autres nations.

Les autorités américaines ont ainsi bâti un arsenal législatif répressif leur donnant les moyens de lutter contre l'expansion économique de leurs concurrents

ou les velléités d'indépendance de leurs partenaires. Et si ces pays refusent de s'y soumettre, les États-Unis peuvent décider de prendre des mesures unilatérales de rétorsion. Ainsi, leur politique de sanctions à caractère extraterritorial s'est largement développée depuis le début des années 1990. Cela se traduit, pour les entreprises et leurs dirigeants, par des poursuites pénales et des sanctions financières importantes.

- **Les cybermenaces** illustrent le fait que la révolution numérique a ouvert de nouveaux espaces à la conflictualité, au crime et à la contestation. Cette révolution a superposé à notre environnement physique un environnement virtuel dans lequel les cinq risques exposés précédemment se manifestent. Mais plutôt que d'évoquer un nouveau type spécifique de menace, il est plus approprié de considérer que toutes les activités malveillantes se déploient désormais à la fois sur le plan physique et sur le plan cybernétique : ainsi sont apparus la cyberguerre, le cybersabotage, la cybercriminalité, le cyberactivisme, la cyberpropagande, le cyberespionnage, etc.

Le champ de préoccupations des responsables publics ou privés de la sécurité s'élargit désormais à de nouveaux domaines qui viennent s'ajouter à leurs missions traditionnelles – lutte contre le terrorisme, criminalité et immigration clandestine – et qui leur imposent de nouvelles conditions de fonctionnement. Dans un environnement en perpétuel bouleversement, ces responsables ne peuvent plus s'affranchir d'une démarche de suivi de ces nouvelles menaces sous peine d'être victimes de surprises et de perdre, à terme, la maîtrise des situations. C'est pourquoi il s'avère indispensable de former et de mobiliser l'ensemble des acteurs de la sécurité autour de la recherche permanente, active et dynamique du renseignement.

Éric Denécé, directeur du Centre Français de Recherche et de Renseignement (CF2R), France



2. TERRORISME

2.1 INTRODUCTION – IMAGE DU PHÉNOMÈNE

La gestion de la menace terroriste en Europe et en France

La franchise djihadiste d'inspiration sunnite originelle, Al-Qaïda (AQ), représente toujours une menace sérieuse pour les pays européens, notamment pour leurs intérêts et leurs ressortissants à l'étranger, en particulier au Sahel. Régulièrement dénoncée, l'action « coloniale » de la France au Sahel, mais aussi le « pillage des ressources économiques nord-africaines et sahéliennes » à laquelle se livreraient les sociétés occidentales font office de facteurs de mobilisation pour des populations marginalisées, perméables à la diffusion des thèses islamistes radicales et insurrectionnelles dans un contexte de minorités ethniques souvent électrisées et agrégées autour de vecteurs de révolte jugés opportuns, dans le discours comme dans l'action.

Si l'affaiblissement de l'État islamique (EI) en Syrie et en Irak se traduit par une réduction des capacités de l'organisation à projeter des attaques de grande ampleur en Europe, la menace n'a pas disparu; elle émane désormais d'acteurs isolés, s'inspirant de la propagande djihadiste et utilisant des moyens rudimentaires, la rendant plus difficile à détecter.

Portée par une propagande djihadiste qui a su s'adapter aux diverses mesures d'entrave, la menace terroriste en Europe est avant tout inspirée. En d'autres termes, motivés par la diffusion sur Internet et les chaînes privées ou par les revendications d'actions terroristes parfois opportunistes de l'agence Amaq, de nombreux acteurs isolés passent à l'acte sur le territoire national ou dans les pays d'Europe occidentale. Le groupe terroriste poursuit ainsi sa stratégie d'occupation médiatique basée, entre autres, sur la récupération opportuniste d'actions « de basse intensité » qui s'inscrivent dans la ligne de son schéma propagandiste.

Le traitement médiatique de ces affaires est susceptible de nourrir *in fine* un effet mimétique au sein de la population endogène. L'attaque au couteau commise le 20 août 2018 en

Espagne par un ressortissant algérien dans le commissariat de Cornellà de Llobregat, près de Barcelone, dans le cadre d'un plutôt vraisemblable « *suicide by cop* », est ainsi venue rappeler l'instabilité de la menace portée en Europe par les radicalisés endogènes, principalement de culture musulmane.

Si la menace d'actions isolées est particulièrement prégnante, on ne peut toutefois exclure l'existence de cellules organisées, comme en témoigne le démantèlement, le 27 septembre dernier, d'une cellule structurée de sept individus aux Pays-Bas. Selon les premiers éléments dont nous disposons, cette cellule était engagée à un stade avancé dans des préparatifs d'assaut armé lors d'un grand événement (sans autres précisions), à l'aide d'armes de guerre (AK 47, grenades à main, armes légères, gilets explosifs) et de véhicules piégés.

Ainsi, si l'usage de procédés rudimentaires et facilement accessibles (armes blanches ou à feu, véhicules-béliers) reste le mode d'action le plus probable, la combinaison de modes opératoires sophistiqués, portée par une cellule dormante, demeure une menace réelle, notamment en France.

On notera que la menace terroriste pesant sur les pays d'Europe occidentale peut également émaner de membres de la mouvance exogène en situation de rupture sociale, religieuse ou linguistique, ou de déshérence migratoire dans leurs pays d'accueil. En effet, plusieurs ressortissants originaires de foyers en crise (Syrie, Irak, Afghanistan, Pakistan) dans lesquels prospèrent des groupes terroristes d'inspiration sunnite ont, depuis 18 mois, diversement frappé ou tenté de frapper la France, l'Angleterre, l'Allemagne, la Suède ou les Pays-Bas, comme l'illustre l'attaque commise à la gare centrale d'Amsterdam par un ressortissant afghan le 31 août 2018.

Par ailleurs, le 1^{er} octobre dernier, une opération de la Garde civile espagnole a permis de démanteler, en milieu carcéral, un réseau structuré de recrutement et d'endoctrinement nommé « Front des prisons » (*Frente de cárceles*), impliquant 25 détenus liés à l'EI qui œuvraient au sein de 17 prisons espagnoles. Ce groupe serait constitué d'individus détenus pour terrorisme islamiste et de prisonniers de droit commun, radicalisés lors de leurs séjours carcéraux. Ce premier

démantèlement d'envergure dans l'univers carcéral en Europe vient à nouveau rappeler la particulière sensibilité de ce milieu fermé, lieu initiatique et vecteur dimensionnant, de fait véritable incubateur de la menace terroriste de demain. Loin d'être un vase clos, comme en témoignent plusieurs interpellations menées par les services de sécurité ces derniers mois, il peut s'y opérer, avec une discrétion entretenue, des transferts de compétences entre islamistes et délinquants de droit commun radicalisés. Cette dernière question a d'ailleurs largement essaimé depuis le début de cette année 2018, notamment sur la base de travaux portés par l'Unité de coordination de la lutte antiterroriste (UCLAT; nous y reviendrons plus loin).

Comme les autres pays d'Europe occidentale, la France a vite été confrontée à une menace grave liée au basculement de plusieurs centaines de personnes dans l'engagement radical violent, le plus souvent en lien avec les filières djihadistes syriennes. L'émergence d'une nouvelle génération de terroristes aguerris susceptibles de frapper le territoire français a appelé de l'État français une réaction déterminée, ferme, efficace et répressive, mais également préventive, visant ainsi à endiguer ce phénomène.

En 2014, alors que plusieurs parents ont été les témoins impuissants du départ de leurs enfants mineurs vers des zones de conflit armé, les autorités françaises ont décidé de mettre en place le Plan de lutte contre la radicalisation violente et les filières terroristes. Ce plan visait notamment à contrarier les déplacements des ressortissants français vers la Syrie, à renforcer l'action des services de renseignement en matière de détection et de surveillance, mais également à apporter un soutien aux familles dont les proches étaient touchés par le phénomène de radicalisation.

Le Centre national d'assistance et de prévention de la radicalisation (CNAPR), constitué d'un numéro vert et d'un formulaire en ligne, apportait ainsi dans ce contexte une possibilité de contact efficace aux familles ou aux proches qui souhaitaient effectuer un signalement ou demander un conseil.

De plus, la nouvelle mesure d'opposition à la sortie du territoire (OST) a permis au titulaire de l'autorité parentale de

s'opposer à la sortie de France de son enfant lorsqu'il craignait que celui-ci envisage de partir à l'étranger, notamment sous l'influence de mouvements radicaux armés. Par la suite, la loi du 13 novembre 2014 ainsi que celle du 30 octobre 2017, dite Loi renforçant la sécurité intérieure et la lutte contre le terrorisme (SILT) mettant fin à l'état d'urgence décrété au lendemain de la tuerie de masse du 13 novembre 2015, ont abouti à la création de nouvelles mesures de police administrative. Ces dernières avaient pour objectif, d'une part, de limiter davantage les mouvements des individus suspectés ou impliqués dans la mouvance radicale violente et, d'autre part, de neutraliser leurs moyens d'action. L'entrave administrative est ainsi devenue une réalité empêchant les velléitaires de partir vers les zones de combat, et les djihadistes étrangers d'entrer en France. Les ressortissants français ayant séjourné sur zone sont quant à eux systématiquement judiciarisés de retour sur le territoire national. Plus de 1 300 Français sur 5 000 Européens ont rejoint la zone syro-irakienne depuis le début de l'insurrection en 2012, dont 300 sont présumés décédés, et plus de 700 seraient toujours sur place, prisonniers, au combat, voire également décédés. Ce sont 260 individus comptabilisés qui sont depuis revenus sur le territoire national.

Ainsi, la nécessité de coordonner l'action des différents services appelés à lutter contre le terrorisme, qui s'est imposée au début des années 1980 en raison de cloisonnements notables des services, d'une connaissance insuffisante des émergences géopolitiques et stratégiques et d'une communication moins élaborée, semble plus que jamais d'actualité. Créée en 1984, en contrepoint de terrorismes séparatistes (Euskadi Ta Askatasuna [ETA], Front de libération nationale corse [FLNC], etc.), d'ultra-gauche (Action directe, dans une internationale que fréquentaient aussi les Brigades rouges italiennes ou la Fraction armée rouge allemande) et d'État (Syrie, Iran), l'UCLAT assure aujourd'hui une large coordination multidisciplinaire et institutionnelle dans le domaine de la lutte contre le terrorisme et les radicalisations violentes.

Avec ses sept départements, son antenne dans le Sud-Ouest français (Pau), dont la création était en lien avec la problématique basque, et ses officiers de liaison, l'UCLAT

assure de nombreuses missions au quotidien, notamment l'actualisation permanente de l'état de la menace terroriste, la centralisation et la coordination des mesures de police administrative ainsi que le suivi des dialogues stratégiques au sein des instances nationales, européennes ou internationales. De plus, l'UCLAT a su démontrer la qualité de son expertise en matière de lutte contre la radicalisation, notamment par la gestion de la plateforme du Centre national d'assistance et de prévention de la radicalisation (CNAPR) et du fichier de signalements qui en est issu en 2015.

On notera enfin que la France est aujourd'hui confrontée à un enjeu principal, à savoir la question des sortants de prison et leur réintégration dans la société.

Compte tenu de la volonté des plus hautes autorités de l'État de voir cette problématique suivie et organisée, le pilotage de ce nouveau dispositif a été confié à l'UCLAT au mois de juin 2018, charge validée et amplifiée par le Plan d'action contre le terrorisme lancé le 13 juillet 2018. L'UCLAT assure ainsi une mission de coordination technique, administrative et logistique visant à mettre en place, en son sein, une structure chargée d'assurer le suivi des détenus terroristes islamistes (TIS) et des détenus de droit commun susceptibles de radicalisation (DCSR) à l'occasion de leur sortie de prison. Cette structure réunit à cette fin chaque mois les services judiciaires, pénitentiaires, de police et de renseignement.

Alors que la plupart des attaques commises sur le territoire national ces deux dernières années ont été le fait d'individus parfois inconnus des services de renseignement, agissant de façon impulsive et isolée, selon un mode opératoire rudimentaire, cette capacité de structuration, offerte aujourd'hui par le huis clos carcéral et facilitée par l'accès à des moyens de télécommunication ainsi que par la concentration des frustrations, apparaît ainsi à court et à moyen terme comme un élément majeur de la menace. Cette menace laisse présager la constitution de cellules autonomes, les passages à l'acte planifiés depuis le lieu de détention pouvant s'opérer in situ, comme ce fut le cas à Vendin-le-Vieil (Pas-de-Calais) où trois surveillants ont été agressés le 11 janvier 2018 avec des ciseaux et une lame de rasoir par un terroriste détenu, ou à Osny (Val-d'Oise) le 4 septembre 2016 lorsque trois détenus

radicalisés attaquaient à l'arme blanche deux surveillants à l'occasion d'une sortie en promenade dans leur quartier réservé. Les passages à l'acte pourraient également être projetés sur le territoire à l'issue de la période d'incarcération.

La question des sortants de prison, comme de nombreuses autres, à l'instar de l'état psychiatrique des radicalisés et des auteurs d'attaques terroristes, est issue d'une focalisation réalisée par un département de l'UCLAT, la Division des études et de la prospective (DEP). Protégé de l'actualité immédiate et de la réactivité à laquelle sont assujettis tous les autres agents du service, ce département est en effet chargé de produire des études denses et documentées visant à dégager les principaux axes d'avancée dans la lutte contre la radicalisation à caractère terroriste et le djihadisme.

L'UCLAT est ainsi totalement engagée dans le combat mondial contre le terrorisme et parfaitement disponible pour apporter son expertise, née malheureusement des nombreux coups portés contre l'intégrité du territoire français depuis 40 ans, sa méthodologie et sa motivation. Il nous reste notamment à retenir des cinq dernières années qu'elles ont vu les services français empêcher la réalisation de 55 actes terroristes, 17 ayant par ailleurs échoué. Les 12 attaques réussies sur cette période, vécues douloureusement, sont ainsi ancrées dans la mémoire pour rappeler l'impérieuse nécessité d'agir ensemble.

Amin Boutaghane, contrôleur général, chef de l'Unité de coordination de la lutte antiterroriste (UCLAT), Police nationale, France

2.2 LUTTE CONTRE LE TERRORISME

2.2.1 PRATIQUES INSPIRANTES

2.2.1.1 Prise en charge des femmes radicalisées dans les pays du bassin du lac Tchad

Dans un rapport de décembre 2014, Pierre Conesa, ancien haut fonctionnaire du ministère de la Défense, mentionne la définition opérationnelle proposée par Charles E. Allen, chef du Bureau Renseignement et Analyse du ministère américain de la Sécurité intérieure sous le second mandat de GW Bush (2005-2009), lors de son audition devant le Sénat US en 2007. Ainsi, d'après Allen, la radicalisation implique « le processus d'adoption d'une croyance extrémiste incluant la volonté d'utiliser, de soutenir ou de faciliter la violence comme méthode de changement de société ».

Cette acception du terme rend compte de la rupture et de l'opposition entre, d'une part, l'individu radicalisé et, d'autre part, l'État, ses institutions et la société. Si, en Occident, les facteurs identitaires semblent être les principales causes de radicalisation, ceux-ci ne peuvent expliquer la présence de groupes terroristes dans le bassin du lac Tchad.

Cette région, qui comprend le nord-est du Nigéria, l'extrême nord du Cameroun, le Niger et le Tchad, est marquée par des facteurs de vulnérabilités permanentes : l'âpreté du climat et des modes de production, les pesanteurs socioculturelles sur les femmes, les classifications sociales, les confrontations des jeunes avec les agents publics aux frontières, l'insécurité récurrente, etc. Ce sont là autant de vecteurs d'irritabilité qui font prospérer les offres de gain facile et de changement social sur fond de propagande religieuse. Selon le Programme des Nations Unies pour le développement (PNUD), la crise qui sévit actuellement affecterait près de 10 millions de personnes.

Boko Haram semble s'être appuyé sur ces facteurs et avoir recruté en grand nombre parmi les praticiens de la frontière et ceux qui exercent les petits métiers informels urbains : contrebandiers, transporteurs par autobus et motocyclettes, détaillants de carburant de contrebande, vendeurs ambulants, élèves des écoles coraniques, pêcheurs, etc. Les adeptes viennent surtout des zones frontalières, poreuses et abritant

souvent les mêmes communautés séparées par la frontière, rendant les contrôles malaisés. Par conséquent, tous les phénomènes criminels y sont transfrontaliers (coupeurs de route, prise d'otages, trafics divers, Boko Haram), voire transnationaux, impliquant des réseaux de ressortissants de deux ou plusieurs pays.

Facteurs spécifiques de la radicalisation des femmes

L'augmentation du nombre de femmes chez les kamikazes s'explique par un changement du mode opératoire de Boko Haram. Les femmes portent traditionnellement des vêtements amples pouvant cacher des explosifs et elles ne sont généralement pas fouillées par les hommes. Il convient de rajouter qu'aux yeux des leaders du mouvement, elles représentent une perte de « moindre importance » que les hommes dont on a besoin au combat : « *[women] are cheap and they are angry for the most part [...] using women allows you to save your men* » (Warner, Jason and Hilary Matfess, 2017).

On peut distinguer certains facteurs favorisant la radicalisation des femmes :

- Celles radicalisées en raison d'un mariage avec des extrémistes. En effet, les pesanteurs culturelles stigmatisent les filles qui « tardent » à trouver un mari. Du fait de cette insécurité matrimoniale et sociale, elles sont plus susceptibles d'aller avec le premier venu.
- Les filles mères devenues des « déclassées sociales » à la suite d'un mariage précoce, suivi d'une répudiation rapide. Elles perdent tout repère, ont des difficultés à se remarier et sont généralement sans emploi.
- Les veuves, les filles démunies, affamées ou désespérées à la suite de la disparition de leurs proches. Elles sont volontaires, forcées ou « payées » (200 nairas) pour commettre des attentats, convaincues de retrouver leurs proches au paradis (Warner, Jason and Hilary Matfess, 2017).

La participation des femmes aux activités terroristes est volontaire ou forcée. Certaines jeunes femmes en couple rejoignent volontairement les rangs de Boko Haram et

contribuent à la création d'une communauté religieuse (Markaz) disposant de tous les attributs sociaux. Elles y assurent les tâches ménagères et la procréation d'une nouvelle génération de disciples. Elles peuvent aussi servir d'assurance contre la désertion des époux et d'hypothèque humanitaire contre les bombardements des camps. Enfin, certaines jeunes filles, à l'instar de celles de Shibok, sont enrôlées de force après avoir été enlevées.

Enjeux et défis de gestion des radicalisés

En l'absence d'une politique nationale camerounaise de gestion des ex-associés de Boko Haram, des réflexions sont en cours dans l'extrême nord impliquant administration et partenaires internationaux. À ce jour, il n'existe aucun encadrement spécifique et, surtout, aucune assistance aux femmes revenues des zones sous emprise de Boko Haram, ce qui suscite l'irritation de leurs époux désengagés à la suite des promesses de réintégration et d'accompagnement. Le mécanisme de justice transitionnelle n'est pas encore conçu. Le rôle des mères de jeunes radicalisés, pourtant essentiel dans le processus de désengagement de leurs enfants, n'est pas assez exploité. Le serment sur le Coran appliqué aux premiers combattants qui se sont rendus n'a pas l'effet escompté, quelques-uns ayant fui le camp pour vraisemblablement rejoindre le groupe terroriste.

Le Décret n° 2018/719 du 30 novembre 2018 portant sur la création du Comité national de désarmement, de démobilisation et de réintégration ainsi que sur ses démembrements régionaux organise la prise en charge des jeunes issus des régions et victimes de l'insécurité : nord-ouest et sud-ouest pour la crise dite anglophone; Adamaoua, nord et extrême nord pour les populations affectées par Boko Haram.

Cécile Oyono, directrice générale adjointe de l'EUFORCES, Cameroun

Référence

Warner, Jason and Hilary Matfess (2017). Exploding stereotypes: The unexpected operational and demographic characteristics of Boko Haram's suicide bombers. Combating Terrorism Center at West Point United States Military Academy.

2.2.1.2 Détection de la radicalisation et de l'extrémisme violent : quel rôle pour la police?

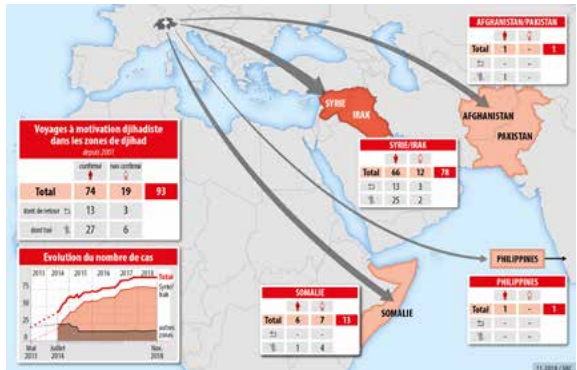
Le Réseau national de sécurité

Le Réseau national de sécurité (RNS) regroupe l'ensemble des instruments de politique de sécurité de la Confédération, des cantons et des communes. Ses organes (la plateforme politique et la plateforme opérative) gèrent la consultation et la coordination des décisions, des moyens et des mesures constituant des enjeux de politique de sécurité qui concernent à la fois la Confédération et les cantons. L'accent est mis sur la sécurité intérieure, où le besoin de coordination est plus important que pour la sécurité extérieure, laquelle relève de la compétence de la Confédération.

Dans le contexte de la lutte contre le terrorisme, le RNS a été mandaté pour élaborer un Plan d'action national contre la radicalisation et l'extrémisme violent (PAN) qui s'adresse à l'ensemble des acteurs de la prévention. Ce dernier a été adopté en décembre 2017 par les instances politiques concernées de la Confédération, des cantons et des communes.

Le contexte du terrorisme en Suisse

La Suisse a été épargnée par des actes terroristes depuis près de 50 ans, mais dès 2012, à l'instar des autres pays européens, elle a dû faire face à des départs de personnes résidant sur son territoire pour rejoindre des organisations terroristes islamistes, en particulier en Syrie et en Irak.



Comme l'indique l'illustration ci-dessus, ce sont aujourd'hui 93 personnes qui ont été formellement recensées. En raison

de la menace croissante, le Conseil fédéral a adopté, en septembre 2015, la première stratégie de la Suisse pour la lutte contre le terrorisme. Cette stratégie s'inscrit dans les quatre domaines que sont :

- la prévention;
- la répression;
- la protection;
- la préparation à une situation de crise.

Les trois premiers domaines sont destinés à empêcher des attentats terroristes en Suisse ainsi que l'exportation ou le soutien du terrorisme à partir de notre territoire. Du fait qu'il n'est pas possible d'exclure que de tels attentats aient lieu en Suisse, les mesures de préparation à une situation de crise doivent garantir que notre pays sera à même de maîtriser un attentat terroriste en renforçant sa capacité de résistance.

Le Plan d'action national contre la radicalisation et l'extrémisme violent

Ce plan constitue la principale mesure mise en œuvre dans le domaine de la prévention. Les travaux ont été coordonnés par le RNS qui, pour ce faire, a réuni les principaux acteurs (social, éducation, police, intégration, etc.) de la Confédération, des cantons et des communes.

Force est de constater que la menace terroriste a, en quelque sorte, lancé un défi au fédéralisme dans le domaine de la sécurité. Toutefois, les différents acteurs ont su relever ce défi en faisant preuve de pragmatisme et d'innovation, démontrant ainsi qu'il est possible, par un travail en réseau bien structuré et coordonné, d'apporter les réponses attendues devant un défi majeur pour la sécurité de notre pays.



Le PAN a pour objectif premier d'élaborer différentes mesures visant en premier lieu à faciliter une détection précoce des personnes en voie de radicalisation. Son champ d'action se situe aussi en amont que possible et s'inscrit dans un véritable

travail en réseau avec tous les acteurs de la chaîne pénale et judiciaire, jusqu'à l'étape ultime de la réintégration et du désengagement.

Le PAN comprend cinq domaines d'action :

- Connaissance et expertise;
- Collaboration et coordination;
- Lutte contre les idéologies et les groupements extrémistes;
- Désengagement et réintégration;
- Collaboration internationale.

Au total, ce sont 26 mesures concrètes qui ont été élaborées et qui devront être mises en œuvre dans un délai de cinq ans. Au cœur de ce plan d'action se trouve le principe de la collaboration institutionnelle et interdisciplinaire qui repose sur les exigences suivantes :

- Échanges d'informations et d'expériences entre les différents acteurs;
- Procédure de travail définie (et instruments appropriés);
- Intégration de la société civile et soutien apporté à celle-ci.

Pour garantir la mise en œuvre des diverses mesures, il est important que l'échelon local (cantons et grandes villes) mette en place à son niveau une structure de coordination réunissant les principaux acteurs que sont la police, les écoles, les services sociaux, les responsables de l'intégration ou encore le domaine de la santé, pour ne citer que ceux-là. Cette structure doit être portée par l'autorité politique qui désigne le service leader. Il appartient ensuite à cette table ronde de développer des mesures de prévention générale et, surtout, d'examiner les différentes situations qui lui auront été présentées par les acteurs de terrain. De manière schématique, chaque cas devra être traité avec les acteurs concernés à qui il appartiendra de se concerter sur les mesures à prendre. Celles-ci pourront rester du domaine de la prévention au sens large, ou être de la compétence des services de renseignement ou de la police, lorsqu'on estime que la personne pourrait présenter un risque pour la sécurité. En effet, seule une prise en charge aussi en amont que possible peut permettre de réduire, autant que faire se peut, le risque de passage à l'acte.

Rôle de la police dans la prévention de la radicalisation

La police est un des acteurs clés de la prévention de la radicalisation, mais nous considérons qu'il ne lui appartient pas d'en être le moteur. En effet, dans la phase de détection précoce, il est important de faire la différence avec le processus judiciaire qui sera déclenché lorsque des risques de passage à l'acte auront été détectés. Pour cette raison, nous recommandons que d'autres organisations (intégration, services sociaux, etc.) assument la conduite de la mise en œuvre des diverses mesures. Plusieurs stratégies ont été mises en place dans plusieurs cantons selon ce principe et elles se révèlent être efficaces.

Deux mesures du PAN ont été spécifiquement consacrées à la police, et nous allons brièvement les présenter ci-dessous.

- A.** Mesure 13 – Intensification du travail de mise en réseau de la police
- Le réseautage, l'établissement de bonnes relations et la confiance avec les communautés étrangères et les différentes associations doivent être intensifiés dans les polices communales et cantonales. Une attention particulière doit être accordée au contact avec des associations et des organisations (culturelles), par exemple des organisations travaillant dans le domaine de l'asile. De cette manière, une confiance mutuelle peut être mise en place, les réseaux entretenus et les problèmes de politique de sécurité discutés. Le modèle « Brückenbauer » mis en place par certaines polices peut être utile pour favoriser l'exécution de ces tâches.

Cette mesure s'inscrit pleinement dans la vision de la police de proximité, qui est chère au monde anglo-saxon. Il s'agit en premier lieu de créer un lien de confiance entre les policiers de terrain et les différentes communautés ou associations actives dans leur secteur d'engagement. Ce travail de contact et d'information doit faciliter une intervention aussi en amont que possible. La police cantonale zurichoise, qui a mis ce concept en place depuis plusieurs années, a pu en mesurer les effets positifs dans le cadre de la prévention de la radicalisation grâce aux contacts établis avec les représentants

des différentes communautés. Dès lors, l'offre de formation de l'Institut suisse de police (ISP) qui, dans notre pays, est responsable de la formation continue des collaborateurs s'est étoffée d'un cours spécifiquement consacré à ce type d'activité qui a d'ores et déjà été repris par les corps de police de plusieurs cantons.

- B.** Mesure 14 – Mise en place et introduction du concept de la gestion des menaces
- La gestion cantonale des menaces sur le plan institutionnel, le plus souvent placée sous la direction de la police, doit identifier suffisamment tôt le potentiel de danger que peuvent présenter des personnes ou des groupes, l'évaluer et finalement le désamorcer par les moyens appropriés. Toute l'attention doit être portée à ce que la radicalisation et l'extrémisme violent soient intégrés au concept de la gestion des menaces. Pour que la radicalisation et l'extrémisme violent puissent être abordés de façon interdisciplinaire, des partenaires ou des connaissances supplémentaires doivent être intégrés si besoin.

Le concept de gestion des menaces s'est développé en Suisse dans le contexte des violences domestiques et de l'augmentation des personnes querulentes dans les administrations. Il repose à la fois sur l'utilisation de divers outils d'évaluation du risque, mais aussi sur des relais dans divers services de l'administration et autres institutions affiliées. Dans ce contexte également, les processus mis en œuvre dans un autre contexte se révèlent être efficaces dans la lutte contre la radicalisation. Les expériences réalisées dans des régions où le concept était déjà en place prouvent que, dans plusieurs situations, les personnes prises en charge ont pu être stoppées dans leur processus de radicalisation ou une telle éventualité a pu être écartée. Pour cette mesure également, une formation a été proposée par l'Institut suisse de police.

Conclusion

Même si la police n'est pas en charge de la coordination des mesures de prévention de la radicalisation et de l'extrémisme violent, elle n'en demeure pas moins un des piliers. En effet, par ses nombreuses collaborations dans son activité quotidienne, elle est à même d'être confrontée à des remontées d'informations qui lui permettront de prendre les premières mesures. Pour cela, il est primordial qu'elle établisse des relations de confiance avec ses partenaires dans une approche de mise en réseau, et non de répression. Le phénomène de la radicalisation pose de nouveaux défis dans le domaine de la prévention. Il faut donc saisir cette occasion pour développer, par l'entremise des mesures proposées, de nouvelles compétences pour la police, lesquelles peuvent s'inscrire dans un cadre plus global.

*André Duvillard, délégué de la Confédération
et des cantons pour le Réseau national de sécurité, Suisse*

2.2.1.3 Formation en ligne sur les menaces extrémistes et l'extrémisme violent

La Sûreté du Québec, police provinciale au Canada, est vouée au maintien de la paix, de l'ordre et de la sécurité publique, ainsi qu'à la prévention et à la répression du crime. Ses membres assurent la sécurité des personnes et des biens, préservent les droits et les libertés, sont attentifs aux besoins des victimes et collaborent avec la communauté. En tant que police provinciale, la Sûreté du Québec soutient la communauté policière, coordonne des opérations policières d'envergure, contribue à l'intégrité des institutions étatiques et assure la sécurité des réseaux de transport qui relèvent du Québec. De plus, elle gère un service central de renseignements, qu'elle met à la disposition des autres corps de police.

Dans le cadre du plan d'action 2015-2018 du gouvernement du Québec intitulé *La radicalisation au Québec : agir, prévenir, détecter et vivre ensemble*, la Sûreté du Québec, sous l'égide du ministère de la Sécurité publique, a mis en œuvre un programme à l'intention des policiers afin de détecter sur le terrain les signes de radicalisation menant à la violence. En 2016, cette initiative s'est traduite par l'élaboration d'un cours en ligne visant à sensibiliser les premiers intervenants au phénomène de l'extrémisme violent et du terrorisme.

En 2018, le sergent Grégory Gomez del Prado, spécialiste en radicalisation menant à la violence au sein du Service du renseignement et de la protection de l'État, a procédé à une évaluation de ce cours en ligne afin d'identifier des pistes d'amélioration. Tout d'abord, l'évaluation a mis en lumière la nécessité de mettre à jour le contenu du cours en ligne. En effet, même si la formation contenait les tendances générales en matière d'extrémisme violent, le contenu pouvait être bonifié davantage, par exemple en y ajoutant les nouvelles formes de menaces qui pèsent actuellement sur la société québécoise. De plus, le format de présentation sous forme de longs chapitres, était moins convivial et limitait les interactions. Dans un contexte d'évolution des technologies de l'information, un tel format constituait un frein à l'apprentissage, particulièrement chez les jeunes policiers. Troisièmement, il était très difficile de suivre la progression des usagers, puisque le système ne permettait pas de colliger le niveau de progression de l'utilisateur au fil de la formation. Par exemple, nous ne pouvions distinguer les usagers ayant seulement accédé au contenu de la formation de ceux qui l'avaient terminé. L'évaluation de l'acquisition des connaissances présentait donc des difficultés. Face à ces constatations, la Sûreté du Québec a lancé un projet de création d'une plateforme d'apprentissage en ligne.

Ce projet, coordonné par le sergent Gomez del Prado en partenariat avec le Service du développement des compétences de la Sûreté du Québec, avait pour objectif de faire connaître les différentes formes de radicalisation menant à la violence (religieuse, politique, idéologique) et les différentes manifestations de l'extrémisme (terrorisme religieux, extrême droite, extrême gauche, mouvements des citoyens souverains et d'autres formes d'extrémisme). Concrètement, cette formation vise à augmenter les capacités de détection des personnes radicalisées sur le terrain et les capacités de lutte contre ces formes d'extrémisme à l'échelle provinciale.

Cette formation en ligne se déroule en trois temps. Par l'entremise de vidéos créées par les auteurs de tueries s'étant déroulées au Canada, d'extraits d'interrogatoires de suspects ou d'extraits de documentaires, les policiers sont en premier lieu amenés à comprendre la différence entre les trois concepts

de la radicalisation, de l'extrémisme et du terrorisme. Ainsi, la radicalisation se réfère à un processus selon lequel des individus sont initiés à un message et à un ensemble de croyances idéologiques qui les incitent à remplacer leurs croyances modérées et généralement admises par des opinions extrêmes. L'extrémisme se réfère à un groupe ou à un individu qui défend une cause à caractère idéologique ou politique et qui, pour parvenir à ses fins, privilégie de façon générale des moyens illégaux ou la violence. Finalement, le terrorisme, défini dans le *Code criminel*¹ du Canada, est un acte commis « au nom – exclusivement ou non – d'un but, d'un objectif ou d'une cause de nature politique, religieuse ou idéologique » en vue d'intimider la population « quant à sa sécurité, entre autres sur le plan économique, ou de contraindre une personne, un gouvernement ou une organisation nationale ou internationale à accomplir un acte ou à s'en abstenir ». Au cours de cette portion de la formation, le participant est appelé à associer les extraits vidéo avec le concept correspondant. Ensuite, les policiers doivent comprendre le cheminement qui mène à l'extrémisme violent. En utilisant l'échelle de Moghaddam², les policiers sont appelés à replacer les étapes de la radicalisation en ordre. Enfin, les types d'extrémisme présents dans la société canadienne sont abordés individuellement. La formation mise sur une présentation visuelle des symboles, des paroles et des comportements associés au processus de radicalisation menant à la violence. Le policier est ainsi exposé à une grande variété d'images et de propos liés à chaque forme d'extrémisme afin qu'il puisse ultérieurement les reconnaître dans ses interventions quotidiennes.

La construction de cette plateforme d'apprentissage en ligne devrait être complétée au cours de l'année 2019. La première phase de déploiement de la formation visera les milliers de policiers de la Sûreté du Québec travaillant sur la patrouille et dans les bureaux d'enquête. Dans une seconde phase, la formation sera disponible et diffusée auprès de l'ensemble de la communauté policière de la province de Québec. Dans une troisième phase, des ententes avec d'autres services de police au Canada et à l'étranger seront envisagées afin de leur partager cette formation.

1 Code criminel (L.R.C. (1985), ch. C-46)

2 Moghaddam, F. M. (2005). The Staircase to Terrorism: A Psychological Exploration. *American Psychologist*, 60(2), 161-169.

Dans un contexte d'évolution constante des menaces et des méthodes pour commettre des actes de violence au nom d'une idéologie, il est prévu que le contenu de cette formation soit actualisé de manière annuelle. Finalement, une évaluation de la validité et de l'efficacité de cette formation est envisagée dans un souci constant d'amélioration des processus d'apprentissage.

Grégory Gomez del Prado, coordinateur aux enquêtes dans le Service de renseignement et de la protection de l'État, Sûreté du Québec, Canada

2.2.1.4 Problématiques de la radicalisation des jeunes d'Afrique de l'Ouest : quelles pistes de solution?

En traçant son historique, on constate que la radicalisation violente en Afrique de l'Ouest semble revêtir un caractère exogène, si l'on en juge par le fait que cela a commencé dans cette région : Maghreb-Sahel depuis 1991; Algérie, avec la crise du Front islamique du salut (FIS) en 1991; naissance du Groupe islamique armé (GIA) en 1992; scission du GIA et naissance du Groupe salafiste pour la prédication et le combat (GSPC) en 1998; reconversion de GSPC en Al-Qaïda au Maghreb islamique (AQMI) en 2007; naissance, plus de 20 ans après, en 2011, du Mouvement pour l'unicité et le jihad en Afrique de l'Ouest (MUJAO) au Mali. Tout cela annonce l'éclosion des groupes pseudodjihadistes au Sahel, à l'exception du groupe Boko Haram, créé en 2002.

Cependant, le contexte des pays ouest-africains en général, et ceux du G5 Sahel en particulier, n'est pas sans tort et constitue également un terreau fertile propice à la radicalisation pour les raisons suivantes : l'extrême pauvreté (avec 50 % de la population qui vit sous le seuil de la pauvreté, et plus en milieu rural); les plus faibles indices de développement humain (IDH) au monde (0,300-0,400); l'insécurité alimentaire chronique; un taux élevé de malnutrition aiguë (15 % des enfants de moins de cinq ans sont en situation de malnutrition globale); les difficultés d'accès aux services sociaux de base (éducation, santé, eau potable, assainissement); les chocs climatiques (sécheresse, inondations, ensablement et tarissement de cours d'eau, péril acridien et invasion des oiseaux granivores, désertification, etc.); les moyens d'existence (agriculture, élevage, pêche) affectés par les effets néfastes du changement climatique;

l'insécurité foncière et les conflits intercommunautaires; le chômage des jeunes, le manque de formations professionnelles et l'absence de débouchés; l'analphabétisme.

Et, malheureusement, malgré tout, la radicalisation en Afrique de l'Ouest reste un domaine très peu documenté.

En effet, le terrain de recherche est inaccessible, et seules les données qualitatives sont prédominantes. Le phénomène est nouveau et est encore faiblement étudié, et les renseignements généraux ne sont pas toujours accessibles.

La constante est que l'analphabétisme, les rares occasions d'emplois et d'autoemplois, la faible connaissance de la religion, l'endoctrinement religieux, le sentiment d'injustice, la méconnaissance de la loi, les conflits locaux ainsi que le faible sentiment national constituent les principaux facteurs de radicalisation, surtout chez les jeunes.

D'ailleurs, malgré l'inexistence de données statistiques, il est avéré que des actes de violence sont commis, dans la très grande majorité des cas, par des jeunes, et parfois par de très jeunes parmi lesquels un nombre important d'« enfants soldats » et d'adolescents enrôlés.

Cette jeunesse – sans distinction aucune de statut social, de niveau de vie et d'éducation – est à prendre en compte et doit être en première ligne de ce combat en raison de sa créativité, de son énergie, de son endurance et de sa détermination.

Ce rôle des jeunes est aujourd'hui largement reconnu par les institutions internationales et régionales, notamment dans la résolution 2250 des Nations Unies sur la jeunesse, la paix et la sécurité ainsi que dans la déclaration de Niamey de mai 2015 sur la radicalisation et l'extrémisme violent des ministres responsables des Affaires religieuses du G5 Sahel.

Ainsi, pour ce faire, il faudra agir sur trois leviers, à savoir : 1) les compétences; 2) la motivation; 3) l'environnement sur les plans institutionnel, socioéconomique et culturel.

1. Renforcer les compétences des jeunes

Comme préalable, prendre en charge les jeunes :

- › du système éducatif formel;
- › du système éducatif traditionnel;
- › et ceux des déperditions de ces deux systèmes éducatifs.

Les systèmes éducatifs doivent être réformés avec, pour objectifs, de :

- Développer la culture de l'excellence, de la compétence, de l'expertise et de l'innovation dans les formations;
- Promouvoir une école qui produit des jeunes qui sont des modèles « licites » de réussite pour les moins jeunes;
- Moderniser les écoles coraniques et de créer des passerelles avec le système formel;
- Promouvoir une éducation adaptée pour les communautés nomades en lien avec la préservation de leur mode de vie;
- Développer des « écoles de la seconde chance »;
- Développer des activités extrascolaires et de loisirs (vacances citoyennes, travaux d'intérêt commun, etc.) comme outils de renforcement de la cohésion nationale.

2. Motiver les jeunes dans leur engagement dans la lutte contre la radicalisation

- Partir de situations que vivent les jeunes et renforcer progressivement leurs capacités et leurs connaissances de leur réalité, et les outiller pour la gérer;
- Utiliser une approche participative et démocratique de manière à détecter les questions qui leur semblent importantes et les aider à trouver des solutions;
- Créer les conditions de leur engagement en faveur de la sécurité sur la **base d'un partenariat avec les forces de l'ordre fondé sur une prise de conscience de l'intérêt à collaborer** (prendre en compte les griefs de leur communauté);
- Identifier des interlocuteurs crédibles et établir des procédures et des méthodes d'action largement inclusives (p. ex. : impliquer la jeunesse féminine) pouvant créer la confiance;
- Soutenir les jeunes dans leurs actions (p. ex. : sensibilisation, information);
- Faire des désengagés et des victimes des acteurs actifs de la lutte contre l'extrémisme violent;
- Promouvoir des outils de suivi d'évaluation permettant de mesurer, avec les jeunes, les progrès accomplis.

3. Promouvoir l'environnement

Sur le plan institutionnel

- Revoir, là où c'est nécessaire, toutes les dispositions qui limitent la participation des jeunes dans l'élaboration des politiques publiques;
- S'assurer que le cadre légal garantit aux jeunes la jouissance pleine et entière de leurs droits fondamentaux, notamment leur liberté de s'organiser, de s'exprimer et d'entreprendre des projets;
- Créer des mécanismes de mise à disposition de ressources publiques auprès des communes pouvant permettre aux jeunes de développer des stratégies locales de lutte contre l'extrémisme violent;
- Promouvoir un service civique national (lutte contre l'analphabétisme, protection de l'environnement, renforcement de la culture citoyenne et de la démocratie).

Sur le plan socioéconomique

- Créer des possibilités d'emplois, de formations, d'accompagnement professionnel et de stages pour les jeunes en tenant compte d'une péréquation géographique;
- Lutter fermement contre la corruption, en particulier contre les taxes « PDG » (police, douane et gendarmerie);
- Développer des mécanismes transparents d'accès à l'emploi et des systèmes de recours crédibles et convaincants.

Sur le plan socioculturel et sportif

- Développer des mécanismes de subvention (utilité publique) pour les organisations de jeunes tels que les mouvements Scouts, Pionniers, Éclaireurs, etc.;
- Créer des complexes polyvalents culturo-culturels (lieux de prière, auditoriums, bibliothèques, salles multimédias, cours de musique, salles de sport, etc.);

- Mettre en place des infrastructures sportives et culturelles dotées d'équipements et d'équipes d'animateurs de qualité;
- Concevoir des activités de compétitions sportives et culturelles entre jeunes au niveau local, sous-régional et national.

Conclusion

La lutte contre l'extrémisme violent n'est pas du tout facile. Il s'agit d'une action coordonnée entre les trois leviers évoqués ci-dessus et, pour en garantir le succès, nous avons besoin :

1. De renforcer la gouvernance démocratique et économique de nos États;
2. De mobiliser des ressources auprès des partenaires qui seront orientées vers des priorités nationales.

C'est à ces conditions que nous pourrons espérer avoir une jeunesse – rempart contre l'extrémisme violent – dotée **d'un esprit sain** dans **un corps sain**, et évoluant dans **un environnement propice**.

Amadou Sall, enseignant, chercheur à l'Université de Nouakchott, chef de la Cellule régionale de prévention de la radicalisation et de l'extrémisme violent au Sahel, Mauritanie

2.2.1.5 Lutte contre la radicalisation

La structure

L'École nationale supérieure de la police (ENSP) est un établissement public placé sous la tutelle du ministère de l'Intérieur et dirigé par un inspecteur général de la Police nationale.

Son siège est à Saint-Cyr-au-Mont-d'Or, près de Lyon, et elle dispose, depuis 2013, d'un second établissement à Cannes-Écluse, en région parisienne, où sont formés les officiers.

La première mission de l'ENSP est de concevoir, d'offrir et de promouvoir des formations initiales et continues pour les commissaires et les officiers de police.

Actuellement, ce sont environ 70 commissaires et autant d'officiers qui suivent la scolarité en formation initiale.

Près de 2 400 cadres de police sont par ailleurs accueillis chaque année en formation continue.

Dans le cadre de son activité partenariale, au titre du continuum de sécurité (complémentarité public-privé en matière de sécurité), l'École forme également des élus locaux, des hauts fonctionnaires et des cadres des collectivités et des entreprises dans le domaine de la sécurité intérieure.

Sur le plan international, l'ENSP est membre de l'Association des collèges européens de police (AEPC), et elle participe à la formation des cadres supérieurs des polices étrangères grâce à ses partenariats avec des agences européennes (CEPOL, FRONTEX) ou INTERPOL.

Formations « lutte contre la radicalisation »

Pour faire face au phénomène de la radicalisation, l'ENSP a mis en place des formations destinées aux cadres de la police et aux partenaires extérieurs.

Les stages

En formation initiale, le sujet de la radicalisation est largement abordé de manière perlée tout au long des 22 mois de formation des commissaires de police. Toutefois, deux journées sont exclusivement consacrées à « **la lutte contre les extrémismes violents** ». La question de la lutte contre la radicalisation

occupe la majeure partie de ces deux journées. Elle est abordée selon le programme suivant :

- Le contexte géopolitique (Direction générale de la sécurité intérieure [DGSI]);
- L'islam radical en France (universitaire);
- Les processus de radicalisation et le plan d'action contre la radicalisation et le terrorisme (l'UCLAT);
- L'action de l'État dans la prévention et la lutte contre la radicalisation au niveau déconcentré (préfecture du Rhône);
- L'activité des services de renseignement, la détection des signaux faibles dans l'exercice des missions quotidiennes de police et la transmission aux services de renseignement (Service central du renseignement territorial [SCRT]/DGSI).

En formation continue

Depuis 2016, l'ENSP propose, sur les questions liées à la radicalisation, **trois stages** respectant une logique de cohérence et de progression pédagogiques. Ils sont susceptibles de s'adresser à des publics spécialistes ou non de la question. Ces stages de formation continue ont une durée comprise entre trois et quatre jours, et sont ouverts aux commissaires de police, aux officiers de police, aux chefs d'unité ainsi qu'aux officiers supérieurs de la gendarmerie. Ils sont aussi susceptibles d'accueillir d'autres publics issus du ministère de l'Intérieur ou d'administrations partenaires. Chacun d'entre eux accueille près de 40 stagiaires.

Le premier stage, s'il n'est pas spécifiquement consacré au phénomène de radicalisation, constitue une introduction aux stages suivants. Il est consacré à la « **connaissance des fondamentaux de l'Islam** ». Il est organisé en partenariat avec l'Institut d'études de l'Islam et des sociétés du monde musulman. Il vise à présenter les fondements théologiques, historiques, sociologiques et politiques de l'Islam en France. Sont abordés les sujets suivants :

- Concepts clés de l'Islam;
- Le droit musulman;
- Les musulmans dans l'espace social et politique français;
- L'organisation et l'exercice du culte musulman en France;

- Islam et laïcité;
- L'Islam militant;
- De l'Islam politique au terrorisme islamiste : des fondamentaux aux enjeux contemporains.

Ce stage s'est tenu du 10 au 13 septembre 2018.

À l'issue de ce stage sont proposés deux modules consacrés à la lutte contre la radicalisation. Le premier, intitulé **Détection et lutte contre la radicalisation, module I**, est un stage destiné aux fonctionnaires et aux militaires non spécialistes de ces questions. Il aborde les thèmes suivants :

- La place de la France dans l'histoire et la géopolitique du djihad;
- Le salafisme;
- Les processus de radicalisation et les indicateurs de basculement;
- Les plans nationaux de prévention et de lutte contre la radicalisation;
- L'action de l'État dans la prévention et la lutte contre la radicalisation au niveau départemental;
- Le rôle de la justice en matière de prévention et de lutte contre la radicalisation;
- L'action des services de renseignement, la détection et la prise en compte.

Ce stage s'est tenu du 4 au 6 décembre 2018.

Le deuxième module, intitulé **Détection et lutte contre la radicalisation, module II**, est un stage d'approfondissement et d'ouverture plus particulièrement destiné aux stagiaires ayant participé au module I ou à des stagiaires connaissant déjà ces questions, notamment parce qu'ils sont issus des services de renseignement. Sont abordés les thèmes suivants :

- Point actualisé sur l'état de la menace et la situation au Proche-Orient;
- La prévention et la lutte contre la radicalisation : devoir d'information et secret professionnel;
- Le financement des réseaux djihadistes;
- La propagande terroriste sur Internet;
- La place des femmes dans le djihad;
- Les politiques de lutte contre la radicalisation dans les pays de l'Union européenne;

- Les expériences de « déradicalisation ».

Ce stage se tiendra en juin 2019.

En plus de faire appel à des universitaires et à des chercheurs, ces formations sollicitent aussi de nombreuses institutions engagées dans la prévention et la lutte contre la radicalisation : services opérationnels de police, Comité interministériel de prévention de la délinquance et de la radicalisation (CIPDR), Parquet, administration pénitentiaire, cabinet du préfet délégué à la défense et à la sécurité du Rhône, Traitement du renseignement et action contre les circuits financiers clandestins (TRACFIN), Mission interministérielle de vigilance et de lutte contre les dérives sectaires (MIVILUDES).

L'objectif de ces stages est avant tout de permettre aux cadres des services de sécurité intérieure de bénéficier d'analyses et d'éclairages pour affiner, approfondir et enrichir leurs connaissances de ces phénomènes. Ils ont aussi la vocation d'offrir à ces praticiens un temps de réflexion et d'échange nécessaire à la prise de recul sur la situation afin de développer une vision plus globale et mieux informée.

À l'évidence, ils répondent à un besoin véritable des stagiaires, quelles que soient leur direction d'appartenance et leur spécialité.

Constamment actualisés, ces stages proposent des contenus et des formules qui restent en lien étroit avec l'évolution du phénomène de radicalisation et des dispositifs mis en place par les pouvoirs publics.

En septembre 2018, l'ENSP a enrichi son offre de stages en proposant une formation intitulée **La laïcité en action, liberté religieuse et neutralité du service public**. Cette formation est animée par des enseignants de l'Université Lyon III, en charge du diplôme universitaire nommé Religion, liberté religieuse et laïcité. Seront traités les thèmes suivants :

- Les enjeux de la laïcité aujourd'hui;
- La formation du principe de laïcité en France;
- L'application du principe de neutralité dans les services publics;
- La liberté de religion, un principe pour quelles limites?;
- Prendre en compte le fait religieux dans la sphère publique.

Ces différents stages, organisés par l'ENSP avec le concours de spécialistes, permettent de sensibiliser un public de cadres de la police et de la gendarmerie concernés par la lutte contre le phénomène de la radicalisation.

Par ailleurs, conformément aux instructions du ministre de l'Intérieur en date du 17 mai 2016, l'ENSP propose chaque année à ses propres agents une formation de deux heures sur la détection de la radicalisation reposant en partie sur les modules de cyberformation.

Sont ainsi présentés le phénomène de la radicalisation, les indicateurs de basculement, le dispositif mis en place par les pouvoirs publics ainsi que l'état de la menace en France.

L'ENSP dispose également de modules destinés à des partenaires extérieurs (élu, responsables de la sécurité des entreprises).

Ces modules, d'une durée d'un ou deux jours pour un auditoire de 10 à 15 personnes, s'intitulent respectivement Le fait religieux en entreprise, L'enquêteur face aux situations complexes induites par la diversité ou Lutte contre la radicalisation en fonction des publics auxquels ils s'adressent.

Pascal Bastide, commissaire divisionnaire, chef du Département des formations préparatoires, partenariales et internationales, École nationale supérieure de police, France

2.2.1.6 Gestion des menaces et prévention de la violence (MPV)

Contexte

Entre les personnes menaçant des figures publiques, les violences interpersonnelles et conjugales graves et répétées, la montée de l'extrémisme, les personnes adoptant des comportements de harcèlement obsessionnel (stalking), les jeunes laissant entendre leur intention de s'en prendre à leur établissement scolaire et les autres personnes troubles débarquant en colère dans l'un ou l'autre des services de l'État (contributions, services sociaux, tribunaux, etc.), la police a régulièrement affaire à des personnes potentiellement dangereuses et troubles mentalement.

La prévention de tout passage à l'acte n'est pas possible, mais on peut atténuer les risques. En effet, les actes ciblés de

violence, comme le drame au parlement de Zoug³, étaient précédés d'indices qui auraient pu être décelés.

À la suite de l'enquête effectuée en 2014, la Prévention suisse de la criminalité (PSC, 2015) a relevé l'importance, pour les cantons, d'avoir une structure en place qui est à même de reconnaître ces signes précurseurs, d'évaluer le potentiel de risque et de travailler à désamorcer la menace.

Un service de gestion des menaces est également un centre de compétence pouvant offrir de la formation et un soutien aux employés des services de l'État devant, par leur fonction, rendre des décisions qui ne sont pas toujours bien acceptées par les citoyens⁴.

Un tel service permet d'aider à la prise de décision pour des interventions de police, répond à un besoin d'autres services de l'État et représente potentiellement un gain de temps et de moyens considérables sur le plan pénal⁵. Ces missions sont donc, avant tout, proactives et préventives.

ÉVOLUTION D'UNE SITUATION DANGEREUSE DÉLIT		
Domaine d'activité traditionnel de la police	Nouveau domaine de la police	Domaine d'activité traditionnel de la police
Information, sensibilisation	« Travail de police proactif »	Enquête préalable, enquête/instruction pénale
Campagnes/travail de communication	Intervenir... avant le passage à l'acte	Mesures prises dans le cadre de la procédure pénale
Avertissement sur les risques et dangers		
PRÉVENTION PRIMAIRE	PRÉVENTION SECONDAIRE	PRÉVENTION TERTIAIRE

3 Forcené qui a tué 14 élus, dont trois conseillers d'État, et blessé 15 autres personnes en 2001, au parlement du canton de Zoug, en Suisse.
 4 Une enquête a été menée en 2010 par l'Institut für Psychologie und Bedrohungsmanagement (IPBm) dans le canton de Soleure auprès de 18 différents services d'État et communes. Sur les 249 employés, 93 % ont eu affaire à des citoyens en colère, 61 % à des personnes querulentes, 60 % ont reçu des menaces, 53 % ont été témoins de menaces de suicide, 33 % ont été agressés physiquement et 23 % ont eu affaire à des citoyens qui ont exhibé une arme. Source : Manuela Müller, Kantonales Bedrohungsmanagement, Polizei Kanton Solothurn.
 5 Un nombre important de comportements querulents sont dans une « zone grise », à la limite du pénal, et un entretien d'évaluation ou une confrontation peut parfois représenter une solution de rechange intéressante avant de lancer une procédure pénale.

Le groupe MPV

À l'instar d'une quinzaine d'autres polices cantonales suisses, la police neuchâteloise a mis en place un service de gestion des menaces, le groupe MPV, qui effectue ce travail de police proactif avec les missions suivantes :

1. Développer les moyens de la police pour repérer les signes précurseurs d'un passage à l'acte;
2. Évaluer le risque et l'imminence d'un possible passage à l'acte en s'entretenant notamment avec l'auteur et en utilisant des instruments d'évaluation conçus à cette fin;
3. Désamorcer le risque d'escalade de la violence, notamment en s'entretenant avec les personnes concernées – auteur et victime – ou en mettant en place des rencontres avec le réseau (Autorité de protection de l'enfant et de l'adulte, ministère public, hôpital psychiatrique, etc.) pour trouver des solutions à moyen et à long terme en intégrant les dimensions préventives pénales et non pénales;
4. Assurer un suivi des personnes à risque en centralisant les informations les concernant.

La taille de notre corps de police⁶, l'irrégularité des situations nécessitant une prise en charge et les moyens à notre disposition nous ont amenés à favoriser l'option d'une structure souple qui pourra être renforcée, au besoin. Sous la responsabilité du chef du Service psychologique de la Police neuchâteloise, le groupe est constitué de six policiers spécialisés dans le domaine des menaces. Particulièrement compétents sur le plan de la communication interpersonnelle, les intervenants MPV ont tous fait un stage de trois semaines en psychiatrie, suivent une formation continue et bénéficient d'une supervision dans le domaine de l'évaluation et de la gestion de menaces (environ dix fois une demi-journée par année). Les intervenants travaillent à temps partiel aux missions MPV. En ce qui concerne l'investissement en temps, la prise en charge du groupe MPV totalise actuellement deux postes à 100 % sur l'année.

Pour appuyer le groupe MPV, des gendarmes sont recrutés

dans les différents postes de police de proximité et formés à la fonction « d'antenne MPV ». Sensibilisés à la thématique, ces derniers prennent en charge les situations liées à des menaces, font une première appréciation et, le cas échéant, la transmettent au groupe MPV.

Les entretiens MPV

Les entretiens MPV, qu'ils soient le fruit d'une approche proactive ou la conséquence d'un fait problématique, ne sont pas des auditions pénales. Même si la participation d'un membre de l'équipe MPV peut être requise dans le cadre de l'audition d'une victime, d'un témoin ou d'un auteur, plus largement pour un regard croisé dans le cadre d'une procédure pénale officielle, l'entretien MPV s'inscrit dans un cadre, mais avant tout une logique quelque peu différente. Là où l'inspecteur de police cherche à établir des faits constitutifs et à contextualiser ces derniers, l'intervenant MPV vise à comprendre la réalité des personnes rencontrées. Dans le cadre des entretiens MPV, il s'agit avant tout de parvenir à créer un lien suffisant avec la personne, ceci afin d'être en mesure d'atteindre les objectifs ci-dessous.

Objectifs des entretiens MPV avec la personne ciblée par les menaces :

- Récolter des informations contribuant à une évaluation initiale;
- Apporter un soutien au travers de propositions de stratégies pour la sécurité des potentielles victimes;
- Lorsque la personne ciblée est la source d'information, garder une position de « sain scepticisme » et évaluer les enjeux ainsi que les motivations sous-jacentes (conscientes ou non) à ses propos;
- Créer un lien de confiance suffisant pour que la personne ciblée puisse continuer dans le futur à nous faire parvenir de l'information sur l'auteur.

Objectifs des entretiens MPV avec l'auteur de menaces ou de comportements inappropriés générant la peur d'un passage à l'acte de violence :

- Récolter les informations nécessaires à une appréciation du risque de passage à l'acte;

⁶ 400 policiers pour 178 000 habitants.

- Exercer une influence sur la personne en cherchant à réduire le danger potentiel qu'elle représente;
- Réunir de l'information sur les possibilités d'aider la personne afin de réduire le risque de violence;
- Informer l'auteur des conséquences de ses comportements et poser des limites;
- Créer un lien de confiance suffisant pour, le cas échéant, faciliter le suivi [monitoring] par la suite.

L'évaluation de risque de passage à l'acte

Traditionnellement, lorsqu'un policier évalue le risque de récidive ou de passage à l'acte d'un citoyen (p. ex. : lorsqu'il est amené à devoir conseiller une victime de harcèlement obsessionnel [stalking]), il va fonder son jugement sur son expérience et sa capacité de discernement. Même si l'intuition est certainement importante pour évaluer si une situation est sérieuse ou non, l'évaluateur est toujours biaisé par ses a priori et aura tendance à percevoir la situation de manière à confirmer ses croyances. Pour éviter ces biais et augmenter la fiabilité de l'évaluation du risque, différentes polices, notamment dans les pays anglo-saxons et en Allemagne, utilisent des instruments plus ou moins complexes, informatisés ou non, certains indiquant le degré de risque par un chiffre ou une couleur, d'autres déterminant des stratégies de gestion de risque en fonction des données enregistrées.

Un exemple d'instrument d'évaluation approfondie est l'Octogone développé par Jérôme Endrass en 2016. Utilisé par plusieurs corps de police suisse, l'Octogone permet un langage commun lors des discussions entre les différents services de gestion des menaces.

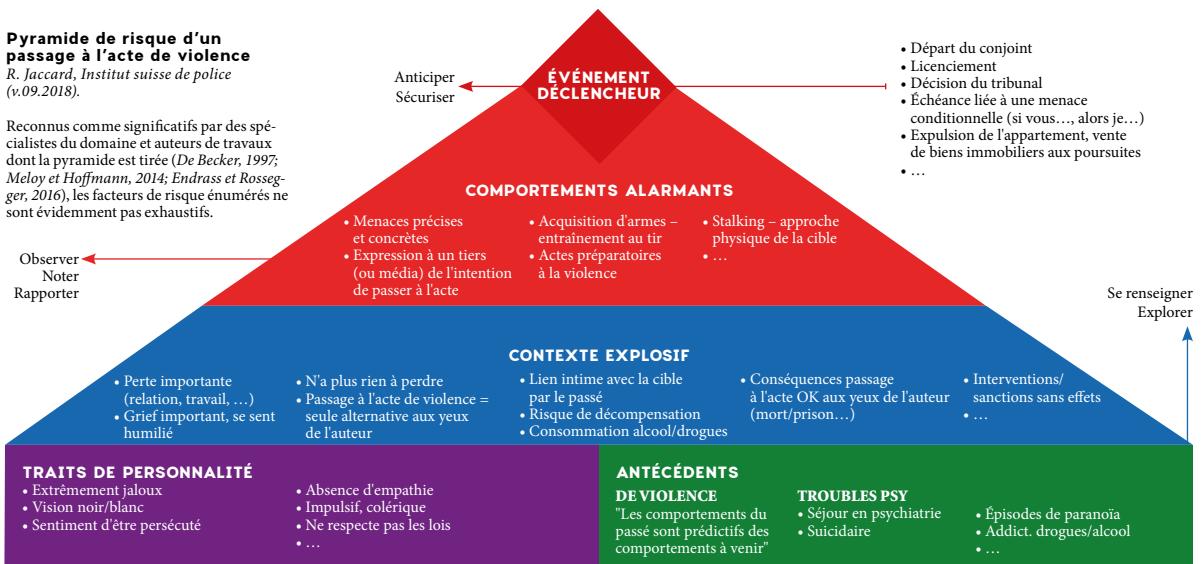
Pour une première appréciation d'une menace, il existe les instruments dits de screening. À titre d'exemple, nous présentons ci-dessous la Pyramide de risque d'un passage à l'acte de violence. Que cela se fasse par téléphone ou lors d'un entretien avec l'auteur ou la cible de menaces, cet instrument permet de poser les bonnes questions et assure une collecte d'informations ciblées sur la présence ou l'absence de facteurs de risque pertinents. Il permet de structurer l'information sur la personnalité de l'auteur des menaces, ses antécédents, le contexte actuel, les comportements observables et les événements qui pourraient déclencher le passage à l'acte.

Il ne s'agit pas d'une simple liste de vérification (check list) dans laquelle le décompte d'un certain nombre de facteurs indiquerait automatiquement que la personne est dangereuse, mais bien d'une aide pour collecter l'information, prendre la distance nécessaire pour une analyse globale de la situation et, en cas de besoin, transmettre la bonne impulsion au service approprié. L'utilisation d'un tel instrument de screening s'inscrit en complément à l'expérience, à l'intuition et au bon sens de l'intervenant.

Pyramide de risque d'un passage à l'acte de violence

R. Jaccard, Institut suisse de police (v.09.2018).

Reconnus comme significatifs par des spécialistes du domaine et auteurs de travaux dont la pyramide est tirée (De Becker, 1997; Meloy et Hoffmann, 2014; Endrass et Rossegger, 2016), les facteurs de risque énumérés ne sont évidemment pas exhaustifs.



Développement

Au niveau cantonal, l'efficacité d'une gestion des menaces repose sur la détection précoce et le travail en réseau. La vision à moyen terme est de former des personnes de contact dans les différents services de l'État, notamment ceux qui ont régulièrement affaire à des citoyens mécontents (p. ex. : les services des contributions, de l'emploi, des poursuites et des faillites, de protection de l'adulte et de la jeunesse, de la consommation et des affaires vétérinaires, des automobiles, etc.). Ces collaborateurs seront formés pour effectuer une première appréciation d'une situation de menace et pour conseiller leurs collègues ou les responsables du service. Ces personnes de contact transmettront ensuite à MPV les situations évaluées comme comportant un risque important et collaboreront étroitement à la gestion de la crise.

Au niveau suisse, l'existence, depuis 2017, d'une formation en gestion des menaces organisée par l'Institut suisse de police (ISP) permet de former des policiers de tous corps de police souhaitant mettre en place et développer un tel service. Cette formation favorise un langage et des instruments communs (p. ex. : l'Octogone) aux intervenants policiers des différents corps de police. D'autre part, dès 2019-2020, quelques bases sur l'évaluation d'une menace (notamment l'utilisation de la Pyramide de risque) seront enseignées dans les différentes écoles d'aspirants de police.

Au niveau européen, l'*Association of European Threat Assessment Professionals (AETAP)* organise chaque année un congrès permettant des discussions entre les professionnels du domaine (policiers, chercheurs universitaires, responsables de la sécurité de multinationales, etc.).

*Raoul Jaccard, chef du Service psychologique
de la Police neuchâteloise, responsable du groupe MPV, Suisse*

Références

De Becker, G. (1997). *The Gift of Fear and other survival signals that protect us from violence*. New York: Dell Publishing

Endrass, J. & Rossegger A. (2018). *Octagon*. Version 1/1.6.2018. Universität Konstanz

Meloy, J. R. & Hoffmann, J. eds. (2014). *International Handbook of Threat Assessment*. New York: Oxford University Press.

Prévention suisse de la criminalité (PSC) (2015). *Gestion des menaces au niveau cantonal : analyse de la situation. Évaluation de l'enquête menée auprès des cantons et premières conclusions. Rapport interne*. Berne, Suisse : PSC.

2.2.2 ÉCHANGES

Juste après l'ouverture du congrès, les débats se sont déroulés autour de la thématique de la lutte contre le terrorisme. Cette dernière a été présentée par plusieurs panels composés d'experts africains et européens. Pour modérer cette première table ronde, M^{me} Lori-Anne Théroux-Bénoni, directrice de l'Institut d'études de sécurité, à Dakar, modératrice de la plénière, a synthétisé les exposés des différents panélistes ainsi que les échanges et le partage d'expérience en deux points.

D'abord, M^{me} Théroux-Bénoni a évoqué la difficulté liée à cet enjeu de discuter dans un esprit de partage afin de se transmettre les bonnes pratiques, car les réalités sont différentes d'un endroit à l'autre. Elle a pris l'exemple, en 2016, des entretiens réalisés avec des jeunes au cours de leurs recherches, qui montrent que la radicalisation ne s'inscrit pas toujours, comme on pourrait le croire, dans une logique d'engagement religieux. La radicalisation peut s'inscrire aussi dans un cadre de protection de sa famille face à certaines menaces.

Les recherches effectuées par le Centre de recherche de la modératrice ont révélé qu'à l'intérieur même du Mali, les logiques de radicalisation étaient différentes selon les régions, que l'on soit au nord ou au sud du Mali. Cela montre la complexité du fait qu'à l'intérieur d'un État, les processus de radicalisation ne sont pas les mêmes.

La difficulté tient aussi au fait que dans le cadre d'un État à un autre, par exemple du Sénégal en France ou en Suisse, les logiques de radicalisation peuvent être, là encore, plus différentes. Là se situent donc la difficulté et le défi de pouvoir partager des pratiques sur des territoires différents. Aussi, dans ce cadre jonché de différences, les groupes qui prônent la radicalisation exploitent les failles liées aux réalités propres à chaque territoire dans le but de profiter de ces éléments de différence leur servant à radicaliser davantage de personnes.

Le deuxième point abordé par la modératrice est celui soulevé par un intervenant suisse, qui est finalement une bonne compréhension du phénomène. Cependant, la quantité de données rend le travail compliqué, d'où l'importance de bien comprendre l'imbrication du phénomène entier.

Toutefois, autour de cette question de la compréhension du phénomène gravitent aussi d'autres questions, notamment celle de la place des femmes ainsi que celle de l'existence de politiques publiques qui traiteraient de la problématique.

Tous ces questionnements sont des éléments à prendre en compte pour limiter l'engagement, d'une part, et, d'autre part, pour éviter le réengagement.

Le professeur Mvomo Ella du Cameroun est le premier intervenant à réagir : d'abord, il fait une première intervention par l'entremise d'une observation générale. En effet, le professeur est rassuré de voir que les travaux élaborés dans le cadre de ses recherches concordent avec ceux évoqués au cours des différentes présentations.

Premièrement, il souligne la complexité de la problématique du terrorisme et de la radicalisation, et l'impératif de la mise en place d'une orientation stratégique globale multisectorielle. Cette observation est concordante, selon le professeur, avec la logique des « trois C » (coordination, complémentarité et cohérence). Ainsi, il fait observer qu'en Afrique centrale, la base de ces travaux est lancée en 2011 par la République centrafricaine avec l'Armée de résistance du Seigneur (LRA pour Lord's Resistance Army). Le terrorisme dont il est question dans la LRA est un terrorisme orphelin, qui occupe un pan du territoire central. Cette réflexion a abouti à la conclusion de la prévention, de la poursuite, puis de la réponse au terrorisme.

S'il est notable de parler du terrorisme dans sa phénoménologie, il est bien de tenir compte du facteur de l'espace-temps en vue de la mondialisation du phénomène. D'un point de vue anthropologique, il y a de vieilles pratiques de violence nommées « prototerrorisme » qui, par exemple, s'assimilent à l'action des coupeurs de route ou à l'action des prises d'otages qui conduisent à plusieurs conséquences. Il faut tenir compte de ce genre de pratiques dans la compréhension du phénomène.

Un deuxième intervenant souhaite partager la compréhension du phénomène en Côte d'Ivoire en posant cette question : « Selon vous, peut-on me radicaliser? » L'intervenant répond lui-même ceci : « Non, car je suis sur des valeurs m'interdisant

de monnayer la vie humaine. » L'analyse qu'il en fait consiste en ce que les terroristes ont besoin de radicaliser les individus pour commettre les actes. Il s'agirait donc de déterminer la cause, puis les facteurs (et ne pas confondre la cause avec les facteurs).

En effet, la cause peut être due au relâchement moral des parents. Dans ce cas, il faut mettre les parents devant leur responsabilité. Ensuite, il faut demander aux autorités d'avoir un langage de vérité et faire en sorte que l'école, qui est un outil important, ne soit pas qu'un lieu d'inscription, mais une veille de conscience pour les jeunes.

L'inspecteur de brigade au Bénin prend la parole en invitant l'assemblée à répondre à deux questions :

- « À quoi les politiques de sécurité en matière de terrorisme contribuent-elles? »
- « N'avons-nous pas l'impression que tout le monde se renvoie la patate chaude, pour utiliser l'expression canadienne, pour ne pas voir le terrorisme à nos portes? »

Quel que soit le taux du terrorisme, il faut en prendre conscience et mettre en place des structures pour percer sa complexité, en tenant compte des contraintes territoriales de chaque zone.

Jacques Antenen pose une question qu'il dit provocatrice au professeur Sall en parlant du manque de perspective des jeunes évoqué dans la présentation du professeur, en essayant de savoir si la politique qui consiste à limiter l'immigration et à fermer les frontières en Europe peut être une perte de semence pour les jeunes d'aujourd'hui, en ce sens qu'elle serait l'une des raisons qui nourrirait ce manque de perspective des jeunes et qui les inciteraient à se radicaliser?

Un intervenant dans l'assemblée fait aussi le constat que, dans son pays, depuis quelques mois, il y a eu l'adoption d'un collectif de lutte contre l'extrémisme violent avec plusieurs piliers concentrés autour de différents axes et plans d'action, dont notamment un pilier essentiel : le dialogue. Les dispositions législatives comme administratives, sont en cours de développement.

Un participant tchadien intervient à son tour en soulignant quelques faits, notamment au sujet de l'intervention du Tchad au Mali et dans le bassin du lac Tchad avec le phénomène Boko Haram.

Dans le cadre de cette opération d'intervention, le Tchad est engagé aux côtés des autres pays de la région depuis le cas de l'attaque en 2015 de Boko Haram à N'Djamena. Les dispositifs sécuritaires ont été réadaptés avec le concours des autorités administratives, les autorités traditionnelles et la société civile. Il faut également ajouter à cette participation le soutien des partenaires, qui a donné lieu à la mise en place d'une composante militaire et policière qui vient d'être créée au Tchad et nommée Unité spécialiste de la composante police. La réponse étatique est suivie par les dispositifs militaires de pointe, puis par la police et la gendarmerie.

Cependant, l'accompagnement que FRANCOPOL peut apporter à tous ces dispositifs mis en place est non négligeable, car, dans la région du lac Tchad, une école de formation continue des forces de sécurité intérieure a été créée. Les services qui y travaillent peuvent se faire aider par FRANCOPOL. L'aide de FRANCOPOL peut se situer dans la création des unités spécialisées, mais aussi dans la formation offerte.

Parmi ses interventions, FRANCOPOL, à l'occasion d'une réunion au Burkina Faso en 2009, a décidé de mettre en place des modules de formation enseignés dans les différentes écoles. Ces modules sont malheureusement sans suite, neuf ans après. Voilà quelques préoccupations soulevées par ce dernier intervenant.

Les panélistes répondent après les interventions par ordre de passage

M^{me} Cécile Oyono, intervenante camerounaise, note que dans son pays, les réponses initiales ont été construites dans l'urgence, du fait de la nouveauté du phénomène. Quelques dispositifs des forces de sécurité ont été mobilisés rapidement, ajoutés à la mobilisation des forces pénitentiaires. C'est autour de ces deux dispositifs qu'une réponse rapide a été apportée dans un premier temps. Concernant l'engagement des femmes, il s'agit d'un engagement spécifique du fait de leur vulnérabilité; de ce fait, il est essentiel d'accompagner les femmes.

Toutefois, la question centrale est celle de la réinsertion de ces femmes engagées. Y a-t-il une réelle volonté de les réinsérer?

Selon le deuxième panéliste, M. André Duillard, les conditions sont très différentes d'un pays à un autre. La Suisse a mis en place un service de renseignement pour contrer le terrorisme afin de faire remonter l'information. Cependant, il ne faut pas perdre de vue que c'est finalement le sentiment d'exclusion qui crée cette situation.

Selon le panéliste Grégory Gomez del Prado, plusieurs études menées en Afrique ont relevé l'absence de corrélation entre la religion et les processus de radicalisation. On parle plutôt d'engagement de personnes qui passent d'une forme d'extrémisme à une autre.

Concernant le traitement de cette problématique, l'approche est la même dans tous les États et dans la plupart des interventions. On met l'accent sur l'importance du cheminement du renseignement, car il faut faire remonter l'information. Il faut également se focaliser sur la spécialisation des intervenants centraux, car ils sont les premiers intervenants lorsqu'il y a un signalement. C'est également à eux que revient le cheminement de l'information vers les services spécialisés. On parle aussi beaucoup d'éducation comme levier pour combattre la radicalisation et l'extrémisme, l'éducation étant également utile pour contrer la radicalisation des jeunes.

Un quatrième intervenant, M. Amadou Sall, note les efforts fournis dans la gouvernance démocratique et la gouvernance économique. Selon lui, le volet prévention est aussi important à développer. À propos de la fermeture des frontières comme une cause supplémentaire de la radicalisation, nous pouvons déjà constater que toute radicalisation part de griefs liés à une exclusion, pas seulement celle liée à la politique migratoire de l'Europe. Il faut aussi noter le phénomène de l'engagement et le phénomène de recrutement dans lequel les recruteurs savent où il faut agir. Par exemple, le discours de la lutte contre la corruption dans certains pays de l'Arabie peut très bien opérer et convaincre les jeunes pourtant issus d'un tissu social favorable.

Le panéliste suivant, M. Pascal Bastide, propose de se focaliser sur les formations : d'abord, une meilleure formation du

cadre de police, puis une ouverture au secteur privé et aux élus pour mettre en place un espace de réseaux de détection.

M. Raoul Jaccard, quant à lui, insiste sur les systèmes d'évaluation des menaces en revenant sur les éléments qui fondent l'évaluation des menaces, d'une part, et en amenant les arguments recevables pour le ministère public afin de faciliter l'appréhension de la problématique par le ministère public et les autres acteurs, d'autre part.

Une septième congressiste de nationalité camerounaise conclut la séance en revenant sur la présentation du service EIFORCES. Ce service organise régulièrement des colloques sur l'extrémisme violent et la radicalisation. À cet effet, le dernier colloque a eu lieu il y a environ deux semaines à Maroua, l'une des zones touchées par le terrorisme, avec la participation d'experts du bassin du lac Tchad. Elle invite l'assemblée à discuter davantage des problématiques évoquées lors de ce colloque.

2.3 GESTION D'INCIDENTS LIÉS AU TERRORISME

2.3.1 PRATIQUES INSPIRANTES

2.3.1.1 Exercice de simultanéité d'attentats terroristes en mai et en octobre 2018 au Burkina Faso, en Côte d'Ivoire, en Guinée-Conakry, au Mali, en Mauritanie, au Niger et au Sénégal

Parmi les menaces qui affectent la sécurité de nos États en Afrique, en Europe ou ailleurs dans le monde, la drogue, qui peut détruire notre jeunesse et déstabiliser certains pays, et le terrorisme occupent les premiers rangs. L'actualité quotidienne le rappelle cruellement. Un État, si puissant soit-il, ne peut lutter durablement et efficacement contre ces menaces. Le renforcement de la coopération est un moyen de lutter plus efficacement pour y faire face. Par ailleurs, au sein d'un même État, un service isolé ne peut lutter seul contre le terrorisme ou le trafic de drogue. L'expérience montre que ces combats ne peuvent être efficaces qu'à la condition que chaque service concerné soit bel et bien un maillon de la nécessaire interministérialité de ces combats.

Autrement dit, deux conditions essentielles doivent être réunies pour lutter plus efficacement et durablement contre le terrorisme et la drogue. D'une part, il s'agit de renforcer l'interministérialité d'un État et, d'autre part, de mettre en œuvre une coopération entre les États.

C'est pour répondre à cela que le ministère de l'Intérieur français a mis en place un « plan Sahel élargi » qui s'est traduit notamment par la création, en janvier 2014, du poste d'attaché régional de sécurité intérieure à Dakar pour coordonner l'activité des attachés de sécurité intérieure du Burkina Faso, de la Côte d'Ivoire, du Mali, de la Mauritanie, du Niger et du Sénégal.

Dans le cadre du renforcement de ce dispositif, plusieurs réunions de haut niveau « Drogue et terrorisme » ont été organisées. La première a eu lieu en novembre 2014 à Nouakchott, suivie de celles au Sénégal sous la bannière des « Rencontres de Dakar 1, 2, 3, 4 ».

Après avoir organisé des premiers exercices sur table, les participants (Burkina Faso, Côte d'Ivoire, Guinée, Mali, Mauritanie, Niger, Sénégal) ont émis le souhait de réaliser des exercices régionaux en situation réelle.

L'exercice régional de simulation d'attentats du 15 au 19 mai 2017

Les trois premières rencontres « Drogue et terrorisme » ont permis de lancer un processus de réflexion et de coopération. Après la réussite d'un exercice régional de livraison surveillée de novembre 2016, pour la première fois, un exercice de simulation portant sur une simultanéité d'attentats dans les capitales du **Burkina Faso, de la Guinée, du Mali, de la Mauritanie, du Niger et du Sénégal** a été organisé du 15 au 19 mai 2018.

Cet exercice inédit visait un double objectif : d'une part, éprouver l'interministérialité de la lutte contre le terrorisme dans les pays participants et, d'autre part, évaluer la coopération entre ces États pour faire face à cette menace.

Cette simulation, réalisée de façon concomitante le 16 mai 2017, a mobilisé plusieurs milliers de membres de forces de sécurité intérieure et de secours. Elle a mis en scène des

unités primo-intervenantes, d'intervention et de secours agissant dans le cadre d'une cellule de crise et sous la direction du procureur de la République pour la partie enquête judiciaire. Dans chaque pays, les exercices ont eu lieu en zones gendarmerie et police.

Dans le scénario de l'exercice, deux équipes de deux plastrons sénégalais se sont rendues à Bamako et à Conakry pour commettre des attentats après avoir rejoint une cellule terroriste.

Au Sénégal, deux simulations d'attentats ont eu lieu en situation réelle, l'une dans un grand hôtel de Dakar en zone police, l'autre en zone gendarmerie dans un centre de conférences, toutes deux supervisées par le Cadre d'intervention et de coordination interministérielle des opérations de lutte antiterroriste (CICO), créé en juillet 2016.

Le retour d'expérience (Retex), intitulé « La rencontre de Dakar pour le renforcement de la coopération en matière de lutte contre le terrorisme », a eu lieu le 18 mai 2017. Il réunissait les délégations des pays participants, et il comportait des chefs d'unités d'intervention de la gendarmerie, de la police, des secours et des procureurs de la République, ainsi que les attachés français de sécurité intérieure.

Le Retex a montré l'utilité et l'importance d'une telle simulation non seulement dans chaque pays, mais aussi au niveau régional, ce qui était innovant.

Les pays membres de l'exercice ont unanimement exprimé le souhait de le renouveler en 2018.

L'exercice régional portant sur une simultanéité d'attentats du 15 au 19 octobre 2018

Tout comme en 2017, le ministre de l'Intérieur de la République du Sénégal a invité ses homologues du Burkina Faso, de la Côte d'Ivoire, de Guinée, du Mali, de la Mauritanie et du Niger à participer à un nouvel exercice de simulation d'attentats.

L'édition 2018, parrainée par FRANCOPOPOL, a eu lieu en présence de M^{me} Sophie Hatt, directrice de la coopération internationale et présidente de l'association. Cet exercice s'est tenu en même temps que l'assemblée générale de FRANCOPOPOL, qui avait lieu pour la première fois en Afrique.

Cet exercice s'inscrit dans la dynamique relevée en 2017 et a contribué une nouvelle fois au renforcement de l'interministérialité de la lutte contre le terrorisme dans les pays participants. Cette année, la simulation se voulait plus dynamique.

Pour mémoire, et par convention d'exercice, en mai 2017, la Katiba Bobaouar avait décidé de frapper l'opinion publique internationale en commettant une simultanéité d'attentats dans les capitales du Burkina Faso, de la Côte d'Ivoire, de Guinée, du Mali, de Mauritanie, du Niger et du Sénégal.

Le scénario par convention d'exercice

En 2018, depuis plusieurs mois, la division spéciale de cybersécurité de la Direction de la police judiciaire du Sénégal a mis en place un dispositif de surveillance des réseaux sociaux, et notamment du Web invisible (*dark Web*). Ces enquêtes ont permis d'apprendre que la Katiba Bobaouar était en train de renaître de ses cendres en préparant une simultanéité d'attentats en fin d'année 2018 pour venger ses frères d'armes morts au combat en 2017.

Selon les informations des policiers sénégalais transmises aux pays concernés (par les attachés de sécurité intérieure), deux équipes de deux présumés terroristes/trafiquants de stupéfiants devaient quitter le Burkina Faso et le Niger pour se rendre à Dakar par avion, tandis qu'une même équipe sénégalaise rejoignait Conakry.

Arrivés aux aéroports de Dakar et de Conakry dès le 14 octobre, ces « terroristes » (qui sont des membres des forces de sécurité des pays concernés) ont été pris en charge par des membres de la cellule locale pour les conduire dans une cachette.

Informés par la division « cyber » de Dakar, les services spécialisés ont mis en place, dès l'arrivée de ces équipes, un dispositif de filature et de surveillance pour les « loger » et pour permettre d'identifier la cellule terroriste.

Les enquêtes ont permis de démontrer que les terroristes/trafiquants transportaient de la drogue dont la vente a permis de financer l'achat d'armes et d'explosifs pour commettre les attentats.

Le 16 octobre 2018, des simulations d'attentats ont eu lieu en même temps au Burkina Faso, en Guinée, au Mali, en Mauritanie, au Niger et au Sénégal selon la chronologie suivante :

- Attentats/tuerie de masse/prise d'otages;
- Mise en place d'une cellule de crise;
- Primo-intervenants;
- Négociations;
- Intervention;
- Secours/prise en charge des victimes;
- Judiciaire : début des enquêtes/constatations, auditions, etc.

Pour la première fois, l'état-major de la Direction de la coopération internationale (DCI) a participé à cet exercice. Les attachés de sécurité intérieure (ASI) ont informé en temps réel leur direction du déroulement de la simulation. La DCI, à son tour, a transmis ces informations à l'ensemble des ASI concernés.

Le retour d'expérience

Il s'est tenu à Dakar les 18 et 19 octobre 2018, étant ainsi la quatrième édition de la « Rencontre de Dakar pour le renforcement de la coopération opérationnelle en matière de lutte contre le terrorisme ».

Il a rassemblé les chefs des unités d'intervention et de secours, ceux des cellules de crise, ainsi que les attachés de sécurité intérieure.

En tout état de cause, ces simulations inédites de mai 2017 et d'octobre 2018, pour la coopération franco-africaine, ont permis à chaque pays participant :

- De présenter son propre Retex aux autres participants;
- De participer et d'animer le Retex régional;
- De formuler des recommandations pour renforcer la coopération régionale; ces recommandations seront mesurées à l'occasion d'un prochain exercice.

Ces simulations d'attentats mobilisant plusieurs milliers de personnes pouvaient paraître, pour les plus sceptiques, comme une gageure. Pourtant, les pays participants ont relevé le défi. Les avoir organisées est déjà un succès en soi.

Ces exercices ont montré l'engagement et le professionnalisme de tous les participants qui travaillent parfois dans des conditions difficiles. Ils ont permis de nouer des liens d'abord humains, puis professionnels entre beaucoup d'acteurs.

Jean-Luc Gonzales, commissaire divisionnaire, attaché de sécurité intérieure près de l'ambassade de France au Sénégal

2.3.1.2 Détection des comportements suspects (Behavior Detection Officer)

Contexte

Tous les quatre ans, le Service central terrorisme de la Police judiciaire fédérale belge publie une stratégie policière détaillée relativement à la lutte contre le radicalisme violent, l'extrémisme et le terrorisme en Belgique. Tout comme la stratégie européenne, celle-ci repose sur quatre piliers : la prévention, la protection, la perturbation (auparavant « poursuite ») et la réaction.

Dans le pilier « Protection », le Service central terrorisme a élaboré un programme de détection des comportements en collaboration avec la police aérienne et la police des chemins de fer.

Au cours d'une phase de test, la police aérienne de l'aéroport de Bruxelles et la police des chemins de fer de Bruxelles ont été formées aux techniques de détection des comportements en vue d'améliorer la protection des frontières internationales.

L'ensemble de la rétroaction récoltée au cours de cette phase a permis de développer davantage la formation.

Mandat du programme

Au cours de l'année 2017, le Comité de coordination de la Police intégrée a accordé un mandat au projet Behavior Detection Officer (BDO) et y a ainsi associé tous les services de la Police intégrée, tant ceux du niveau local que ceux du niveau fédéral.

Le mandat de projet comporte deux axes principaux :

- L'élaboration et l'organisation de formations sur mesure destinées au personnel policier régulièrement responsable de la gestion des foules;
- La validation scientifique des techniques, de leur mise en œuvre sur le terrain et des formations.

Objectifs

Concrètement, le programme de détection des comportements vise à :

- Sensibiliser davantage l'ensemble du personnel policier à la sécurité;
- Offrir un outil supplémentaire pour la protection des frontières et garantir la sécurité de l'environnement de travail quotidien de chaque fonctionnaire de police;
- Augmenter le niveau de compétence des fonctionnaires de police;
- Intégrer la technique dans la formation de base des nouvelles recrues;
- Élaborer une formation de trois jours pour les policiers opérationnels;
- Élaborer une formation de 10 jours pour les équipes BDO désignées et les unités spécialisées.

La formation opérationnelle a été offerte au cours du dernier trimestre de 2017 grâce à une campagne *train-the-trainer* qui a abouti à une équipe de 135 formateurs. À ce jour, plus de 800 BDO ont été formés et déployés sur le terrain.

L'organisation de la formation

La formation BDO de trois jours destinée aux utilisateurs finaux s'articule autour de présentations en classe consacrées aux aspects théoriques de la technique et d'exercices pratiques dans un environnement réel comme un aéroport ou une gare ferroviaire importante.

Cette alternance de modules théoriques très interactifs et d'exercices pratiques nécessite la mise en œuvre d'une équipe de plusieurs personnes pour l'organisation de chaque session :

- Deux formateurs pour les cours théoriques et les aspects liés au contenu des exercices;

- Deux personnes pour l'appui logistique et organisationnel des exercices;
- Au moins huit acteurs pour les exercices de jeux de rôles.

Contenu : objectif et sujets

La formation doit faire prendre conscience aux participants de la nature du comportement humain, leur apprendre comment reconnaître les indicateurs d'un comportement déviant, comment y réagir et comment vérifier si ce comportement peut s'avérer suspect.

Les sujets abordés concernent entre autres :

- Le plan en quatre étapes de la détection et de l'évaluation d'un comportement déviant, et la décision d'entreprendre une action ou non;
- Le cycle de planification hostile;
- Les processus psychologiques qui sous-tendent la perception et le comportement humains;
- L'entretien analytique;
- Les dispositifs;
- Le cadre législatif;
- Les conditions de base d'un attentat;
- Les différents niveaux de sécurité et la sécurité aux frontières.

Les exercices pratiques permettent aux participants d'appliquer ce qui leur a été enseigné en classe. Ils varient de la méthode de l'équipe rouge (*red teaming*) – faire ressentir aux participants ce que cela fait d'être de l'autre côté, de préparer un attentat et de dissimuler la vraie nature de leurs actions face aux policiers qui s'adressent à eux – à des exercices de jeux de rôles basés sur différents scénarios tels que celui d'un pickpocket, d'une reconnaissance des lieux par un terroriste, de l'abandon d'un bagage contenant une bombe, etc.

Éléments clés

Les participants apprennent à ne pas se baser sur du profilage ethnique, mais à recourir uniquement à des indicateurs objectifs tels que le comportement. Bien que des données (statistiques) puissent aider à définir la priorité des tâches de la police, on ne peut jamais baser des actions policières sur l'apparence ou le contexte ethnique.

En outre, les participants apprennent à ne jamais laisser de place au doute. S'il y a un doute quant à la menace qu'une personne peut présenter, il faut lever ce doute. À cet effet, il faut être en mesure de s'adresser directement à la personne et être prêt à le faire, et l'interroger sur son comportement et ses intentions. Même si cette démarche est logique, la plupart des participants semblent avoir du mal à franchir ce seuil.

Équipe de projet et propriété

Une fois par an, le réseau des formateurs se réunira afin d'échanger des bonnes pratiques, de mettre à jour les informations du cours, de débattre de nouveaux problèmes et de nouvelles approches, d'inviter de nouveaux partenaires, etc.

Un nombre restreint de formateurs chevronnés (les *master trainers*) sont responsables des formations *train-the-trainer*. Ils assurent également la fonction de comité de pilotage pour le programme BDO et de comité consultatif à l'égard du Service central terrorisme et de l'Académie nationale de police.

Mise à jour, innovation et évaluation

La formation BDO est offerte aussi bien en néerlandais qu'en français; une traduction en allemand sera fournie par des formateurs de la communauté germanophone de la Belgique. La formation sera ainsi disponible dans les trois langues nationales. Une version anglaise doit encore être mise à jour.

Ces versions permettront également au comité de pilotage de partager ses connaissances avec des partenaires internationaux et de débattre d'innovations et de mises à jour sur la base d'une évaluation comparative (*benchmarking*) avec d'autres organisations policières.

Les présentations PowerPoint et le plan de cours seront mis à jour chaque année et tiendront compte des dernières techniques et connaissances.

Partenariats et avenir

Afin de parvenir à la validation scientifique des techniques appliquées par la police, des partenariats étroits ont été établis aussi bien avec le milieu scolaire qu'avec des sociétés privées actives dans ce domaine.

En collaboration avec différentes universités, un contrôle de qualité est mis en place en vue d'évaluer l'efficacité des techniques, les résultats et le niveau de compétence des BDO sur le terrain. Une première étude de maîtrise a été menée au début de l'année 2018 sur l'efficacité des techniques et la manière dont elles sont appliquées par les unités de terrain. Cette étude se poursuivra en 2019 et, en parallèle, des négociations sont en cours pour une thèse de doctorat ayant pour objet la validation des techniques et l'efficacité de la formation.

Les services publics fédéraux « Intérieur » et « Justice », ainsi que des organismes de défense des droits de l'homme tels qu'Amnistie internationale sont engagés dans le programme.

Enfin, des relations étroites sont établies avec d'autres organismes gouvernementaux et organisations policières aussi bien au niveau national qu'à l'étranger en vue de partager notre expertise et de tirer des enseignements de leurs expériences.

La France et le Canada, entre autres, ont déjà participé aux formations belges, et plusieurs organismes militaires et civils œuvrant dans le domaine de la sécurité ont adressé des demandes de formation au comité de pilotage du programme BDO.

Le projet se terminera en décembre 2020, mais la détection des comportements a assurément trouvé sa place au sein de la Police intégrée belge, et le programme continuera de former du personnel policier jusqu'à ce qu'il ne constitue plus seulement un outil, mais qu'il fasse également partie intégrante d'un nouvel esprit de sécurité.

*Bart Cappaert, premier commissaire de la Police judiciaire fédérale,
Service central terrorisme, Belgique*

2.3.1.3 Riposte à un accrochage

À titre de rappel, dans le cadre de la **formation AMOK 2.0**, le coordinateur romand de la formation en Suisse, M. André Etter, a été sollicité par la Conférence des commandants des polices cantonales de Romandie de Berne et du Tessin (CCPC RBT) afin d'appuyer le groupe de travail de veille AMOK, dirigé par le chef de la Gendarmerie fribourgeoise, à l'élaboration des ajustements liés à la formation dans ce domaine d'actualité et dans le contexte des attentats terroristes qui se sont déroulés plus particulièrement en France et en Belgique. En effet, l'apparition d'actions terroristes par le biais de tireurs actifs a changé la donne, qui était auparavant essentiellement focalisée sur les actions à l'intérieur d'un établissement. Dans ce nouveau cas de figure, la police constitue une cible privilégiée pour l'adversaire. De plus, l'action ne se déroule plus seulement dans un établissement scolaire, soit en milieu fermé, mais n'importe où dans la rue ou à l'intérieur d'établissements publics, en particulier dans les endroits très fréquentés.

Le module **Riposte à un accrochage**, premier module présenté dans ce concept, inclut :

- - le tir offensif;
- - la notion de 360° et de 3D (trois dimensions);
- - l'utilisation des couverts.

La notion de policier « primo-intervenant » a été introduite, car :

- tout policier peut être préférentiellement pris pour cible;
- tout policier peut être le premier à pouvoir ou à devoir :
 - › mettre un terme à la tuerie par tous les moyens possibles tout en réduisant au maximum ses risques,
 - › simplement survivre.

La notion d'« accrochage » signifie que :

- quel que soit l'adversaire, le policier accroché doit répliquer :
 - › avec du feu, du couvert, du mouvement, etc.,
 - › seul ou à 2, 3, 4, etc., que l'on soit à l'intérieur ou à l'extérieur.

Ce module primordial intègre les techniques présentées par un ancien militaire professionnel au sein de l'armée israélienne, consultant spécialisé dans le domaine du contre-terrorisme, lors de sa démonstration du 19 mai 2015, en présence d'une délégation de **l'ensemble des moniteurs romands**, présentation qui a remporté un vif succès.

Il s'agit pour tout policier de pouvoir se comporter de manière adéquate lors d'une action terroriste ou en présence d'un tireur actif, comme en Tunisie, à Paris et à Bruxelles, le **premier intervenant** étant celui qui a les capacités **d'agir immédiatement**. Pour la formation des moniteurs romands, il a été décidé de mettre sur pied, dans une première phase, **trois cours d'un jour** qui se sont déroulés avec succès les 16, 17 et 18 janvier 2016.

Les attentats terroristes ont tous les **mêmes buts**, à savoir :

- semer le chaos en générant des destructions soudaines;
- attaquer des cibles civiles (molles);
- effectuer des dégâts et des pertes de masse;
- agir de préférence dans des lieux et à des heures inattendues;
- mobiliser les médias.

La police est également devenue une cible privilégiée (*blue target*). Il en résulte évidemment une couverture inévitable par les médias sur le plan mondial (publicité indirecte).

Il s'agit donc d'un **nouveau paradigme**, si l'on compare avec le criminel classique :

Le TERRORISTE :

- recherche la reconnaissance ou une exposition médiatique;
- a un objectif politique;
- terrorise par la crainte de mourir;
- a la volonté de se sacrifier pour sa cause;
- cible les forces de sécurité.

Le CRIMINEL :

- enfreint la loi pour des profits personnels;
- vit de ses activités délictueuses;
- veut rester vivant;
- évite les forces de sécurité.

On constate donc un décalage entre la formation traditionnelle et la menace liée à cette typologie d'agresseurs. En effet, les tirs à l'entraînement sont en général toujours faits sur **des cibles en papier** qui ne réagissent pas aux impacts et, surtout, qui ne ripostent pas. Le policier est essentiellement entraîné pour agir face à un criminel classique, qui tentera d'abord de prendre la fuite, avant de tirer sur la police. À l'entraînement, cela se passe généralement bien, avec 80 % des impacts en cible en moyenne. À l'engagement, le nombre d'impacts en cible diminue radicalement, avoisinant les 10 à 20 %. En effet, dans un contexte terroriste, l'adversaire engage son arme à feu, qui peut être un fusil d'assaut, bouge et est très agressif.

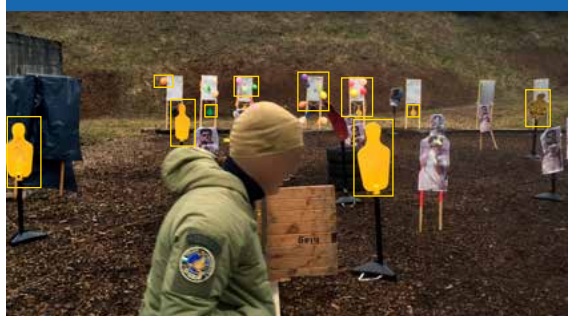
Dans ce cas de figure, le policier n'a que **quelques secondes** pour agir avec succès. De plus, au début de l'intervention, il est **seul**. En effet, ses collègues ou les unités spéciales alertées ont besoin de temps pour se rendre sur place. Dans le cadre de l'activité classique, la police isole ou boucle le secteur et observe. Dans le cas d'une action terroriste, c'est différent; il doit réagir rapidement, ce qui implique une adaptation des règles d'engagement.

On peut donner la définition suivante de l'adversaire :

- L'adversaire, qu'il soit un terroriste ou un tireur actif motivé par la vengeance, ou toute autre forme de justification, va tout faire pour causer le plus de victimes possible. Le terroriste va encore prendre les forces de sécurité comme cibles privilégiées. Il se peut, dans des situations exceptionnelles, que des délinquants, particulièrement dangereux, déterminés ou acculés, se comportent comme des terroristes à la vue de la police. Dans ce cas, le policier se trouve donc aussi dans un registre AMOK.

Le **programme général** du module, **d'une durée d'un jour**, a permis d'intégrer les principes suivants en utilisant un système à coûts réduits, avec des cibles réactives en plastique (tombantes ou qui bougent à l'impact) et des obstacles classiques pouvant être disposés dans n'importe quel *stand* de tir ouvert ou couvert.

CIBLES RÉACTIVES



Les cibles sont variées et réactives à l'impact, permettant au tireur de savoir lorsqu'il les a touchées (coups au but).

COUVERTS/OBSTACLES



Des obstacles sont présents sur le pas de tir, permettant au tireur de choisir une protection adéquate lors de la riposte.

TIR/COURSE



Il s'agit, pour le tireur, de se déplacer rapidement et d'éviter de rester statique afin de ne pas représenter une cible facile à atteindre.

COUVERT/TIR



Il s'agit également, pour le tireur, de choisir un couvert afin de ne pas s'exposer lors de la riposte et de présenter la silhouette la plus petite possible.

PRISE DE DÉCISION DANS L'ACTION/SOUS STRESS



La prise de décision sous stress doit également faire l'objet d'un entraînement et permet au tireur d'agir en fonction de la situation dans laquelle il se trouve.

360°/3D



La notion de la vision à 360° est primordiale afin de ne pas se laisser surprendre par un adversaire qui tente de contourner le tireur. Il s'agit aussi de briser l'effet tunnel.

L'instructeur anime les divers scénarios selon une méthode **compliquant progressivement** la tâche de l'élève. Tout d'abord, les exercices sont faits « à sec » afin de contrôler les déplacements, la tenue de l'arme (canon vers le bas et doigt hors de la détente, etc.) et les prises de position (couvert,

silhouette réduite). Ensuite, le travail est conduit par le formateur, l'apprenant se déplaçant de cône en cône (d'abord deux, puis trois, etc.) en prenant une **position de tir basse** (silhouette réduite). Ensuite, l'instructeur **déclenche des stimulus** (voix, sifflet, signes, etc.) que le tireur doit percevoir tout en **gardant l'œil** sur les **cibles** et en se tenant prêt à **rejoindre le couvert** le plus proche et le plus adapté. Les cônes peuvent être déplacés pendant le parcours afin de toujours forcer l'apprenant à être **attentif à l'environnement sur 360°**.

Il y a aussi possibilité de travailler en « *live drill* » avec **Simunition^{md}** ou le tir à microbilles (*airsoft*), en remplaçant les cibles par des plastrons qui ripostent (*force to force*).

Ce concept, testé depuis près de deux ans, a permis d'améliorer de manière substantielle la capacité d'action des policiers de terrain, qui aiment beaucoup la dynamique de cette formation.

Il s'agit de renforcer la fréquence de la formation continue dans ce domaine, et tous les élèves des centres régionaux de formation en Romandie suivent ce module spécifique en formation initiale.

*André Etter, coordinateur de la formation
policière en Suisse romande, Suisse*

2.3.1.4 Riposte en deuxième échelon – Concept ÉGIDE

Situation géographique

La Suisse, un pays situé au centre de l'Europe, est entourée par la France, l'Allemagne, l'Italie, le Liechtenstein et l'Autriche. Notre pays est constitué de 26 cantons. Le canton de Vaud a pour chef-lieu Lausanne et compte une population de 800 000 habitants. Il bénéficie d'une superficie de 3 212 km². Depuis 2015, j'exerce la fonction de commandant de la Gendarmerie vaudoise, partie intégrante de la Police cantonale. Cette institution regroupe les Services généraux, la Gendarmerie vaudoise et la Police de sûreté. Notre pays a la particularité d'un État fédéral dans lequel la responsabilité de la sécurité publique est de compétence cantonale. Chaque canton développe des stratégies policières qui sont ensuite discutées, comparées et unifiées à tout le territoire helvétique.

Niveau de risque en Suisse

Depuis plusieurs années, la Suisse est aussi la cible de plusieurs événements de type AMOK, dont le plus meurtrier a été perpétré dans la salle du Grand Conseil à Zoug, en Suisse centrale. Quatorze députés et conseillers d'État sont décédés sous le feu d'un seul meurtrier. Entre 1986 et 2012, sur l'ensemble du territoire, on recense au moins une dizaine de situations (AMOK) dans lesquelles des citoyens ont été grièvement blessés ou sont décédés.

À ce jour, nous ne répertorions aucun attentat perpétré sur le territoire helvétique; par contre, des actes préparatoires ont été déjoués. Particulièrement attentive aux nombreuses attaques aux États-Unis comme en Europe, que ce soit sur le plan du terrorisme ou de la tuerie de masse, la Suisse ne peut ignorer que ce type d'attaque pourrait également survenir sur son territoire. Ce risque évolue constamment avec des auteurs qui font preuve d'inventivité, de détermination et d'une totale abnégation. Il fallait dès lors étudier, analyser, réfléchir et penser à la manière de développer, mais surtout de déployer des moyens opérationnels efficaces permettant d'appréhender et de faire face à de telles situations pour notre canton. Les autres cantons font de même pour leurs propres territoires.

Des expériences vécues, il ressort qu'un des éléments prépondérants pour la gestion de telles crises est la capacité, pour les forces de l'ordre, à prendre le dessus le plus rapidement possible sur la partie adverse. Cela passe notamment par une augmentation de la puissance de feu liée à l'emploi d'un armement spécialisé et de tactiques adaptées.

À l'instar des autres polices occidentales, le constat a été fait que l'action des primo-intervenants est prépondérante pour endiguer ou stopper une menace terroriste. Les procédures et l'équipement standard des patrouilles de police et de la gendarmerie sont adaptés, cela aussi bien dans la lutte contre la moyenne et la grande criminalité que dans leur rôle de primo-intervenants au cours d'une attaque terroriste. Ils font l'objet de réflexions et de consolidations permanentes. L'hypothèse de doter la totalité des primo-intervenants d'armes de guerre et de modifier les critères d'engagement de l'arme de tous les collaborateurs soulève des questions de

proportionnalité, d'économie des moyens, d'image, d'éthique et de doctrine pour tous les collaborateurs œuvrant dans le canton de Vaud. Elle n'a rapidement pas été retenue.

Les groupes tactiques d'intervention, quant à eux, apportent une expertise incontournable dans cette thématique. Toutefois, pour être efficaces, ces groupes doivent avoir la possibilité de se préparer minutieusement. Un délai de mise en œuvre doit alors être accepté.

Dès lors, la disponibilité d'un moyen d'intervention au profil intermédiaire, entre les primo-intervenants et les groupes tactiques d'intervention ou les unités d'appui, se pose comme une réponse rationnelle à l'état de la menace latente dans nos régions. Ce moyen intermédiaire est doté d'un armement adapté et formé aux tactiques d'engagement qui y sont relatives.

Notre réponse : concept ÉGIDE

Au terme des réflexions menées, le concept ÉGIDE a été créé.

ÉGIDE, dans la mythologie grecque, représente une arme merveilleuse, offensive autant que défensive, symbole de la puissance souveraine.

Explication du concept

Les objectifs de ce moyen intermédiaire entre les primo-intervenants et les groupes tactiques sont déclinés comme suit :

- Augmente la puissance de feu;
- Permet de fixer et de neutraliser la menace;
- Disponible 24 heures sur 24;
- Capable d'un effort principal sur la durée;
- Discret;
- Rationnel;
- Flexible;
- Proportionné à la menace dans nos régions.

Les opérateurs ÉGIDE sont formés à l'usage du fusil d'assaut et aux tactiques correspondantes y étant relatives; ils sont disponibles quotidiennement ou sur mobilisation. Ils agissent dans le cadre de leur patrouille ou en unités constituées. En cas d'engagement, les opérateurs ÉGIDE se positionnent dans le même état d'esprit et en complément des primo-

intervenants. Ils profitent de leur puissance de feu et de leurs connaissances tactiques pour reprendre le dessus et faire cesser la menace.

Formation

Pour être en adéquation avec les nouvelles menaces, les opérateurs ÉGIDE sont astreints à trois jours de formation de base et, par la suite, à quatre journées et demie par année de formation continue, et ce, en collaboration avec l'armée et l'Institut suisse de police. Les entraînements se basent principalement sur la maîtrise des techniques et des tactiques de progression, et sur celle du maniement et du tir aux armes longues. Chaque année, un test valide les compétences de ces opérateurs et autorise ainsi leur engagement opérationnel.

Critères de sélection

Afin d'optimiser ce concept, des exigences sont imposées à chaque collaborateur souhaitant intégrer ce moyen. Pour être opérateur, il faudra faire preuve d'une grande maîtrise de soi, d'un sens des responsabilités développé et d'aptitudes au tir reconnues. En outre, il sera demandé une parfaite connaissance des procédures applicables pour les cas de tuerie de masse.

Déploiements possibles

La majorité des collaborateurs sont intégrés aux unités opérationnelles de la Gendarmerie, contribuant ainsi à une disponibilité 24 heures sur 24. Chaque jour, dans leur champ d'activité standard, les opérateurs validés ÉGIDE œuvrent avec l'armement et le matériel spécifiques à leur mission. En cas d'événement impromptu et lorsqu'ils se trouvent dans le canton, les opérateurs ÉGIDE convergent sur ordre vers l'effort principal.

Lors d'une attaque par un tireur isolé ou par un terroriste, c'est la mise en place de ce processus opérationnel entraîné qui arrive, dans les premières minutes, juste après les primo-intervenants. Dans l'intervalle, les groupes d'intervention spécialisés se préparent et seront prêts à se déployer.

Buts

Jusqu'à présent, la Suisse a été épargnée par les attaques de

type terroriste. Chaque tragédie, que ce soit en France, en Belgique, en Allemagne, en Suède ou aux États-Unis, pour n'en citer que quelques-unes, aussi dramatique qu'elle soit, nous oblige à étudier sans relâche les méthodes employées. Nous devons chercher à les comprendre pour développer et affiner de nouvelles stratégies. Celles-ci devront évoluer au même rythme que la société et ses dangers potentiels.

Conclusion

Nous savons que, lors de tueries de masse, de cas AMOK ou d'attaques terroristes, les premières minutes sont décisives, voire capitales. Le concept ÉGIDE offre alors une rapidité d'action permettant d'intervenir dans les meilleurs délais selon l'endroit de l'attaque. Les opérateurs étant armés en conséquence, leurs interventions répondront avec efficacité à la menace dès leur arrivée sur les lieux choisis par les assaillants.

*Colonel Alain Gorka, commandant de la Gendarmerie vaudoise
et commandant du Groupement latin de sécurité publique
et de maintien de l'ordre (GMO), Suisse*

2.3.1.5 Gestion opérationnelle d'une tuerie de masse

À la suite des attaques qui ont touché Paris en 2015 et pour répondre à un certain nombre de difficultés rencontrées sur le terrain, l'École nationale supérieure de la police (ENSP) a mis en place un certain nombre de formations sur la gestion opérationnelle d'une tuerie de masse.

En formation initiale

Ce sont 21 heures qui sont consacrées à la gestion opérationnelle d'une crise au profit des élèves commissaires.

En formation continue

À la suite des attentats qui ont ensanglanté Paris le 13 novembre 2015 (130 morts et plus de 400 blessés), la Direction générale de la police nationale (DGPN) a mis en place, en avril 2016, un schéma national d'intervention permettant la mise en œuvre d'une réponse urgente et adaptée à l'attaque en définissant le rôle respectif des différentes forces en fonction de leurs compétences et de leur proximité avec la scène d'attaque.

Dans la droite ligne de ces instructions, l'ENSP propose, depuis 2016, une formation intitulée *Gestion opérationnelle d'une tuerie de masse* destinée aux cadres de police (commissaires et officiers-chefs des services).

Cette formation, d'une durée de cinq jours et qui réunit environ 25 stagiaires, recourt aux compétences des policiers du Groupe national d'intervention (RAID), à des psychologues, à des responsables des services de secours et à des spécialistes de la gestion de crise. Elle intègre de nombreux exercices pratiques, des mises en situation et des séquences de *debriefing* en appui à la formation théorique.

Les différentes séquences se répartissent comme suit :

- L'intervention dans un contexte de tuerie de masse (1 h 30 min);
- Caractéristiques et approches tactiques d'une tuerie de masse; état de la menace (1 h 30 min);
- Gestion globale d'une tuerie de masse; accent mis sur le rôle des centres d'information et de commandement CIC (1 h 30 min);
- Formation des effectifs de premier et de deuxième niveau (1 h 30 min);
- Rôle des forces dites de troisième niveau (forces d'intervention spécialisées) dans la gestion d'une tuerie de masse (1 h 30 min);
- Soutien médical tactique et gestion d'une tuerie de masse (1 h 30 min);
- Gestion du stress en situation de crise (1 h 45 min);
- Retex technique sur l'attaque du Bataclan (salle de spectacles parisienne) en novembre 2015 avec témoignages de participants à l'intervention;
- Préparation en amont d'un service de gestion opérationnelle d'une tuerie de masse (2 h);
- Communication institutionnelle en temps de crise (1 h 30 min);
- Exercices pratiques et interactifs (8 h).

Objectif principal

Effectuer une gestion opérationnelle du dispositif mis en place dans le cadre d'une tuerie de masse par un cadre de la Police nationale.

Il s'agit de former des responsables hiérarchiques à la gestion en urgence d'une tuerie de masse tout en les préparant à l'anticipation de la crise.

Cette formation revient notamment sur les différents niveaux d'intervention 1 (primo-intervenants), 2 (brigades anticriminalité, brigades de recherche et d'intervention de province, compagnies d'intervention) et 3 (RAID, groupe d'intervention de la Gendarmerie nationale et Brigade de recherche et d'intervention [BRI] Paris), ainsi que sur la notion de procédure d'urgence absolue qui efface les compétences territoriales au profit de l'urgence de l'intervention.

Elle aborde la notion de commandant des opérations de police (COP), de mise en place des postes de commandement des opérations de police (PC COP) et de secours (PC COS), du triple zonage (intervention/extraction des victimes/gestion des personnes impliquées) en insistant sur la répartition des compétences et les concours interservices.

La formation aborde concrètement les notions de zones d'exclusion (les zones de contact avec les terroristes réservées aux services spécialisés d'intervention, la zone contrôlée dans laquelle sont installés le PC COS et le PC COP, et qui abrite un couloir d'extraction, ainsi que la zone de soutien où sont positionnés les services de secours).

Il convient de préciser que les exercices pratiques réalisés sur le site impliquent à la fois des services opérationnels de police et de secours, mais également des membres du personnel de l'ENSP sollicités pour jouer le rôle de plastrons.

Résumé

À la suite de la vague d'attentats qui ont ensanglanté Paris en novembre 2015 et Nice en juillet 2016, la Direction générale de la police nationale a pris des mesures d'organisation et de gestion de crise qui ont eu des répercussions profondes sur le fonctionnement des services.

Pour aider les commissaires et les commandants à mieux gérer ces crises majeures et à assurer la gestion interservices, l'ENSP a conçu une formation continue intitulée *Gestion d'une tuerie de masse*.

Cette formation aborde tous les aspects théoriques, mais aussi très pratiques de la gestion d'une tuerie de masse en amont, pendant et après la crise.

En formation initiale, les élèves commissaires et les officiers bénéficient également d'actions de sensibilisation sur cette thématique.

Pascal Bastide, commissaire divisionnaire, chef du Département des formations préparatoires, partenariales et internationales, France

2.3.1.6 Équipe multidisciplinaire d'extraction des blessés (Formation Casualty Extraction Team)

Contexte

À l'instar d'autres pays dans le monde, la Belgique est, elle aussi, touchée par une nouvelle forme de terrorisme, la « tuerie de masse », que les autorités françaises ont définie ainsi : **« Homicides multiples perpétrés dans des lieux publics qui se singularisent par la détermination de leurs auteurs à faire le plus grand nombre de victimes en un temps réduit et à mourir peu après le déclenchement de la tuerie. »**

Les tueries de masse se caractérisent par trois phases :

- Une phase d'homicides multiples;
- Une confrontation armée avec les forces de l'ordre qui sont engagées les premières, suivie d'un retranchement;
- Un assaut suicide contre les forces de l'ordre.

Il est également constaté que la *modus operandi* terroriste est basé sur un modèle d'entreprise décentralisée. Ce qui caractérise les terroristes impliqués dans les attentats est qu'ils agissent sur la base d'une idéologie sans être effectivement commandés par une organisation. Ils suivent un message, une recette qu'ils décident eux-mêmes de réaliser. Ce côté non commandé et arbitraire rend la prévention de ces actes difficile, voire impossible. Dès lors, il est nécessaire, pour l'organisation policière, de s'adapter et de pouvoir donner une meilleure réponse réactive en cas d'apparition d'un tel passage à l'acte. Cela doit se traduire par des principes d'intervention révisés consistant à limiter prioritairement le nombre de victimes initiales.

1. Procédures d'intervention de la police (discipline 3)

En Belgique, nous disposons de deux circulaires ministérielles qui définissent la manière d'intervenir des policiers devant un incident de « tuerie de masse », ainsi que la répartition des tâches selon les compétences et les aptitudes de ces policiers.

La circulaire GPI 48 bis prévoit qu'en cas d'incident AMOK, « il convient de mettre un terme aux actes de l'auteur le plus rapidement possible. La police doit investir le plus vite possible les lieux, et donc également, s'il échet, le bâtiment dans lequel se déroulent les faits afin de mettre fin aux actes de l'auteur. **Tout retard représente en effet un danger pour les personnes présentes** ».

Il s'agira de neutraliser l'auteur pour le contraindre à cesser la tuerie et, éventuellement, à se retrancher.

La circulaire GPI 81 de 2014 prévoit trois niveaux d'assistance (passage à l'échelon supérieur en fonction de l'escalade du danger ou de la violence) :

- Niveau 1 : « assistance régulière », par exemple par une patrouille supplémentaire;
- Niveau 2 : « assistance spéciale » de la police locale;
- Niveau 3 : « intervention et appui spécialisés » de la police fédérale.

Il s'agit là d'une répartition des tâches en fonction des compétences (de base ou qualifiées). Ces différents degrés d'assistance sont une mise en œuvre d'un appui à la fonction de police de base (essentiellement d'intervention).

Les deux circulaires définissent des règles d'engagement (*rules of engagement*) de nos policiers confrontés à une situation à risque élevé telle qu'une tuerie de masse. Elles constituent la base de notre doctrine d'intervention du primo-intervenant, mais cette doctrine doit faire l'objet d'une adaptation sur la base de l'arsenal policier dont on dispose sur notre territoire et, surtout, en fonction de la « cinétique de la crise » inhérente à ce type d'événement et composée de quatre phases : massacrer, se retrancher, maintenir l'attention (par l'entremise des médias) et mourir en martyr.

Comme indiqué précédemment, il existe trois niveaux d'assistance à la fonction de police de base. Cela se traduit

par l'existence d'une unité d'intervention spécialisée (DSU) ainsi que par la mise en place d'unités d'assistance spéciale (ou particulière) au sein de certains corps de police locale (voir la cartographie à la fin de l'article).

Ces deux niveaux d'assistance renvoient à des compétences définies comme qualifiées. Cela implique que ces policiers sont, dans leur niveau respectif, mieux formés, entraînés et équipés que la majorité de leurs collègues. Ainsi, nous pouvons nous inspirer de l'analyse faite par les Français quant à trois niveaux d'unités d'intervention : les unités élémentaires, les unités intermédiaires et les unités spécialisées.

- **Les unités élémentaires sont composées de primo-intervenants** qui, compte tenu de leurs équipements, ne doivent intervenir de façon offensive que dans les cas d'urgence ou de péril imminent.
- **Les unités intermédiaires sont composées également de primo-intervenants** (unités d'assistance spéciale) qui, compte tenu du niveau de formation de leurs membres, constituent des éléments d'intervention de proximité dont l'engagement doit être privilégié.
- Les **unités d'intervention spécialisée** (DSU).

Chacun de ces niveaux se voit attribuer des tâches en vue de gérer la menace :

1^{er} niveau d'intervention

Les policiers qui sont engagés les premiers sur une tuerie de masse, de manière fortuite, sur ordre ou à leur initiative, ont pour mission d'évaluer la menace (AMOK, tuerie de masse, prise d'otages, « fort Chabrol »), puis de fixer le ou les auteurs pour les contraindre à cesser la tuerie et à se retrancher, et de renseigner l'échelon de commandement jusqu'à l'arrivée du deuxième niveau.

2^e niveau d'intervention (unités d'assistance spéciale)

Le déploiement sous court délai du deuxième niveau d'intervention, présent essentiellement dans des grandes ou moyennes villes de Belgique, doit permettre, au plus vite, la relève de la patrouille primo-engagée au contact. L'objectif

de ce niveau est, au minimum, de fixer le tireur ou, encore mieux, de le neutraliser.

Bien sûr, cela n'implique pas une exclusivité d'intervention en vue de neutraliser le ou les auteurs, mais il faut garder à l'esprit que la plupart des policiers des unités élémentaires ne disposent d'aucun moyen supplémentaire que leur armement individuel et leur gilet pare-balles individuel.

3^e niveau d'intervention (unités d'intervention spécialisée)

Les unités d'intervention spécialisée de la police fédérale (DSU) sont déployées pour faire face à des situations présentant un degré de risque élevé (situations pour lesquelles il existe une certitude que les auteurs sont dangereux et armés), conformément aux procédures de demande et de mise en œuvre en vigueur.

Les tueries de masse ne relèvent pas de l'exclusivité des unités d'intervention spécialisée, étant donné que l'objectif principal de celles-ci est de limiter prioritairement le nombre de victimes initiales; ces circonstances constituent toutefois des situations présentant un degré de risque à ce point élevé que ces unités seront vraisemblablement les seules, en raison de leurs procédures de mise en œuvre, de leur entraînement et de leur équipement, à pouvoir résoudre la crise.

2. Procédure d'intervention de pompiers (discipline 1)

Les pompiers interviendront également, sur tout le territoire national, lors de tueries de masse.

Les caractéristiques de ces interventions très spécifiques nécessitent de parfaitement coordonner l'action de tous les intervenants et d'adapter la réponse opérationnelle des pompiers.

La Direction générale de la sécurité intérieure a développé une procédure d'opération standard (*Standard Operating Procedure [SOP]*) qui s'inscrit dans le cadre établi par l'arrêté royal du 16 février 2006 relativement aux plans d'urgence et d'intervention, et qui tient compte des prescrits de l'arrêté royal de 2016 portant sur la fixation du plan d'urgence relatif à l'approche d'une prise d'otages terroriste ou d'un

attentat terroriste. Cette procédure introduit de nouveaux principes quant à la coordination opérationnelle ainsi que dans l'organisation des lieux d'intervention.

De cette procédure découle une fiche opérationnelle ayant pour titre Intervenir lors d'une situation crise nécessitant le déclenchement d'un plan d'urgence et d'intervention (tuerie de masse, attentat terroriste, etc.). Cette fiche a notamment pour objectif de définir les règles d'engagement et le rôle des *Casualty Extraction Teams* (CET).

Les CET auront pour tâche, alors même que la situation de tuerie n'est pas encore résolue (auteur ou auteurs non encore neutralisés), de pénétrer dans une zone partiellement sécurisée par les forces de police équipées d'un armement et d'une protection balistique adéquats, et ce, afin d'y prendre en charge les victimes présentes et d'entamer leur extraction de la zone partiellement sécurisée vers la zone d'isolation où elles seront prises en charge selon les principes qui régissent les plans d'urgence et d'intervention de la discipline 2 (secours médicaux sanitaires et psychosociaux).

Finalité de la formation Protection des *Casualty Extraction Teams*

Il s'agit d'organiser une formation, des entraînements et des exercices conjoints pour atteindre la synergie et la coopération opérationnelle nécessaires à la réussite de ces missions. Il s'agit là de développer des procédures interdisciplinaires.

L'objectif global de cette formation se lit comme suit :

« Lors d'une situation de crise nécessitant le déclenchement d'un plan d'urgence national relatif à l'approche d'une prise d'otage terroriste ou d'un attentat terroriste, permettre aux membres de la discipline 3 de garantir la sécurité des membres spécialisés des services de secours (*Casualty Extraction Team*) afin qu'ils puissent prendre en charge les victimes le plus rapidement possible. » (Dossier d'agrément)

Éléments de compétence développés pendant la formation

La future équipe CET des pompiers suit d'abord, pendant deux jours, deux cours étendus, soit *Terror Awareness* et *Tactical Emergency Casualty Care* (TECC) :

Terror Awareness :

- Manière dont la police procède et déroulement d'une collaboration multidisciplinaire en cas d'incident terroriste ou de tuerie de masse;
- Éléments auxquels il faut prêter attention en tant que pompier lors de l'arrivée sur les lieux d'un incident;
- Explications relatives au déroulement de ce type d'incident;
- Déroulement d'une explosion et possibilités de s'échapper;
- Différents types d'armes et de balles, avantages et inconvénients des gilets pare-balles;
- Dispositifs pièges (*boobytraps*);
- Éléments d'alerte à prendre en considération.

Tactical Emergency Casualty Care (TECC) :

- Soin des blessures de guerre;
- Utilisation des tourniquets, des bandages compressifs et des couvertures thermiques.

Ensuite, les équipes CET des pompiers rejoignent les policiers qui suivent la formation intitulée *Protection des Casualty Extraction Teams*, composée de six modules (16 heures, dont 12 de pratique) :

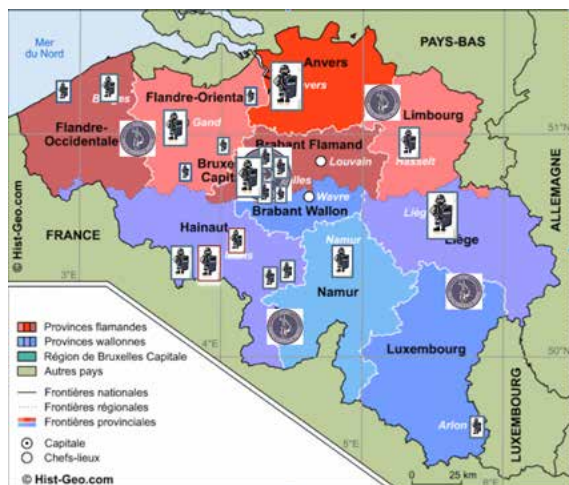
- Contexte opérationnel;
- Principes d'évolution tactique avec protection balistique;
- Techniques et tactique d'intervention;
- Réaction en présence d'armes ou d'explosifs;
- Mise en œuvre des techniques;
- Exercices situationnels.

Les équipes CET pourront ainsi aligner au mieux leur fonctionnement sur celui de la police, et ce, grâce à une pédagogie basée sur la résolution de problèmes mise en exergue par la capacité d'adaptation des intervenants aux situations qui leur sont proposées.

Retour sur investissement

En juillet 2017 commençait le projet pilote par la formation de 90 pompiers de la Région de Bruxelles-Capitale et près

de 25 formateurs policiers provenant des unités d'assistance spéciale. Aujourd'hui, trois autres zones de secours sont formées, et la formation devrait vraisemblablement s'élargir à tous les policiers de Belgique. Les unités CET des pompiers assistent régulièrement les unités spéciales de la police fédérale dans le cadre de « fort Chabrol » et de prises d'otages afin d'améliorer leur connaissance réciproque.



Cartographie des unités d'assistance spéciale et des unités d'intervention spécialisée

Organisation des secours en cas de tuerie de masse

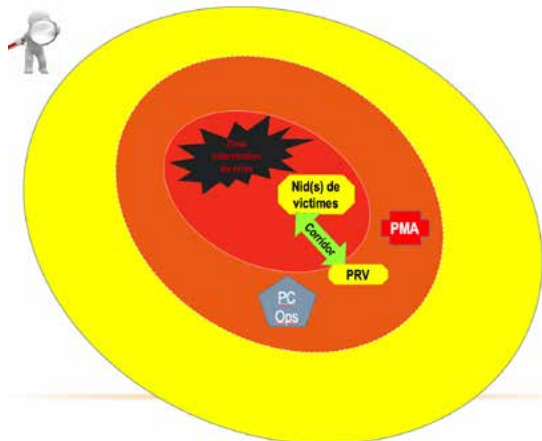


Image 1 | Bâtiment abritant des services de la direction de l'École nationale de police

Cinétique de la crise	GPI 48 Niveaux de compétence		GPI 81 Niveaux d'assistance	Discipline 1 Pompiers
Massacre	Niveau de base	Policier de base	Assistance régulière	Pompiers de base
Retranchement	Niveau qualifié	Policier d'assistance spéciale	Assistance spéciale	Pompiers CET
Affrontement		Policier d'intervention spécialisée (DSU)	Assistance spécialisée	

Cinétique de la crise et les différents niveaux d'intervention

Claude Passchier, commissaire divisionnaire de la Police fédérale belge, chef du Département de la maîtrise de la violence et sport, Belgique

2.3.1.7 Gestion de scènes de crime complexes par la Gendarmerie nationale : les capacités opérationnelles de l'Institut de recherche criminelle de la Gendarmerie nationale

L'Institut de recherche criminelle de la Gendarmerie nationale (IRCGN) est un laboratoire de sciences judiciaires couvrant 48 disciplines. Mais, au-delà d'un laboratoire, c'est aussi une composante tactique et opérationnelle disponible 24 heures sur 24. Des spécialistes hautement qualifiés de l'Unité investigations et identification (U2i) peuvent être rapidement déployés sur des scènes de crime complexes ou de grandes catastrophes, avec des moyens matériels spécifiques et adaptés. Cette composante opérationnelle regroupe deux unités, soit l'Unité gendarmerie d'identification des victimes de catastrophes et l'Unité nationale d'investigation criminelle, qui sont déployables sur tous les points du territoire national, voire à l'étranger.

La Gendarmerie nationale a pour particularité d'être présente sur l'ensemble du spectre des missions régaliennes de sécurité. Cette omniprésence est relayée à l'IRCGN dans sa réalisation d'actes ayant trait à l'investigation judiciaire et à l'identification de victimes (catastrophe de masse), qui doivent pouvoir s'accomplir en tout lieu, en tout temps et en toute situation.

L'Unité gendarmerie d'identification des victimes de catastrophes

Lorsqu'un événement majeur se produit sur le territoire national impliquant un grand nombre de victimes ou dès lors que des ressortissants français comptent parmi les victimes d'un événement semblable à l'étranger, l'Unité gendarmerie d'identification des victimes de catastrophes (UGIVC) est activée.

L'UGIVC, tout comme l'Unité nationale d'investigation criminelle, est une unité de circonstance composée d'**experts de l'IRCGN** (empreintes digitales, génétique, médecine légale, odontologie, anthropologie, etc.), et elle est modulable en fonction du type de catastrophe. Selon la typologie de la mission d'identification (incendie, carambolage, explosion, etc.), d'autres experts peuvent se joindre à l'équipe. L'UGIVC peut également compter sur le renfort de médecins légistes ou de dentistes (d'active ou de réserve) du Service de santé des armées.

Créée en 1992 à la suite de l'accident du mont Sainte-Odile, l'UGIVC a depuis été déployée à plus de cent reprises en France, outre-mer et à l'étranger, majoritairement dans une cadre judiciaire, mais également dans des procédures extrajudiciaires (ou administratives), notamment pour l'identification de Français décédés à l'étranger.

L'**identification des victimes** de catastrophes est délicate pour plusieurs raisons. L'ampleur de l'événement joue sur la sensibilité de l'opinion publique, et donc sur le traitement médiatique en de pareilles situations. La présence de victimes de différentes nationalités ajoute nécessairement un volet diplomatique à la mission. Ainsi, l'UGIVC répond à une méthodologie stricte et s'appuie sur des **recommandations d'INTERPOL**.

Le principe de l'identification des victimes repose sur une analyse comparative d'informations (données dentaires, empreintes digitales, ADN, etc.) collectées sur le site de la catastrophe (données *post mortem*) avec ces mêmes informations, cette fois relatives à la personne disparue de son vivant (données *ante mortem*). Elle permet l'**identification formelle des victimes et la restitution des corps à leurs proches**. Cette mission nécessite de déployer simultanément différentes

équipes distinctes permettant le traitement du site de la catastrophe (relevé des corps et des éléments d'information), la réalisation des opérations d'autopsie ainsi que la collecte des informations *ante mortem* auprès des familles, des médecins ou des dentistes traitants.

L'UGIVC assiste également ses homologues étrangers pour la collecte d'informations *ante mortem* ou *post mortem*. Enfin, elle est impliquée dans différents groupes de travail, notamment INTERPOL, et participe régulièrement à des séminaires en France ou à l'étranger sur l'identification de victimes.

Voici quelques interventions majeures de l'UGIVC :

- 20 janvier 1992 : un Airbus A320 s'écrase sur le mont Sainte-Odile (Bas-Rhin), causant la mort de 87 passagers. L'IRCGN crée alors la Cellule d'identification de victimes de catastrophes (CIVC).
- 24 mars 1999 : un incendie dans le tunnel du mont Blanc (Savoie) provoque la mort de 39 automobilistes.
- 27 juillet 2000 : un avion Concorde d'Air France s'écrase à Gonesse (Val-d'Oise) peu après son décollage; 117 victimes seront recensées (passagers et occupants d'un hôtel).
- 26 décembre 2004 : un tsunami d'une rare violence ravage l'Asie du Sud-Est et une partie de l'océan Indien; 184 000 victimes seront recensées.
- 1^{er} juin 2009 : un Airbus A330 reliant Rio de Janeiro à Paris s'abîme dans l'océan Atlantique avec 228 passagers et membres d'équipage.
- 24 juillet 2014 : un avion McDonnell Douglas MD-83 s'écrase au Mali, causant la mort des 118 personnes à bord.
- 24 mars 2015 : un Airbus A320 de la compagnie Germanwings s'écrase sur le massif des Trois-Évêchés dans les Alpes-de-Haute-Provence, causant la mort de 150 passagers et membres d'équipage.
- 23 octobre 2015 : une semi-remorque entre en collision avec un autocar à Puisseguien, en Gironde; 43 corps seront dégagés des carcasses calcinées.

- 14 novembre 2015 : le déraillement d'une rame de TGV test à une dizaine de kilomètres de Strasbourg provoque la mort de 11 personnes.
- 20 novembre 2015 : une fusillade, suivie d'une prise d'otages à l'hôtel Radisson Blu de Bamako (Mali), fait 22 morts.
- 15 janvier 2016 : l'attaque contre un restaurant et un hôtel d'Ouagadougou fait 29 morts.

L'Unité nationale d'investigation criminelle

L'exploitation des indices matériels constitue un maillon essentiel de l'enquête judiciaire. Lorsque l'ampleur, la complexité ou le caractère épineux d'une affaire dépasse les moyens départementaux de la Gendarmerie nationale, magistrats et enquêteurs ont la possibilité de demander le soutien de l'Unité nationale d'investigation criminelle (UNIC), subordonnée au Pôle judiciaire de la Gendarmerie nationale.

L'UNIC est composée d'experts de l'IRCGN (gel de l'état des lieux, empreintes digitales, génétique, balistique, microtraces, informatique, électronique, traces de sang, faune-flore, etc.). Elle est modulable en fonction du type de scène de crime à traiter et des besoins du directeur d'enquête. Dotés d'un équipement de pointe, les experts de l'UNIC apportent leur expertise, complémentaire au travail des équipes techniques locales. En effet, cette synergie avec les techniciens en identification criminelle (TIC) départementaux, avec d'autres unités spécialisées telles que la Cellule nationale d'investigation cynophile de la Gendarmerie (équipe dotée de chiens de recherche de cadavre) et avec les techniciens en identification subaquatique (TIS) apporte une réelle valeur ajoutée au **traitement de cas complexes**.

Le chef de l'UNIC coordonne l'action du personnel déployé, en concertation avec le coordinateur local des opérations de criminalistique. Ce coordinateur des opérations de criminalistique (COCRIM) assure un lien nécessaire entre le directeur d'enquête, le directeur des opérations, les scientifiques et les magistrats.

L'UNIC participe à la **formation** du personnel de la Gendarmerie (techniciens, enquêteurs) ou des magistrats.

Cette unité maintient une ouverture constante vers l'extérieur, participant régulièrement à des groupes de travail et à des séminaires sur le traitement de scènes de crime, en France ou à l'étranger. L'UNIC, c'est ainsi **plus de 200 interventions par an sur des scènes de crime** en France métropolitaine ou outre-mer, voire à l'étranger.

L'UNIC est dotée d'**équipements spécifiques et d'appareils sophistiqués transportables** permettant aux experts de mener à bien leur mission, et ce, quelles que soient les circonstances. À cet effet a été conçu un laboratoire d'analyse projetable au plus près de la zone de travail : le **Lab'UNIC**. Il est composé d'un poste de commandement et il est doté de liaisons radio et satellite, ainsi que d'un espace d'analyse modulable et en totale autonomie énergétique.

Le Groupe d'investigations en milieu dégradé

La Cellule nationale nucléaire, radiologique, biologique et chimique de la Gendarmerie nationale (C2NRBC), unité stratégique pour la Gendarmerie nationale, porte l'expertise en milieu contaminé et dimensionne ou complète la capacité d'action des unités de recherche de la Gendarmerie dans le traitement de ce type particulier de scène d'investigations.

L'activation de la C2NRBC permet au personnel de l'IRCGN de mener les levées de doutes, les constatations et les investigations. Ces dernières années, cette synergie opérationnelle s'est consolidée par la croissance des interventions à caractère judiciaire, assurant ainsi une réponse criminalistique cohérente et globale.

Dans le cadre de scènes d'intérêt en ambiance dégradée, l'IRCGN a développé une expertise en partenariat avec la C2NRBC : le Groupe investigation en milieu dégradé (GRID).

Le GRID participe à des exercices qui ont permis l'élaboration de protocoles d'intervention en milieu contaminé et développé cette capacité supplémentaire de constatations en ambiance dégradée. Il a été déployé à plusieurs reprises en milieu hostile (traitement de scènes de crime ou autopsies).

L'IRCGN, par l'entremise du GRID, a également mis en place un programme de formation spécifique à l'identification de victimes de catastrophes en milieu contaminé qui est

complété par des exercices de mise en situation pour chacune des composantes (*ante mortem*, *post mortem*, etc.). À cette occasion, tous les équipements (techniques, logistiques, analytiques, informatiques, etc.) sont déployés, testés et utilisés, y compris dans les domaines de l’alerte et de la mise en route du personnel. Près de 150 militaires d’active et de réserve sont ainsi formés et recyclés chaque année. Le personnel du GRID, issu des divisions criminalistiques, appartient à des spécialités couvrant la majorité du spectre analytique : physique-chimie, numérique et identification. Ces balisticiens, informaticiens, chimistes ou biologistes sont habilités au port d’équipements de protection individuelle (appareil respiratoire individuel, scaphandre, etc.) et s’entraînent à la mise en œuvre d’actes de constatation et de révélation dans ces différents domaines.

Le modèle d’intervention de l’IRCGN repose sur l’accomplissement d’un maximum d’actes techniques sur des éléments de preuve contaminés, d’identification de victimes (médioclégaux) et de transferts d’information d’intérêt judiciaire depuis la zone d’exclusion. Cette approche est motivée par l’urgence de mettre à disposition des informations destinées aux magistrats et aux enquêteurs, mais aussi en raison du risque de perte d’informations (traces et indices) et des délais générés par des opérations de décontamination préalables à une exploitation en laboratoire conventionnel. Une chaîne de traitement criminalistique est ainsi déployée sur zone, de même qu’une chaîne d’identification de victimes.

L’état de la menace terroriste impliquant tout type de dispositif appelé communément « bombe sale » demeure important sur le territoire national ainsi qu’en tout lieu où la France a ses ressortissants. L’UNIC peut être appelée à titre de soutien ou de conseil au profit d’un pays étranger. Un engagement constant du maintien de cette capacité opérationnelle et de son haut niveau d’expertise est nécessaire, notamment grâce à la réalisation d’exercices et à sa participation à différents groupes de travail, tant nationaux qu’internationaux.

Grégory Briche, lieutenant-colonel, chef de la Division criminalistique physique et chimie de l’IRCGN, France

2.3.1.8 Entraînement au tir « vidéo assisté »

L’entraînement au tir « vidéo assisté » (EVA^{md}) est un dispositif d’entraînement au tir à balles réelles et de formation, mobilisant des techniques de vidéo-projection peu coûteuses (bois, papier, petit matériel vidéo). Il fonctionne sur le modèle du simulateur et propose aux apprenants des mises en situation leur permettant de réagir, notamment en situation d’agression armée. Le dispositif permet le développement de compétences d’adaptation. En même temps qu’un entraînement au tir, les apprenants sont formés à l’analyse des situations grâce à une pédagogie active qui leur permet de juger la situation. Cet outil pédagogique développe les compétences liées au tir dans des conditions les plus proches possible de la réalité de terrain grâce à un travail de contextualisation effectué en amont de la formation : les lieux de travail habituels des gardiens sont filmés et proposés dans le film.

Explication détaillée

Depuis plusieurs années, la Police nationale était à la recherche d’un outil d’entraînement au tir à balles réelles permettant de travailler le discernement et la prise de décision. L’acuité de la menace terroriste et la définition, par le législateur, de nouveaux cadres légaux d’usage des armes (article L 435-1 du Code de la sécurité intérieure) renforçaient encore ce besoin de contextualisation des séances de tir.

Les simulateurs disponibles sur le marché ne correspondant pas totalement aux attentes, tant en ce qui a trait aux fonctionnalités qu’aux coûts, la Direction centrale du recrutement de la



formation (DCRFPN) a décidé d'investir dans un dispositif développé par un formateur aux techniques et à la sécurité en intervention de la préfecture de police de Paris, le major Pascal Tran. Mis à l'honneur à l'occasion de l'édition 2017 du Prix de l'innovation organisé annuellement par la DCRFPN, le système EVA^{md} permet de professionnaliser l'entraînement au tir des policiers, tant dans leur rapport à l'arme (de poing comme d'épaule) que dans la prise de décision de son usage en offrant une contextualisation de situations de police par l'intermédiaire de vidéos.

À ce titre, le système EVA^{md} présente plusieurs avantages :

- Il autorise le tir à balles réelles;
- Il intègre un simulateur de situations de tir;
- Il est peu coûteux (soit environ 1 000 € pour équiper un champ de tir);
- Il permet de concevoir des scénarios personnalisables tenant compte de l'environnement de travail des agents.

Le dispositif technique repose sur un équipement basique adaptable à la plupart des champs de tir implantés sur le territoire national. Le système EVA^{md} se compose ainsi :

- d'un vidéoprojecteur;
- d'un lecteur vidéo Blu-ray;
- d'une clé USB;
- d'une enceinte amplifiée;
- d'un pointeur laser;
- d'un écran papier.

Les supports vidéo disponibles permettent de travailler deux catégories d'exercices :

— Les exercices de perfectionnement technique

Ces exercices servent à évaluer le niveau des tireurs et permettent par ailleurs de renforcer leur dextérité, leur maîtrise de l'arme et le discernement simple sans prise en compte de l'environnement juridique. À cette fin, ils s'appuient principalement sur l'apparition de cibles imagées prenant la forme de silhouettes humaines de différents gabarits. Le niveau de difficulté varie selon les séries grâce aux mouvements latéraux

ou longitudinaux donnés aux cibles, ou encore à la variation de leur temps d'apparition.

— Les exercices d'entraînement opérationnel et d'immersion de voie publique

Ces exercices sont classés par série, chacune comportant une succession de courtes séquences vidéo (exercices opérationnels) ou d'un unique film d'une durée limitée (immersion voie publique) projetant le ou les tireurs dans une situation d'intervention de police. Le niveau de difficulté est ici établi par la complexité progressive des actions attendues.



Ces exercices ont pour but de développer la capacité d'analyse du tireur, et ce, en prenant en compte tant la menace elle-même que l'environnement. En plus de renforcer les capacités individuelles, ils permettent de travailler la gestion collective de ces situations de police.

Au regard de ces différentes fonctionnalités, une séance de tir utilisant EVA^{md} est constituée d'un ou de plusieurs cycles comportant chacun trois phases :

1^{re} phase : l'évaluation (diagnostic)

Le formateur s'appuie sur le panel de vidéos proposées parmi la catégorie d'exercices de perfectionnement technique ou d'entraînement opérationnel (à l'exclusion des exercices « immersion voie publique ») pour réaliser un diagnostic du niveau de maîtrise technique des tireurs. Lors de cette phase, le choix des vidéos appartient au formateur, en fonction du niveau avéré ou supposé des stagiaires présents.

2^e phase : le renforcement des compétences techniques et juridiques

Le formateur se sert des constats réalisés à l'occasion de la phase du diagnostic pour mettre en place des exercices permettant de renforcer les compétences techniques, tactiques et juridiques des stagiaires. Pour ce faire, les vidéos des deux premières catégories d'exercices peuvent être utilisées, en fonction du niveau du public ou des objectifs pédagogiques poursuivis par le formateur.

3^e phase : la restitution dans l'action

En fonction du niveau du public, la poursuite de la séance intègre l'utilisation de vidéos dites « immersion voie publique » ou « exercices opérationnels ». Le nombre de cartouches servant à cette catégorie d'exercices ne doit pas dépasser un tiers du total des cartouches consacrées à l'ensemble de la séance.

Conclusion

Compte tenu de l'intérêt pédagogique d'EVA^{md} et des retours positifs des premières expérimentations, la DCRFPN a décidé de déployer le dispositif sur une centaine de sites répartis sur tout le territoire national. Ce plan de déploiement s'accompagnera d'une formation spécifique à l'outil des formateurs aux techniques et à la sécurité en intervention (FTSI) qui sont responsables des entraînements au tir. À cette occasion, un guide d'animation sera mis à leur disposition. Par ailleurs, sous réserve de leur validation par la DCRFPN, les FTSI pourront enrichir de manière collaborative la bibliothèque de vidéos disponibles.

Pierre-Henri Machet, *commissaire divisionnaire, chef du Pôle anticipation, analyse, conseil, adjoint à la sous-direction du développement des compétences de la Direction centrale du recrutement et de la formation de la Police nationale, France*

2.3.2 ÉCHANGES

La première partie a été consacrée à la thématique de la lutte contre le terrorisme par sept panélistes. Ils ont tous mis l'accent sur les pratiques formatives proposées dans le cadre de la gestion d'incidents liés au terrorisme avec, comme modérateur, M. Mamadou Ndour, commissaire divisionnaire, attaché au Cadre d'intervention et de coordination interministérielle

des opérations de lutte antiterroriste du Sénégal.

À ce niveau, l'essentiel des échanges part du constat qu'il y a un déficit de coordination dans le cadre de la gestion des menaces terroristes. De ce fait, il a été recommandé de renforcer la coordination et d'assurer une spécialisation continue des unités des forces de l'ordre déjà existantes en unités spécialisées, en lieu et place de la création de nouvelles forces.

Après l'exposé du sujet de chaque intervenant, le modérateur invite l'assistance à verbaliser leurs interventions.

Dans un premier temps, l'intervenant du Mali, le commissaire principal Kante, soulève deux points : le premier est une contribution, alors que l'autre est une observation sur la méthode EVA^{md} présentée par le professeur Bastide.

Le premier point est en rapport avec l'attentat que le Mali a connu le 20 novembre 2015 à l'hôtel Radisson Blu. Ce jour-là, on a noté le manque de coordination entre les forces armées et l'absence de gestion de la zone d'action du côté de la police. À la suite de ce manque de coordination, on a mis en place l'entité FORSAT (Forces spéciales antiterroristes), placée sous la responsabilité du ministre de la Haute Sécurité nationale, dont l'objectif est de mieux coordonner les interventions entre les forces armées, notamment entre la police et la gendarmerie.

L'acte de terrorisme de mars 2016 a donc amené la naissance de cette FORSAT, même si la force était déjà là, en ce sens que les services de police et de gendarmerie étaient fonctionnels. La nouveauté est le regroupement de ces forces dans le cadre d'une menace. Le grand progrès est que l'on n'a plus besoin de passer par le circuit administratif en matière de déclenchement de la menace, lequel peut s'avérer très long et retarder l'intervention de deux à trois heures. Tout ce dispositif de FORSAT mis en place a conduit à la gestion du phénomène en partant des primo-intervenants jusqu'à la force spéciale d'intervention des unités d'ordre de la gendarmerie et de la police.

L'intervenant pose une question en ce qui concerne son deuxième point d'observation. Il s'interroge sur la vidéo projetée sur le dispositif EVA^{md}. La question concerne

l'utilisation des armes de pointe par les policiers dans ce même dispositif.

Le panéliste Pierre-Henri Machet répond à la question posée sur le dispositif EVA^{md} en précisant que même si les scénarios sont adaptables à une arme longue, il faudrait cependant créer un environnement qui permettrait d'utiliser ce genre d'arme.

Par ailleurs, l'idée est de former les primo-intervenants; l'accent n'a donc pas été mis de façon volontaire sur l'arme utilisée dans la mesure où, dans le cadre de travail retranscrit, les agents ne sont pas dotés de ce type d'arme. Dès lors, le travail est axé seulement sur l'arme de pointe.

Un intervenant béninois, secrétaire de brigade dans son pays, intervient sur le film en ce qui concerne la préparation vidéo diffusée par le panéliste suisse. La question posée est celle de savoir pourquoi des agents apprenants évoluent, armes baissées vers le sol, entre un abri et un obstacle, le fait de baisser l'arme pouvant constituer un danger pour l'agent des forces.

Le panéliste suisse répond en indiquant que la formation est destinée au primo-intervenant. Lors de la mise en place d'un scénario avec le personnel des forces, il était pertinent, pour plonger les agents en situation, de mettre des caméras à la place des cibles. Le premier constat est que les situations ne sont pas forcément différentes de celles retranscrites dans le cadre d'une formation traditionnelle. On constate que les agents des forces de l'ordre restent souvent droits, se déplacent lentement et font de bonnes cibles. C'est pour cela qu'on leur impose de rester droits : c'est une pédagogie pour leur permettre de rester sur des stimulus classiques. En effet, une personne ayant vécu les attaques en Israël a fait remarquer, lors de son témoignage, que l'attaquant cherche d'abord à se cacher, donc à se couvrir plutôt qu'à riposter.

Puis, le panéliste revient sur la deuxième question, à savoir pourquoi l'arme de l'agent est dirigée vers le sol. Selon lui, l'arme des agents est dirigée vers le sol simplement parce que c'est l'une des prescriptions standard pour éviter de manœuvrer devant les caméras.

Après la réponse à ces questions par les panélistes, un intervenant d'Ouagadougou a voulu revenir sur l'avant-

dernière communication en ajoutant le fait que l'attaque d'Ouagadougou s'inscrit dans le cadre des nouvelles menaces qu'évoquait au début de la présentation un panéliste policier français. De ce fait, il est bien de la rappeler. L'intervenant précise que l'attaque du Burkina n'était pas une petite réplique. L'intervenant fait également le constat qu'il y a eu les mêmes problèmes de coordination des forces armées que ceux évoqués par les autres panélistes lors de leurs interventions.

En s'appuyant sur le cas du Burkina, l'intervenant fait observer que la gendarmerie et la police ont eu un problème de coordination, si bien que l'attaque a été déclenchée à 20 h, et ces patrouilles sont arrivées trois à quatre heures après le déclenchement de l'attaque.

De plus, les services des forces de différentes composantes de la police et de la gendarmerie ont failli se tirer dessus. En effet, ce risque d'incident entre les services des forces de l'ordre, lié au manque de coordination, a conduit au fait que les services arrivaient dans des directions opposées.

À la suite de cette absence de coordination, les services des forces armées ont pu mettre en place un centre unifié de crise. Il ne s'agissait pas de créer une nouvelle force, mais un centre de coordination qui prend en compte les secours des différentes composantes de l'armée (armée de terre, armée de l'air, etc.).

La mise en place de ce service a permis de revoir la façon de gérer les interventions en cas d'attaque et d'évaluer le service lors de la seconde attaque en août 2017 et en mars 2018. Le constat est positif dans la mesure où le temps d'intervention a été réduit. En effet, la situation a été gérée au maximum en trois heures, comparativement à la première pour laquelle le temps d'intervention était de cinq à six heures.

L'intervenant met fin à son observation par une appréciation des tirs des primo-intervenants diffusés dans la vidéo de l'intervenant français. Selon lui, les tirs permettent de s'adapter à une situation, car il y a du mouvement en tous sens et les personnes courent de gauche à droite : « Il faut donc que les policiers se mettent à l'abri, qu'ils ripostent et qu'ils ne tirent pas sur les personnes qui courent. »

Le policier français panéliste répond, dans un premier temps, sur la réplique qu'il a utilisée lors de sa démonstration. Il indique que la notion de « réplique face à une menace de tout type » n'est pas forcément applicable dans le cadre du terrorisme. Dans le cas de l'exercice, il n'était pas question de terrorisme. Le panéliste partage tout de même la réflexion de l'intervenant sur le fait que les policiers, dans une situation de terrorisme, doivent redoubler de vigilance.

Le panéliste revient sur le fait que pour ce qui est du terrorisme, on peut rajouter l'attentat de Grand Bassam. Au cours de cette attaque, les services de sécurité français ont mis en place des unités d'intervention dans de courts délais. En effet, lorsqu'il y a des victimes françaises dans une attaque terroriste, on mobilise le ministère des Affaires étrangères afin de permettre le déploiement des unités françaises.

Cette mobilisation des services français n'est toutefois pas liée uniquement à la seule présence de victimes françaises; elle s'effectue aussi en présence de victimes d'intervention tant françaises qu'occidentales, ou en présence de victimes originaires du pays pris par l'assaut.

La question suivante est posée par Thierry Dierick au panéliste sur la façon dont la menace est gérée : « Quels sont les services mobilisés en France? »

C'est le panéliste belge qui répond en premier en précisant que la problématique n'est pas de coordonner les services en Belgique. La phase la plus importante et la plus complexe est, selon lui, la phase de réflexion qui, pendant les premières minutes, va être fondamentale. À la suite de cette phase complexe, le panéliste affirme qu'ils ont formé les premiers officiers à s'informer sur ce qu'il y a lieu de faire en situation de crise.

La coordination est simple à Liège : toutes les unités arrivent dans une situation AMOK, mais la rapidité avec laquelle ils participent est l'élément central, car le premier intervenant doit pouvoir renseigner les autres unités, d'où l'importance de former les primo-intervenants à coordonner les premières réactions par rapport aux intervenants. Le panéliste mentionne qu'il y a beaucoup de dispatcheurs (répartiteurs), à savoir des techniciens, qui doivent être formés à organiser les premières

réactions sur le terrain. Il faut donc réfléchir à la façon dont on doit armer les policiers et coordonner l'arrivée des renforts. La Belgique développe actuellement ce programme.

M. Bastide tente de répondre à la question en rappelant brièvement que le plus important est « qu'il faut anticiper, répertorier des lieux possibles pouvant faire l'objet d'éventuelles cibles. Repérer ces lieux permet d'étudier la façon d'être le plus efficace et de mieux réagir lors d'une intervention ».

À propos de la question de la formation des cadres leaders des groupes primo-intervenants, le panéliste précise que « tout le monde n'est pas forcément leader; on développe des formations pour le travail en équipe et en binôme ». Il précise aussi que les primo-intervenants cadres ne peuvent pas forcément tout gérer, car ils n'ont pas toujours l'étoffe de chefs de file. Il faut donc aussi penser à des modèles collectifs de formation, soit en binôme, soit en travail d'équipe.

Le modérateur, M. Mamadou Ndour, conclut sur ce qui a été dit en évoquant le cas du Bissoco, une structure antiterroriste à Dakar. Il explique qu'il n'a pas suffi, pour le Sénégal, de mettre en place une structure de lutte contre le terroriste. Une unité d'intervention conduite par la police et la gendarmerie a été ajoutée à cette structure dans une optique de cohésion des forces de l'ordre.

À la suite de ce constat, le modérateur formule des observations d'ordre général, s'adressant à tous les congressistes sur la perfectibilité de leurs systèmes :

Il faut que les modalités d'intervention soient définies, sinon on se retrouve face à un système flou.

La connaissance de la cible est importante dans le cadre d'une intervention, car tout dépend de cette cible [avec le terme « cible », ici, le modérateur fait allusion à la maîtrise des lieux susceptibles d'être attaqués].

En effet, la qualité d'une intervention dépend du fait que la cible est protégée ou non. Si la cible est protégée, c'est-à-dire qu'il s'agit d'un quartier où les forces de l'ordre sont présentes et où le lieu est connu des forces de sécurité, la primo-intervention est conduite par les forces de sécurité en appui à la structure d'antiterrorisme. Quand l'attaque a

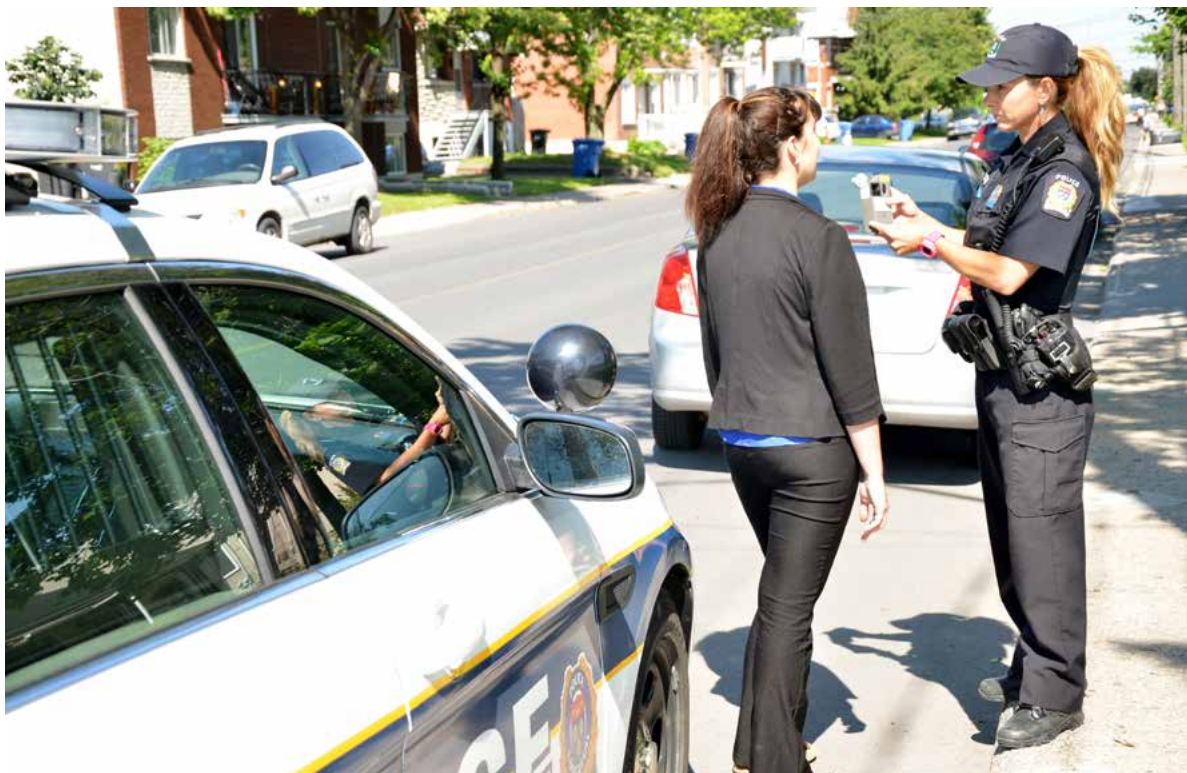
lieu sur une cible qui n'est pas protégée, la mise en place des dispositifs liés à l'antiterrorisme avec la coordination des forces de l'ordre ne peut pas être la même sur les primo-intervenants.

Quand on pousse le débat plus loin, il y a des sites qui ne font pas l'objet d'un dispositif global, comme c'est le cas à l'intérieur du pays. Dans ce cas, il faut une anticipation. Il faut également que les intervenants soient formés à ce genre de situation liée au changement de la circonférence géographique. C'est pour cela qu'il faut voir depuis la base une unité d'intervention.

Mais l'action terroriste requiert la rapidité, et toute l'action réside dans le temps et la capacité opérationnelle à pouvoir soutenir une intervention de telle envergure. C'est pourquoi il faut produire un aide-mémoire pour déterminer la responsabilité de chaque

intervenant et la procédure à suivre. Au Sénégal, on dispose de plusieurs cadres interministériels; on a même un cadre régional conçu avec le Cadre d'Intervention et de Coordination interministériel des Opérations de lutte anti-terroriste (CICO). Ces cadres permettent de mettre en place une organisation qui entoure tout le monde lorsqu'il y a une attaque terroriste. Il a été révélé que lorsque les brigades spécialisées ont fait appel aux trois forces armées au cours d'une intervention, le résultat final parvient à une coordination et à une cohésion de l'opération, mais seulement dans le cas où toutes les forces sont coordonnées. Il faut donc, afin de trouver une réponse rapide, se coordonner, établir un cadre pour arriver à apporter une réponse efficace au terrorisme dans les pays respectifs des différents intervenants.

C'est sur ces derniers mots que M. Thierry Dierick met fin à la matinée en invitant les congressistes à déjeuner.



3. CYBERCRIMINALITÉ

3.1 INTRODUCTION

– IMAGE DU PHÉNOMÈNE

C'est avec beaucoup d'honneur que j'interviens devant cette assemblée d'experts pour ouvrir les débats sur la problématique de cybercriminalité qui nous tiendra encore en haleine pour des décennies.

Aussi allons-nous aborder l'image du phénomène de la cybercriminalité en faisant d'abord un bilan succinct. Ensuite, nous vous ferons parcourir les réponses apportées par la Côte d'Ivoire pour endiguer le **fléau transfrontalier qu'est la cybercriminalité**.

I. LE CONSTAT : UNE CYBERCRIMINALITÉ EN EXPANSION

La cybercriminalité s'est propagée comme la peste sous l'impulsion du triptyque de l'Internet, des nouvelles technologies et de la numérisation. Les cyberattaques ont affecté les personnes physiques et morales, les États, les institutions publiques et privées, nationales et internationales, ainsi que les activités primaires, secondaires et tertiaires⁷. Avec les bouleversements géopolitiques, socioéconomiques, industriels et, surtout, technologiques, la cybercriminalité s'est métamorphosée en cyberdjihadisme, en cyberterrorisme, en cyberpédophilie, en crise migratoire, en cryptovirus, en blanchiment d'argent, etc., complexifiant ainsi les menaces encourues par la communauté des nations.

Devant toute cette cybercriminalité, les combats pour la sécurité humaine et la paix mondiale ne trouveront de solutions efficaces que dans des forums internationaux. Ceux-ci donnent l'occasion de partager des expériences et des connaissances pour aboutir à la synchronisation de la lutte sur le plan international.

C'est pourquoi je saisis cette occasion pour remercier FRANCOPOL, qui a eu l'ingéniosité de réunir des experts sur des thématiques de sécurité. Les défis majeurs s'amoncellent, entraînant de nombreux questionnements relativement à la migration humaine et technologique, à l'harmonisation des textes de loi, à la capacité opérationnelle⁸, au choc des intérêts stratégiques, à la politique de collecte des données à l'égard de la protection des libertés et des droits fondamentaux des personnes, à l'extranéité des preuves et à la coopération des fournisseurs d'accès (la question des géants du Web, soit Google, Apple, Facebook et Amazon [GAFÀ]). À cette liste non exhaustive d'équations se superposent les attermoissements à la mise en œuvre des conclusions et des recommandations des ateliers et des colloques.

II. LA RÉPONSE DE LA CÔTE D'IVOIRE DANS LA LUTTE CONTRE LA CYBERCRIMINALITÉ

Pour sa part, la Côte d'Ivoire a répondu à la lutte contre la cybercriminalité en adoptant une série de lois et en instituant des organes de gouvernance. Ainsi, une série de lois ont principalement été adoptées en 2013, et des institutions ont été créées, dont la Direction de l'informatique et des traces technologiques (DITT).

Démembrement de la Police nationale, la DITT a pour mission non seulement de fournir les preuves numériques, mais aussi de soutenir les actions des services de la police, de la gendarmerie et de la justice au moyen de méthodes technologiques. Elle s'est donc structurée autour de la technologie, de l'investigation et du soutien aux investigations. Ces tâches ont été confiées au Service de conduite de projets, au Laboratoire de criminalistique numérique (LCN) et à la Plateforme de lutte contre la cybercriminalité (PLCC) mise en place par convention avec l'Autorité de régulation des télécommunications de Côte d'Ivoire (ARTCI) et son agence de résilience Côte d'Ivoire Computer Emergency Response Team (CI-CERT). Grâce à cette structuration, la DITT se place au centre de la lutte contre la cybercriminalité en Côte d'Ivoire.

7. Même les structures de protection informatique ont été victimes de cyberattaques (voir <http://www.lenetexpert.fr/kaspersky-annonce-etre-victime-d-une-cyberattaque-le-net-expert-informatique>).

8. Chaque État y va avec ses capacités, les stratégies étant différentes. Les États-Unis sont en voie de dégager 50 milliards de dollars pour lever une armée du cyberspace.

Dans le cadre de cette lutte, la DITT mène des actions de répression contre les cybercriminels, essentiellement des cyberescrocs. Mais, avant tout, elle a axé ses efforts sur la coopération ainsi que sur la communication et la sensibilisation. Elle a aussi développé des activités qui lui permettent de participer activement à la sécurité des personnes. L'on peut citer le réseau de communication LTE, la vidéo de protection et la flotte de drones dont elle s'est dotée. Ces acquisitions lui font bénéficier de la confiance des autorités qui lui ont confié la surveillance de deux événements majeurs tenus à Abidjan en 2017 : celle du 5^e Sommet Union africaine-Union européenne ainsi que celle des Jeux de la Francophonie.

Relativement à la coopération, la DITT s'est attelée à construire un réseau d'actions avec les institutions et les organes nationaux du secteur public, et elle n'a pas manqué d'y associer aussi ceux du secteur privé. Sur le plan international, la DITT collabore constamment avec les ambassades, les services de police étrangers, les organisations et les agences internationales, dont FRANCOPOL. Elle a ainsi bénéficié de formations et de retours d'expérience qui lui ont permis d'enrichir ses actions. Elle s'est mise à la disposition de la sous-région, de la région et du monde à travers des formations, et des conduites de dossiers dans l'éradication des cybercriminels, communément appelés les « brouteurs »⁹ (affaire Patrick Paré, interpellation des djihadistes au Niger, etc.). Elle a fait de la coopération « police à police » un axe principal de l'entraide judiciaire. Une invitation particulière est faite aux acteurs du secteur privé, principalement les GAFAs, détenteurs des données et des preuves électroniques, en vue d'aider à dynamiser la cybersécurité. Ce partenariat avec le privé demeure un des éléments à parfaire.

Enfin, la DITT a beaucoup misé sur la prévention dans son combat contre la cybercriminalité. C'est pourquoi notre Direction a mis en avant la communication et la sensibilisation. Ainsi, des ateliers et des séminaires de formation et d'information sont organisés pour les populations cibles. Des publications dans les médias de masse et sur les réseaux sociaux sont constamment utilisées. Des productions cinématographiques commanditées ou produites sont des voies déjà explorées. Dans une logique de prévention, la DITT

s'est donné les moyens de faire des patrouilles technologiques pour anticiper certains phénomènes sociaux.

J'ai l'espoir que les questions énumérées ci-dessus seront abordées au cours de ces assises et que les résolutions seront mises en application. La Côte d'Ivoire et la DITT, quant à elles, restent à votre disposition pour contribuer à rendre notre monde un peu plus sûr.

Augustin Ochogni, commissaire en charge des questions juridiques et de la coopération à la Direction de l'informatique et des traces technologiques, Côte d'Ivoire

3.2 PRATIQUES INSPIRANTES

3.2.1 Présentation des travaux du comité technique sur la cybercriminalité de FRANCOPOL

Historique

Le comité technique sur la cybercriminalité a été créé peu de temps après la naissance de FRANCOPOL, en 2008. Ayant été très dynamique pendant plusieurs années, le groupe a complètement changé entre 2014 et 2016. En juin 2017, une réunion regroupant certains nouveaux membres a eu lieu à Paris. Ce fut l'occasion de tisser des liens et d'orienter les actions futures vers une vision commune.

L'année 2019 servira à ce groupe de travail à poursuivre sa reconstruction tout en consolidant ses liens. L'ajout de membres, notamment en provenance d'organisations policières et académiques œuvrant dans des pays actuellement absents du comité, est souhaitable. Notons également qu'actuellement, les femmes sont sous-représentées. Il serait donc opportun d'encourager l'adhésion de ces dernières, et ce, afin d'élargir la vision du groupe de travail. Nul besoin de préciser qu'en matière de cybercriminalité, la complémentarité des connaissances acquises par les membres d'une équipe de travail doit être valorisée.

9. Affaire Patrick Paré, un exemple de coopération ivoiro-canadienne.

Projets 2019

Le comité technique sur la cybercriminalité a actuellement le projet d'organiser une journée thématique « cyber » en marge de la réunion ICANN 66 (Internet Corporation for Assigned Names and Numbers) qui se tiendra à Montréal, au Canada, du 2 au 7 novembre 2019. Bien que les membres du comité soient tous ouverts à cette proposition, d'autres idées sont actuellement discutées, telles que la tenue de séances de formation dans les pays du continent africain.

Jean Lafrenière, capitaine et coordonnateur du comité technique sur la cybercriminalité de FRANCOPOL, responsable du Service des projets d'enquêtes spécialisées, Québec, Canada

Introduction

La cybercriminalité est une matière transversale. Il existe bien entendu des spécificités en fonction de la région géographique, et le Sud a ses propres particularités, par exemple « l'escroquerie nigériane ».

D'autre part, hormis les crimes et les délits visant le système informatique lui-même (piratage, sabotage informatique), la cybercriminalité reste, la plupart du temps, la transposition numérique des infractions ordinaires, avec toutefois ses propres caractéristiques.

Parmi celles-ci, la volatilité de la preuve numérique, l'instantanéité des transmissions électroniques, l'aspect international par nature, avec ce que cela sous-entend comme difficultés pour la collecte de la preuve et la poursuite des auteurs.

Tous les services d'enquête, lorsqu'ils sollicitent aujourd'hui les fournisseurs de services Internet (FSI), et principalement les FSI majeurs tels que Facebook, Twitter, Google, Microsoft et Apple, sont tributaires de la seule bonne volonté de ces FSI pour obtenir une réponse à une réquisition.

La nécessité d'une adaptation d'un cadre légal au niveau international s'impose devant cette façon de travailler. À ce sujet, la Commission européenne travaille actuellement à l'élaboration d'une « proposition de production » devant permettre aux États d'imposer aux FSI de répondre aux réquisitions portant sur les données d'identification, les

historiques de connexion, mais aussi les données de contenus. Il va de soi que ce serait une avancée majeure, du moins pour les pays de l'Union européenne.

Il convient aussi de souligner l'importance de ratifier la Convention sur la cybercriminalité, communément nommée convention de Budapest, pour permettre les échanges bilatéraux entre les pays dans la lutte contre la cybercriminalité.

La formation

L'investigation numérique nécessite des compétences techniques approfondies et des formations continues.

Elle nécessite aussi des standards pour l'uniformisation des méthodes de travail. Ces standards ne peuvent que faciliter les échanges et le partage des informations policières entre les pays.

L'approche de la **formation** doit être **intégrale** et **intégrée**.

L'approche **intégrale** comprend les formations de base, intermédiaires et expertes (p. ex. : analyses de supports de données, réseaux informatiques, cryptomonnaies, Internet des objets, recherches en sources ouvertes [OSINT], etc.).

L'approche **intégrée** vise à sensibiliser et à former les premiers intervenants à repérer les éléments numériques potentiellement utiles à une enquête et à geler une situation en attendant l'arrivée des spécialistes. Les magistrats aussi doivent être informés des mesures à prendre ainsi que des procédures nationales et internationales.

Les écoles de police, la gendarmerie et les écoles de magistrature ont donc un rôle très important à jouer dans cette matière tout aussi incontournable que quotidienne.

Rapprochement du comité technique sur la cybercriminalité avec l'Association francophone des spécialistes de l'investigation numérique

Le comité technique sur la cybercriminalité souhaite effectuer un rapprochement avec l'Association francophone des spécialistes de l'investigation numérique (AFSIN) en permettant des échanges à instaurer au travers de tables rondes ou d'autres types de collaboration en rapport avec

l'investigation numérique et la lutte contre la cybercriminalité.

L'AFSIN est une association française dite « Loi 1901 », soit une association sans but lucratif.

Bien que le siège social soit situé en France, cette association a bel et bien une vocation internationale; elle a pour mission de développer une réflexion permanente en langue française sur l'investigation numérique en tous domaines, en toutes circonstances et sous tous ses aspects scientifiques, techniques, philosophiques, déontologiques, méthodologiques, économiques, juridiques, évolutifs et comparatifs avec les autres pays francophones, le tout grâce à un dialogue constant entre les différents participants, techniciens, juristes. En revanche, elle n'a pas pour but d'effectuer des investigations ni de se substituer aux activités de ses membres.

Les critères d'admission de l'AFSIN sont les suivants :

- Être membre d'un service d'investigation de l'État (Intérieur, Défense, Finances, Justice, etc.), être magistrat, expert judiciaire ou être issu du monde académique et œuvrer dans le domaine de l'investigation numérique.

Ou, pour ceux qui ne répondent pas à ces critères, mais qui souhaitent néanmoins faire partie de l'association :

- Être parrainé par au moins deux membres de l'association;
- Être francophone ou savoir s'exprimer en français.

FRANCOPOL et l'AFSIN partagent les mêmes objectifs, à savoir :

- Partager;
- Diffuser;
- Échanger;
- Développer;
- Communiquer en matière de bonnes pratiques et d'utilisation de logiciels d'aide à l'investigation numérique.

D'autre part, l'AFSIN compte parmi ses membres fondateurs des services ou des institutions tout à fait semblables à ceux de FRANCOPOL.

Comme le déclarait la vice-présidente associative de FRANCOPOL, M^{me} Cazaux-Charles, en ouverture du 5^e Congrès international, FRANCOPOL vise une approche globale de la sécurité.

Le comité technique sur la cybercriminalité et l'AFSIN visent un sous-objectif de cette déclaration, soit une approche globale en matière de cybercriminalité.

Devant tant de points communs, y compris la langue française, il serait dommage de ne pas profiter de cette possibilité de partenariat entre le comité technique sur la cybercriminalité et l'AFSIN.

N'oublions pas que le partage de la connaissance accroît l'efficacité!

Rédaction d'un glossaire d'acronymes informatiques

Ce glossaire français/anglais et anglais/français compte plus de 2 300 définitions; il vise à combler la carence de documentation en français dans le domaine de la cybercriminalité.

Ce projet était validé par l'Organisation internationale de la Francophonie (OIF), qui a dégagé un budget pour l'édition de ce document (mise en page, conception, etc.).

La rédaction a été assurée par le capitaine Stéphane Robinot de la Police nationale, Sous-direction de la lutte contre la cybercriminalité (SDLC).

La langue de l'informatique étant dominée par l'anglais, ce glossaire sera certainement une aide appréciable pour mieux appréhender certains termes techniques anglophones.

Il sera utile à l'enquêteur qui pourra par ailleurs documenter ses constatations avec des définitions en français, mais nul doute qu'il sera aussi utile au procureur, au juge d'instruction et, enfin, au juge de fond.

Ce glossaire pourra être mis à la disposition de tous les membres de FRANCOPOL par l'entremise de la plateforme CFIS (Carrefour FRANCOPOL de l'information et du savoir).

*Serge Houtain, chef de service RCCU-CTI,
Police judiciaire fédérale de Mons-Tournai, Belgique*

3.2.2 Présentation de la Division spéciale de cybersécurité

La révolution numérique gagne du terrain dans toutes les sphères du monde moderne. Les sociétés profitent du cyberspace pour leur développement technologique, mais cette dépendance croissante au cyberspace a engendré de nouveaux risques : compromission de données et de systèmes clés, attaques informatiques, cyberterrorisme. Les criminels organisés et les terroristes exploitent les failles technologiques. Les cybercriminels mènent des activités illicites contre lesquelles l'État, à travers ses services régaliens chargés de la sécurité, doit faire face pour préserver la sécurité nationale. Pour lutter contre le phénomène de la cybercriminalité, la Police nationale du Sénégal a mis en place une unité spécialisée nommée **Division spéciale de cybersécurité**.

Cette division, qui s'inscrit dans la volonté de l'autorité à définir une bonne stratégie de lutte contre les cybermenaces, a été créée dans le cadre de la coopération franco-sénégalaise au sein de la Direction de la Police judiciaire. Elle est le fruit des mutations opérées dans le dispositif de la Police nationale en matière de cybercriminalité.

D'abord Brigade spéciale de lutte contre la cybercriminalité en 2013 et logée au sein de la Division des investigations criminelles dont j'ai l'honneur d'être membre fondateur, elle est ensuite devenue une unité autonome rattachée directement à la Direction de la Police judiciaire.

1. Résumé des missions de la Division spéciale de cybersécurité

Le but de cette nouvelle entité est de répondre aux exigences de la prévention et de la répression du phénomène, et de faire face aux défis que la lutte commande, notamment la lutte contre la montée du terrorisme et la criminalité transnationale organisée.

La cybersécurité est ainsi devenue un enjeu à la fois gouvernemental, citoyen et entrepreneurial, et elle soulève des dimensions qui expliquent la volonté des autorités de créer cette nouvelle division pour empêcher toute tentative de déstabilisation intérieure, notamment par l'entremise des systèmes d'information.

De nos jours, le numérique se superpose au monde physique et l'inonde progressivement. Il bouscule les processus de conception et les règles de procédures en matière de police judiciaire et administrative, et surtout en matière de collecte de renseignements.

Pour être toujours en phase avec cette transformation numérique, la Police nationale, à travers cette division, entend adapter son dispositif tout en composant avec d'autres acteurs, entreprises et sociétés civiles.

Une telle approche lui permet d'anticiper les risques, de prévenir les menaces à l'ordre public ainsi que celles liées à la criminalité transfrontalière organisée sous toutes ses formes et, le cas échéant, de réprimer les auteurs de ces infractions.

2. Organisation générale et fonctionnement

La Division spéciale de cybersécurité est organisée de la manière suivante :

- **Une section opérationnelle**, composée d'enquêteurs spécialisés dans les infractions spécifiques aux technologies de l'information et des communications (TIC), et celles qui sont facilitées par les TIC.
- **Une plateforme d'assistance technique, nommée « Laboratoire national de criminalistique informatique » (LNCI)**, spécialement équipée d'équipements et de logiciels d'investigation, assure l'assistance aux services d'enquêtes et la formation des enquêteurs spécialisés en criminalité informatique. À l'aide de moyens techniques et de son expertise, elle assiste les services dans le cadre de la recherche de preuves électroniques, notamment à l'audit ainsi qu'à l'analyse des systèmes d'information, des supports ou des périphériques tels que les disques durs d'ordinateurs, les téléphones et autres supports de stockage.
- **Une cellule d'analyse et de documentation opérationnelle nommée « Veille technologique et de la documentation opérationnelle »** qui traite les informations des services dans le domaine de la cybercriminalité. Cette entité procède à l'analyse

générale des informations qui lui sont communiquées et met en œuvre une analyse criminelle sur la base d'un mode opératoire spécifique de l'activité d'un groupe de cybercriminels identifiés ou non. Elle a pour rôle d'assurer le partenariat à l'échelle nationale et internationale avec d'autres agences d'application de la loi, les services de coopération judiciaire, les fournisseurs d'accès et les intermédiaires techniques. Elle constitue le point de contact de la convention de Budapest.

— **Le Centre de formation à vocation interministérielle et internationale** a pour but de former les forces de sécurité et de défense, les acteurs de la justice ainsi que les entreprises des secteurs publics et privés, de renforcer les capacités des acteurs et de participer à la sensibilisation de la population, de la société civile, des universitaires et des élèves. Le Centre de formation en rapport avec la cellule d'analyse et de documentation élabore et publie également des guides en matière d'investigations numériques et de cybersécurité.

— **Une plateforme de renseignement appelée « Cyberpatrouille »**, composée de fonctionnaires spécialisés qui sont chargés d'infiltrer les réseaux et le *dark Web*, de collecter des informations, et de procéder à l'analyse qualitative permettant de comprendre et d'anticiper les modes de pensée et d'action terroristes. Cette plateforme permet de détecter des contenus liés au terrorisme ou à son apologie, aux actes ou aux propos racistes, aux appels à la violence ou à la désobéissance civile, aux propos de nature à compromettre la sécurité publique et la stabilité nationale, et aux contenus pédopornographiques.

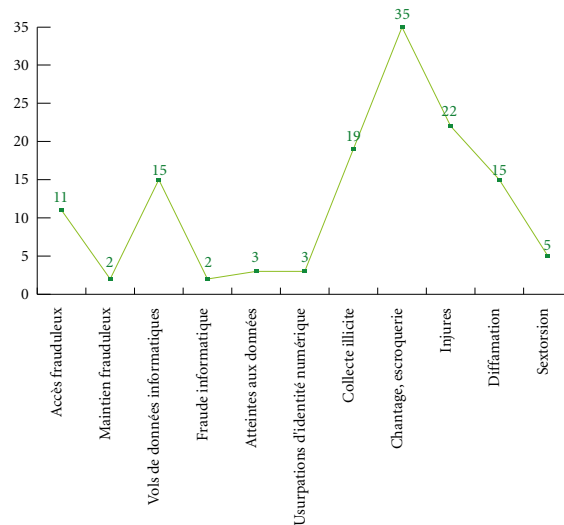
— **Une plateforme de signalement et de téléphonie en cours d'installation** a pour objectif de permettre à toute personne de dénoncer, de manière anonyme, des sites ou des contenus contraires aux lois et aux règlements. Dès lors que des contenus sont qualifiés juridiquement, et donc répréhensibles, ils sont transmis et traités par des services de police territorialement compétents.

3. Quelques statistiques

- Le nombre de personnes dénoncées : 125 (nationalités, genres et âges différents);
- Demandes d'assistance technique : 109;
- Supports analysés : 240.

Typologie des infractions constatées par la division spéciale de cybersécurité

- Accès frauduleux (piratage des systèmes bancaires avec des ramifications internationales);
- Maintien frauduleux;
- Vol de données informatiques;
- Fraude informatique;
- Atteinte aux données;
- Usurpation d'identité numérique;
- Collecte illicite, traitement déloyal de données à caractère personnel;
- Atteinte à la vie, à l'image, à la dignité, à la réputation et à la représentation des personnes;
- Chantage, extorsion et escroquerie;
- Acte de propagande, désinformation de nature à troubler la sécurité publique;
- Injures et diffamation par l'entremise des systèmes d'information.



Niveau mensuel des infractions

Perspectives

- Extension du service d'enquêtes;
- Rénovation du laboratoire national de criminalistique informatique;
- Poursuite de la mise en place de la plateforme de signalement et de téléphonie;
- Renforcement de la coopération nationale, régionale et internationale dans les domaines public et privé;
- Formation des premiers intervenants;
- Mise en place d'antennes dans les régions.

*Dr Papa Gueye, commissaire de police,
chef de la Division spéciale de cybersécurité, Sénégal*

3.2.3 Présentation de l'École nationale à vocation régionale

Au Sénégal, le secteur numérique a fait l'objet d'une stratégie intitulée Sénégal numérique 2016-2025 afin de soutenir l'industrie informatique et de promouvoir la confiance numérique par la mise en œuvre de mécanismes de sécurité. Ces mécanismes permettent notamment d'assurer une veille des cybermenaces afin de prévenir les actes de cybercriminalité et de les réprimer.

C'est dans ce cadre que le chef de l'État sénégalais a mis en place le dispositif suivant pour assurer véritablement une gouvernance de la sécurité, traduisant ainsi une volonté de diriger et de piloter la sécurité pour dominer les risques liés au numérique :

- La Politique de sécurité des systèmes d'information de l'État du Sénégal (PSSI-ES), avec l'instruction présidentielle n° 003/PR du 3 janvier 2017;
- La Stratégie nationale de cybersécurité du Sénégal (SNC2022) qui articule la vision et les objectifs du Sénégal en matière de cybersécurité : « En 2022, au Sénégal, un cyberspace de confiance, sécurisé et résilient pour tous »;
- Un projet de loi d'orientation sur la cybersécurité qui permettra d'adopter, entre autres, une loi sectorielle sur la cybercriminalité;
- La création, par le décret no 2018-683 du 27 mars

2018, à Dakar, d'une École nationale de cybersécurité à vocation régionale, en partenariat avec la France, pour répondre aux menaces exercées à travers les usages malveillants du cyberspace et des outils numériques.

Il s'agit d'un projet d'une importance capitale annoncé par Son Excellence, M. Jean-Yves Le Drian, ministre de l'Europe et des Affaires étrangères français, à Dakar, lors du 4^e Forum international 2017 sur la paix et la **sécurité** avec, comme vision, « qu'il faut faire en sorte que la cybersécurité soit prise en compte par les autorités africaines et que cet enjeu soit parmi les priorités du futur. C'est un espace sur lequel la souveraineté étatique doit pouvoir s'établir ».

L'École est ancrée institutionnellement au plus haut sommet de l'État du Sénégal (présidence de la République), compte tenu de sa dimension nationale et internationale, et elle est hébergée, à titre provisoire, à l'École nationale d'administration (ENA) en attendant l'affectation de locaux au niveau du Pôle urbain de Diamniadio.

Les objectifs de l'École nationale de cybersécurité à vocation régionale sont de :

- Renforcer la résilience de la République du Sénégal et des États africains face aux menaces technologiques visant les réseaux d'information par l'offre de formations techniques destinées aux opérateurs responsables de la sécurité informatique, de la lutte contre la cybercriminalité, de l'usage d'Internet à des fins terroristes et du renseignement numérique;
- Contribuer au renforcement de la gouvernance dans le domaine de la cybersécurité et au respect des souverainetés africaines dans le cyberspace par des actions de formation et de sensibilisation adaptées.

C'est donc un établissement public qui s'érige en véritable « Institut africain de cybersécurité » et qui doit commencer à offrir ses formations en 2019.

Le chef de projet et directeur des études de l'école, soit l'expert technique international (ETI), a été désigné avec l'accord de la France. L'expert technique français qui sera responsable

de la formation avec les experts sénégalais a également été désigné. Il en est de même du point focal technique sénégalais.

Ainsi, les principales missions de l'École nationale de cybersécurité sont les suivantes :

- Former et sensibiliser les agents de l'État, le personnel et les auditeurs nationaux et étrangers des secteurs public et privé à la cybersécurité afin d'améliorer leur compréhension des risques et des menaces dans ce domaine;
- Former et orienter régulièrement le personnel des CERT/CSIRT (centres de veille, d'alerte et de réaction aux attaques informatiques) afin qu'il puisse faire face aux cyberattaques les plus sophistiquées;
- Former et orienter périodiquement le personnel des institutions étatiques et de la sous-région afin qu'il ait la capacité et les connaissances pour préparer, protéger, intervenir et effectuer les retours d'incidents;
- Former et orienter en continu le personnel des services de sécurité et celui des autorités judiciaires afin de renforcer leurs capacités et leurs connaissances techniques en vue de traiter des cas de cybercriminalité;
- Former aux investigations numériques et à la manipulation des preuves le personnel des services de sécurité, les autorités judiciaires et les autres organismes nationaux et sous-régionaux œuvrant dans la détection et la poursuite d'actes de cybercriminalité;
- Soutenir, en matière de formation, de recherche et d'innovation en cybersécurité, les établissements des niveaux secondaire et supérieur, en collaboration avec les ministères de tutelle.

L'accent sera mis sur la formation permanente pour permettre au Sénégal et aux autres États africains intéressés de renforcer leur souveraineté numérique.

Pour cet important établissement, il faut tenir compte de certaines exigences :

- Avoir une vision à la pointe de la modernité;
- Avoir une représentation pertinente de l'État du Sénégal en Afrique et dans le monde;
- Avoir une école vivante et une formation graduée;
- Offrir un plateau technique de haut niveau aux auditeurs sénégalais et étrangers; ce plateau pourra être mis à la disposition des grandes écoles supérieures de formation, notamment les écoles polytechniques du Sénégal;
- Développer un partenariat privé, notamment dans le cadre de l'acquisition de certains équipements qui coûtent très chers tels que les simulateurs d'attaques;
- Former une équipe pédagogique qui sera composée d'éminents spécialistes (des Sénégalais, des coopérants français, mais aussi des spécialistes de la sous-région).

Au titre de son administration, l'École nationale de cybersécurité comprend :

- Un conseil d'administration;
- Un comité de direction;
- Une direction générale;
- Un conseil d'orientation pédagogique et scientifique;
- Un conseil de discipline.

Le conseil d'orientation pédagogique et scientifique est notamment responsable des orientations pédagogiques et méthodologiques de l'École, et des délibérations sur les questions relatives aux programmes et aux méthodes d'enseignement, ainsi qu'au régime des études. Les programmes de formation sont fixés par arrêté du président de la République (sécurité informatique, lutte contre la cybercriminalité, renseignement numérique et gouvernance de la cybersécurité).

En conclusion, l'École nationale de cybersécurité à vocation régionale permettra au Sénégal et à d'autres pays, notamment africains, de disposer, avec l'appui de la partie française, de cadres et d'opérateurs suffisamment formés pour faire face au terrorisme, aux actes de cybercriminalité et, partant, pour assurer la sécurité numérique et la gouvernance de la cybersécurité.

Dr Babacar Ndaw, *secrétaire permanent*
de la Commission nationale de cryptologie, Sénégal

3.2.4 Primo-intervenants en cybercriminalité

Description sommaire



Devant l'évolution technologique et ses usages par les auteurs d'infractions, la Direction centrale du recrutement et de la formation de la Police nationale (DCRFPN) a conçu, en partenariat avec la

Direction centrale de la Police

judiciaire (DCPJ), une mallette pédagogique destinée aux primo-intervenants en cybercriminalité (PICC) afin de développer leurs compétences liées à la découverte, à la manipulation et à la primo-analyse des supports numériques et des ordinateurs. Les fonctionnaires sont formés à des logiciels spécialisés gratuits mis à jour régulièrement, dont ils seront dotés à l'issue de la formation pour travailler au quotidien. Grâce à des activités concrètes sur les supports numériques, les fonctionnaires apprennent à prendre en compte les matériels numériques dans le cadre des enquêtes et à réaliser une primo-analyse en respectant la légalité et les éléments de preuve. Cette mallette pédagogique vient utilement compléter l'offre de formation de la Police nationale, qui était principalement constituée jusqu'ici d'une formation « experte » de 24 jours réservée aux investigateurs en cybercriminalité (ICC) et d'un module *Enquêter sur Internet et les réseaux sociaux* de cinq jours ouvert à un public large.

Explication détaillée

D'un format court (cinq jours en présentiel), la mallette pédagogique PICC vise à former les enquêteurs ayant satisfait à des tests de prérequis à l'environnement numérique (définition de la cybercriminalité, identification des intervenants spécialisés, identification des principaux supports numériques, etc.) et à la primo-analyse des matériels numériques découverts dans le cadre de leurs investigations, avec une attention particulière portée à la sauvegarde des données volatiles. À l'issue du stage, les enquêteurs sont aptes à déterminer si un support numérique est susceptible d'abriter des informations utiles à l'enquête en cours, sans altérer le support et les données, évitant ainsi toutes les contestations ultérieures. À cette fin, à l'issue de leur formation, les stagiaires sont

formés à l'utilisation de logiciels gratuits téléchargeables à partir d'un espace sécurisé.

La conception de la mallette PICC s'est accompagnée de la recherche de suites logicielles gratuites adaptées aux besoins des enquêteurs en cybercriminalité. Grâce au concours de la Sous-direction de la lutte contre la cybercriminalité (SDLC) de la DCPJ, trois applications répondant aux spécifications ont été ciblées pour servir de base à la formation : DARWIN (Discrimination Analyse Rapide WIndows), développé par la SDLC; FIRST (First Responder's Scan Tools), développé par l'University College Dublin (UCD) pour EUROPOL et OSTriage, développé par un ex-agent du FBI. Ces outils de recherche et de triage des fichiers, aux fonctionnalités complémentaires, offrent aux enquêteurs d'excellentes capacités d'investigation, et ce, que le support soit éteint ou allumé.


La formation PICC s'appuie largement sur les fonctionnalités de la plateforme e-campus de la Police nationale, accessible sur Internet. Les enquêteurs désirant suivre la formation doivent tout d'abord satisfaire à un test en ligne destiné à s'assurer qu'ils disposent des connaissances de base suffisantes. Ces tests de prérequis visent trois objectifs : 1) optimiser le taux de réussite au test final du stage, et donc le nombre de primo-intervenants en cybercriminalité formés; 2) éviter aux stagiaires de se retrouver en difficulté dans ce stage très technique; 3) permettre aux formateurs d'animer la formation dans les meilleures conditions possible.

De la même façon, afin de valider les compétences acquises et de garantir l'efficacité des primo-intervenants en cybercriminalité en situation de travail, les stagiaires font l'objet, à l'issue de leur formation, d'une évaluation prenant la forme de deux examens : 1) un test théorique (questions à choix multiples); 2) un cas pratique en ligne permettant de s'assurer que les stagiaires sont capables de mettre en pratique les compétences attendues, et notamment de trouver les éléments de preuve dissimulés en utilisant efficacement les logiciels mis à leur disposition. La réussite à cette évaluation donne lieu, pour les agents formés, à l'obtention d'un diplôme ainsi qu'à la reconnaissance officielle d'une compétence nouvelle inscrite dans le système d'information des ressources humaines (SIRH) de la Police nationale.

Enfin, il est apparu nécessaire de structurer un dispositif d'accompagnement des primo-intervenants en cybercriminalité à l'issue de leur formation. En effet, la matière est par essence évolutive, et les enquêteurs ne disposent pas toujours du temps nécessaire pour assurer une veille technique. Un espace collaboratif destiné à la communauté des primo-intervenants en cybercriminalité a donc été ouvert sur le e-campus de la Police nationale. Chaque agent formé ayant satisfait aux tests d'évaluation peut s'y connecter pour accéder aux différentes fonctionnalités : libre accès à plus de 200 fiches techniques régulièrement mises à jour ainsi que mise à disposition de tutoriels et de forums thématiques d'échanges.

Déployée à partir du premier trimestre de 2017 par les formateurs en investigations numériques de la DCRFPN, la mallette pédagogique a d'ores et déjà permis de former près de 300 primo-intervenants en cybercriminalité. Les retours des stagiaires sont très positifs, avec un niveau de satisfaction particulièrement élevé.

Conclusion



Avec ce nouveau produit pédagogique, la Police nationale est en mesure de proposer à ses agents une offre complète de formation dans le domaine de la cybercriminalité qui prend en compte les différents niveaux d'intervention et de spécialisation des services enquêteurs. La mise à disposition du module d'autoformation intitulé Bases de l'investigation numérique, au courant de l'année 2018, est venue parfaire ce dispositif en permettant à tout policier de se forger en 12 heures la culture minimale nécessaire dans son métier en matière d'informatique, d'Internet et de réseaux sociaux, et d'acquérir les connaissances fondamentales pour optimiser ses enquêtes en milieu numérique.

Pierre-Henri Machet, commissaire divisionnaire,
chef du Pôle anticipation, analyse, conseil, France

3.2.5 Enquêtes sur des cybercrimes

Comment définir la cybercriminalité

Les technologies de l'information et de l'Internet (« cyber ») ont augmenté de façon considérable la portée et la gravité de l'activité criminelle. Des méthodes novatrices et très complexes sont maintenant utilisées pour commettre des crimes tout à fait nouveaux ainsi que des crimes existant sous de nouvelles formes.

Contexte et défis

La cybercriminalité est un important problème de sécurité publique et d'application de la loi au Canada, et un problème complexe qu'une organisation ne peut pas régler isolément. En tant que service de police national du Canada, la Gendarmerie royale du Canada (GRC) a le vaste mandat d'enquêter sur les criminels dans l'espace cybernétique afin de les arrêter ou de perturber leurs activités. La *Stratégie de lutte contre la cybercriminalité de la Gendarmerie royale du Canada*, publiée en 2015, vise à réduire la menace, les répercussions et le nombre de victimes de la cybercriminalité au Canada par la répression policière.

Malgré les progrès réalisés à ce jour, les organismes d'application de la loi font face à plusieurs défis dans leur lutte contre la cybercriminalité. Compte tenu de la nature multiterritoriale de la cybercriminalité, il doit y avoir une grande coordination entre les services de police et une convergence à l'échelle nationale et internationale. Actuellement, les services de police luttent contre la cybercriminalité en vase clos, au cas par cas; la capacité d'établir des liens dans différentes sphères est limitée. Cela entraîne un manque d'efficacité, des chevauchements et des occasions ratées.

En outre, la cybercriminalité est sous-déclarée, et il existe divers moyens de signalement au Canada, ce qui sème la confusion chez le public. L'*Enquête canadienne sur la cybersécurité et le cybercrime* de 2017, menée par Statistique Canada, a révélé qu'environ 10 % des entreprises touchées par un incident de cybersécurité l'ont signalé à un service de police en 2017. Malgré la sousdéclaration, le nombre de cybercrimes signalés à la police au Canada a augmenté au cours des dernières années. En 2017, près de 28 000 cybercrimes

ont été signalés aux services de police canadiens, ce qui représente une augmentation de 83 % par rapport à 2014.

Il y a des lacunes et des défis en ce qui concerne la formation des policiers. Pour être en mesure de lutter efficacement contre la cybercriminalité, les responsables canadiens de l'application de la loi doivent disposer d'une expertise et de compétences de haut niveau, mais ils sont nombreux à ne pas avoir bénéficié d'une éducation et d'une formation spécialisée adéquate. Finalement, pour mener une lutte efficace, les services de police doivent travailler et avoir un lien avec un plus grand nombre de partenaires externes, y compris avec le secteur privé et à l'échelle internationale.

Lutter contre la cybercriminalité

En 2018, le gouvernement du Canada a annoncé des investissements de 507,7 millions de dollars sur cinq ans et de 108,8 millions annuellement par la suite afin de financer la nouvelle *Stratégie nationale de lutte contre la cybercriminalité*.

Les mesures prises par les organismes d'application de la loi pour lutter contre la cybercriminalité sont essentielles à cette nouvelle stratégie. En réponse à certains des défis mentionnés ci-dessus et pour renforcer la capacité du mandat du Canada à lutter contre la cybercriminalité, 201,3 millions de dollars sur cinq ans, puis 43 millions de dollars par année par la suite seront consacrés à la création de l'Unité nationale de coordination de la lutte contre la cybercriminalité de la GRC et à l'augmentation du nombre d'équipes d'enquêtes sur la cybercriminalité.

La Stratégie nationale de lutte contre la cybercriminalité comprend la création du Centre canadien pour la cybersécurité.

Unité nationale de coordination de la lutte contre la cybercriminalité

Actuellement, les policiers interviennent au cas par cas (de façon isolée). De nombreux services de police éprouvent de la difficulté à mener des enquêtes par manque de compétences, en l'absence d'un point de contact spécialisé, en raison de la complexité des dossiers et d'une coordination limitée. Il n'existe aucun mécanisme clair de signalement des incidents de cybercriminalité pour les Canadiens.

En tant que service de police national, l'Unité nationale de coordination de la lutte contre la cybercriminalité (UNCLC) assurera la coordination et la convergence des enquêtes sur la cybercriminalité au Canada et collaborera avec des partenaires à l'échelle internationale. Des conseils et des avis sur les enquêtes comportant des éléments de preuve numériques seront prodigués aux services de police canadiens. Un point de contact sera créé pour les services de police canadiens permettant d'établir des liens, de coordonner les pratiques de cybercriminalité et de produire des renseignements, ce qui aidera les policiers à faire enquête et à perturber les activités néfastes des cybercriminels. L'UNCLC établira un mécanisme national de signalement public que les citoyens et les entreprises du Canada pourront utiliser pour signaler des incidents de cybercriminalité aux organismes d'application de la loi. Ce système aura la capacité de gérer de grandes quantités de signalements chaque année et de produire des statistiques pertinentes.

L'UNCLC mettra en place une plateforme pour faciliter l'échange d'informations sur la cybercriminalité entre les services de police canadiens et établir des partenariats avec des organismes de l'étranger. Elle collaborera étroitement avec le Centre canadien pour la cybersécurité, les partenaires du secteur privé et le secteur de la sécurité informatique afin de poursuivre les cybercriminels. Il s'agit d'un bon modèle avec des objectifs stratégiques qui font suite à des études et à des consultations professionnelles et évolutives.

L'UNCLC devrait atteindre sa capacité opérationnelle initiale en 2020 et sa capacité opérationnelle optimale d'ici 2023.

Institut d'apprentissage en criminalité technologique

Le Collège canadien de police (CCP) offre de la formation avancée et spécialisée ainsi que des programmes de perfectionnement de cadres aux agents d'application de la loi de tout territoire de compétence. L'Institut d'apprentissage en criminalité technologique (IACT), qui fait partie du CCP, offre différents cours avancés dans le but d'améliorer les connaissances spécialisées et d'éviter la création d'une mauvaise jurisprudence. Les instructeurs et les animateurs sont des policiers ou des experts de l'application de la loi et du secteur privé.

Cela dit, il existe des écarts dans la capacité de l'IACT d'offrir une formation professionnelle et de donner des cours sur la cybercriminalité. Alors que l'IACT jouit d'une réputation accrue au niveau national et international, elle n'arrive pas actuellement à répondre aux demandes des services de police de l'ensemble du Canada. Des stratégies sont en cours de développement pour combler ces écarts et soutenir la stratégie nationale.

Cours offerts à l'Institut d'apprentissage en criminalité technologique

Informatique judiciaire De 11 à 13 semaines	Cybercriminalité De 4 à 7 semaines
Exploitation des enfants De 4 à 7 semaines	Analyse de renseignements en ligne De 1 à 2 semaines

Conclusion et voie à suivre

Pour lutter efficacement contre la cybercriminalité, il faut une stratégie globale portant sur les mesures de cybersécurité à prendre et sur les mesures d'application de la loi qui s'imposent pour poursuivre les cybercriminels. Les récents investissements au Canada permettront de soutenir les efforts de répression, la convergence et le renseignement. Des partenariats solides doivent être formés avec le secteur privé et les partenaires étrangers. Dans le recrutement, on met actuellement l'accent sur la diversité et l'inclusion. Finalement, l'échange d'informations avec des partenaires clés est essentiel, y compris avec des organismes d'application de la loi à l'étranger, ainsi que l'accès aux données connexes afin d'apporter des services efficaces et de favoriser l'amélioration du programme.

France Thibodeau, gestionnaire de l'Institut d'apprentissage en criminalité informatique au Canada, Collège canadien de police, Canada

Références

Gendarmerie royale du Canada (GRC). (2015). *Stratégie de lutte contre la cybercriminalité de la Gendarmerie royale du Canada*. Repéré à <http://www.rcmp-grc.gc.ca/wam/media/1089/original/ela9d988ea543658c8ea1463d588c6b0.pdf>.

Statistique Canada. (2017). *L'incidence du cybercrime sur les entreprises canadiennes, 2017*. Repéré à <https://www150.statcan.gc.ca/n1/fr/daily-quotidien/181015/dq181015a-fra.pdf?st=fzS36ObZ>.

3.2.6 Nouvelles technologies et préservation des preuves, genèse d'un projet national de formation de base pour les policiers

Quelque 18 000 policiers répartis dans 26 corps de police cantonaux sont actifs sur le territoire helvétique. Chacun a suivi une formation policière de base complète. La gestion des supports de données numériques, comme les appareils nomades (téléphones intelligents, tablettes numériques), ne faisait pas partie des acquis de cette formation. Pourtant, qu'il s'agisse d'une interpellation, d'un accident de la route, d'un dépôt de plainte ou encore d'une disparition de personne, dans la plupart des cas, des supports de données numériques sont à prendre en compte. Le projet intitulé Nouvelles technologies et préservation des preuves (NT2P) a donné naissance à la formation e-CC (*e-learning Cybercrime*) qui ambitionne de donner à chaque policier les clés de lecture requises pour appréhender le monde numérique, prendre les mesures de préservation adéquates des preuves, reconnaître les risques et les possibilités en matière d'exploitation des traces, et connaître ses propres limites de compétences en la matière. Cette formation constitue le socle d'un programme de formations spécialisées débouchant sur une hiérarchie de compétences en matière numérique au sein de la police suisse.

Le constat est sans appel : la plupart des affaires auxquelles sont confrontés les policiers helvétiques contiennent une composante numérique. Qu'il s'agisse d'une interpellation sur rue, d'un accident de la route, d'un dépôt de plainte pour escroquerie, de chantage ou de diffamation au guichet, ou encore d'une perquisition ou d'une levée de corps, les ordinateurs, les téléphones intelligents, les assistants personnels, les supports de données et les autres lieux de stockage dans le nuage informatique (*cloud*) ont ajouté une nouvelle teinte à l'environnement qui fait le quotidien des policiers helvétiques. Le Plan d'étude cadre pour policier/policrière (PEC) mentionne certes la cybercriminalité, mais ce point ne fait pas partie de la formation de base. De ce fait, le traitement des traces numériques sur le terrain n'est pas assuré de manière optimale ni, d'ailleurs, la prise en charge des plaignants.

Les corps de police disposent de compétences numériques, souvent personnifiées par des équipes de spécialistes de

pointe en matière d'investigation numérique ou d'enquête informatique. Ces équipes se trouvent toutefois en situation de surcharge de travail presque systématiquement, sollicitées dans une multitude de cas allant de la préservation de traces numériques à l'analyse de données stockées dans le nuage informatique en passant par les inévitables extractions de données de téléphones intelligents. La vitesse de traitement des affaires s'en ressent grandement.

Le projet NT2P, né en 2013 déjà, visait trois objectifs découlant directement de ce constat :

- Développer les compétences de tous les policiers en matière de préservation des traces numériques;
- Contribuer à l'optimisation du traitement des cas

comprenant une composante « cyber » afin de permettre à chaque policier, à son niveau respectif, de développer son autonomie dans le domaine numérique tout en assurant une délimitation claire des limites de compétences en la matière et en favorisant ainsi l'émergence d'un système de référents numériques;

- Décharger les spécialistes IT afin de leur permettre de se concentrer sur les affaires nécessitant leurs compétences de pointe.

Le concept de formation, né des travaux du groupe de travail qui s'est consacré à cette tâche, peut se résumer schématiquement sous la forme suivante :

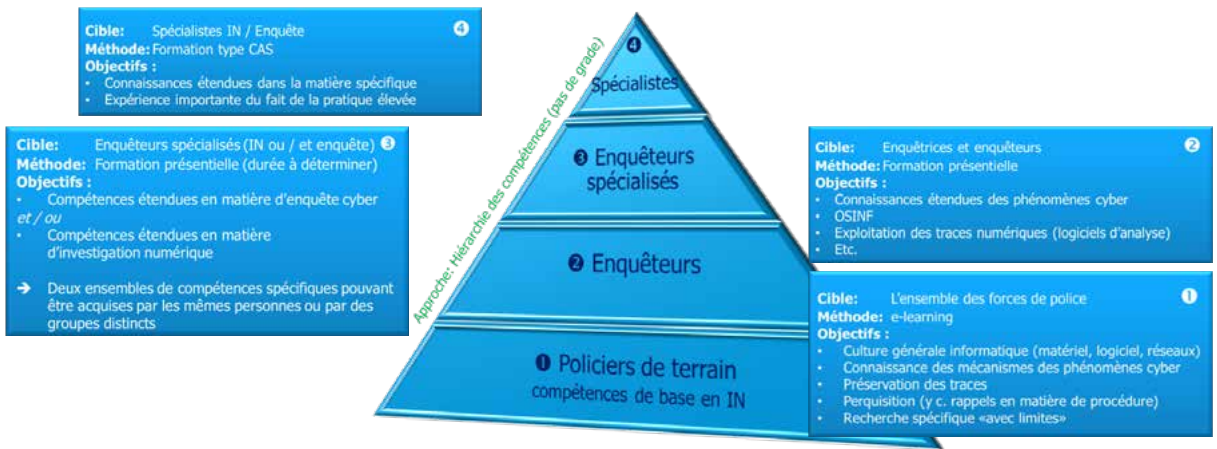


Figure 1 : Schéma du concept de formation

Les fondations comprennent, d'une part, le développement des éléments d'apprentissage permettant à l'ensemble des policiers d'acquérir une culture générale en matière d'informatique. Cette étape est particulièrement importante, car les compétences de base des policiers sont hétérogènes. Il faut par ailleurs tenir compte de la problématique générationnelle. En l'occurrence, les baby-boomers côtoient les générations Y et même Z sur les mêmes lieux de travail. Il va sans dire que toutes ces personnes ne sont pas entrées dans la vie active avec les mêmes connaissances numériques. La formation de base *Cybercrime* (e-CC) fournit, en outre, des outils

permettant de mieux comprendre les mécanismes liés aux phénomènes cybercriminels sans pour autant dévier vers une spécialisation. En effet, à ce stade, l'objectif est d'assurer la préservation des traces numériques au quotidien.

Pour réaliser ces objectifs, il a été décidé de travailler sur la base de cas concrets (cas guichet, cas rue, cas enquête). La transmission des connaissances en matière numérique s'effectue donc sous l'angle de la pratique, et non de manière purement théorique. L'apprentissage en ligne e-CC applique rigoureusement cette démarche.



Figure 2 : Illustration de la page d'accueil de l'apprentissage en ligne e-CC

La salle de classe (*classroom*) est l'espace dans lequel les notions de base sont expliquées. Elle se veut explicative. Quelques interactions y sont toutefois proposées. Les missions sont axées sur la pratique : le policier est confronté à un cas concret (p. ex. : une perquisition). Les connaissances acquises lors de la phase d'apprentissage sont alors appliquées.

Lors de chaque mission, le policier a la possibilité de revenir aux connaissances de base pour combler d'éventuelles lacunes. Enfin, lorsque toutes les missions ont été réalisées avec succès, un test permet de valider les connaissances acquises. Ce test ne vise en aucun cas à sanctionner la réussite ou l'échec de l'apprentissage; il constitue au contraire une nouvelle étape d'acquisition de connaissances. À ce titre, il peut être répété autant de fois que souhaité.



Figure 3 : Exemple de mission

L'accès à l'e-CC se fait sur la Plateforme nationale de formation policière (PNFP). Chaque policier suisse dispose d'un accès (identifiant) à cette plateforme lui permettant de suivre les formations en ligne mises à sa disposition.

À l'heure actuelle, la formation est déployée en Suisse dans les trois langues nationales (français, allemand et italien). La majorité des quelque 18 000 policiers concernés l'a déjà suivie avec succès. Les retours des principaux intéressés sont positifs et démontrent que les objectifs d'apprentissage définis ont été transposés de manière efficace.

En référence à la figure 1, le développement d'une hiérarchie de compétences implique que des référents soient formés à plusieurs niveaux afin de faire le lien entre le policier de terrain et le spécialiste. Le concept élaboré par le groupe de travail prend en compte deux échelons de formation intermédiaire. Le niveau qui suit la formation de base est constitué d'une formation présentielle avancée. Cette formation est destinée à un nombre restreint d'enquêteurs appelés à acquérir des compétences plus pointues dans le domaine informatique au profit de leur travail d'enquête. Dans la formation avancée comme dans la formation de base, l'accent est mis sur les éléments concrets pouvant bénéficier à la pratique policière. À l'heure actuelle, la formation avancée n'est offerte en Suisse que sous la forme de cours pilotes. Cette phase d'essai s'étendra jusqu'en 2019 sur la base d'un processus d'apprentissage et moyennant quelques ajustements successifs. Le troisième échelon de cette formation, visant les enquêteurs spécialisés, est pour l'heure au stade de projet. Il ne sera mis sur pied que lorsque les apprentissages de la phase précédente auront été acquis. Ces formations requièrent en effet une cohérence didactique, mais également pratique, puisque les personnes formées seront finalement amenées à collaborer avec leurs référents respectifs (en référence à la hiérarchie des compétences illustrée dans la figure 1). Notons que les formations proposées sont réalisées grâce à une collaboration entre le monde policier et le monde scolaire. L'Institut de lutte contre la criminalité économique de la Haute École Arc (HES-SO) participe ainsi à l'élaboration de ces programmes ainsi qu'à la formation, notamment pour les formations continues certifiantes de type CAS (*Certificate of*

Advanced Studies). Il convient de mentionner qu'un CAS en investigation numérique est proposé aux spécialistes depuis 2009 (<https://www.he-arc.ch/gestion/cas-in-st>).

L'Institut suisse de police poursuit par ailleurs son engagement dans la formation numérique. Il a notamment développé très récemment une autre formation en ligne consacrée à la coopération policière internationale (e-CPI), également accessible sur la PNFP. L'Institut consacrera par ailleurs un dossier spécifique à la formation numérique, à ses enjeux et à ses défis, intitulé « La police dans une société plurielle », dans le prochain numéro de format magazine de la *Revue de formation et de recherche policières*, à paraître début de 2019.

Sébastien Jaquier, responsable adjoint à l'Institut de lutte contre la criminalité économique (ILCE) de la Haute École de gestion Arc, Haute École spécialisée de Suisse occidentale (HSE-SO), Institut suisse de police (ISP), Neuchâtel, Suisse

3.3 ÉCHANGES

La cybercriminalité est une problématique transversale qui peut toucher au terrorisme. Cette ambivalence du phénomène oblige les acteurs à avoir une approche holistique et transversale dans la lutte contre le terrorisme et la cybercriminalité, et à mettre l'accent sur le renforcement des capacités opérationnelles des unités spécialisées, notamment en les équipant en matériel logistique et technologique de dernière génération.

M. Jacquart questionne les panélistes en demandant : « Qu'est-ce que c'est, une "cyberpatrouille" ? »

Le panéliste ayant fait un exposé sur la question, M. Augustin Ochogni, répond en précisant qu'il s'agit d'une troupe policière chargée de faire des investigations sur Internet. Cela peut concerner la recherche d'informations sur les réseaux sociaux de type Facebook, Google, Twitter, etc. Le but est, dans un premier temps, de rechercher des informations qui pourraient compromettre les intérêts de l'État.

Cependant, la cyberpatrouille, compte tenu de l'ampleur actuelle d'Internet, va au-delà des intérêts étatiques et touche aussi aux personnes. Il y a ce qu'on appelle la « *face invisible cyberpatrouille* ». Il s'agit du « *dark work* » aussi connu sous le nom de « *travail au noir* » ou « *travail au black* ». Cela concerne davantage les activités illicites telles que le trafic de produits ou de drogues, ou des activités liées au terrorisme qui peuvent avoir des répercussions sur la stabilité de l'État.

M. Ochogni termine son intervention en précisant que ce genre de patrouille nécessite une formation mise en place par les services pour permettre aux cyberpatrouilleurs de mener à bien leurs missions.

Un congressiste pose la question suivante au commissaire de police Papa Gueye : « Votre service investit-il toutes les scènes de crime ? » Le congressiste continue son interrogation en supposant :

Imaginons qu'un service investit une scène de crime. Ma réflexion se porte au niveau où, dans la mesure où les policiers peuvent intervenir sur une scène de crime en leur qualité de primo-intervenants,

les policiers peuvent donc collecter l'information et mener à terme une conclusion sur une scène de crime en qualifiant l'acte récusé comme étant « un crime ». Mais si le service spécialisé en cybersécurité intervient sur la scène du crime, ce service peut s'intéresser à ce que l'utilisation du téléphone peut faire dans la requalification d'un acte de crime en fonction des données qu'ils exploiteront dans les objets de téléphonie connectés sur les lieux du crime.

Le congressiste fait une recommandation commune selon laquelle les services concernés doivent s'intéresser aux outils informatiques qui sont censés perfectionner le diagnostic lié à une scène de crime.

M. Papa Gueye répond à la question du congressiste en commençant par quelques éclaircissements : « Il faut comprendre que, dans le cadre du fonctionnement des services spécialisés, le service de cybersécurité reste tout d'abord un service de police judiciaire qui a pour but d'administrer en matière de prévention et de répression. »

Le panéliste argumente en affirmant que l'activité du service de sécurité liée au support d'information est une partie des missions du service de cybersécurité. Ce service peut porter secours aux autres services sur l'investigation de la scène de crime. Aussi, l'activité du service de cybersécurité ne se limite pas qu'à une simple assistance, mais aussi à de l'assistance judiciaire en rapport parfois à la localisation de la personne suspecte par l'entremise de l'exploitation des objets connectés.

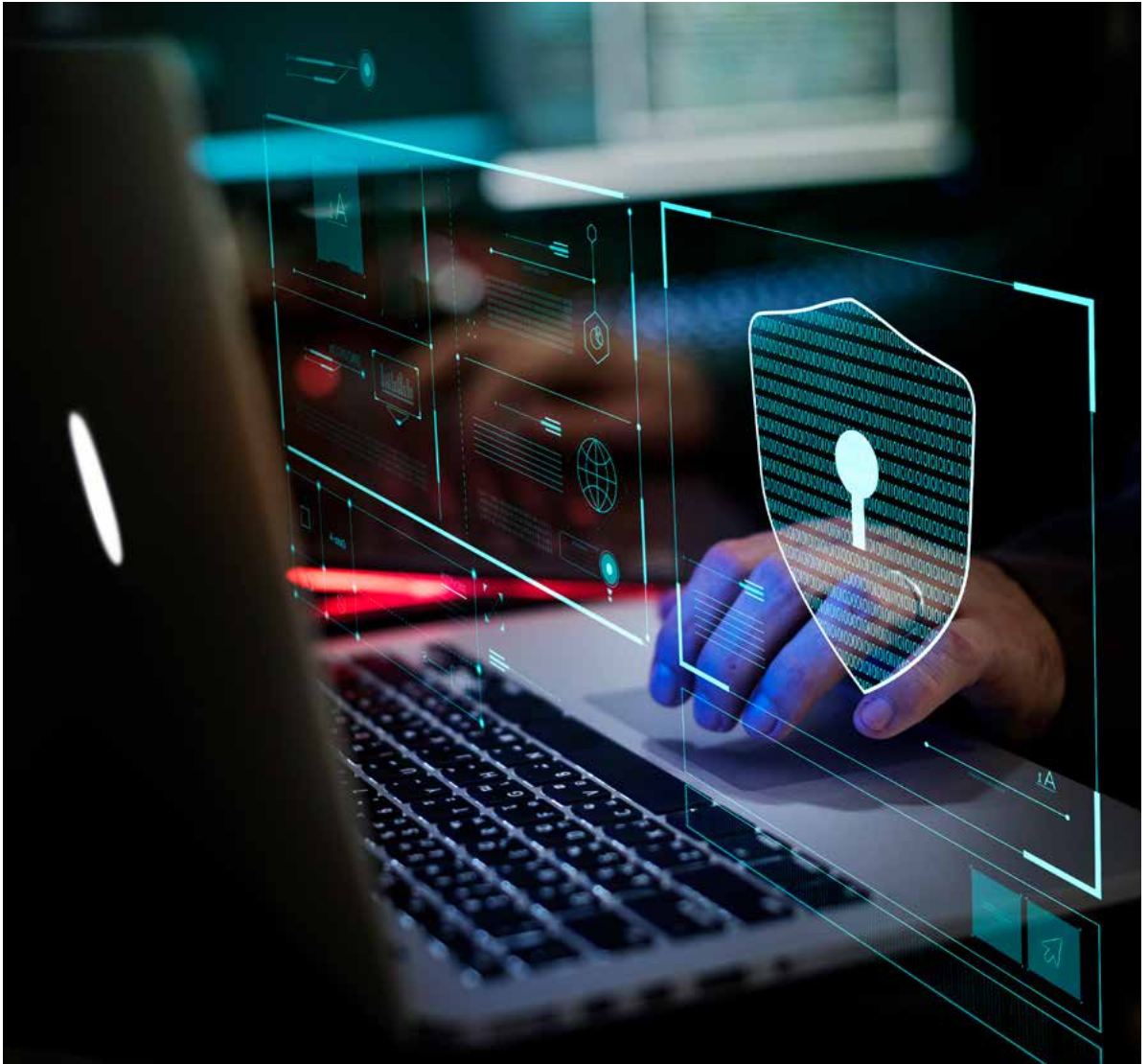
M. Papa Gueye répond *in fine* en arguant que les techniques d'investigation peuvent voir quel a été le dispositif technique mis en place par l'individu pour commettre le crime. Il y a donc une stratégie qui est mise en place en passant par les soutiens techniques pour investir la scène de crime.

M. Papa Gueye continue son intervention en répondant à une deuxième question posée par un congressiste, à savoir si les services de cybersécurité se déploient ou non. En effet, sur cette question, le panéliste répond que « nous ne couvrons pas le territoire national, mais quand les services déployés ont des difficultés, on peut communiquer avec eux

et leur donner quelques informations. C'est pour ça que le gouvernement sénégalais a mis en place la réforme du service de cybercriminalité pour pallier le besoin récurrent de l'aide dans la quête des données ».

Le commissaire de police représentant la Côte d'Ivoire affirme être séduit par le modèle sénégalais de lutte contre la cybercriminalité. Le commissaire pose la question suivante : « Dans la mesure où ce genre de service, tel que le service de

cybersécurité, a comme allié des infrastructures économiques et techniques, quelles initiatives avez-vous prises pour anticiper les coupures d'électricité? » M. Papa Gueye répond : « Pour mener des activités d'investigation, il faut des infrastructures, car l'objectif est d'assurer avant tout l'intégrité du service de cybersécurité pour qu'il puisse fonctionner. Par exemple, en ce qui concerne les coupures de courant, à notre service, nous avons un groupe électrogène; en plus, nous avons un dispositif interne et externe pour préserver le service. »



4. GESTION DES FLUX MIGRATOIRES

4.1 INTRODUCTION

– IMAGE DU PHÉNOMÈNE

Migrations et défis sécuritaires

Les migrations constituent une des données majeures de notre époque. Elles sont aujourd’hui au centre des relations internationales et des perspectives de construction d’un nouvel ordre migratoire qui tient compte des configurations de notre système international. En effet, on estime que les migrants internationaux représentent pas moins de 244 millions de personnes en 2015, soit 3 % de la population mondiale.

Cette mobilité des hommes, des biens et des services s’accompagne de plusieurs corollaires liés à l’existence du phénomène. En réalité, la non-maîtrise de la migration irrégulière entraîne des défis protéiformes cruciaux qui viennent s’agréger solidement à l’architecture nationale, régionale et globale de gouvernance des migrations. Parmi ces défis, la sécurité occupe une place prépondérante.

Par défi sécuritaire, il faut comprendre l’ensemble des actions, des comportements et des phénomènes d’origine humaine ou non ayant un lien avec les migrations, et qui affecte la paix et la stabilité d’un pays ou d’une région donnée. Ces défis demeurent une réalité que le fondamentalisme religieux, la circulation et le trafic d’armes, l’intensité des réseaux criminels transfrontaliers, le trafic de drogues, la contrebande ainsi que la traite des êtres humains viennent quotidiennement nous rappeler avec une violence inouïe.

Aujourd’hui, la persistance des bravades sécuritaires en lien avec les migrations remet continuellement à jour la question de la gouvernance des flux migratoires, mais bien au-delà, elle met en relief les limites structurelles dans la gestion des migrations et l’absence d’établissement de politiques *ad hoc*, surtout par les États africains.

Comment concilier la nécessaire circulation des personnes et de leurs biens, et l’impératif de sécurité de nos États et de leurs intérêts? Quelles alliances stratégiques pouvons-nous établir pour une gouvernance sécuritaire des migrations

devant l’éminence des risques et les nouvelles menaces? Quels sont les liens entre les forces de police et les enjeux sécuritaires dans l’espace francophone? Comment les polices francophones peuvent-elles sécuriser les phénomènes migratoires? Quels liens les polices francophones peuvent-elles tisser entre elles pour assurer une mobilité humaine avec moins de risques?

À ces questions, nous tenterons d’apporter une réponse pratique qui est celle de la nécessité, pour les États francophones, de trouver des moyens appropriés pour faciliter la circulation légitime des personnes et des biens tout en maintenant leur sécurité aux frontières. En d’autres termes, il faut trouver un juste équilibre entre des frontières ouvertes et des frontières contrôlées.

Quels sont les liens entre les forces de police et les enjeux sécuritaires dans l’espace francophone?

Pour mieux appréhender la complexité des défis et des enjeux auxquels est confrontée la gouvernance du secteur de sécurité dans l’espace francophone, il convient de se pencher sur les spécificités propres aux appareils de sécurité des États et des gouvernements de l’espace francophone, qui présentent un grand nombre de caractéristiques communes. En effet, au-delà du partage d’une langue véhiculaire commune, la majorité des États francophones ont en partage un modèle spécifique d’un point de vue institutionnel, organisationnel et procédural, tel que le système dual des polices francophones (police et gendarmerie). À cela s’ajoutent les nombreux soubresauts qui ont agité l’espace francophone au cours de la décennie écoulée et qui démontrent la nécessité d’entreprendre de profondes réformes du système de sécurité dans de nombreux pays, particulièrement en Afrique.

En effet, il est aujourd’hui plus que nécessaire de développer une connaissance fine des particularités propres au fonctionnement des appareils de sécurité de ces États afin de corriger les lacunes criantes dans la connaissance des pratiques et des expériences développées dans la gestion migratoire : le partage des informations et des données liées à la mobilité des personnes et des biens demeure essentiel. Nous avons vu et mesuré les possibilités, mais aussi les limites d’INTERPOL, en particulier dans les luttes contre la traite des êtres humains.

Les forces de police sont garantes de la sécurité des individus aussi bien à l'intérieur du territoire qu'aux abords des frontières.

À l'interne, la police **fournit un service de sécurité intérieure qui consiste en un travail d'analyse, d'études et d'enquêtes** sur les tendances et les phénomènes violents susceptibles de survenir sur les territoires. Il est impossible de prévenir les actions violentes sans un bon service de renseignement. Que la menace provienne d'un groupuscule, d'une association d'individus, d'une organisation criminelle ou d'un État tiers, c'est ce travail opéré en interne sur la mobilité des personnes et des biens qui est à la source des missions de lutte contre le terrorisme et l'extrémisme au sens large.

Les polices des frontières sont, en quelque sorte, le guichet (*front office*) des États, et c'est à elles qu'il incombe de traiter les flux de personnes et de biens aux points d'entrée et de sortie des tensions, ainsi que de repérer et de réguler les cas de tentative de franchissement illégal des frontières, et d'en prévenir les conséquences sur la sécurité et la stabilité des pays.

Des services de police structurés et efficaces dans la gestion de proximité des frontières, s'appuyant sur des frontières et sur des agents de l'immigration bien formés, qui pratiquent une gestion juxtaposée de la migration, permettent non seulement de favoriser une gestion ordonnée des mouvements aux frontières et de prévenir la migration irrégulière, mais aussi de détecter la présence de migrants introduits clandestinement (enfants non accompagnés en Europe et en Afrique) et de victimes de la traite, dans le but de démanteler des réseaux criminels organisés et de protéger les droits de ces personnes vulnérables.

Comment les polices francophones peuvent-elles sécuriser les phénomènes migratoires?

Il s'agit de mettre en perspective les politiques nationales de mise en visibilité du contrôle frontalier, d'une part, et les pratiques locales de contrôle et de coopération policière, d'autre part. Il faudrait s'inscrire dans un contexte plus large de redéfinition des formes de contrôle et de mise à l'écart des risques et des nouvelles menaces. Pour ce faire, les polices francophones devraient être impliquées à toutes les échelles de gestion de la problématique migratoire. Elles doivent être déterminées à accompagner les gouvernements dans

les défis opérationnels que pose la migration, et à mettre en place des mécanismes de gestion de mouvements ordonnés et respectueux de la dignité humaine, et ce :

- Par la surveillance et la sauvegarde du respect des droits des êtres humains, quel que soit le statut du migrant (régulier ou irrégulier) ainsi que par la formation et l'information du personnel de sécurité sur la législation en vigueur dans les différents pays qui partagent ou non les mêmes frontières;
- Par la mise en place d'observatoires sur la mobilité des personnes et des biens, et les échanges d'informations systématiques entre les personnes responsables de la gouvernance de la migration dans les pays d'origine, d'accueil et de transit;
- Par l'assurance de la qualité du processus migratoire aux niveaux national, régional et international; cela concerne la sauvegarde de l'intégrité du processus et celle des personnes et des autres ressources concernées.

Quels liens les polices francophones peuvent-elles tisser entre elles pour assurer une mobilité humaine avec moins de risques?

Les polices francophones devraient accompagner les États membres de la Francophonie à élaborer des politiques, des législations, des structures administratives et des systèmes opérationnels, et à constituer la base des ressources humaines nécessaires pour pouvoir relever avec efficacité les divers défis migratoires et frontaliers, et instituer une gouvernance appropriée en matière de migration. Ces actions devront aider les États à renforcer leurs structures et leurs procédures de gestion des frontières et des migrations, et elles doivent être conçues sous la forme de partenariats avec, comme critères premiers :

- **L'éducation et la formation sur les thématiques migratoires et sécuritaires, et sur la gestion des liens entre ces deux phénomènes;**
- **La maîtrise de l'information pertinente et le partage imminent de celle-ci;**

- La responsabilité de la protection des droits des migrants, et ce, quel que soit leur statut;
- L'établissement de règles communes de lutte contre la cybercriminalité, la criminalité transfrontalière, la traite et le trafic d'êtres humains, la diffusion du fondamentalisme religieux et de ses conséquences sur les familles et nos sociétés vulnérables, ainsi que le terrorisme;
- La coopération internationale ainsi que l'harmonisation des pratiques et des politiques sur le plan interne, au sein des États, et dans un contexte sous-régional et régional, afin de les mettre en conformité avec les normes internationales communes.

Je souhaiterais dire ici que la gestion des migrations entre pays francophones ne peut plus relever des seules relations bilatérales entre gouvernements d'accueil et d'origine, mais qu'elle requiert des initiatives intégrées et des synergies d'actions concertées à l'échelle d'ensembles géopolitiques plus larges.

Il est temps que les polices francophones intensifient la réforme de leur système de travail. C'est pour cela qu'en Afrique et ailleurs, on a entamé la réforme du secteur de sécurité (RSS), dont celle de la police, qui en est partie intégrante et qui est basée sur les trois « P » : prévention, poursuites et protection.

Je propose, dans la perspective des conclusions de nos travaux, que cette conférence de FRANCOPOL, qui coopère avec INTERPOL, intègre dans ses mécanismes de fonctionnement la perspective de l'égalité femme-homme, qui demeure un outil de performance pour le secteur de la sécurité humaine, mais qui est aussi un indicateur de choix dans les réformes du secteur de la police dans tous nos pays.

Professeure Ndioro Ndiaye, coordinatrice du Réseau francophone pour l'égalité femme-homme, présidente de l'Alliance pour la migration, le leadership et le développement (AMLD), Sénégal

4.2 PRÉSENTATION DE L'ÉQUIPE CONJOINTE D'INVESTIGATION

L'Équipe conjointe d'investigation (ECI) Niger a été créée pour lutter contre les réseaux criminels liés à l'immigration irrégulière, à la traite des êtres humains, au trafic illicite de migrants et à la fraude documentaire. Composée de 20 fonctionnaires de police au total, avec précisément 14 policiers du Niger, trois de la France et trois de l'Espagne, l'ECI est basée à Niamey et dispose de deux autres antennes interrégionales à l'intérieur du pays. Son administration est assurée par le chef de la mission, M. Fernando Guerrero, policier espagnol, assisté de M. Patrick Muscat, commandant de la Police française. La gestion financière est coordonnée par un opérateur public-privé espagnol nommé Fondation internationale et ibéroaméricaine pour l'administration et les politiques publiques (FIIAPP), mais le volet opérationnel est coordonné par le chef de la Division des investigations spéciales, le commissaire de police Abdoul Salam Moumouni, secondé par l'officier de police Ahmadou Tidjani Abdou Ali, tous des policiers nigériens. Financée par le fonds fiduciaire d'urgence de l'Union européenne à hauteur de six millions d'euros, cette équipe a vu le jour en décembre 2016 à l'issue des multiples rencontres des dirigeants africains et européens sur la thématique de la migration irrégulière, dont le sommet de La Valette de 2015 en est une illustration parfaite. Cependant, elle n'a officiellement commencé à être opérationnelle qu'en mars 2017 à la suite d'un protocole tripartite de coopération policière signé le 13 mars 2017 à l'hôtel Gaweye de Niamey entre les directeurs généraux de la Police nationale du Niger, de la France et de l'Espagne, ainsi qu'en présence des ministres de l'Intérieur de ces trois pays. En effet, la multiplication des drames de migrants dans le désert nigérien à la frontière avec la Libye et dans la Méditerranée ces dernières années, ajoutée à une forte présence des migrants en situation irrégulière dans les pays européens, avait suscité une vive inquiétude des dirigeants de ces deux continents.

Ainsi, pour se conformer à tous ses engagements pris lors des différentes rencontres sur la lutte contre les réseaux criminels et aux différents instruments juridiques internationaux

tels que la convention de Palerme de 2000 et de ses deux protocoles additionnels relatifs à la lutte contre la traite des personnes et le trafic illicite de migrants, le Niger, qui constitue l'un des pays de transit incontournables dans la migration irrégulière, s'est doté d'un texte (Loi 2015-036 du 26 mai 2015) qui prévoit et réprime le trafic illicite de migrants en dépit de l'ordonnance 2010-086 du 16 décembre 2010 déjà existante relativement à la lutte contre la traite des personnes.

Pour mettre en application tous ces textes, la Division des investigations spéciales, responsable de mener des enquêtes judiciaires en équipe conjointe avec les policiers espagnols et français, a été créée au sein de la Direction de la surveillance du territoire (DST).

Cette équipe, qui a pour mission de lutter contre les réseaux criminels liés à l'immigration irrégulière, à la traite des personnes et au trafic illicite de migrants, est compétente sur le plan national.

En effet, conformément à ses missions qui lui sont assignées et aux différents instruments juridiques nationaux et internationaux en vigueur, l'ECI mène, depuis mars 2017, une lutte sans relâche contre les réseaux criminels liés à l'immigration irrégulière, à la traite des personnes, au trafic illicite de migrants et à la lutte contre la fraude documentaire, et ce, en parfaite collaboration avec les parquets des différents tribunaux du pays. Elle contribue aussi au renforcement des capacités opérationnelles et judiciaires des services de la Police nationale impliqués dans cette lutte et à l'amélioration de la gestion policière des frontières. Les enquêtes de l'ECI se font sur la base des renseignements et des surveillances-filatures, ainsi que sur la base des infiltrations de réseaux de trafiquants par des agents de police ou par des indicateurs fidèles.

Par ailleurs, il est important de préciser que l'ECI collabore avec plusieurs institutions gouvernementales et non gouvernementales, surtout en matière de gestion des migrants qui font l'objet d'un trafic et des personnes victimes de traite. Avec un peu plus d'un an d'activité à son actif, l'ECI a enregistré des résultats satisfaisants malgré les nombreux défis qui se dessinent à l'horizon avec les nouvelles stratégies et l'influence des trafiquants. La coopération avec les États voisins n'étant pas très élargie, l'ECI n'arrive pas à mettre la

main sur certains présumés trafiquants cités dans plusieurs procédures et qui se trouvent dans d'autres pays voisins. Alors, l'adoption d'une nouvelle loi semblable à la loi 2015-036, qui permettrait de faciliter la coopération et l'entraide judiciaire entre les États de la sous-région dans le domaine de la répression du trafic illicite de migrants, s'avère nécessaire. Il faut aussi songer à renforcer les capacités techniques et logistiques des antennes interrégionales, et intensifier la formation de tous les acteurs de la chaîne pénale au Niger et dans les autres pays, car, en dehors du Niger, aucun pays de la sous-région ne dispose à l'heure actuelle d'un dispositif juridique interne et d'une unité d'enquête spéciale en matière de trafic illicite de migrants, et cela rend la coopération difficile.

Ahmadou Tidjani Abdou Ali, adjoint au chef de la Division des investigations spéciales contre le trafic illicite de migrants, la traite des personnes et la fraude documentaire, membre de l'ECI et formateur à l'École nationale de police et de la formation permanente, Niger

4.3 ÉCHANGES

M. Diallo Babacar, directeur du Centre d'études diplomatiques et stratégiques de Dakar, est le premier congressiste intervenant à cette table ronde. Avant toute chose, il remercie la modératrice et FRANCOPOPOL d'avoir inscrit la migration à l'ordre du jour. Puis, il continue son intervention dans ces termes :

Mon intervention vient en complément [à celle] de la professeure Ndioro. Pour l'essentiel, la question de la migration a été créée *a priori* pour réprimer et pour punir. Mais à part l'aspect « trafic humain », on a besoin d'un langage humanisé; la migration est un phénomène naturel, elle est aussi naturelle que le mouvement des vents, et personne ne peut l'empêcher. Mais la question est sans doute celle des mécanismes régulateurs, ou comment mettre en place une gestion concertée pour trouver une solution dans la gestion des flux migratoires.

Les Africains ne sont pas encore arrivés à connaître l'Afrique. En effet, depuis l'Indépendance, les politiques publiques migratoires en Afrique n'ont pas été mises en place. Nous avons développé une réponse répressive et punitive face à la question migratoire, alors qu'il s'agit désormais de se rassembler pour mettre en place une approche globale des questions migratoires propres aux territoires africains.

La modératrice, M^{me} Lacroix, précise de nouveau que cette approche globale de la question des flux migratoires est certes très importante (c'est ce qui est actuellement discuté sur le pacte mondial), mais qu'il faut se focaliser sur les réponses que peut apporter la police (les pistes francophones que les polices peuvent mettre en place). La question centrale à laquelle nous devons tenter de répondre est celle-ci : « Comment étudier la façon dont les polices francophones peuvent sécuriser la question migratoire? »

M. Moussa Mamadou, directeur adjoint de la police du Niger, prend la parole en tant que congressiste en précisant que l'immigration illicite est combattue au Niger, notamment dans la région d'Agadez, qui représente à elle seule les deux tiers de la superficie du Niger. Agadez est une région qui vit essentiellement du tourisme en raison de la sécheresse de la région, car il ne pleut pas. Cependant, le tourisme a disparu avec la chute de la Libye. L'immigration illicite s'est donc installée.

Après la disparition du tourisme comme source de revenus avec la chute du régime libyen, toute la population du Niger vivait de l'immigration illicite. La population du Niger ne pouvait vivre et se nourrir que par l'entremise de cette activité principale, même si elle était illicite. Ce n'est que grâce à l'aide de partenaires que le Niger a été amené à criminaliser cette action illicite.

La professeure Ndiaye rappelle que le rôle de la police doit justement permettre de sécuriser tout le processus du flux migratoire. Ce processus de sécurisation existe déjà dans les pays européens; la question est alors de savoir ce qui a été fait en matière de police dans les pays africains pour sécuriser les flux migratoires.

Il y a manifestement un manque de rigueur quant au traitement de la problématique des migrants en Afrique. Prenons, par exemple, le cas des statistiques évoquées par l'intervenant du Niger. Si on note que les autorités arrivent à appréhender 18 trafiquants, ce nombre est considérable et doit permettre à l'assistance de se rendre compte qu'il y a un problème avant tout géopolitique extraordinaire. Alors, demandons-nous tous ce que nous faisons pour les migrants non traités par l'Organisation internationale des migrants. Que fait l'Afrique? Que fait FRANCOPOL?

La panéliste M^{me} Ndiaye poursuit son intervention en soutenant que l'on ne peut sécuriser la politique migratoire de l'Afrique sans appréhender le problème, de même que l'on ne peut pas poser la problématique de la gouvernance des flux migratoires sans voir la part de responsabilité de l'Afrique vis-à-vis des violations des droits de la personne.

Selon la panéliste, ce qui manque à ce débat, et qu'il faut retenir, est le fait que l'on pourrait trouver une solution internationale et locale dans la gouvernance migratoire. Au fond, la véritable question est la suivante : « Que faire des personnes qui sont passées "à la trappe" et qui ont pu entrer dans le territoire impunément et, ainsi, qui n'ont pas fait l'objet d'une arrestation? » Cependant, on se préoccupe de trouver du travail à ces personnes-là, alors que ce sont des récalcitrants ou des trafiquants d'êtres humains, et qu'on laisse les populations locales à côté démunies de toute situation sociale décente.

Le panéliste sénégalais Abdou Wahabou Sall fait le constat, amer, que les politiques migratoires qui ont été mises en place n'ont pas pu sortir du cadre sous-régional, en parlant de la Communauté économique des États de l'Afrique de l'Ouest (CEDEAO). Mais le panéliste se félicite du fait qu'aujourd'hui, le Sénégal bénéficie de plusieurs projets en matière de gestion des flux migratoires. Il précise que la plupart des gens concernés par cette problématique sont des pêcheurs :

Le phénomène de la migration est une frontière où les gens se reconvertissent très vite. Par exemple, en Italie, l'arrivée massive des populations au large des mers a poussé les gens à se reconvertir. Il faut prendre en compte ces gens qui se reconvertissent; c'est le phénomène de la résilience, car les gens qui ont fini par se reconvertir dans le trafic humain vivent de ce trafic. Il faut donc trouver les alternatives économiques. La question de la sécurité et celle de l'articulation entre sécurité et libre circulation sont au cœur du débat. Alors, la question qui se pose aujourd'hui est : « Comment concilier les deux? »

Émile Pérez, ancien président de FRANCOPOPOL, remercie les panélistes et les intervenants d'avoir porté le débat à un très haut niveau. Il ajoute que la réponse policière est indispensable pour lutter contre les criminels, qui ne sont pas les migrants, mais bien les trafiquants d'humains.

Si la résolution que nous devons adopter est d'ordre politique, une organisation comme FRANCOPOPOL doit pouvoir faire passer ce message pour convaincre les politiques au niveau national et international afin de permettre à chaque État de régler le problème à la source. La migration est certes naturelle, mais les migrants sur l'Europe préfèrent rester chez eux avec leurs familles. C'est donc tout l'enjeu de FRANCOPOPOL « de traiter le problème de manière humaine, car lorsque la marchandise est l'être humain, cela devient inadmissible ».



5. GESTION DES RISQUES PSYCHOSOCIAUX

5.1 SANTÉ MENTALE DANS L'UNIVERS POLICIER

5.1.1 Introduction

J'ai toujours cru que la façon dont vous traitez vos employés est la façon dont ils traitent vos clients, et que les gens s'épanouissent lorsqu'ils sont félicités.

– Richard Branson

Cette citation, que les policiers et les policières du Service de police de l'agglomération de Longueuil affichaient pendant les dernières négociations, renvoie à une problématique longuement passée sous silence dans les milieux policiers : la santé et le bien-être des policiers. En même temps, la citation de Branson nous rappelle ce qu'on sait (ou devrait savoir) déjà : des employés en bonne santé offriront des services de qualité à la population.

Au Canada, de plus en plus d'associations policières et de chercheurs en santé tirent des signaux d'alarme : en plus de travailler dans un milieu fortement exigeant par sa nature, les policiers doivent composer avec un changement de types d'activités, tout en « faisant de plus en plus, en moins de temps ».

Par exemple, selon une étude récente de l'Institut de recherche Robert-Sauvé en santé et en sécurité du travail (IRSST), « 15 % des policiers québécois souffrent ou ont souffert de stress post-traumatique » (IRSST, 2018)¹⁰.

Deux facteurs de risque de l'état de santé des policiers et des policières retiennent l'attention :

- A. l'écart entre l'idéal du métier de policier;
- B. les valeurs et les normes de la culture policière traditionnelle.

10. Dans le même sens, « [L]es données de la CNESST révèlent que le groupe des policiers/détectives est parmi les plus touchés avec 76 jours d'absence en moyenne et des débours de près de 1,4 million \$ pour 163 cas ayant un désordre post-traumatique » (IRSST, 2018).

5.1.1.1 L'écart entre l'idéal du métier de policier

Attirés par cette profession, les jeunes diplômés de l'École nationale de police du Québec ont hâte de revêtir leurs uniformes de policiers combattants du crime, courageux et invincibles. Ils rêvent au succès et à la gloire, et beaucoup d'entre eux croient profondément à l'idéal de leur profession. Mais, progressivement, une faille se crée entre cet idéal et les réalités du terrain, pour se confronter finalement à une tout autre réalité : la « gestion de la misère humaine ». C'est une réalité à laquelle les jeunes policiers doivent faire face, sans pour autant avoir été préparés : loin d'être les héros qu'ils auraient voulu être, ils sont « les ramasseurs des saletés ».

- Par exemple, 69 % des interventions des policiers du Service de police de l'agglomération de Longueuil (SPAL) au cours de l'année 2017 n'étaient pas liées à des infractions de nature criminelle; un bon nombre concernait des personnes dont l'état mental était perturbé (SPAL, 2018).

5.1.1.2 La culture traditionnelle policière

Dans la culture traditionnelle policière, celle du « combattant du crime », la question de la « santé mentale des policiers » est un tabou : ou elle ne se pose même pas, ou quand elle se pose, elle stigmatise (Ratel, 2018). Cette *culture* favorise la banalisation des émotions et *ne facilite pas la verbalisation du* ressenti des émotions.

Cette réticence génère ce qu'on appelle une « dissonance émotionnelle » : une rupture qui se manifeste quand les émotions ressenties sont en contradiction avec les normes organisationnelles. Cette dissonance émotionnelle est fortement liée, entre autres, à l'épuisement émotionnel et à l'insatisfaction au travail (Van Hoorebeke, 2005).

Dans toutes ces situations, les conséquences sont lourdes à la fois pour : a) les personnes qui se trouvent dans des situations pareilles, b) leurs familles; c) les services de police.

1. Les conséquences sur le **plan individuel** se traduisent par une confusion émotionnelle que certains policiers peuvent vivre, une dévalorisation de leur estime de soi, un sentiment de culpabilité

et de non-accomplissement professionnel, une démotivation de plus en plus importante, du cynisme et une tendance à l'énervement. Certaines personnes peuvent présenter de plus en plus des manifestations psychosomatiques qui « font écran » aux problèmes de santé mentale (raison pour laquelle la problématique de la santé mentale au travail est sous-estimée sur le plan statistique).

2. Sur le **plan familial**, les difficultés inhérentes à une telle situation (accompagnement, prise en charge) sont aggravées quand il s'agit des couples (familles) des policiers.
3. Sur le **plan institutionnel**, on note le « présentisme », les comportements inappropriés des policiers sur le terrain, les coûts financiers des remplacements, la réduction des effectifs et l'accumulation des tâches, etc.

5.1.2 Trois initiatives de Montréal et de Longueuil

Les trois initiatives que je présenterai ici sont :

1. Les pairs aidants, Service de police de l'agglomération de Longueuil (SPAL), 911, Service d'incendie de Longueuil;
2. Le *Module d'intervention en soutien aux employés (MISE)*, Service de police de la Ville de Montréal (SPVM);
3. Martine Laurier et les ateliers de sensibilisation sur le suicide, Service de police de la Ville de Montréal (SPVM).

5.1.2.1 Projet Pairs-aidants triparti, agglomération de Longueuil

Brève description du projet

Contexte : Le contexte général que je viens de présenter, soit les signaux d'alarme qui viennent du milieu policier, mais aussi de celui de la recherche en santé du travail.

Mandat : Dans ce contexte, le SPAL et deux autres services de l'agglomération de Longueuil, le 911 et le Service d'incendie, veulent se doter d'un cadre d'intervention et d'outils efficaces pour des situations de détresse sociopsychologique de leurs employés.

Quand : Étape de projet.

Quoi : Mettre en place un système de « pairs aidants », une méthode d'intervention qui a de multiples bienfaits tant pour les personnes qui reçoivent que pour celles qui donnent, mais aussi pour l'organisation.

Objectifs :

- Augmentation du sentiment d'être respecté, compris, de ne pas être jugé et sanctionné;
- Augmentation de l'espoir et de la confiance en soi;
- Bonification des compétences d'entraide et de partage des responsabilités;
- Renforcement du sentiment d'appartenance à une communauté;
- Diminution de la frustration et des épisodes dépressifs; mise en place d'un système d'échange d'expériences et d'idées.

Nous nous appuyerons entre autres, dans nos démarches de mise en place de ce programme, sur deux initiatives proposées par le SPVM : le MISE et l'atelier de sensibilisation sur le suicide.

5.1.2.2 Module d'intervention en soutien aux employés (MISE) (SPVM)

Brève description du MISE

Contexte : Ce module a été pensé à la suite du mouvement « Printemps érable » de 2012 lors duquel le SPVM a été intensément sollicité. L'objectif de cette initiative était de se donner le cadre et les outils afin de prévenir adéquatement et efficacement les comportements inappropriés ou à risque au sein du personnel du SPVM.

Objectif/mandat : Le MISE agit indépendamment des autres instances chargées des situations de ce type. Il repose sur un lien de confiance et tient à « préserver l'engagement et la fierté des membres de l'organisation » (SPVM, 2018, p. 1). D'une part, il élabore des plans de prise en charge individualisés et structurés des personnes qui présentent des facteurs de vulnérabilité et, d'autre part, il accompagne et soutient le personnel qui a repéré les comportements à risque.

Qui : Un sergent et quatre agents-conseillers; équipe flexible qui mobilise des réseaux de professionnels tant à l'interne qu'à l'externe.

Pour qui : Employés, mais aussi gestionnaires et superviseurs du SPVM.

Quand : Depuis 2014 jusqu'au présent.

Description détaillée du MISE

Prévention : À la différence d'autres instances qui se chargent de ce type de situation dans une perspective punitive de contrôle et de sanctions (les ressources humaines [RH], la Direction des affaires internes et normes professionnelles [DAINP], déontologie, mesures administratives), la vocation du MISE est d'agir en amont, **de prévenir les comportements à risque avant** que la personne se trouve dans une situation qui impose une sanction, ou **de travailler le contexte plus large** d'une personne (de travail, familial) **après** que celle-ci a subi une sanction.

Types d'interventions : 1) prévention des comportements à risque du personnel du SPVM sur le plan tant individuel qu'organisationnel grâce au développement des outils de prévention; 2) identification et évaluation du risque sur le plan des comportements et des vulnérabilités; 3) accompagnement dans la prise en charge de ces types de comportements, et soutien des gestionnaires et des superviseurs.

Principes mobilisés : Le soutien par les pairs et le caractère volontaire.

Outils : Élaboration du *Guide d'accompagnement pour l'identification des comportements à risque et leur prise en charge* afin de permettre, comme le nom l'indique, l'identification des types possibles de comportements à risque : usage de la force inappropriée (abusif ou sous-utilisation), comportements contraires à l'intégrité (relations douteuses ou négligence) ou comportements contreproductifs.

Démarche : Le MISE intervient à deux moments. Premièrement, lors de l'accompagnement de la personne confrontée à une telle situation :

- Le MISE détermine les causes qui ont mené à un comportement inadéquat aux valeurs et aux principes du SPVM :
 - › outiller la personne pour agir sur les sources des problèmes : mise en place d'un réseau de soutien composé des différents acteurs impliqués dans le développement de la résilience chez la personne (famille, entourage social).

Deuxièmement, le MISE intervient lors du retour au travail de la personne :

- Le MISE mobilise des ressources afin d'atténuer les risques et d'offrir un leadership fort tant lors de la prise en charge par les gestionnaires que par le MISE, qui peut accompagner les gestionnaires afin de coordonner les ressources impliquées : ressources humaines (RH), Programme d'aide aux policiers et policières (PAPP), santé et sécurité du travail (SST), bureau médical, experts de l'organisation, etc.

Conclusions concernant le MISE

Depuis sa création, les trois principaux types de comportements à risque pris en charge par le MISE visent : a) les compétences et les pratiques professionnelles contreproductives (61 % du nombre total des signalements, soit 212); b) l'emploi inapproprié de la force (24 %); c) les pratiques contraires à l'intégrité de la police (15 %).

Le MISE est très apprécié par le milieu ainsi que par les organisations partenaires, notamment pour le caractère volontaire, ce qui le rend unique et novateur dans la culture organisationnelle d'un service de police. Il est d'autant plus apprécié puisque le soutien se fait par les pairs, c'est-à-dire par les personnes qui connaissent intimement le travail du policier, ses risques, mais aussi ses exigences et ses tabous.

5.1.2.3 Atelier de sensibilisation sur le suicide : Tournée 5.0 (SPVM)

Brève description de l'atelier

Contexte : Cet atelier de sensibilisation sur le suicide est l'initiative d'une policière, aujourd'hui retraitée, M^{me} Martine

Laurier. L'atelier, lancé en janvier 2015 au sein du SPVM, a pour but de provoquer le dialogue. Il permet de constater, au sein des participants, que le suicide est une réalité bien présente et bien trop souvent étouffée par une culture interne et inavouée, et que le quotidien du policier est tout autant – voire davantage – voué au potentiel de suicide et de dépression que tout autre métier.

Qui : Martine Laurier et Mariano Lopez. Martine Laurier est une rescapée de cette réalité, ayant par deux fois tenté de s'ôter la vie, mais ayant réussi, à l'issue d'un travail sur soi et grâce à l'amour de ses enfants, à surmonter tout désir d'en finir pour de bon.

Pour qui : Personnes principalement issues du milieu policier, mais non exclusivement.

Quand : Depuis 2015.

Objectif : L'atelier vise à choquer les esprits et à susciter, au travers du vécu et de la théorie, une prise de conscience quant à la réalité et à la prépondérance du suicide dans le milieu policier, et au risque qu'engendre pour soi-même comme pour ses collègues cette culture du silence qui décourage toute ouverture et tout partage de sentiments de vulnérabilité, toxiques à l'image virile et invincible que devrait prétendument véhiculer tout policier.

Description détaillée de l'atelier

Déroulement/fonctionnement : Cet atelier a pour objectif non seulement de démystifier la réalité associée au suicide, mais aussi de faire prendre conscience à l'auditoire que le vrai courage, particulièrement au sein du métier de policier, consiste à être capable de lever la main et de demander de l'aide. Se retrancher dans les valeurs associées à son métier et autocensurer sa souffrance ne fait qu'entretenir un statu quo qui ne rend service à personne et qui condamne d'autres personnes, à leur tour, à taire le fardeau qui leur pèse, entretenant à tort l'illusion qu'ils sont seuls et qu'ils sont des maillons faibles d'un corps de métier baliser par l'inavouable. L'issue de cet atelier se penche ainsi, de concert avec les participants, sur les solutions potentielles à mobiliser pour favoriser l'ouverture et le soutien à ces collègues démunis et en détresse.

Conclusions concernant l'atelier

Depuis son lancement en 2015, l'atelier a été reçu avec enthousiasme par les participants, lesquels soulignent l'importance de briser les tabous. Il constitue un bon équilibre entre la théorie et le vécu.

Fady Dagher, directeur du Service de police de l'agglomération de Longueuil, Canada

Références

Institut de recherche Robert-Sauvé en santé et en sécurité du travail (IRSST) 2018. *Désordres post-traumatiques chez les policiers et les préposés du 9-1-1 : une comparaison de l'efficacité et des coûts entre l'intervention habituelle et une intervention novatrice*. Repéré à <http://www.irsst.qc.ca/recherche-sst/projets/projet/i/5403/n/desordres-post-traumatiques-chez-les-policiers-et-les-preposes-du-9-1-1-une-comparaison-de-l-efficacite-et-des-couts-entre-l-intervention-habituelle-et-une-in-2015-0029>.

Ratel, Marie-Hélène. 2018. « Des policiers veulent se faire entendre sur les risques de suicide », ICI Radio-Canada, 11 septembre 2018.

Service de police de l'agglomération de Longueuil (SPAL). (2018). Rapport des activités 2017 du SPAL. Repéré à <https://www.longueuil.quebec/fr/publications/2018/rapport-activites-2017-du-spal>.

Service de police de la Ville de Montréal (SPVM). (2018). Module d'intervention en soutien aux employés. État de situation – octobre 2018.

Van Hoorebeke, Delphine. 2005. « La dissonance émotionnelle au travail : une approche ethnométhodologique », *Management & Avenir*, vol. 3, no. 1, pp. 61-75.

5.2 PRATIQUES INSPIRANTES

5.2.1 SOLVE, une approche intégrée de la gestion des risques psychosociaux dans une organisation

Les problèmes psychosociaux nécessitent une approche très différente des efforts traditionnels. Ils constituent des menaces majeures pour les performances de l'organisation. Ensemble, ils peuvent être responsables d'un grand nombre d'accidents et de maladies au travail, provoquant incapacités, maladies et décès. Ces problèmes ont des répercussions considérables sur la productivité, les coûts et la survie même de l'organisation. Ces problèmes affectent presque tous les pays, quel que soit leur niveau de développement, tous les secteurs et toutes les catégories de travailleurs. Le Bureau international du Travail (BIT) a conçu la méthode **SOLVE** dans le but d'intégrer la promotion de la santé aux politiques de santé et sécurité au travail.

L'approche **SOLVE** est ainsi conçue pour offrir une réponse intégrée sur le lieu de travail aux problèmes de stress, de

drogue, d'alcool, de violence, de sida et de tabagisme qui s'y manifestent souvent. En liant directement les questions de santé et de sécurité au travail aux problèmes de gestion et de développement de l'organisation, **SOLVE** offre les outils d'une politique autonome et d'une action immédiate sur le lieu de travail pour réduire et prévenir les difficultés en question. Cette approche permet ainsi d'améliorer les conditions de travail sur le plan psychosocial.

Dans ce contexte, **SOLVE** est un outil qui peut contribuer à traiter la question des dangers et des risques psychosociaux liés au travail. L'expérience du BIT en matière de dialogue social lui a permis de mettre en œuvre avec succès certaines initiatives traitant de cette question, tant sur le lieu de travail qu'au sein des collectivités, en associant employeurs, travailleurs, préventeurs, gouvernements, décideurs politiques, services publics et organisations non gouvernementales.

En effet, la gestion des problèmes émergents liés à la santé au travail doit être envisagée d'un point de vue holistique prenant en compte une approche qui examine aussi bien les niveaux d'influence que les effets de synergie négative provoqués par de multiples causes et effets. Ces problèmes ont des répercussions très importantes sur la productivité, sur les coûts directs et indirects, et sur l'existence même de l'organisation.

D'une manière plus générale, ils peuvent être la source indirecte de certains problèmes au sein et à l'extérieur du milieu de travail, comme la violence, l'usage de drogues, le tabagisme et l'abus d'alcool, des tensions dans les relations familiales, la dépression, voire le suicide. Les coûts y étant associés sont potentiellement énormes, tant en ce qui a trait à la détresse humaine qu'à la charge économique.

Pour l'Organisation internationale du travail (OIT), la promotion de la santé au travail joue pleinement son rôle lorsque des activités de promotion de la santé viennent compléter les mesures de sécurité et de santé au travail (SST) en s'intégrant aux pratiques de gestion de la SST afin de prévenir accidents et maladies, et lorsque ces mêmes activités protègent et améliorent la santé et le bien-être des hommes et des femmes au travail.

Le milieu de travail est donc aujourd'hui l'endroit idéal pour traiter la question des risques psychosociaux émergents, cela grâce à l'action conjointe des employeurs, des travailleurs et des pouvoirs publics. Cette démarche requiert la mise en œuvre d'une politique de santé au travail consistant à :

- prévenir les maladies professionnelles et d'autres pathologies liées au travail, ainsi que les accidents du travail;
- améliorer les conditions de travail et l'organisation du travail;
- intégrer les risques psychosociaux aux mesures d'évaluation des risques;
- déterminer quels sont les besoins propres à l'organisation en étudiant les interactions qui lui sont inhérentes, celles qui intéressent les individus et celles qui associent individus et organisation lors de l'évaluation des conditions nécessaires à la santé des travailleurs.

À titre d'exemple, le métier de policier peut être considéré comme particulièrement stressant. Les fonctionnaires de police sont en effet constamment exposés à des risques et à la violence, tandis qu'ils se sentent totalement démunis lorsqu'ils doivent traiter de problèmes tels que l'alcoolisme ou les maladies mentales pour lesquels il n'existe pas de structures appropriées.

Une étude réalisée par des chercheurs canadiens insiste aussi sur le fait qu'ils doivent constamment être prêts à faire face à des urgences. La police se heurte par ailleurs aux mêmes problèmes que beaucoup d'autres institutions.

Ainsi, selon une étude effectuée en 1990 au Royaume-Uni, les policiers jugent les problèmes d'organisation et de gestion beaucoup plus stressants que les opérations de police proprement dites.

Parmi ces opérations, les plus stressantes sont celles qui conduisent à assister à une mort brutale, à arrêter une personne violente, à s'occuper des victimes et à informer leurs familles.

Aux États-Unis, où les crimes de sang sont nombreux, un psychologue qui a travaillé dans plusieurs services de police a constaté que de plus en plus de policiers craignaient d'être abattus : « L'opinion générale est que la vie a de moins en moins de prix, que l'on hésite de moins en moins à tuer. »

Des représentants syndicaux de policiers indiquent que ces derniers sont beaucoup plus stressés aujourd'hui en raison du trafic de drogue, et que cela provoque fatigue, alcoolisme et problèmes familiaux.

Aux États-Unis, les trois quarts des crises cardiaques dont sont victimes les policiers seraient liés au stress, et les tribunaux ont statué que tout policier victime d'une crise cardiaque, même s'il n'est pas en service, a droit à une indemnisation.

Dans ce contexte, un système global de gestion de la SST devrait prévoir d'englober les risques psychosociaux afin de pouvoir en gérer efficacement les effets selon les mêmes principes de gestion que ceux appliqués aux autres risques professionnels et d'intégrer des mesures de promotion de la santé en vue d'améliorer les pratiques de prévention.

En effet, la promotion de la santé au travail possède un potentiel d'amélioration de la vie active qui constitue un facteur important de stimulation de la productivité et des performances au travail.

L'intégration de la promotion de la santé dans les politiques de SST présente des avantages tant pour les travailleurs que pour les employeurs en ce qu'elle améliore le bien-être des travailleurs et de leurs familles sur le long terme, et qu'elle sollicite moins lourdement les systèmes de santé, de protection et de sécurité sociales. L'intégration des mesures destinées à promouvoir la santé dans les systèmes de gestion de la SST améliore les pratiques de santé au travail et contribue à construire une culture préventive.

C'est ainsi que la première édition de **SOLVE**, publiée en 2002, avait été conçue pour répondre directement aux besoins des mandants de l'OIT en vue de protéger les travailleurs contre les risques psychosociaux émergents et de promouvoir leur santé et leur bien-être au travail.

La deuxième édition a été révisée et considérablement augmentée afin de relever les nouveaux défis d'un monde du travail en pleine mutation. Les cinq thèmes de départ ont été revus à la lumière des progrès scientifiques et des bonnes pratiques. La nouvelle version intègre d'autres aspects relatifs à la promotion de la santé tels que la nutrition, le sommeil et l'activité physique. S'il est nécessaire d'évaluer les facteurs psychosociaux pour gérer et réduire le stress lorsque l'organisation du travail et la culture du lieu de travail changent, il convient également, en période de mutation, d'examiner les nouvelles situations susceptibles de contribuer au stress d'origine économique.

La nouvelle formation à la méthode **SOLVE** couvre neuf sujets liés à la promotion de la santé au travail. Cette méthode, largement interactive, vise à fournir aux participants les connaissances et les compétences nécessaires pour intégrer les thèmes en question dans une politique de sécurité et de santé au travail, ainsi que dans un programme d'actions destinées à promouvoir la santé sur le lieu de travail.

Pour atteindre ces objectifs, la méthode **SOLVE** est délibérément :

Centrée sur les personnes. Il est de plus en plus évident que les travailleurs représentent un atout décisif pour le succès de toute organisation. Leur bien-être est essentiel au développement de la « nouvelle » entreprise, qui se doit d'être saine, flexible, compétitive, fondée sur les connaissances et axée sur la qualité.

À visée préventive. La prévention est un mode d'action beaucoup plus efficace en ce qui a trait aux coûts et à la réussite que la réaction *a posteriori* à un problème. Une organisation du travail et un environnement professionnel sains sont des conditions préalables au succès d'une organisation productive.

Sensible aux différences hommes-femmes. Les modalités selon lesquelles les risques psychosociaux affectent tant les hommes que les femmes sont prises en compte. Au cours de ses activités de formation et de promotion, **SOLVE** recherche l'équilibre entre les sexes tout en évitant d'assigner un rôle spécifique à chacun d'eux.

Tournée vers les résultats. Le succès ne peut se mesurer qu'aux résultats obtenus en milieu de travail. Agir en vue de promouvoir des changements sur le lieu de travail doit être le prolongement naturel de la démarche SOLVE.

Adaptable. Les situations sont complexes et les solutions, multiples. Une approche unique pour un problème donné ne fournit pas de réponses adaptées à chaque environnement et à chaque culture. Plusieurs approches et diverses options sont présentées et discutées afin que les utilisateurs puissent mettre au point les programmes et les actions qui répondront à leurs propres besoins dans leur situation particulière.

Autonome. Les programmes et les moyens d'action mis au point pour répondre aux besoins des employeurs et des travailleurs doivent fournir des résultats positifs, pouvoir être modifiés pour s'adapter aux changements de situation et être économiquement justifiés. Le programme de formation vise à une action pérenne qui pourra facilement se poursuivre dans l'entreprise tout en restant rentable.

En définitive, SOLVE propose une approche innovante grâce à laquelle la santé, la sécurité et le bien-être des travailleurs s'intègrent au développement de l'organisation et à sa pérennité économique en contribuant à sa productivité et à sa compétitivité dans une économie mondialisée. SOLVE procure aussi des outils qui permettent d'élaborer une telle politique et de mettre en place immédiatement les démarches visant à réduire ou à éliminer les risques émergents liés à ces problèmes en milieu de travail.

*Marie Diallo, directrice de la prévention
des risques professionnels, Caisse de sécurité sociale, Sénégal*

5.2.2 Prévention des impacts psychologiques dans la pratique des métiers d'urgence : présentation d'une formation en ligne pour les policiers, les techniciens ambulanciers paramédics et les pompiers

Depuis quelques années, le milieu de la recherche et les médias s'intéressent de plus en plus aux impacts psychologiques inhérents au métier des intervenants en situation d'urgence. Qu'il s'agisse de pompiers, de policiers ou de techniciens ambulanciers paramédics, tous ces travailleurs se retrouvent

quasi quotidiennement exposés à des événements bouleversants, stressants ou traumatisants. Dans les faits, rares sont les moments où l'on fait appel à eux pour des événements heureux.

Bien que ces intervenants aient été conscients de la réalité de leur métier au moment de leur embauche, il n'en demeure pas moins que cette exposition répétée à des événements bouleversants, stressants ou traumatisants peut, à différents degrés, finir par les affecter sur le plan psychologique. D'ailleurs, plusieurs études démontrent que les métiers du domaine de l'urgence sont plus à risque, dans leurs fonctions, d'être touchés par des problématiques telles que la détresse psychologique, le stress et les syndromes post-traumatiques (Carlier et Gersons, 1994; De Soir, Daubechies et Van Den Steene, 2012; Gersons et Carlier, 1992, 1994; Lilly et Allen, 2015). Les conséquences de cette « usure » se répercutent non seulement sur l'intervenant, mais aussi sur l'ensemble de l'organisation. Dans la même veine, l'Organisation internationale du travail relève que la mauvaise santé psychologique au travail coûte près de 4 % du produit intérieur brut des pays de l'Union européenne et qu'aux États-Unis, les dépenses publiques liées à la dépression s'élèvent annuellement entre 30 et 44 milliards de dollars (Gabriel et Liimatainen, 2000).

Devant ce constat, il importe, pour les intervenants, de bien comprendre les risques psychologiques de leur travail et de bien s'outiller afin de favoriser une meilleure adaptation et une récupération à la suite de l'exposition à des événements bouleversants, stressants ou traumatisants.

Dans cet esprit, nous avons développé une formation en ligne adaptée pour chacun des métiers d'urgence suivants : policier, technicien ambulancier et pompier. En effet, bien que le canevas général soit le même, chaque métier a une formation qui lui est propre avec, notamment, des témoignages de pairs.

Plus spécifiquement, les **objectifs généraux** de cette formation visent à :

- Améliorer la compréhension des impacts psychologiques inhérents au métier d'intervenant en situation d'urgence;
- Soutenir les pairs quant à leurs besoins psychologiques;

- Clarifier les rôles et les responsabilités en ce qui a trait à la prévention psychologique auprès des pairs;
- Connaître les principaux outils de prévention qui s'offrent aux intervenants en situation d'urgence;
- Comprendre les différentes réactions des intervenants pourtant exposés au même événement potentiellement traumatisant;
- Développer des stratégies d'adaptation personnelles pour contrer les impacts psychologiques;
- Comprendre le concept de résilience chez les intervenants en situation d'urgence.

Cette formation en ligne offre **plusieurs avantages**. Elle permet de s'adapter aux capacités organisationnelles, d'offrir de la flexibilité à l'utilisateur (courtes sessions, horaires variés, possibilité de faire des pauses), d'être accessible sur différents types d'appareils (ordinateur de table, tablette électronique, cellulaire) et a l'avantage d'être mise à jour régulièrement afin de s'adapter aux recommandations et aux nouvelles pratiques.

D'une durée totale approximative de **cinq heures**, cette formation **se divise en quatre modules** :

1. Le soutien des pairs;
2. Les outils de prévention;
3. Les variabilités individuelles;
4. Les stratégies d'adaptation et la résilience.

Le module *Le soutien des pairs* explique non seulement l'importance du soutien des pairs, mais il apporte aussi plusieurs informations quant aux diverses réactions et aux divers symptômes possibles lors d'événements stressants, bouleversants ou potentiellement traumatisants. Ce module permet donc aux participants de répondre aux questions suivantes :

- Pourquoi le soutien des pairs est-il important?
- Quels sont les faux pas à ne pas faire quand on aide un pair?
- Pourquoi est-ce difficile pour un intervenant de demander de l'aide?
- Quelles réactions normales possibles peuvent apparaître à la suite d'un événement stressant,

bouleversant ou potentiellement traumatisant?

- À partir de quand une réaction normale devient-elle un symptôme?
- Est-ce que les termes « stress », « anxiété » et « traumatisme » sont des termes similaires?
- Les *flash-back* sont-ils toujours forcément négatifs?
- Qu'est-ce qu'un état de stress post-traumatique? Qu'est-ce qu'un état de stress aigu?

Le module *Les outils de prévention* explique au participant les notions de base liées à la prévention primaire, secondaire et tertiaire. Pour chacune de ces formes de prévention, des actions concrètes sont présentées afin d'améliorer la compréhension des outils couramment offerts aux intervenants. Au terme de ce module, les participants seront en mesure de répondre aux questions suivantes :

- Pourquoi la prévention est-elle essentielle?
- Quelles sont les trois formes de prévention?
- Quelles sont les actions préventives concrètes?
- Quelle est l'importance de la préparation mentale?
- Quels sont les outils de prévention secondaire et tertiaire pour les intervenants?
- En quoi une consultation psychologique peut-elle être bénéfique pour les intervenants?

Dans le module *Les variabilités individuelles*, les thèmes abordés permettent au participant de comprendre les différences de réactions entre les intervenants pourtant exposés au même événement. Pour ce faire, différents concepts sont vulgarisés afin de permettre au participant de comprendre les réponses aux questions suivantes :

- Pourquoi y a-t-il des différences de réactions entre les intervenants?
- Qu'est-ce que l'identification à la victime?
- Qu'est-ce que l'usure de compassion?
- Qu'est-ce que l'accumulation de facteurs de risque?
- Existe-t-il des différences générationnelles?

Et, finalement, le module *Les stratégies d'adaptation et la résilience* aborde des sujets en lien avec l'adaptation et la récupération à la suite de l'exposition à des événements bouleversants, stressants ou traumatisants. Or, à la fin de

ce module, les intervenants seront en mesure de répondre aux questions suivantes :

- Qu'est-ce que l'adaptation?
- Quelles sont les meilleures stratégies d'adaptation?
- Comment améliorer sa gestion du stress?
- En quoi le discours interne de l'intervenant est-il important?
- Qu'est-ce que la résilience?

Afin de rendre chaque formation en ligne plus attrayante et plus ludique, **divers outils pédagogiques** sont proposés au participant. En outre, les informations sont transmises par l'entremise de courtes capsules vidéo, de bandes dessinées, de présentations PREZI (présentations qui utilisent des mouvements, des zooms et des relations spatiales pour donner vie à la théorie), de questionnaires, d'autoévaluations, de lectures et de vidéos de témoignages d'intervenants.

En terminant, l'École nationale de police du Québec déploie constamment des efforts afin d'offrir des services et des outils à la fois efficaces et conformes aux meilleures pratiques. C'est dans cette perspective que l'École s'est affiliée avec la professeure Andrée-Ann Deschênes de l'Université du Québec à Rimouski afin de valider l'efficacité engendrée par cette formation en ligne. Ainsi, dans les prochains mois, **une étude** évaluera les effets organisationnels et personnels sur la santé psychologique au travail d'une telle formation et déterminera, si nécessaire, des pistes d'amélioration à partir des résultats de cette recherche.

Pour plus de renseignements, nous vous invitons à communiquer avec madame Josée Bergeron, psychologue à l'École nationale de police du Québec.

Yves Guay, directeur général,

École nationale de police du Québec, Canada

Références

Carlier, I. et Gersons, B. (1994). Trauma at work: Post-traumatic stress disorder – An occupational hazard. *Journal of Occupational Health Safety Australia and New Zealand*, 19, 264-266.

De Soir, E., Daubechies, F. et Van Den Steene, P. (2012). *Stress et trauma dans les services de police et de secours*. Somersstraat, Belgique : Maklu.

Gabriel, P. et Liimatainen, M. (2000). *Mental health in the workplace*. Genève, Suisse : International Labour Office.

Gersons, B. et Carlier, I. (1992). Post-traumatic stress disorder: The history of a recent concept. *British Journal of Psychiatry*, 161, 742-748.

Gersons, B. et Carlier, I. (1994). Treatment of work-related trauma in police officers: Post-traumatic stress disorder and post-traumatic decline. Dans M. B. Williams et J. F. Sommer (dir.), *Handbook of post-traumatic therapy: A practical guide to intervention, treatment and research*. Westport, CT : Greenwood Press.

Lilly, M. M. et Allen, C. E. (2015). Psychological inflexibility and psychopathology in 911 telecommunicators. *Journal of Traumatic Stress*, 28(3), 262-266.

5.2.3 Analyse de risque intégrée dans le cadre de la préparation, de la gestion et de l'évaluation des événements d'ordre public, tant sur le plan opérationnel que sur celui du bien-être et de la sécurité

Introduction

Le modèle d'analyse de risque intégrée est développé dans le cadre d'événements d'ordre public, mais peut être appliqué dans de nombreux domaines du travail policier.

La police belge a opté pour une approche qualitative et pas quantitative, parce qu'il est nécessaire, pour pouvoir gérer correctement un événement d'ordre public, d'en examiner les contextes ainsi que les facteurs de risque concrets liés à cet événement spécifique. À cette fin, une méthode unique a été développée et validée au sein de la police intégrée.

L'analyse de risque intégrée englobe deux parties : une analyse de risque policière (qui détecte et réduit les risques opérationnels) et une analyse de risque sécurité et bien-être (qui doit contrer les risques que courront les policiers en exécutant les mesures déterminées dans la première analyse).

Les deux analyses doivent être contextualisées en vertu du cadre légal et philosophique belge. Elles sont indissociablement liées; il s'agit de déterminer les mesures policières avant de prendre les mesures de sécurité et de bien-être concrètes.

Pourquoi une analyse de risque?

Pour pouvoir gérer un événement d'ordre public de grande envergure, il ne suffit pas de disposer d'informations, il faut également une méthode pour les traiter. Des événements du passé nous ont appris que sans analyse, on ne peut pas détecter les risques. Et quand on ne connaît pas les risques, on peut difficilement prendre des mesures pour les contrer, même en prévoyant des effectifs policiers importants sur le terrain.

De plus, le responsable de la direction et de la coordination d'un événement d'ordre public est contraint par la loi de faire une analyse de risque.

Le cadre légal et philosophique

Dans le contexte actuel, où la police doit faire face à de nombreuses problématiques et défis allant du terrorisme et de la radicalisation à la criminalité organisée au niveau mondial, nous ne pouvons pas perdre de vue qu'à côté de ces phénomènes, la société veut (et doit) pouvoir exercer ses droits et libertés fondamentaux. Quand on parle d'ordre public, on parle de liberté d'expression, de liberté de réunion, de rassemblement et de manifestation.

La liberté de se réunir, à condition que ce soit sans armes et paisiblement, est une liberté constitutionnellement garantie. Elle est également consacrée par la Déclaration universelle des droits de l'homme (1948) et par la Convention de sauvegarde des droits de l'homme et des libertés fondamentales (1950), plus connue sous le nom de Convention européenne des droits de l'homme.

L'ordre public est indissociablement lié à l'exercice de ces droits individuels, et le maintien de l'ordre public belge s'inscrit dans un concept libéral et dynamique visant à créer les conditions nécessaires au développement démocratique de la société par le dialogue.

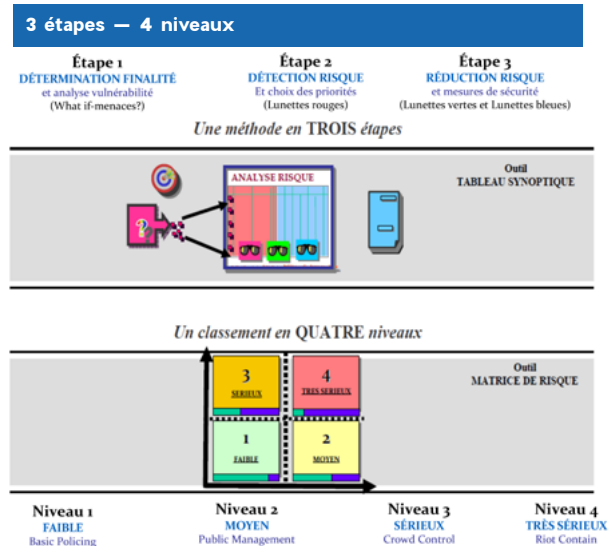
La police a longtemps considéré que l'occupation de l'espace public lors de rassemblements et de manifestations de tout ordre constituait une menace ou même une perturbation de l'ordre public normal. Elle partait du principe que sa mission était de maintenir cet ordre public en tout temps, sans prendre en considération les aspirations des participants à un rassemblement ni leurs libertés individuelles. Cela avait comme conséquence que la police était focalisée sur de possibles perturbations de l'ordre et que l'attitude policière était induite par le scénario du pire (*worst-case scenario*).

La gestion négociée de l'espace public passe par une préparation poussée réunissant autour de la table les différentes parties intéressées au dialogue. La responsabilité de la gestion des événements est partagée avec l'organisateur et l'autorité, laquelle fixe les limites de la tolérance en la matière. Dans

le modèle de gestion négociée de l'espace public, ce n'est plus l'ordre, mais bien les libertés et les droits individuels qui s'imposent en ce qui a trait aux objectifs. Lors de la préparation d'un événement, la police cherche activement le dialogue et fait preuve de compréhension.

Depuis 2001, la police belge est une police intégrée, structurée sur deux niveaux. Afin d'optimiser la sécurité lors d'événements publics, la circulaire ministérielle OOP41 a vu le jour en 2014. Cette circulaire interprétative concerne la police administrative générale, et plus précisément les aspects liés aux événements touchant l'ordre public. Dans ce cadre, une attention toute particulière est entre autres accordée aux aspects suivants : dialogue, concertation, responsabilisation, coordination et sécurité, sous la régie des autorités compétentes. L'importance de l'analyse de risque et d'une approche favorisant la désescalade est également soulignée.

L'analyse intégrée (policière, et sécurité et bien-être)



Cette analyse intégrée « policière, et sécurité et bien-être » est réalisée lors de toute préparation et évaluation d'un événement dans le cadre de la gestion négociée par le responsable à qui la « direction et la coordination des missions de police est confiée » (communément appelé *Gold Commander*).

L'analyse intégrée se compose de trois parties : les deux premières (analyse de risque policière et analyse de risque sécurité et bien-être) déterminent en trois étapes la finalité de l'analyse, la détection et la réduction des risques. Elles sont rédigées avant l'événement, et toutes les mesures de prévention sont intégrées dans l'ordre d'opération. La troisième partie est consacrée à l'évaluation des mesures prises et est réalisée après l'événement.

1. L'analyse de risque policière

Cette analyse se fait en trois étapes et aboutit à un classement en quatre niveaux.

La première étape, appelée « détermination de la finalité », est l'analyse des contextes de l'événement, ainsi que les directives des autorités administratives et judiciaires. Cela nous permettra de déterminer un concept policier pour cet événement (concept d'hospitalité, concept de contrôle ou d'éloignement, etc.). Dans cette première phase, il faut également détecter les vulnérabilités sur la base de la méthode « *What if?* ». Cette méthode n'est rien de plus qu'un remue-méninges (*brainstorming*) par un groupe d'experts : on se pose des questions sur un nombre d'hypothèses réalistes et leurs conséquences (p. ex. : Que se passe-t-il si un groupe de manifestants quitte l'itinéraire en direction d'un point vulnérable? Que se passe-t-il si le terrain du festival est surpeuplé [*overcrowding*]?). À la fin de ce remue-méninges, on localise ces menaces dans l'espace et dans le temps (où et quand).

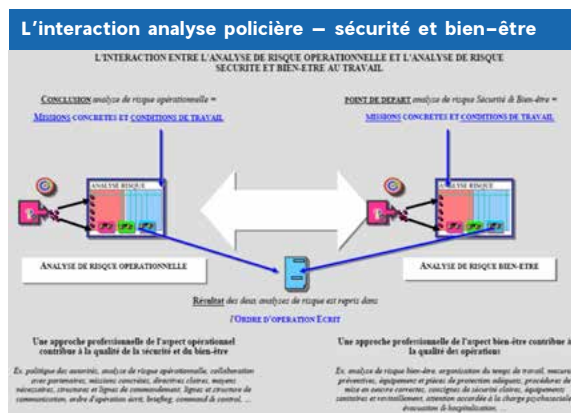
Dans la deuxième étape, appelée « détection du risque », il faut analyser les facteurs de risque humains et matériels liés aux points d'importance et leur incidence sur la probabilité et les conséquences. Il faut ensuite classer les risques selon les priorités, c'est-à-dire définir les risques concrets sur la base de la probabilité qu'un risque se réalise et les conséquences possibles s'il se produit. Pour cela, on classe les risques sur une matrice en fonction de leur importance et en quatre niveaux : vert = pc (faible probabilité, conséquences limitées) = point potentiellement important; jaune = Pc (haute probabilité, conséquences limitées) = point important; orange = pC (faible probabilité, conséquences élevées) = point potentiellement critique; rouge = PC (haute probabilité, conséquences élevées) = point critique. Le résultat de la deuxième étape est une matrice PC et une image du risque du terrain. Le positionnement des points sur la matrice PC

donne une indication des mesures de police qu'il conviendra de prendre pour un point précis. Par exemple, pour un point potentiellement important (point vert), on va orienter la police de base, des dispositifs de routine, la police de quartier, sans investissement particulier supplémentaire. Par contre, pour un point critique (point rouge), il faudra, en plus des mesures prises pour les trois autres niveaux, orienter prioritairement l'information tactique, prévoir des dispositifs préventifs (protection active) et des opérations réactives prioritaires.

La troisième étape, appelée « réduction du risque », va déterminer les mesures de police de base et d'intervention, après avoir impliqué les partenaires (services communaux, transports publics, organisateur, etc.). Après le transfert d'une partie des risques aux partenaires, les risques restants (dits « résiduels ») seront à la charge de la police, et le niveau de risque global pour l'événement sera déterminé (faible, moyen, sérieux, très sérieux). C'est en fonction de ce niveau de risque que les mesures de police seront prises.

Il est à noter que 95 % des événements d'ordre public sont de niveau 1 et sont gérés par le fonctionnement quotidien (marché, rue piétonnière, brocante, kermesse, etc.).

2. L'analyse de risque bien-être et sécurité



Tout employeur a l'obligation d'élaborer une politique ainsi qu'une stratégie en matière de bien-être au sein de son établissement, ce qui est également le cas pour la police intégrée. Cette politique, qui vise à déterminer, à analyser et à évaluer les risques présents dans le milieu de travail, permet

de les éliminer, de les gérer ou d'en diminuer les dommages pour ainsi favoriser le bien-être. La politique en matière de bien-être est opérationnalisée par l'entremise du système dynamique de gestion des risques. Le système est orienté en fonction de l'activité de l'organisation. Il doit concorder avec la politique de bien-être en place et se traduit par la mise en œuvre de la stratégie développée par l'employeur. Concrètement, ce système se base sur les domaines du bien-être, dont la sécurité au travail, la protection de la santé au travail, les risques psychosociaux, etc. Ce système regroupe donc un ensemble de procédures qui sont mises en œuvre de manière régulière. Il s'adapte en permanence à la réalité de l'organisation. En bref, nous pouvons, de manière imagée, considérer que toutes les mesures de prévention découlant du système dynamique de gestion des risques sont analogues au contenu d'une armoire.

Le résultat d'une analyse policière est étroitement lié à l'analyse de risque pour le bien-être et la sécurité du personnel et les mesures qui y sont liées. Ces mesures dépendent entre autres de la mission confiée (information, circulation, judiciaire, maintien de l'ordre), du niveau de risque global qui a été déterminé et d'autres conditions de travail (météo, terrain, équipement, etc.).

La conclusion de l'analyse de risque policière constitue les missions concrètes et les conditions de travail. C'est en même temps le point de départ de l'analyse de risque sécurité et bien-être.

Le lien entre les deux est que l'approche professionnelle de l'aspect opérationnel (p. ex. : des missions concrètes, les structures et les lignes de commandement et de communication, un *briefing* détaillé, etc.) contribue à la qualité de la sécurité et du bien-être, et inversement (p. ex. : l'organisation du temps de travail, l'équipement et les pièces de protection, les consignes de sécurité claires, etc.).

L'analyse de risque sécurité et bien-être adopte la même méthode que l'analyse policière : elle se traduit en trois étapes et en un classement en quatre niveaux.

Lors d'une analyse de risque en préparation d'un événement d'ordre public, le *Gold Commander* devra, outre les mesures opérationnelles, prendre des mesures de sécurité et de bien-être. Pour cela, il puisera d'abord dans les mesures de base déjà existantes (l'armoire) et y ajoutera, selon le contexte dans

lequel se déroule l'événement, des mesures opérationnelles et des mesures spécifiques non opérationnelles. Un exemple de mesures prises dans le cadre d'une mission « isolement de l'Eurozone » figure ci-dessous.

L'analyse de risque dans la formation

MISSION : ISOLER l'EUROZONE (Point Critique = PC) à l'occasion d'une Manifestation « European Milk Board » en 2017



Surtout risques de niveau 4 ordre public: U constituées (GNEP B)

Mesures de base employeur (armoire) : équipement maintien d'ordre, armement individuel + collectif, éléments de protection, bouclier, radio, formation et entraînement niveau GNEP B...

Mesures policières (valise) : choix emplacement position contrôle, ruban police (symbolique), choix GNEP niveau B, envergure U, directives OO, accumulation graduelle, chevaux de frise ancrés, arroseuse, réserve, team vidéo, cougar (lacry), spray collectif (pepper), OO complet et clair + briefing, structure de commandement clair et logique, choix tenue + équipement, Officier de liaison + dialogue police, INDIA (info), JUDI (judiciaire)...

Mesures spécifiques (valise) : accords organisateur pour Itinéraire + service d'ordre interne, info aux participants, fermer/vider chantiers proximité, dispositif de décontamination (fumier, lait, lacry, pepper,...), débriefing, service médical, mesures <> tracteurs, service psycho-social, bouchons oreilles, ravitaillement, tournante (pause)...

L'analyse policière et l'analyse relative à la sécurité et au bien-être sont organisées en deux modules distincts sur la base de cas pratiques. Ces analyses sont intégrées dans plusieurs formations : la formation initiale de commissaire, le brevet de direction, la formation *Gold Commander*, etc.

Si la méthode est universelle, la complexité des cas examinés est adaptée au niveau de formation. Dans chaque formation, il y a une partie théorique et une partie pratique qui consiste à effectuer le cycle de l'analyse de risque à l'aide d'un document de base et à déterminer les mesures : mesures de base ainsi que mesures opérationnelles et spécifiques.

Freya Oosterlinck, commissaire de police, chef de département de la Police administrative à l'Académie nationale de police, Police fédérale, Belgique

5.2.4 Nouvelle approche de formation en désescalade à l'École nationale de police du Québec

Depuis 50 ans, l'École nationale de police du Québec offre des formations et des activités afin de développer et de maintenir les compétences des policiers et des acteurs de la sécurité publique.

En vue d'exercer la profession policière au Québec, deux programmes de formation successifs et complémentaires doivent être complétés :

- Le programme de formation en techniques policières, offert dans l'un des collèges d'enseignement supérieur, d'une durée de trois ans;
- Le programme de formation initiale en patrouille-gendarmerie de l'École nationale de police du Québec, d'une durée de 15 semaines, permettant l'intégration à un poste de police-école.

L'École offre également plus d'une centaine de cours de perfectionnement policier en matière d'intervention policière, d'enquête et de gestion, dont plusieurs de niveau universitaire. Elle dispose d'un réseau de formateurs accrédités, notamment dans le domaine de l'emploi de la force au sein de tous les services de police du Québec.

La communication

Parmi les différentes fonctions du policier, l'une des tâches les plus communes et les plus récurrentes est certainement celle d'interagir avec les citoyens. Ainsi, qu'il s'agisse de saluer, de questionner, de rassurer ou d'ordonner, le policier adresse au quotidien un message à un citoyen, témoin, plaignant, victime, suspect qui, selon sa perception, réagira de façon positive ou non. C'est dans ce contexte que la communication est considérée comme une option permettant au policier de maîtriser une situation et, par conséquent, de faciliter son intervention.

Dans son offre de formation, l'École privilégie les stratégies de communication suivantes : la relation d'aide, la désescalade ainsi que la communication active et tactique.

La désescalade

Le concept de désescalade vise à axer la communication sur la diminution progressive d'une crise ou d'une tension, à rétablir l'équilibre de la personne, à restaurer la prévisibilité de son comportement et à résoudre de façon pacifique la situation tout en tenant compte des considérations tactiques.

Au cours des dernières années, au Canada, plusieurs interventions impliquant des policiers auprès de personnes en crise dont l'état mental était perturbé ou encore de personnes aux prises avec des problèmes de santé mentale ont nécessité de bonifier certaines pratiques policières afin d'y intégrer des stratégies de communication adaptées à ces circonstances.

De plus, étant donné qu'une intervention policière implique une dimension humaine, une attention particulière est portée au savoir-être, à la gestion du stress ainsi qu'aux habiletés du policier à interagir auprès des personnes afin de rétablir un climat de confiance.

Principaux éléments de désescalade intégrés aux formations

Établir un contact avec la personne en...

- gardant une distance sécuritaire;
- pensant à la personne d'abord, en adoptant une attitude aidante;
- créant un environnement calme et non menaçant;
- ne brusquant pas la situation s'il n'y a pas urgence d'agir.

Aider à trouver ou à suggérer des solutions en...

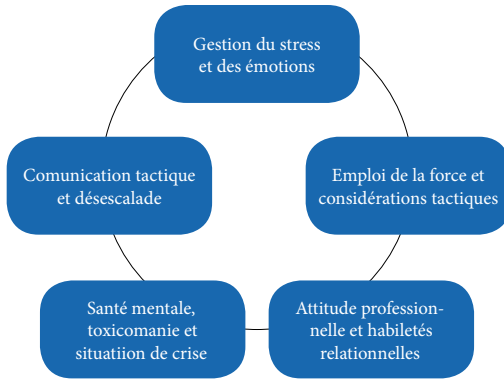
- déterminant les besoins immédiats de la personne;
- offrant des solutions communes;
- connaissant les ressources disponibles qui permettront de combler les besoins immédiats de la personne.

Assurer une conclusion pacifique de l'intervention en...

- accompagnant ou en dirigeant la personne vers les ressources de la communauté les plus appropriées;
- encourageant la personne dans son choix de collaborer;

- utilisant une communication orientée de façon à répondre à ses besoins immédiats;
- effectuant un suivi à court terme.

Cette stratégie vise une approche intégrée de la communication :



Déclinaison du concept de désescalade dans nos activités de formation

Formation initiale des futurs policiers

Au cours des trois années de formation collégiale en techniques policières, le programme intègre plusieurs énoncés de compétence en lien avec l'intervention policière auprès d'une personne aux prises avec un problème de santé mentale.

En ce qui concerne la formation initiale des aspirants policiers à l'École, elle a été bonifiée sur le plan de l'intensité physique, du contrôle des émotions, de la résistance au stress ainsi que du renforcement des techniques de désamorçage et de désescalade de situation de crise :

- Ajout d'un séminaire sur la gestion du stress et des émotions;
- Ajout de stratégies de communication relatives aux problématiques de santé mentale;
- Mises en situation complémentaires auprès de personnes en crise et vulnérables avec plusieurs variantes : sujet armé, non armé, suicidaire; suicide par policier interposé; délire agité; conscience altérée. L'objectif est d'axer l'intervention sur l'utilisation

des techniques de désescalade, de communication et d'intervention physique et tactique.

De plus, l'École a amélioré plusieurs activités existantes afin d'augmenter l'intensité et le réalisme des interventions simulées :

- Ajout de variantes aux mises en situation afin de les rendre plus intenses et plus réalistes;
- Intégration de signes à repérer par les aspirants policiers faisant face à des individus ayant un état mental perturbé;
- Ajout de comportements et de paroles dans le cadre des jeux de rôles et des mises en situation qui ont pour but de provoquer une charge émotive;
- Ajout d'intensité physique, de complexité et de tournage des mises en situation par des caméras citoyennes.

Perfectionnement policier

L'École procède à la mise à jour de l'ensemble des formations en emploi de la force et en communication tactique afin d'intégrer de nouveaux éléments en lien avec la désescalade, et ce, afin d'avoir une approche plus intégrée des interventions.

De plus, l'École a conçu une formation pratique offerte sur le campus et en région : *Intervenir sécuritairement auprès d'une personne en crise*.

Cette formation permet à l'étudiant de déterminer les stratégies adaptées à un contexte de tension sociale ou auprès d'une personne dont l'état mental est perturbé. L'étudiant pourra ainsi réactiver ses compétences relatives à la communication tactique et à la désescalade, ainsi que le Modèle national de l'emploi de la force.

Une offre de formation portant spécifiquement sur la désescalade est offerte en ligne avec, en complément, une portion pratique déployée par le réseau de formateurs.

Désescalade – État mental perturbé (formation en ligne)



Destinée aux intervenants de première ligne, cette formation de sept heures a comme objectif d’outiller le patrouilleur afin qu’il intervienne de manière adéquate auprès des personnes dont l’état mental est perturbé en favorisant un dénouement pacifique des situations de façon à réduire les risques de blessures et de décès.

La formation en ligne se divise en modules comprenant de l’autoapprentissage de notions théoriques visant à mieux comprendre les personnes dont l’état mental est perturbé et les techniques de désescalade.

Formation pratique Désescalade – État mental perturbé (volet pratique)

À la suite de la formation en ligne, les participants sont invités à participer à la formation pratique qui se donnera au sein de leur organisation grâce au réseau des formateurs accrédités par l’École.

D’une durée de sept heures également, cette formation pratique permettra l’intégration des connaissances apprises lors de la formation en ligne, à l’intérieur de mises en situation reflétant les cas les plus observés au sein des corps de police. L’objectif de cette phase 2 est d’augmenter la capacité à intervenir auprès des personnes dont l’état mental est perturbé.

Formation des moniteurs Désescalade – État mental perturbé – Le moniteur

Les formateurs qui offrent la formation pratique au sein de leur organisation doivent préalablement avoir suivi une formation d’une durée de deux jours à l’École nationale de police du Québec.

Le webdocumentaire *Vulnérable*



Réalisé en 2013, le webdocumentaire *Vulnérable. Intervention policière auprès d’une personne en crise* est toujours d’actualité. On recense plus de 40 000 sessions individuelles ou de groupe d’une durée moyenne de 18 minutes depuis sa création.

Cet outil de formation vient en soutien à l’ensemble des programmes de formation initiale et de perfectionnement. Il est également disponible gratuitement pour les policiers du Québec ainsi que pour les partenaires internationaux. Des écoles de police belges et suisses l’utilisent dans certaines formations.

Il plonge l’étudiant au cœur de l’intervention policière auprès d’une personne présentant un trouble mental et en crise.

Vous y trouverez l’expertise de spécialistes en intervention en situation de crise; vous serez témoins de réelles interventions policières avec un agent spécialiste en santé mentale et vous plongerez directement au cœur du processus de communication avec une personne en crise; vous entendrez le point de vue des gens atteints qui ont fait l’objet d’une intervention policière alors qu’ils étaient en crise. Tout au long des vidéos, des policiers de différents corps de police du Québec s’adressent directement aux experts.

Ensemble, experts, policiers et personnes atteintes partagent avec l’étudiant les stratégies les plus efficaces, les plus sécuritaires et les plus humaines pour désamorcer une crise.

Défi : Un modèle de requalification à améliorer

Au cours des dernières années au Québec, plusieurs recommandations en provenance de diverses instances

s'interrogent sur la requalification et le maintien des compétences des policiers au cours de leur carrière. Les activités de perfectionnement professionnel sont encore partiellement éclatées et manquent parfois de cohérence.

Le système québécois de requalification et de maintien des compétences des policiers mérite d'être renforcé et consolidé dans des domaines critiques comme l'emploi de la force, dont l'utilisation de l'approche de désescalade, la conduite d'urgence, les enquêtes et l'intervention policière en lien avec de nouvelles réalités sociales.

La piste de solution réside dans l'analyse de faisabilité de mise en place d'un système en requalification semblable à certaines autorités qui exigent une requalification des policiers, sur diverses thématiques, à fréquence déterminée, dans une approche intégrée et évolutive.

Pierre St-Antoine, directeur des affaires institutionnelles et des communications, École nationale de police du Québec, Canada

5.2.5 Gestion de la santé mentale psychologique au travail des policiers : les six principes incontournables pour une meilleure pratique organisationnelle

Le travail rémunéré est l'une des responsabilités les plus prédominantes de la vie adulte. Cela soulève un questionnement légitime quant à la portée du milieu de travail sur la vie de l'individu. De ce fait, la santé psychologique au travail fait partie intégrante des préoccupations des travailleurs dans l'ère d'aujourd'hui, et ce, tous statuts confondus. Au Québec, en 2008, un travailleur sur cinq présentait un niveau de détresse psychologique élevé (Vézina, St-Arnaud, Stock, Lippel et Funès, 2011). Les chercheurs avancent que d'ici 2020, la dépression sera la deuxième cause d'invalidité à l'échelle mondiale, tout juste derrière les maladies cardiaques (Organisation mondiale de la Santé, 2001). Plus encore, l'enquête nationale de Morneau Shepell (2015) précise que 58 % des employés canadiens indiquent que le stress au travail a eu des répercussions négatives sur leur productivité. L'Organisation internationale du travail relève que la mauvaise santé psychologique au travail coûte près de 4 % du produit intérieur brut des pays de l'Union européenne et qu'aux États-

Unis, les dépenses publiques liées à la dépression s'élèvent annuellement entre 30 et 44 milliards de dollars (Gabriel et Liimatainen, 2000). La situation est donc préoccupante autant pour les travailleurs que pour leurs gestionnaires.

Plusieurs études démontrent que les métiers du domaine de l'urgence sont plus à risque d'être touchés par des problématiques telles que la détresse psychologique, le stress et les syndromes post-traumatiques (Carlier et Gersons 1994; De Soir, Daubechies et Van Den Steene, 2012; Gersons et Carlier, 1992, 1994; Lilly et Allen, 2015). En effet, les forces policières représentent l'une des premières lignes en matière d'intervention publique quant au besoin de contrôle de la criminalité, des situations d'urgence, des atteintes à l'ordre public et des réponses à une large variété de demandes de services provenant de citoyens. Leur travail est complexe, considérant la gestion de l'inattendu, du soudain, de l'incontrôlable et de l'imprévisible, de multiples facteurs avec lesquels ils doivent composer. En plus de ces facteurs opérationnels, le policier compose avec des particularités organisationnelles telles qu'une hiérarchie de type paramilitaire, un horaire de travail irrégulier, le négativisme du public et celui des médias (De Soir *et al.*, 2012).

Kleim et Westphal (2011) expliquent que lorsque les premiers répondants vivent de la détresse psychologique liée au travail, des coûts personnels et publics importants peuvent en résulter, dont des répercussions négatives sur les services offerts à la population. Considérant la portée de leur rôle pour la société et les effets bénéfiques d'une saine santé psychologique au travail, il est important de consacrer des efforts pour assurer une gestion adéquate de la santé psychologique au travail des policiers.

Qu'est-ce que la santé psychologique au travail?

La santé psychologique au travail se compose de dimensions bipolarisées, soit la détresse psychologique et le bien-être psychologique. Dans leurs travaux, Gilbert, Dagenais-Desmarais et Savoie (2011) mettent en évidence trois facteurs pour chacune de ces dimensions. Ces facteurs définissent les rapports du travailleur avec lui-même : au travail, avec son travail et avec son entourage au travail. Ces trois facteurs s'expriment différemment en fonction des dimensions positive ou négative de la santé psychologique au travail. Selon Gilbert et al. (2011), lorsqu'une personne éprouve du bien-être psychologique au travail, elle se sent sereine, en paix avec elle-même (sérénité); elle aime son travail et ses réalisations, elle a le désir et l'ambition de s'engager (engagement); elle est à l'écoute d'autrui, se sent appréciée et aimée, et entretient de belles relations avec son entourage au travail (harmonie sociale). À l'inverse, les individus en état de détresse psychologique au travail éprouvent de l'agressivité, de l'irritabilité et de l'impatience à l'égard d'autrui. Face à eux-mêmes, ils se sentent anxieux, tristes, dépressifs, stressés et ont peine à affronter leurs problèmes. En regard du travail, ils n'éprouvent plus grand intérêt, se sentent diminués, voire inutiles, et n'ont plus envie d'entreprendre des projets. En somme, les individus vivant un plus grand bien-être psychologique au travail ressentent plus d'optimisme, perçoivent leur environnement de travail comme étant plus juste et équitable, et présentent un environnement de travail plus sain (Gilbert et al., 2011).

Points de vigilance de la santé psychologique des policiers

Plusieurs études indiquent que la nature du travail des policiers n'apparaît pas comme étant particulièrement liée à la détresse (Hart, Waering et Headay, 1995; Kop et Euwena, 2001; McCreary et Thompson, 2006; Shane, 2010). Brown, Cooper et Kirkcaldy (1996) soutiennent que la plus grande source de stress dans le contexte du travail policier constitue la

structure organisationnelle. Tout compte fait, les expériences organisationnelles semblent plus déterminantes que les expériences opérationnelles pour déterminer la détresse psychologique et le bien-être psychologique au travail des policiers. À titre d'exemple, selon l'étude de Deschênes, St-Hilaire, Crête, Emeriau Farges et Desjardins (2019), il est vrai que l'événement potentiellement traumatique vécu lors des tâches opérationnelles du policier peut être nocif pour la santé psychologique de ce dernier. À titre indicateur, en 2008, 32 % des policiers mentionnaient avoir vécu un tel événement (Leclercq, 2008), alors qu'en 2017, il est recensé que 50 % de ces derniers ont été exposés à un événement potentiel traumatique. Toutefois, la prise en charge déficiente de l'organisation policière à la suite d'une telle exposition est plus susceptible de faire vivre de la détresse psychologique au policier que l'événement en tant que tel.

Qu'est-ce qu'un événement potentiellement traumatique?

L'événement potentiellement traumatique est considéré comme tel s'il provoque chez le travailleur une réaction émotionnelle affectant ou étant susceptible d'altérer son fonctionnement au travail (Josse, 2014). L'auteure ajoute qu'un événement potentiellement traumatique peut s'avérer traumatisant pour une personne et ne pas l'être pour une autre. Plus encore, il peut être traumatisant aujourd'hui et ne pas l'être demain.

Selon les résultats de l'étude de Deschênes, Desjardins et Dussault (2018), le policier serait plus vulnérable sur le plan de la santé psychologique au travail à partir de la sixième année de service dans la même organisation policière, et ce, jusqu'à sa vingtième année de service. Les auteurs rapportent qu'après la sixième année de service, le policier remet en question sa profession à l'égard de ses aspirations futures. Il connaît de mieux en mieux la réalité policière à l'inverse de ses idéologies de début de carrière. Force est de constater que le policier pourrait, entre autres, commencer à manifester de l'usure de compassion lors de cette période de vulnérabilité.

Comment gérer la santé psychologique au travail des policiers?

Des études réalisées spécifiquement dans le contexte des organisations policières à travers le monde s'entendent sur six grands principes de la gestion de la santé psychologique au travail dans le milieu policier (Brown *et al.*, 1996; Burke, 1998; Burke et Mikkelsen, 2006; Deschênes *et al.*, 2018) :

PRATIQUES DE GESTION À PRIVILÉGIER	EXEMPLES
Sensibiliser et éduquer le personnel policier aux problématiques de la santé psychologique au travail afin d'éliminer les tabous et les jugements.	Donner accès à des formations sur le sujet. Éviter de juger ou de minimiser les problématiques psychologiques. Encourager les bienfaits de l'accompagnement psychologique.
Avoir une procédure de prise en charge du personnel policier à la suite d'une exposition à un événement potentiellement traumatique, et ce, sans banaliser l'effet d'un type d'événement.	S'assurer de l'existence de procédures de suivi dans l'organisation à la suite d'une telle exposition.
Renforcer le lien social, le développement de relations positives entre les collègues.	Organiser des activités de consolidation d'équipe. Donner du temps aux équipes de travail pour discuter à la suite d'une intervention, quand c'est possible.
Mettre en place des méthodes de reconnaissance de la part de l'organisation et du supérieur immédiat à l'égard du policier.	Reconnaître les efforts du policier et ses méthodes de travail, et non seulement sa performance. Exercer des pratiques de reconnaissance régulièrement.
Opter pour un style de gestion participatif en utilisant l'autonomie et la créativité du personnel policier.	Prendre en compte les idées de l'équipe de travail lors d'une prise de décision les concernant. Favoriser l'émergence d'idées novatrices chez les policiers au lieu de les restreindre à leurs fonctions habituelles.
Favoriser le soutien de la direction dans la tâche du policier.	Démontrer des disponibilités à discuter avec le policier (présence physique ou téléphonique). Partager régulièrement des rétroactions avec l'équipe de travail.

À la lumière de ces constats, force est d'admettre qu'il est devenu un incontournable pour les organisations policières d'opter pour des pratiques de gestion favorisant la santé psychologique au travail. L'objectif de cet écrit consistait à proposer des pistes de réflexion concrètes pour soutenir les gestionnaires du milieu policier dans le développement de ces stratégies. Il est possible de croire qu'une fois ces méthodes mises en place, toutes les parties impliquées bénéficieront des avantages.

Et si la gestion de la santé psychologique au travail des policiers était devenue un levier de la performance et de l'efficacité des organisations policières?

Andrée-Ann Deschênes, Université du Québec à Rimouski;

Annie Gendron, École nationale de police du Québec;

Josée Bergeron, École nationale de police du Québec;

Manon Beaumier, Université du Québec à Trois-Rivières

Références

- Brown, J., Cooper, C. et Kirkcaldy, B. (1996). Occupational stress among senior police officers. *British Journal of Psychology*, 87, 31-41.
- Burke, R. J. (1998). Work and non-work stressors and wellbeing among police officers: The role of coping. *Anxiety, Stress & Coping*, 11(4), 345-362.
- Burke, R.J. et Mikkelsen, A. (2006). Burnout among Norwegian police officers: Potential antecedents and consequences. *International Journal of Stress Management*, 13(1), 64-83.
- Carlier, I. et Gersons, B. (1994). Trauma at work: Post-traumatic stress disorder – An occupational hazard. *Journal of occupational Health Safety Australia and New Zealand*, 19, 264-266.
- Deschênes, A.-A., Desjardins, C. et Dussault, M. (2018). Psychosocial factors linked to the occupational psychological health of police officers: Preliminary study. *Cogent Psychology*, 5(1).
- Deschênes, A.-A., St-Hilaire, G., Crête, E., Emeriau Farges, C. et Desjardins, C. (2019). L'événement potentiellement traumatique et la santé psychologique au travail des policiers; une perception d'un impact unique? *Psychologie du travail et des organisations* (Document soumis).
- De Soir, E., Daubechies, F. et Van Den Steene, P. (2012). *Stress et trauma dans les services de police et de secours*. Somersstraat, Belgique : Maklu.
- Gabriel, P. et Liimatainen, M. (2000). *Mental health in the workplace*. Genève, Suisse : International Labour Office.
- Gersons, B. et Carlier, I. (1992). Post-traumatic stress disorder: The history of a recent concept. *British Journal of Psychiatry*, 161, 742-748.
- Gersons, B. et Carlier, I. (1994). Treatment of work-related trauma in police officers: Post-traumatic stress disorder and post-traumatic decline. Dans M. B. Williams et J. F. Sommer (dir.), *Handbook of post-traumatic therapy: A practical guide to intervention, treatment and research*. Westport, CT : Greenwood Press.
- Gilbert, M.-H., Dagenais-Desmarais, V. et Savoie, A. (2011). Validation d'une mesure de santé psychologique au travail. *Revue européenne de psychologie appliquée*, 61(4), 195-203.

Hart, P. M., Wearing, A. J. et Headey, B. (1995). Police stress and well-being: Integrating personality, coping and daily-work experience. *Journal of Occupational and Organizational Psychology*, 68(2), 133-156.

Josse, É. (2014). *Le traumatisme psychique chez l'adulte*. Bruxelles, Belgique : De Boeck.

Kleim, B. et Westphal, M. (2011). Mental health in first responders: A review and recommendation for prevention and intervention strategies. *Traumatology*, 17(4), 17-24.

Kop, N. et Euwema, M. (2001). Occupational stress and the use of force by dutch police officers. *Criminal Justice and Behavior*, 28(5), 631-652.

Leclercq, C. (2008). *Les modalités de la prise en charge et de la gestion des événements traumatiques vécus par les policiers au cours de leurs fonctions au Québec*. (Thèse de doctorat inédite). Université de Montréal.

Lilly, M. M. et Allen, C. E. (2015). Psychological inflexibility and psychopathology in 911 telecommunicators. *Journal of Traumatic Stress*, 28(3), 262-266.

McCreary, D. R. et Thompson, M. M. (2006). Development of two reliable and valid measures of stressors in policing: The operational and organizational police stress questionnaires. *International Journal of Stress Management*, 13(4), 494-518.

Morneau Shepell. (2015). *Priorités en matière de santé mentale au travail*. Repéré à <https://www.morneaushepell.com/sites/default/files/documents/3464-rapport-sur-les-priorites-en-matiere-de-sante-mentale-au-travail-2015/11227/2015-morneaushepellbooklet-avantages.pdf>.

Organisation mondiale de la Santé. (2001). *Rapport sur la santé dans le monde 2001 - La santé mentale : nouvelle conception, nouveaux espoirs*. Genève : Organisation mondiale de la Santé.

Shane, J. M. (2010). Organizational stressors and police performance. *Journal of Criminal Justice*, 38(4), 807-818.

Vézina, M., St-Arnaud, L., Stock, S., Lippel, K. et Funès, A. (2011). *Enquête québécoise sur des conditions de travail, d'emploi, de santé et de sécurité du travail 2007-2008 (EQCOTESST). Chapitre 9 : santé mentale* (Rapport R-691). Montréal, Québec : Institut de la statistique du Québec, Institut national de santé publique du Québec et Institut de recherche Robert-Sauvé en santé et sécurité du travail.

5.2.6 ÉCHANGES

Yves Guay, un panéliste québécois, mentionne à l'assistance « qu'aucune organisation n'a les moyens de travailler seule. Il faut partager et adapter les initiatives à son milieu ».

Un congressiste commissaire de police divisionnaire pose une question sur l'analyse de risque intégrée, présentée par M^{me} Freya Oosterlinck. L'intervenant inscrit sa question dans le cadre de la prise de décision en s'étonnant du fait que la panéliste a fait une présentation sur le cadre d'action planifié, alors que « la police intervient dans les situations d'urgence, et non pas dans le cadre d'une action planifiée ».

La panéliste M^{me} Freya Oosterlinck répond que la structure de commandement initialement présentée prévoit de mettre en place un outil. Concernant l'aspect sécurité, la structure prévoit aussi un plan d'intervention policier d'urgence qui aboutira à la mise en place d'une procédure de commandement.

Un congressiste, le colonel Briche, veut savoir quant à lui si, dans le cadre des recherches, il est imaginé que, tous les huit ou 10 ans, on puisse prendre en charge les policiers et que, au moment de leur retraite, on leur offre une « séance de purge » afin de les faire reprendre une vie normale.

M. Guay répond de façon très brève en certifiant que dans les services québécois de police, il existe des services spécialisés accompagnant les policiers aussi bien tout au long de leur parcours que pendant l'importante phase de la retraite.

6. CONCLUSION

Le congrès est clôturé par M. Roger Ouédraogo, vice-président Afrique de FRANCOPOL. Plus qu'un discours de fermeture de session, M. Ouédraogo dresse le bilan des trois jours du congrès. De cette conclusion, il fait émerger quelques recommandations.

De manière générale, la lutte contre l'action terroriste requiert la célérité dans la riposte, combinée à une bonne capacité opérationnelle à pouvoir soutenir une intervention d'envergure. Dès lors, le congrès recommande :

- Le renforcement accru des renseignements opérationnels;
- La définition conjointe des modalités d'intervention avec l'ensemble des forces;
- La réorganisation des unités spécialisées pour pouvoir intervenir le plus rapidement et le plus efficacement possible;
- La production d'un aide-mémoire pour déterminer la responsabilité de chaque intervenant et la procédure d'intervention;
- Une organisation qui entoure tout le monde lorsqu'il y a une attaque terroriste;
- L'anticipation des interventions, permettant de répertorier des lieux susceptibles d'être attaqués et de s'entraîner à mieux réagir pour étudier la façon d'être le plus efficace possible.

Dans le domaine de la cybercriminalité, le congrès recommande :

- La création de centres de formation en criminalité technologique;
- La dotation des unités spécialisées en matériel technologique de dernière génération;
- Des formations de renforcement des capacités des enquêteurs spécialisés dans le domaine de la cybercriminalité.

S'agissant de la migration irrégulière et de ses conséquences, le congrès recommande à tous les États :

- Le plein engagement dans la lutte contre cette activité criminelle;
- La création d'emplois pour les jeunes Africains qui tentent par tous les moyens possibles de migrer vers l'Europe;
- De prévoir un plan de réinsertion professionnelle pour ceux qui vivaient de cette activité du trafic illicite de migrants (particulièrement pour le cas du Niger qui, d'ores et déjà, a pris des dispositions criminalisant ce fait).

Et, enfin, dans le domaine de la gestion des risques psychosociaux, le congrès recommande aux responsables, compte tenu des risques énormes entourant les activités de la police, de toujours bien analyser, bien évaluer les conséquences qui pourraient surgir avant de mettre en exécution une activité policière quelconque. Il est également recommandé de procéder en amont à une analyse pertinente avec tous les experts en la matière avant de s'engager, car cela pourrait sans nul doute diminuer les risques.

7. UN REGARD EXTÉRIEUR

Le congrès vu par Dorlie Kabieni Amboyi, doctorante en droit international public à la Faculté d'Angers, spécialiste des questions conflictuelles en Afrique

C'est sur le sol africain que FRANCOPOL a choisi de tenir son 5^e Congrès international et de fêter par la même occasion son 10^e anniversaire. Le choix de l'Afrique n'est sans doute pas anodin, car si ce continent est aujourd'hui une destination touristique incontournable, malheureusement, c'est aussi le territoire qui constitue le terreau de la conflictualité, avec le plus de personnes tuées chaque jour par balles de guerre.

C'est dans une Afrique tiraillée entre ce paradoxe de la guerre et de l'hospitalité que se sont ouverts à Dakar, le mercredi 17 octobre 2018, les débats de FRANCOPOL sur la thématique « Gestion des risques et des nouvelles menaces ». Ce rendez-vous de grande importance a réuni pas moins de 164 membres en provenance d'une vingtaine de pays francophones. Le congrès s'est notamment réjoui de la présence inédite du Cambodge et des Émirats arabes unis.

Les problématiques évoquées sont épineuses. En effet, il s'agit de vies humaines, comme a pu le rappeler le président d'honneur, Émile Pérez, de personnes dont les pertes sont innombrables au quotidien. Quatre thématiques ont été débattues autour de tables rondes réunissant des spécialistes africains et occidentaux, pour certains théoriciens, pour d'autres, praticiens, mais tous rassemblés dans une optique de partage.

La première thématique discutée a été le terrorisme. Cette table ronde a réuni le plus de participants tout au long du congrès. Les présentations évoquaient les aspects préventifs de la menace terroriste en essayant de répondre à la question : « Comment prévenir le terrorisme? » Si l'opinion publique fait encore l'amalgame entre le terrorisme, la radicalisation et la religion, la quasi-totalité des présentations a montré que « la radicalisation ne s'inscrit pas toujours, comme on pourrait le croire, dans une logique d'engagement religieux », comme a pu le noter la modératrice du panel, Lori-Anne Théroux-Benoni.

Les débats ont mis en lumière le fait qu'au fond, qu'il soit question de l'Occident ou de l'Afrique, les populations qui rejoignent les rangs du djihad font souvent face à l'exclusion sociale, à l'isolement, à l'incompréhension par tous et, parfois, à la négligence des pouvoirs publics. Si le sentiment d'exclusion sociale est davantage exacerbé en Occident, en Afrique, c'est la mauvaise gouvernance politique, le rang social rétrograde des femmes, des enfants et de certaines minorités qui se radicalisent le plus. Pour comprendre le phénomène, il faut d'abord analyser les raisons qui poussent les individus à partir, celles qui poussent les individus à monnayer la vie humaine. Les gens se radicalisent parce qu'ils ont faim de tolérance ou de réhabilitation dans la communauté, faim d'un repas décent, faim de sécurité ou simplement faim d'une vie meilleure.

Cette première partie a permis de comprendre que prévenir le terrorisme n'est pas toujours lié à la prégnance du dogme religieux, comme on pourrait le penser, mais qu'il s'agit davantage d'un problème économique, social et très souvent politique.

Le deuxième panel a également été consacré au terrorisme, mais a touché une phase beaucoup plus offensive de la menace. Les États mesurent leur capacité à répondre lorsque le phénomène s'est enclenché. Comment riposter au terrorisme sans causer de nombreuses pertes humaines? Le remède tient au maître-mot faisant partie de « la logique des trois C », à savoir « coordination », « complémentarité » et « cohérence », logique à laquelle on ajoute un quatrième « C », soit « coopération entre les différents services des forces armées ». Il en ressort aussi que pour vaincre le terrorisme, il faut faire tomber les questions de compétences matérielles et de compétences territoriales. Les primo-intervenants considérés comme appartenant aux corps des forces de sécurité peuvent être tout à la fois des gendarmes ou des policiers, parfois même des militaires lorsqu'il s'agit d'opérations musclées comme les attentats de Bassam en Côte d'Ivoire ou du Mali avec des forces armées permanentes.

La deuxième thématique, la cybercriminalité, a mis en lumière la transversalité et la dangerosité de la cybermenace, avec le côté « *dark Web* » qui prend de l'ampleur. D'outil de communication à outil d'information rapide, puis outil de travail perspicace et privilégié, Internet est devenu indispensable dans le quotidien. C'est ce caractère irremplaçable à l'ère du numérique qui complexifie le travail des policiers dans la lutte contre la cybercriminalité. Le pouvoir appartient désormais aux firmes et aux groupes privés tels que WhatsApp, Facebook ou Twitter, qui sont les premiers détenteurs d'informations. Ce bouleversement a eu une incidence considérable dans la gestion de la cybercriminalité, avec notamment le renversement de la preuve. Cette question a divisé les panélistes, certains pensant qu'il faut peut-être faire front devant ces firmes internationales qui se sentent toutes-puissantes, d'autres pensant plutôt qu'il faut collaborer davantage avec elles et multiplier les coopérations. Dans tous les cas, il faut s'unir, car toutes les menaces constituent aujourd'hui des cybermenaces du fait de la ramification d'Internet, outil indispensable, et qui fait lien entre toutes les menaces.

La troisième thématique, soit la gestion des flux migratoires, tout aussi passionnante, a été écourtée, compte tenu du respect du temps imposé. La réponse apportée à cette thématique semble être, comme pour le premier panel sur le terrorisme, l'importance de la dimension sociale, politique et économique avec, d'une part, les trafiquants d'êtres humains avides de ressources qui ont fait du trafic leur moyen de vivre et, d'autre part, les migrants qui s'exposent à un péril absurde au prix de leur vie, à la recherche d'un idéal social meilleur.

La gestion des risques psychosociaux a été une belle conclusion au congrès, car elle permis de prendre en compte, avec les dernières contributions, que toute révolution commence à l'intérieur de soi, dans un corps sain et un esprit sain. Mais c'est aussi savoir communiquer, avec l'exemple du modèle canadien composé des policiers retraités qui aident les jeunes policiers dans toutes les étapes de leur carrière, ou encore l'exemple du modèle suisse basé sur le principe de mise en récit (« *storytelling* ») de témoignages d'anciens policiers désireux, par le partage de leur expérience, de tendre la main à d'autres policiers en difficulté.

Bien que la plupart des plaidoyers soient davantage d'ordre politique, économique et social que policier, FRANCOPOL, comme l'a affirmé son président d'honneur, est l'endroit idéal pour faire remonter ces doléances aux différentes instances concernées.

MERCI À NOS COMMANDITAIRES

OR



ARGENT



IVOIRE





F
FRANCOPOL
Réseau international francophone de formation policière

ORGANISATION
INTERNATIONALE DE
la francophonie