

# Manuel du contributeur de données au CIDB

## Introduction

Le Canadian Incident Database (CIDB) est une base de données accessible au public destinée aux chercheurs étudiant le terrorisme et l'extrémisme violent au Canada. Le CIDB vise à être un document vivant, mis à jour régulièrement. Ce court manuel est conçu pour fournir aux contributeurs de données du CIDB des critères standardisés pour ajouter et modifier des entrées, des conseils concernant les sources, ainsi que des réponses aux questions fréquentes.

## Critères de sélection des événements

Pour être inclus dans le CIDB, un événement doit répondre à la définition de « terrorisme » ou « d'extrémisme violent » de TSAS.

## Définir le terrorisme

Le Code criminel du Canada définit un acte terroriste comme étant 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 (Code criminel, L.R.C. 1985, art. 83.01).

Le terrorisme représente une forme spécifique d'extrémisme violent de nature criminelle et politique. En pratique, cela signifie que pour envisager l'inclusion d'un incident dans le CIDB en tant qu'acte terroriste, les trois attributs suivants doivent être présents :

1. L'incident doit être intentionnel : le résultat d'un calcul conscient de la part de l'auteur;
2. L'incident doit comporter un certain niveau de violence ou de menace de violence, incluant la violence contre la propriété, ainsi que la violence contre les personnes; et
3. Les auteurs des incidents doivent être des acteurs sous-nationaux. Cette base de données n'inclut pas les actes de terrorisme d'État.

Le terrorisme est une définition plus restrictive que l'extrémisme violent.

## Définir l'extrémisme violent

L'extrémisme violent est défini comme les menaces sérieuses, les méfaits, le meurtre, le chaos ou les dommages à la propriété motivés et justifiés par des croyances extrémistes. (Les événements peuvent être codés à la fois comme terrorisme et extrémisme violent).

Tous les incidents terroristes sont considérés comme de l'extrémisme violent; cependant, ce ne sont pas tous les incidents d'extrémisme violent qui répondent aux critères du Manuel du contributeur de données au CIDB — 14 mars 2015 pour le terrorisme (voir ci-dessus). Alors que les classifications d'un incident comme extrémisme violent ou terrorisme se chevauchent souvent, l'extrémisme violent se distingue généralement du terrorisme par son manque de « méfait social plus large; il vise plutôt des acteurs spécifiques responsables de maux sociaux perçus » (Powers, 2014, p. 235).

### **Ajouter des entrées :**

Toutes les entrées sont ajoutées par l'entremise du site web CIDB [www.extremism.ca](http://www.extremism.ca) à l'aide des identifiants fournis au contributeur de données par TSAS.

Si un événement répond aux critères de sélection, des renseignements au sujet de l'évènement sont entrés dans la base de données à l'aide du formulaire en ligne. Il existe un certain nombre de variables quantitatives, ainsi qu'une description qualitative, pour tout incident. Sept variables sont nécessaires pour générer l'identification de l'évènement :

1. Année;
2. Mois;
3. Date;
4. Identification du lieu;
5. Identification du type d'évènement;
6. Identification de la cible; et
7. No d'enregistrement.

L'identification de l'évènement est utilisée pour exporter les données et sert également de contrôle contre les entrées dupliquées. Le livre de codes du CIDB fournit des renseignements approfondis sur la façon de remplir les variables.

Par exemple, si un incident terroriste s'est produit le 23 octobre 2014, impliquant une bombe tuyau dans une résidence privée à Vancouver en Colombie-Britannique, un contributeur de données entre l'évènement de la manière suivante :

Les huit premiers chiffres de l'identification de l'évènement sont composés de l'année, du mois et du jour de l'évènement. Assurez-vous que la date de l'évènement est la date de l'incident, et non la date du reportage. L'heure de l'évènement devrait être enregistrée si elle est connue avec précision, mais elle n'est pas nécessaire pour générer l'identification de l'évènement.

Les deux chiffres suivants de l'identification de l'évènement indiquent l'identification du lieu de l'incident, qui représente la province du Canada où l'évènement s'est produit. Veuillez noter que si l'incident s'est produit à l'extérieur du Canada, le lieu de l'incident est codé « 99 » — Non applicable Manuel du contributeur de données au CIDB — 14 mars 2015

Les six caractères suivants de l'identification de l'évènement correspondent aux identifications du type d'évènement et de cible. Dans cet exemple, l'incident était un attentat à la bombe/à l'explosif; l'identification du type d'évènement est donc codée E03.

L'identification de la cible correspond à la classification du site physique de l'attaque. Une résidence privée serait classée comme une cible dans la catégorie « Citoyens privés et

propriétés privées », alors elle est codée T14. Cette section de l'identification de l'évènement est donc codée E03T14.

Les trois derniers caractères de l'identification de l'évènement correspondent au numéro d'enregistrement de l'incident. Il peut y avoir plusieurs enregistrements pour un incident si un attentat a visé plusieurs lieux, par exemple, des menaces d'attentat à la bombe visant trois bâtiments gouvernementaux différents dans une ville le même jour seraient enregistrées comme 001, 002 et 003. Dans cet exemple, si des numéros d'enregistrement séparés n'étaient pas utilisés, il y aurait des identifications d'évènement dupliquées dans la base de données qui créeraient des problèmes en exportant les données.

De multiples numéros d'enregistrement sont aussi occasionnellement utilisés pour des incidents séparés à l'étranger. Comme l'identification de lieu pour tous les incidents se produisant à l'étranger est « 99 », peu importe le pays, il existe davantage de possibilités de numéros d'enregistrement dupliqués. Par exemple, s'il y a un attentat à la voiture piégée visant des civils le même jour en Afghanistan et au Pakistan, des numéros d'enregistrement séparés sont utilisés pour distinguer les deux identifications d'évènement et exporter et comprendre les données plus facilement.

Il existe deux codes de données spéciaux pour les données manquantes ou incomplètes :

### **Modifier des entrées**

Il existe plusieurs cas où des entrées existantes devraient être modifiées : Manuel du contributeur de données au CIDB — 14 mars 2015

1. De nouveaux renseignements à propos d'un incident existant (p. ex. auteurs, sous-type d'arme, idéologie du groupe) qui n'étaient pas disponibles au moment de l'entrée justifient le recodage de variables existantes;
2. Les variables existantes d'un incident sont codées alors qu'elles devraient être inconnues « -88 » ou non applicables « -99 ». Autrement dit, on a découvert que des renseignements présumés vrais sont incorrects; et
3. On a découvert que plusieurs incidents apparemment séparés dans une journée sont liés. Dans cet exemple, le contributeur de données générerait de nouvelles identifications d'évènement identiques et ajouterait simplement des numéros d'enregistrement additionnels (001, 002, 003, etc.)

En modifiant les variables d'un incident, les contributeurs de données doivent s'assurer que l'identification de l'évènement reflète ces changements.

### **Citations**

Toutes les citations dans le CIDB doivent provenir de matériel accessible au public. Les contributeurs de données peuvent citer des sources d'informations en ligne, des ensembles de données existants, des documents juridiques, des livres, des journaux et tout autre matériel à source ouverte. Le matériel pertinent devrait être téléchargé dans le formulaire d'entrée en ligne; les liens vers des sites web peuvent être cités par leur URL.

TSAS utilise la hiérarchie suivante de crédibilité, en priorité, pour évaluer la fiabilité de ses sources :

1. Procédures judiciaires d'appel;
2. Autres procédures judiciaires;
3. Mises en accusation;

4. Chronologies et rapports gouvernementaux;
5. Articles, livres et bases de données scientifiques évalués par les pairs;
6. Rapports des médias;
7. Rapports et bases de données de groupes de veille;
8. Sites web extrémistes; et
9. Autres sources.

Bien que TSAS reconnaisse que le manque de documentation officielle relatant des événements très récents peut pousser les contributeurs de données à s'appuyer fortement sur les rapports de médias, les contributeurs de données devraient corroborer les renseignements à l'aide de sources multiples, lorsque cela est possible, pour améliorer la fiabilité des données, et ajouter la documentation officielle à mesure qu'elle devient disponible.

Toutes les sources, incluant les URL, doivent être citées dans le fichier de données brutes. Les documents PDF peuvent être joints au dossier de l'évènement.

### **Chercher des incidents**

Les incidents existants peuvent être cherchés en utilisant l'outil de « Recherche d'incident » sur le site web du CIDB. Manuel du contributeur de données au CIDB — 14 mars 2015

Les incidents peuvent être cherchés par date, lieu, type (terrorisme ou extrémisme violent), validité des données, motivation idéologique de l'incident, type de cible, type d'évènement ou mots clés.

### **Foire aux questions**

*Q : Qui prend la décision d'inclure certains événements comme des actes terroristes?*

R : Le CIDB est continuellement mis à jour et évalué par l'équipe principale du projet, ainsi que par ses contributeurs de données approuvés. Les contributeurs de données sont des professionnels de la sécurité nationale, des chercheurs et des étudiants aux cycles supérieurs.

*Q : J'aimerais devenir un contributeur de données. Avec qui devrais-je communiquer?*

R : Veuillez consulter nos critères concernant les contributeurs de données. Si la personne répond aux critères, elle devrait communiquer avec [Joshua.Kilberg@carleton.ca](mailto:Joshua.Kilberg@carleton.ca).

*Q : Quelle est la méthode pour traiter des incidents particulièrement controversés?*

R : Dans le cas d'un incident ou d'un point de données particulièrement controversé, veuillez consulter un membre de l'équipe CIDB qui consultera des collègues et, si l'évènement ne peut être résolu, l'information sera transmise au conseil d'administration du CIDB.

*Q : Le CIDB inclut-il des complots ayant échoué ou ayant été déjoués?*

R : Lorsque cela est possible, le CIDB inclut des complots/attentats qui ont échoué ou qui ont été déjoués par des forces de sécurité. Le critère est tel que des mesures concrètes

doivent avoir été prises de la part de l'individu ou du groupe pour réaliser l'attentat avant son échec ou sa perturbation.

*Q : Comment devrais-je coder les « canulars » à savoir s'ils ont réussi ou non?*

R : Un canular devrait être codé comme réussi s'il perturbe les opérations de l'installation ou du mode de transport menacé, ou s'il affecte la routine quotidienne de citoyens privés en raison de la menace. Un canular ayant échoué (ou ayant été déjoué) peut être inclus dans le CIDB, le cas échéant. Manuel du contributeur de données au CIDB — 14 mars 2015

*Q : Qu'est-ce qui constitue une « cible canadienne »?*

R : Une cible canadienne est un ou plusieurs des éléments suivants : un citoyen canadien, un résident permanent, ou un bâtiment officiel, au Canada ou à l'étranger (p. ex. une ambassade, un consulat, ou une entreprise détenue/dirigée par des Canadiens).

*Q : Pourquoi la collecte de données commence-t-elle seulement en 1960?*

R : En consultation avec nos partenaires gouvernementaux et autres, TSAS a décidé qu'une limite temporelle était nécessaire afin d'avoir un portrait complet du terrorisme moderne au Canada. On a estimé que recueillir des données à partir de 1960 était la meilleure utilisation des ressources de TSAS et la façon la plus efficace de tirer profit des capacités de nos contributeurs de données approuvés, tout en présentant un portrait complet du terrorisme moderne au Canada.

### **Personnes-ressources**

En cas de divergences dans les données ou de questions concernant l'ajout ou la modification d'entrées non abordées dans le manuel, veuillez communiquer avec :

James O. Ellis III – Chef de projet : [James.Ellis@ubc.ca](mailto:James.Ellis@ubc.ca)

Dr Richard Frank – Chef technique : [rfrank@sfu.ca](mailto:rfrank@sfu.ca)

Dr Joshua Kilberg – Chef de recherche : [Joshua.Kilberg@carleton.ca](mailto:Joshua.Kilberg@carleton.ca)