Defence Research and Development Canada
Recherche et développement pour la défense Canada

DEFENCE R&D DÉFENSE

Canadian Extremist Crime Database

Methodological Primer

Sean Norton
DRDC Centre for Security Science

Christian Leuprecht
Royal Military College

Defence R&D Canada – Centre for Security Science

Technical Memorandum
DRDC CSS TM 2013-004
May 2013

Canada

Canadian Extremist Crime Database

Methodological Primer

Sean Norton
DRDC Centre for Security Science

Christian Leuprecht
Royal Military College

Defence R&D Canada – CSS

Technical Memorandum
DRDC CSS TM 2013-004
May 2013

Principal Author

Original signed by Sean Norton

Sean Norton

Defence Scientist

Approved by

Original signed by Denis Bergeron

Denis Bergeron, Ph.D.

Manager, Decision Support Section

Approved for release by

Original signed by Dr. Andrew Vallerand

Andrew Vallerand

A/Chair Document Review Board, DRDC CSS

Abstract

This paper addresses the need for an historical, Canadian, national incident database on criminal extremism, and highlights methodological issues and challenges inherent in its development. While the contents are suggestive, 18 recommendations are enumerated that should be of interest to policy advisors, subject-matter-experts and those researchers who, ultimately, will be responsible for creating the database. Creating a Canadian database on domestic extremist crime is thought to be a useful undertaking, as there can be many benefits. However, as this report makes clear, creating a useful and beneficial tool that stands the test of time is a complicated task and considerable undertaking that requires much forethought.

Résumé

Ce document se penche sur la nécessité d'une base de données nationale, canadienne et historique sur les incidents liés à l'extrémisme criminel et souligne les difficultés méthodologiques inhérentes à sa conception. Même si le contenu est de nature suggestive, on y énumère 18 recommandations qui devraient intéresser les conseillers en politiques, les experts en la matière et les chercheurs qui seront chargés de créer la base de données. La création d'une base de données sur la criminalité terroriste nationale est jugée utile, car elle peut présenter de nombreux avantages. Toutefois, comme il est clairement établi dans le rapport, la création d'un outil utile et bénéfique qui résiste à l'épreuve du temps constitue une tâche complexe et considérable qui nécessite beaucoup de réflexion préparatoire.

Executive Summary

Canadian Extremist Crime Database: Methodological Primer
Sean Norton and Christian Leuprecht; DRDC CSS TM 2013-004; Defence R&D Canada Centre for Security Science

This paper is intended as a proposal to create an historical, Canadian, national incident database on criminal extremism – similar to what has been done in the U.S. – to address a perceived gap in national security information that is publically available for research purposes. No comprehensive database on Canadian domestic extremist crime currently exists. In addressing the need for such a database, this report highlights methodological issues and challenges inherent in its development; as such, is intended as a guide for use by policy advisors, subject-matter-experts and by those who, ultimately, might be tasked with creating the database. A database such as the one proposed can provide benefits to policy, security, intelligence and law enforcement communities. However, as this report makes clear, creating a useful and beneficial tool that stands the test of time is a complicated task and considerable undertaking that requires much forethought. This paper is not exhaustive, but rather is intended as a first step by alerting interested parties to some of the many relevant issues. It includes 18 recommendations, which in our view are some main considerations.

We can foresee basically three approaches to developing the database. The one approach involves the development of a conceptual framework from which definitions of criminal extremism, and a set of inclusion criteria, can be constructed, that will then guide data collection. This is a theoretical approach that entails the creation of a typology of criminal extremism. Incidence of criminal extremism in Canada has no doubt changed over time. A typology would permit a systematic approach by structuring the collection of empirical data in a way that minimizes gaps and limits implicit bias towards any one manifestation of extremism. Epistemologically, we don't know what we don't know. By relying on an explicit framework, we can at least be assured of capturing data on the various manifestations of criminal extremism without unduly showing preference for one type or assuming, perhaps, incorrectly, that extremism is manifest, over time.

Whereas, developing an useful conceptualization of "extremist crime" at the outset may be viewed by some as overly difficult and time-consuming, terrorism, representing an unique subset of violent extremism, is relatively easy to define based on the Canadian *Criminal Code*. If the database is to have practical value to police and security agencies, then the incidents it includes must be based on Canadian legislative definitions even if terrorism charges were not laid.

The second overall approach is less theory-driven and more general and inductive. Instead of spending time grappling with the concept of "extremism", and defining a typology to account for its various manifestations, it entails the creation and adoption of broad inclusion criteria. This is a way of capturing incidence of criminal extremism that fall within a broad set of criteria. It is a way of capturing as many data points as possible before an effort is made to categorize the data.

The third approach is the most pragmatic, but also the most problematic, if it is solely undertaken. Researchers might prefer to focus their efforts on very particular manifestations of criminal extremism that are currently of interest to police and security agencies. If so, then this approach involves clearly defining these types of extremism, creating inclusion criteria, before proceeding

to collect data, solely on these manifestations. While this third approach involves less theory and less structure, and greater implicit bias, it may be useful if there are specific policy questions that need to be answered regarding current or past incidence of a particular form of criminal extremism. However, this approach risks missing important information, such as the relative and changing incidence of different forms of criminal extremism over time, or even whether there are changes in the way certain types of violent extremist movements (e.g., right-wing) are structured and behave over time. As such, this approach is not recommended.

Whichever approach is taken, researchers should seek to ensure that the definitions, inclusion criteria and variables that are created for the Canadian database permit valid comparisons, possibly also the sharing of data with other databases (e.g., U.S. Extremist Crime Database, Global Terrorism Database, etc.). Even where definitions vary, it is recommended that data be structured in a way that will permit users to apply their own definitions, similar to what was done for the Global Terrorism Database. For instance, the data captured with a broad set of inclusion criteria can be coded in a way that allows users to filter the data based on their own definitions.

Another area of consideration for the database involves the relationship between hate and extremist crime. While it is fair to suggest that all hate crimes are extremist in nature, whether a hate crime constitutes an extremist crime or even an act of terrorism warrants further consideration. The definition of a terrorist act in the *Criminal Code* may provide a useful way of classifying acts of hate that are also extremist or, as the case may be, terrorist acts. For instance, researchers should explore ways to capture acts of hate that are motivated by extremist ideology and seek to differentiate between spontaneous, personal or retributive attacks and those representing deliberate and/or systematic acts of hate by individuals, groups or entities.

The Centre for Criminal Justice Statistics (CCJS) at Statistics Canada collects data on hate crimes through the Uniform Crime Reporting (UCR) and Homicide surveys. Even though the data cannot be publically released nor integrated into a database, it is conceivable that CCJS could complete some analyses that would further an understanding of extremist crime in Canada. For instance, it is conceivable that CCJS could code law enforcement officers' narrative description in the Homicide Survey to examine how many cases, if any, meet a definition of extremist crime.

The series of 18 recommendations, enumerated in the Conclusion, while complicated and numerous, represent an otherwise logical series of steps. Ideally, concepts should be defined before inclusion criteria are developed. A set of inclusion criteria are necessary before an exhaustive set of search terms can be created, and a comprehensive list of sources need to be identified before searches can be undertaken. Open-source searches are necessary to identify cases, but those cases cannot be coded until a list of variables and a relational database are created. A pilot will be necessary to check for errors before such time as the data collection phase can commence; whereas, a set of well-articulated protocols in the form of a comprehensive Codebook is needed to guide investigators. A quality control process is what will then help to ensure data collection proceeds smoothly and uniformly to minimize gaps and inconsistencies.

Sommaire

Canadian Extremist Crime Database: Methodological Primer
Sean Norton and Christian Leuprecht; DRDC CSS TM 2013-004; R & D pour la défense Canada- Centre des sciences pour la sécurité

Ce document a pour objectif de présenter une proposition visant la création d'une base de données nationale, canadienne et historique sur les incidents liés à l'extrémisme criminel – semblable à celle créée aux États-Unis – dans le but de combler les lacunes existantes relativement aux renseignements sur la sécurité nationale rendus publics à des fins de recherche. Il n'existe actuellement aucune base de données sur les crimes extrémistes nationaux au Canada. En se penchant sur la nécessité d'une telle base de données, le présent rapport souligne les difficultés méthodologiques inhérentes à sa conception; il se veut donc un guide à l'intention des conseillers en politiques, des experts en la matière et de ceux qui pourraient être chargés de créer la base de données. Une base de données telle que celle qui est proposée peut être utile aux milieux des politiques, de la sécurité, du renseignement et de l'application de la loi. Toutefois, comme il est clairement établi dans le rapport, la création d'un outil utile et bénéfique qui résiste à l'épreuve du temps constitue une tâche complexe et considérable qui nécessite beaucoup de réflexion préparatoire. Ce document n'est pas exhaustif; il s'agit plutôt d'une première étape consistant à mettre les parties intéressées au courant de certaines des nombreuses questions pertinentes. Il comprend 18 recommandations qui, à notre avis, sont les principales considérations.

Essentiellement, nous pouvons prévoir trois approches pour l'élaboration de la base de données. La première approche comprend l'élaboration d'un cadre conceptuel à partir duquel on pourra rédiger des définitions de l'extrémisme criminel et un ensemble de critères d'inclusion, qui guideront ensuite la collecte de données. Il s'agit d'une approche théorique qui entraîne la création d'une typologie de l'extrémisme criminel. L'incidence de l'extrémisme criminel au Canada a sans contredit changé au fil du temps. Cette typologie permettrait l'adoption d'une approche méthodique en structurant la collecte de données empiriques d'une façon qui minimiserait les lacunes et limiterait les préjugés implicites à l'égard de toute manifestation d'extrémisme. Du point de vue de l'épistémologie, nous ne savons pas ce que nous ne savons pas. En nous fondant sur un cadre explicite, nous pouvons au moins nous assurer que nous recueillons des données sur les diverses manifestations de l'extrémisme criminel sans montrer une préférence indue pour un certain type ou supposer, possiblement à tort, que l'extrémisme est évident, avec le temps.

Alors que certains pourraient estimer que l'élaboration dès le départ d'un cadre conceptuel utile de la criminalité extrémiste soit trop difficile et chronophage, le terrorisme, qui représente un sous-ensemble unique de l'extrémisme violent, est relativement facile à définir à l'aide du Code criminel. Si la base de données doit être utile aux services de police et de sécurité, les incidents qu'elle contient doivent être fondés sur des définitions provenant des lois canadiennes, même si aucune accusation de terrorisme n'a été portée.

La deuxième approche générale est moins théorique et plus générale et inductive. Au lieu de consacrer du temps à saisir le concept d'« extrémisme » et à définir une typologie expliquant ses différentes manifestations, elle consiste à créer et à adopter des critères généraux d'inclusion. Il

s'agit d'une façon de déterminer l'incidence de l'extrémisme criminel dans un large éventail de critères et de saisir autant de données que possible avant de déployer des efforts pour les catégoriser.

La troisième approche est davantage pragmatique, mais sera également plus problématique si elle est adoptée. Les chercheurs pourraient préférer concentrer leurs efforts sur des manifestations très particulières de l'extrémisme criminel qui intéressent actuellement les services de police et de sécurité. Si c'est le cas, cette approche consiste à définir clairement ces manifestations de l'extrémisme et à créer des critères d'inclusion avant de recueillir des données seulement sur ces manifestations. Alors que cette approche requiert moins de théorie et de structure, et davantage de préjugés implicites, elle peut s'avérer utile s'il est nécessaire de répondre à des questions stratégiques précises concernant l'incidence actuelle ou passée d'une forme particulière d'extrémisme. Toutefois, l'utilisation de cette approche entraîne le risque de ne pas recueillir des renseignements importants, comme l'incidence relative et changeante de différentes formes d'extrémisme criminel au fil du temps, ou même les changements possibles dans la structure et le comportement de certains types de mouvements d'extrémisme violent (p. ex. l'extrémisme de droite). Par conséquent, cette approche n'est pas recommandée.

Peu importe l'approche adoptée, les chercheurs devront s'assurer que les définitions, les critères d'inclusion et les variables créés pour la base de données canadienne permettent d'effectuer des comparaisons valides, et possiblement d'échanger des données avec d'autres bases de données (comme la base de données sur l'extrémisme criminel et la base de données mondiale sur le terrorisme des États Unis). Même quand les définitions varient, il est recommandé de structurer les données d'une façon qui permettra aux utilisateurs d'appliquer leurs propres définitions, comme ce qui a été fait pour la base de données mondiale sur le terrorisme. Par exemple, il est possible d'attribuer un code aux données recueillies à l'aide d'un ensemble général de critères d'inclusion qui permettra aux utilisateurs de filtrer les données en fonction de leurs propres définitions.

Un autre domaine de restriction pour la base de données concerne la relation entre les crimes motivés par la haine et les crimes extrémistes. Alors qu'il est juste de suggérer que tous les crimes motivés par la haine sont de nature extrémiste, il est nécessaire d'examiner un tel crime plus en détail pour déterminer s'il constitue un crime extrémiste ou même un acte terroriste. La définition d'activité terroriste dans le Code criminel peut aider à cibler les actes motivés par la haine qui sont également extrémistes ou, le cas échéant, terroristes. Par exemple, les chercheurs devraient examiner des façons de cibler les actes haineux qui sont motivés par une idéologie extrémiste et tenter d'établir une différence entre les attaques spontanées, personnelles ou punitives et celles qui constituent des actes haineux délibérés ou systématiques commis par des personnes, des groupes ou des entités.

Le Centre canadien de la statistique juridique (CCSJ) de Statistique Canada recueille des données sur les crimes motivés par la haine au moyen de la Déclaration uniforme de la criminalité et de l'Enquête sur l'homicide. Même s'il n'est pas possible de diffuser les données au public ou de les intégrer à une base de données, il est envisageable que le CCSJ puisse compléter certaines analyses qui permettraient d'approfondir notre compréhension de la criminalité extrémiste au Canada. Par exemple, le CCSJ pourrait attribuer des codes aux descriptions formulées par les agents d'application de la loi dans l'Enquête sur l'homicide afin d'examiner combien de cas, s'il y en a, correspondent à la définition de la criminalité extrémiste.

Les 18 recommandations énumérées en conclusion, même si elles sont compliquées et nombreuses, représentent une série logique d'étapes à suivre. Idéalement, il faudrait définir des concepts avant d'élaborer les critères d'inclusion. Il est nécessaire de définir un ensemble de critères d'inclusion avant de créer des termes de recherche, et il faut dresser une liste exhaustive de sources avant d'entreprendre des recherches. Il est nécessaire de mener des recherches dans les sources ouvertes afin de cibler les cas, mais il ne faut pas attribuer de code à ces cas avant d'avoir créé une liste de variables et une base de données relationnelle. Il faudra mener un projet pilote afin de déceler les erreurs avant le début de la phase de collecte de données; et un ensemble de protocoles bien articulés rédigés dans une liste exhaustive de codage doit être préparé pour guider les enquêteurs. Il sera ensuite nécessaire de choisir un processus de contrôle de la qualité qui aidera à assurer l'uniformité le bon déroulement de la collecte de données, afin de minimiser les lacunes et les contradictions.

Table of contents

List of Figures

List of tables

1. Introduction

In 2011, The Defence R&D Canada (DRDC) Centre for Security Science (CSS) Chemical, Biological, Radiological-Nuclear and Explosive (CBRNE) Research and Technology Initiative (CRTI) funded a project (CRTI 09-428RD), in part to identify and fill a gap in national security information publicly available for research purposes. This is a proposal to create an historical, Canadian, national, incident database of extremist crime in order to fill this gap. Instead of continuing to rely on anecdotal or case study data, the objective of the prospective database is to collect, code and store data, systematically and uniformly, on past incidents of Canadian domestic extremist crime, suspects, and victims. The resulting database will permit those in government and academia to undertake systematic, geospatial and temporal assessments of the types and frequency of extremist crimes, targeting patterns, regional variations, and trends over time. The proposed database could also assist in better understanding patterns in the emergence and dissolution of criminal extremist/terrorist groups, movements and campaigns of violence.

Through a better understanding of the nature and scope of domestic violent extremism, security, intelligence and law enforcement agencies, in Canada, will be able to conduct more accurate threat and risk assessments, and optimize the allocation of scarce resources, which in turn, will position them better to respond to and prevent such behaviour. Ongoing data collection and analysis will also yield metrics against which to measure the performance of policies and programs. Data analysis should permit evidence-based decision-making, guide the development of policies, and support academic research on domestic violent extremism.

No comprehensive database on Canadian domestic extremist crime currently exists. This report is intended as a starting point by raising some of the methodological issues and challenges inherent in its development. Through a concise review of the Canadian Criminal Code, existing terrorism and extremist crime databases, and relevant literature, this report discusses options and provides recommendations for defining concepts, identifying, searching, coding, and storing cases for the prospective database. Its contents are merely suggestive, not exhaustive.

2. Conceptual Territory

Before a database on domestic extremist crime can be developed, a clear delineation of scope conditions and terminology is needed. While there is also a need for transparency and consistency when searching and coding potential incidents, this section deals, first and foremost, with the need for clarity regarding the types of incidents the database will contain. What constitutes domestic extremism? The types of crimes that will be captured by way of this initiative vis-à-vis other such initiatives need to be clearly articulated. Mapping out the conceptual domain will permit the establishment of inclusion and exclusion criteria: the rules by which those collecting data will decide what crimes to include and exclude from the database. While a clear understanding of the criteria governing the types of incidents to be in/excluded will help to ensure a consistent approach to data collection, it is also necessary for people who subsequently analyze and report on the data to know what that data represents. A high degree of conceptual clarity, consistency and transparency in collection and coding will facilitate comparison among databases.

Terrorism

The term "terrorism" is controversial. There is no internationally-agreed definition. Hundreds exist (Coady 2005:37, Schlaghek, 1988:1) and whether actions are labelled as "terrorism" varies based on ideology and politics. The United Nations Security Council (UNSCR) established a Working Group in 1996 to create a comprehensive legal framework of conventions on international terrorism[1]. Among them was a comprehensive convention on international terrorism that would ensure criminal responsibility for terrorist acts based on a clear, well-known definition of terrorism. The intention was to bring together all of the international counter-terrorism conventions, international customary law, the Geneva conventions or the Rome Statutes, in which all forms of terrorism are prohibited, to create a compelling normative framework for non-State actors concerning the use of force (United Nations General Assembly 2004). A deadlock regarding the definition of terrorism continues to this day, which has prevented its international adoption by UN member states.

The failure of the United Nations General Assembly in defining terrorism, according to a Secretary-General's High-Level Panel on Threats, Challenges and Changes "…prevents the United Nations from exerting its moral authority and from sending an unequivocal message that terrorism is never an acceptable tactic, even for the most defensible of causes." (United Nations General Assembly 2004, 48). While the legal and normative framework governing States' use of armed force against civilians is believed strong, a framework of equal authority is still being sought governing the use of force against civilians by non-state actors.

After the school massacre in Beslan, Russia in 2004, Security Council Resolution 1566 (2004) was adopted, which, to date, provides the only UN definition of terrorism, as follows:

> "*Recalls* that criminal acts, including against civilians, committed with the intent to cause death or serious bodily injury, or taking of hostages, with the purpose to provoke a state of terror in the general public or in a group of persons or particular persons, intimidate a

[1] See General Assembly resolution 51/210

> population or compel a government or an international organization to do or to abstain from doing any act, which constitute offences within the scope of and as defined in the international conventions and protocols relating to terrorism, are under no circumstances justifiable by considerations of a political, philosophical, ideological, racial, ethnic, religious or other similar nature, and calls upon all States to prevent such acts and, if not prevented, to ensure that such acts are punished by penalties consistent with their grave nature"
>
> United Nations Security Council (2004)

What constitutes a terrorist offense in Canada is relatively easy to define if the definition is based on the Canadian *Criminal Code* (Annex A). It fully accounts for ten existing UN conventions to combat terrorism, and while it defines a "terrorist act" in a way that largely corresponds to Resolution 1566, it also differs in important ways. For instance, the *Criminal Code* includes a motivation requirement that is missing from the Resolution. Terrorism is condemned by the UN as a criminal act that is not justifiable for any reason, but only the act itself is condemned not the motivation. Resolution 1566 includes a comprehensive view of possible motives, (e.g., "philosophical", "racial", "ethnic" or other forms of justification). Three motives (i.e., political, religious or ideological) are recognized in the Canadian *Criminal Code*. In other respects, however, section 83.01 of the *Criminal Code* is broader than Resolution 1566. In Canada, acts are included that cause serious risks to health and safety, significant property damage, or serious interference with or disruption to essential services, facilities or systems (Annex A).

International disagreement regarding a definition of terrorism revolves around states' use of armed force against civilians and the rights of people under foreign occupation to resistance and self-determination without being labelled as terrorists (United Nations General Assembly 2004). While these issues certainly relate to definitions of "international terrorism", they are unlikely to pose a challenge when constructing a Canadian extremist crime database. Without going into too much detail, there is a fundamental criterion that can be used for purposes of identifying incidents for possible inclusion as "terrorism" cases in a domestic database; terrorism involves the deliberate targeting and killing of civilians and non-combatants. Whatever other definitional confusion and disagreement exist, the UN is unequivocal in their view that deliberate attacks on innocent civilians is never justifiable regardless of whether it is committed by State or non-State actors.

Ultimately, Canadian terrorism legislation should influence the definitions that are used to develop a database of domestic extremist crime, of which terrorism is a principal aspect. However, determining which acts to include in such a database need not be constrained by the manner in which they were prosecuted. There are plenty of criminal acts that fall within the legislative definition of "terrorism" but are not prosecuted as such for one reason or another. For example, whether the Animal Liberation Front, with which convicted Canadian terrorist Darren Thurston sympathizes, is engaged in terrorism, sabotage, illegal direct action or extremism is debatable. A definition of "terrorism" can be used for purposes of gathering statistical information, even if, from a legal standpoint, certain events are not defined as such or as the case may be, are prosecuted under a different article of criminal legislation. If the database is to have practical value to police and other security agencies, it has been suggested that incidents must be included that are based on Canadian legislative definitions even if terrorism charges were not laid.

The United States Law Code (U.S.C. Title 22, Ch. 38, Section 2656f(d)[2]) serves as an example. United States law contains a definition of terrorism that allows the U.S. National Counterterrorism Centre to compile an annual database on terrorist incidents, entitled the Worldwide Incidents Tracking System (WITS). It defines terrorism as "premeditated, politically motivated violence perpetrated against non-combatant targets by subnational groups or clandestine agents" (The National Counterterrorism Centre 2012). The U.S.C. definition is solely intended to permit the cataloguing of statistics and, according to the annual report, judgments are "…not intended to be a legally binding determination that an event is a terrorist act." (7).

The definition of terrorist acts in Canadian law is more expansive than the above U.S.C. definition. First, whereas the above U.S.C. definition refers, solely, to politically-motivated acts, Canadian law contains a broader motivation clause. The Canadian definition includes acts committed "in whole or in part for a political, religious or ideological purpose, objective or cause" found in Section 83.01(1)(b)(i). Anti-terrorism laws in the United Kingdom, Australia, New Zealand and South Africa have a similar requirement of motive (Department of Justice 2008). Second, the U.S.C. definition does not make reference to the aim of terrorism, which, arguably, is a defining feature of terrorism vis-à-vis other criminal acts. Acts that intentionally intimidate the public or a segment thereof, or that intend to compel a person, government or organization to do or refrain from doing any act is cited in Resolution 1566 and the Canadian *Criminal Code* (Annex A). Third, the U.S.C. definition, solely, includes initiated and executed acts of violence, which despite its omission from the actual definition, apparently, can also mean damage to critical infrastructure (The National Counterterrorism Centre 2012). It neglects to include acts committed with the intent to cause harm, as in Resolution 1566, or an attempt or threat to commit a terrorist act, which is in the Canadian definition. Hoaxes, spontaneous hate crimes, and genocide are also excluded from the WITS (7)(7)(7). While not explicitly included as part of the Canadian definition, terrorism hoaxes are captured in Section 83.231(1); Sections 430(4.1) and 718(2) that make provision for hate crimes; and Section 318(1) and (2) of the *Canadian Code* refers to genocide.

While a clear definition of the relevant crimes and set of inclusion criteria is needed to guide data collection efforts, others view it as problematic to rely too heavily on a given definition. Notwithstanding possible changes to legislation, some see benefits to coding data in a way that permits users to filter the data based on their own views. Originally, the Global Terrorism Database (GTD1 1970-1997), collected by the Pinkerton Global Intelligence Service (PGIS) relied on a definition of terrorism:

> "the threatened or actual use of illegal force and violence by a non-state actor to attain a political, economic, religious, or social goal through fear, coercion, or intimidation."(National Consortium for the Study of Terrorism and Responses to Terrorism (START) 2012b).

During the second phase of data collection (GTD2 1998-2007), incidents were coded more broadly so that users could single out only those cases that met their own definition of terrorism. In order to be included in the database, three attributes must still be present: (1) Incidents must be intentional acts that are consciously decided and instigated against an identified target by a perpetrator; (2) Incidents must involve violence or the threat of violence against property or people; (3) Whether or not states are believed to sponsor attacks, the actual perpetrators must be sub-national actors. (Table 1). In addition, at least two of three additional criteria must be present for an incident to be included in the GTD2 – henceforth referred to simply as the GTD. Two of the now optional criteria were referred to in the PGIS definition. The first involves the motive (i.e., a political, economic, religious or social goal), and the second involves the aim (i.e., intention to coerce, intimidate or publicize to a larger audience than the immediate victims).. According to the third criterion, the act must fall outside the parameters of international Humanitarian Law (IHL). According to the GTD codebook, this last criterion deals "…particularly [with] the prohibition against deliberately targeting civilians or non-combatants" (National Consortium for the Study of Terrorism and Responses to Terrorism (START) 2012a, 8). Incidents are coded as terrorism if they contain the first three attributes, and any two of the three criteria below.

Table 1: Global Terrorism Database Inclusion Criteria

To consider an incident for inclusion in the GTD, all three of the following attributes must be present:

- The incident must be intentional – the result of a conscious calculation on the part of a perpetrator.
- The incident must entail some level of violence or threat of violence -including property violence as well as violence against people.
- The perpetrators of the incidents must by sub-national actors. This database does not include acts of state terrorism.

In addition, at least two of the following three criteria must be present for an incident to be included in the GTD:

Criterion 1: The act must be aimed at attaining a political, economic, religious, or social goal. In terms of economic goals, the exclusive pursuit of profit does not satisfy this criterion. It must involve the pursuit of more profound, systemic economic change.
Criterion 2: There must be evidence of an intention to coerce, intimidate, or convey some other message to a larger audience (or audiences) than the immediate victims. It is the act taken as a totality that is considered, irrespective if every individual involved in carrying out the act was aware of this intention. As long as any of the planners or decision-makers behind the attack intended to coerce, intimidate or publicize, the intentionality criterion is met.
Criterion 3: The action must be outside the context of legitimate warfare activities. That is, the act must be outside the parameters permitted by international humanitarian law (particularly the prohibition against deliberately targeting civilians or non-combatants).

Reproduced from: National Consortium for the Study of Terrorism and Responses to Terrorism (START) (2012a)

Coding data in a way that accounts for different ways of defining key concepts, such as "terrorism" appears to make sense, and should be further explored when developing the Canadian database. However, in the case of the GTD, it is unclear how the last criterion actually permits users to define terrorism in a way that is different than before. International Humanitarian Law (IHL) specifically governs acceptable conduct of *States* during times of war. Since only two of the three criteria need to be met for incidents to be included in the GTD, one is lead to believe that criterion three broadens the scope of the database. Were it not for the explicit statement: "this database does not include acts of state terrorism" (7), one might think that criterion three is meant to capture State's use of force against civilians. Instead, it appears that this criterion deals more narrowly with a definition of "legitimate" targets (i.e., combatants versus non-combatants). Some of the other relevant provisions of the IHL are not specified except in an earlier version of the Codebook, which refers to: the appropriate treatment of those no longer involved in hostilities; protection and humane treatment of captured combatants; constraints on the means and methods of warfare; and, the need to distinguish among civilian and military persons and targets (19)(19)(19). The latest version of the Codebook only refers to guidelines regarding when military, paramilitary, and police can be viewed as being "legitimate" targets based on changes in status (National Consortium for the Study of Terrorism and Responses to Terrorism (START) 2012a, 38).

Unlike the WITS, the GTD also includes unsuccessful attacks. Though, unlike the *Criminal Code*, the GTD, like the WITS, does not appear to include hoaxes. These differences will need to be accounted for when constructing the Canadian database if there is to be some degree of comparability between the Canadian database and the GTD.

One of the difficulties associated with the *Canadian Criminal* Code definition of terrorism concerns the ambiguity surrounding the motivation requirement. A clear definition of political, ideological or religious motivation is missing from the Code. This is surprising given that proving the motivation behind a given act in a court of law can be highly burdensome. It is as though a "we-know-it-when-we-see-it" attitude exists, given the lack of clarity that appears to exist concerning the meaning of these concepts. Obviously, the court system is meant to provide a forum in which motivational claims can be debated. For purposes of constructing a database, however, conceptual clarity is needed to permit uniform data collection and a clear understanding of which incidents are included and excluded.

Extremism

Many consider terrorism synonymous with "violent extremism". Yet, people clearly alternate between their use of one label or the other depending on their interests, bias, and interpretation of events. Individuals or groups may be labelled "terrorists" for purely ideological or political reasons. It is a highly emotive and pejorative label that seeks to delegitimize a person or group. In other instances, people or groups are referred to as "terrorists" when they employ unconventional, shocking and terror-inducing means and methods of achieving political aims or when they attack what are perceived as innocent civilians. In the public eye, terrorism, such as violent extremism, is considered to be an extreme violation of societal norms. Yet, extremism is not necessarily criminal, whereas, by most accounts, terrorism is always criminal; hence the focus on "violent extremism" in this paper – actions that are necessarily criminal. At the same time, terrorism is probably a unique form of violent extremism that people tend to associate with persons or groups who use violence, oftentimes, against civilians, to provoke fear among the general public, to intimidate, to subvert or to manipulate a government or organization to political ends. The question that still needs to be addressed for the prospective database involves the scope of the initiative, and the extent to which it should account for the full breadth of criminal extremism, by defining and creating inclusion criteria for its various manifestations, treating terrorism as a subset that probably refers to only certain types of violent criminal extremism.[2]

The U.S. Extremist Crime Database (ECDB), despite being highly specific to the U.S. context, is an initiative that represents most closely what a Canadian database might look like. In fact, the original CRTI funding submission was largely motivated by the desire to create a Canadian version of the ECDB. The ECDB collects data that allows U.S. researchers to examine policy-related questions that, owing to scope conditions, cannot be answered by other terrorism-focused databases (Freilich and Chermak 2010, 3). The database involves criminal cases that are not exclusively terrorist in nature, but are deemed relevant to the study of terrorism. Included, are ideological crimes committed by far-right extremists, animal/environmental rights extremists, Islamic jihadists, and Arab nationalists. Also included is non-ideological criminal activity.

The Canadian Criminal Code does not define "ideological" motivation and the term is not defined in the ECDB Codebook either. The ECDB does contain definitions of specific, ideological crimes that it captures (Annex B). Among the variables being coded, however, some are said to capture group involvement in non-ideological criminal activities (i.e., crime, white collar crime, money, arms, drugs, human or sex trafficking, smuggling, robbery, kidnapping), but no further explanation is given. The codebook contains a list of other, undefined variables (e.g., non-ideological, alcohol-related crime, ideological traffic offenses, etc.), which confuses matters. This may be a situation of "we-know-it-when-we-see-it", where data collectors rely on an implicit definition, or they receive more direction than what is publically available. Either way, these are good examples of the need to confront conceptual issues to avoid confusion.

One approach to data collection for the prospective Canadian database is to replicate the ECDB structure, which codes for 80 variables in relation to specific types of criminal extremist behaviour. The problem with that approach is that it might unduly constrain the focus of inquiry by presupposing that other types of extremism – besides those being captured by the ECDB – do not exist or are not worth examining for one reason or another. For instance, in the 2009-10 annual report the Canadian Security Intelligence Service (CSIS), identifies issue-motivated groups, such as eco-extremists and Aboriginal extremists as posing a serious threat in Canada (Canadian Security Intelligence Service 2010). While the ECDB does not collect data on what the CSIS report refers to as "Aboriginal extremists", it does collect data on environmental-rights extremists. However, a closer examination of the definition and inclusion criteria for this category is necessary to determine if its manifestation in Canada is similar to that in the U.S. The definition and inclusion criteria may need to be revised to suit the Canadian context. Right-wing extremism encompasses a broad spectrum of activity. In light of concerns over a particular manifestation of right-wing violent extremism in the U.S., it is not surprising that the ECDB database began by focusing on a particular manifestation of this activity. However, a clear understanding of the phenomena as it exists in Canada is also needed before such time as the U.S. ECDB definition can be adopted. In any case, it may be useful to cast a wider net when developing the Canadian

[2] Violent and criminal forms of extremism have been emphasized in this report in order to limit confusion surrounding the purpose of the database. Extremism is not against the law. The initiative purely intends to capture data on criminality. However, not all forms of criminal extremism employ violence. This paper has tended to focus on violent manifestations of criminal extremism, somewhat arbitrarily, in order to limit the scope of the discussion. Though, clearly, data on such things as cyber- or financial crime could also be captured if stakeholders agree that the scope of the initiative should be expanded to include such acts.

database by adopting a broader definition of political, ideological and religious, extremist crime; at least until such time as data is available that might indicate the need to focus any one type that is deemed to have greater incidence or be a cause for greater concern.

A statement made in reference to the Anti-Terrorism Act on the Department of Justice website may prove helpful for overcoming some conceptual challenges regarding the definition of extremism. It states that "the motive requirement [s. 83.01(1)(b)(i)(a)] is useful because it aims directly at the ideological dimension of terrorism which seeks to undermine the normative foundations of liberal democracy" (Department of Justice 2008). Whilst this viewpoint was made in reference to terrorism, the underlying motivational dimension could just as easily apply to other types of political extremism. According to a similar statement made by Backes (2007), political extremism is the antithesis of constitutional democracy. Political extremism represents "ideologies/movements which aim at the elimination of the constitutional state or the exclusion of parts of the population from assuring essential basic rights" (252) or both. Backes (2007) separates the dimensions of democracy and constitutionalism into four ideal types that may provide a useful way of conceptualizing "political extremism"; hence, defining and establishing inclusion criteria for its various manifestations (see Annex C for a detailed discussion of this theoretical approach), where such acts also involve violence, planned violence or the threat of violence. It warrants being said, the purpose of the prospective database is not to capture extremist thought or behaviours that do not also involve illegality and the commission of crimes.

We can foresee basically three approaches to developing the prospective database. The one approach involves the development of a conceptual framework from which definitions of criminal extremism, and a set of inclusion criteria, can be constructed, that will then guide data collection. This is a theoretical approach that entails the creation of a typology of criminal extremism, similar to what Backes (2007) has done. It is a way of checking our assumptions. Incidence of criminal extremism in Canada has no doubt changed over time. A typology would permit a systematic approach by structuring the collection of empirical data on incidence of criminal extremism in Canada in a way that minimizes gaps and limits implicit bias towards any one manifestation. Epistemologically, we don't know what we don't know. By relying on an explicit framework, we can at least be assured of capturing data on the various manifestations of criminal extremism without unduly showing preference for one type or assuming, perhaps, incorrectly, that extremism is manifest, over time. This step is recommended, but need not occur at the outset.

The second approach is less theory-driven and more general and inductive. Instead of spending time grappling with the concept of "extremism", and defining its various manifestations, it entails the creation and adoption of broad inclusion criteria. This is a way of capturing incidence of criminal extremism that fall within a broad set of criteria. This approach is not concerned with differentiating between types of extremism, except in fairly rudimentary terms. Rather, it is a way of trying to capture as many data points as possible before an effort is made to categorize the data.

The GTD may be a good example of this second approach. While the GTD relies on a specific definition of terrorism, the inclusion criteria are remarkably broad (Table 1). If one were to strip out the definition of terrorism from the Codebook and simply focus on the inclusion criteria, then it could almost be viewed as being an extremist crime, instead of terrorism database. The GTD Codebook identifies sub-national actors who intentionally engage in violence or the threat of violence for political, economic, religious, or social goals in order to coerce, intimidate, or convey some other message to a larger audience than the immediate victims (National Consortium for the

Study of Terrorism and Responses to Terrorism (START) 2012a, 6-8). If the GTD inclusion criteria lent greater emphasis to ideological motivation or goals, then the structure of the database would be virtually indistinguishable from one that focuses more broadly on violent extremist crime.

The third approach is the most pragmatic, possibly also, the most problematic, if undertaken exclusively. It involves less theory and less structure, and greater implicit bias. If there are very particular manifestations of criminal extremism that are of interest to the law enforcement, security intelligence community, then this approach involves clearly defining these types, creating inclusion criteria, proceeding to collect data, solely on this type of extremism. This approach may be useful if a very specific policy question needs to be answered regarding the current or past incidence of a particular form of criminal extremism, for instance. However, this approach risks missing important information, such as the relative and changing incidence of different forms of criminal extremism over time, or even whether there are changes in the way certain types of violent extremist movements (e.g., right-wing) are structured and behave over time. One risks missing such information by relying on assumptions regarding specific manifestations of extremist crime at a particular point in time.

It may thus be preferable that steps one and two be undertaken, although not necessarily in order. As social science researchers, our preference is clearly the development of theoretical frameworks that can then be empirically tested and validated. But there is no reason why data collection could not proceed on the basis of a broad set of inclusion criteria, similar to what is done for the GTD, at the same time or before such time as a suitable framework is developed. Ultimately, the value of a database is not determined by the volume of data, but in its ability to usefully categorize data, hence distinguish between data, and to avoid gaps and inconsistencies in data collection.

Hate Crimes and Extremism

Canada has several hate crime provisions in the *Criminal Code* that are worth discussing for their relationship to a database on extremist crime. Sections 430(4)(1) accounts for bias, prejudice or hate-based acts of mischief in relation to property that is primarily used for religious worship or a cemetery. Section 318(1) deals with “advocating genocide” against any identifiable group (i.e., the section of the public distinguished by colour, race, religion, ethnic origin or sexual orientation). Section 319(1) and (2) account for the communicating of statements, publicly, which incites hatred or wilfully promotes hatred against any identifiable group. There is also a sentencing provision (s. 718.2) if there is evidence that a crime was motivated by bias, prejudice or hatred towards an identifiable group.

The Centre for Criminal Justice Statistics (CCJS) at Statistics Canada collects data on hate crimes through the Uniform Crime Reporting (UCR) and Homicide surveys. Such extant data stand to complement other data collection. In the case of the UCR 2.2, there is thought to be five years of decent coverage; at least, according to CCJS research staff. However, there are issues involving the use of this data that must be considered. For one, the data does not identify links between hate crimes and extremist and/or terrorist acts. For instance, spontaneous hate crimes committed by individuals are not differentiated from those acts representing a deliberate strategy, undertaken by groups or entities, in order to intimidate segments of the public and compromise their security.

This approach is consistent with the literature since hate crimes are often only seen as being committed by individuals, as opposed to groups or entities (Green, McFalls, and Smith 2001). It can also be difficult to distinguish between individual acts and those committed by groups even though efforts to do so would be useful and instructive when studying extremist behaviour[3].

An even greater issue involves the inability to extract incident-level data from these sources. Staff at CCJS was asked about whether special permission might be received to access limited data (e.g., date, location, event type) that could support an open-source data collection initiative. However, it has since been confirmed that no data can be publicly released that could be used to identify the specifics of an incident, in accordance with the Statistics Act and the Privacy Act. As such, the only foreseeable way that this data might be used to support the creation of a database is as a benchmark when collecting open-source data. By knowing the aggregate number of cases that were reported by law enforcement in a given year, researchers will know to keep searching for open-source data until such time as they reach or exceed the reported number of cases.

Victimized communities are torn over hate crime and terrorism legislation, including the distinction between the two. For instance, B'nai Brith Canada (2005) refer to acts of mischief against religious property that are motivated by bias, prejudice or hate (s. 430 (4.1) *Canadian Criminal Code*) as first and foremost, being too narrow, since the Code still neglects to include religious institutions, such as religious-based schools and organizational offices. In their view, such acts can also be viewed as terrorism, since the potential for harm can far outweigh damage to property (7)(7)(7). B'Nai Brith refers the United Talmud Torah elementary school firebombing that occurred in Montreal in 2004 as exemplifying these concerns. This incident was prosecuted as an act of arson (ibid.). Apparently, the prosecutor did not view this building as falling within the narrower hate crime provision of mischief to property that is primarily used for religious worship (s. 430(4.1) of the *Criminal Code*). But even where it had been seen as falling within this hate crime provision, it is questionable whether such an act would also have been viewed as constituting an act of terrorism under section 83.01 of the *Criminal Code*. It may be that many such incidents have occurred, over time, which are not accounted for in official statistics as acts of terrorism or even hate, but perhaps should have been for the purpose of a prospective database that is meant to capture such information.

The definition of a terrorist act in Section 83.01(b) of the *Criminal Code* may provide a useful way of classifying acts of hate that are also extremist or, as the case may be, terrorist acts. Acts of hatred can readily serve a broader, political, religious or ideological purpose, objective or cause that intends or serves to intimidate segments of the public with regard to their security (s. 83.01 (1b.i) *Canadian Criminal Code*). Acts of hate might also be viewed as criminal extremism or even terrorism when they are deliberately committed by individuals or members of groups or entities, and when they cause death or serious bodily harm, serious risk to health and safety, substantial property damage or serious interference with private or essential services.

From the perspective of the *Criminal Code*, deliberate and systemic acts of hate by groups or entities that are directed at a segment of the population should be contrasted with spontaneous or

[3] The Criminal Extremism Analysis Section of the Royal Canadian Mounted Police compiled a chronology of criminal extremism incidents occurring in Canada between 1970 and 2001 in which they sought to differentiate between hate crimes perpetrated by individuals and groups. Their approach was to look at the group membership or affiliation of individual perpetrators and for incidents involving multiple perpetrators.

personal attacks. This is the approach taken by the Global Terrorism Database. Hate crimes are viewed as terrorism in the GTD if they target a broader audience, and are coercive; that is, aimed at attaining a political, economic, religious or social goal. By contrast, acts of hate that are instrumental or merely retributive or personal are not viewed as terrorism, hence are excluded from the GTD. The matrix in Table 2 can be used as a simple means of further exploring the relationship between hate and extremist crime by including reference to these attributes.

Table 2: Relationship between Hate and Extremist Crime

	Hate Crime	
Extremist Crime	Yes	▪ Bias, prejudice or hate-based acts committed for political, religious or ideological motives or goals ▪ Deliberate, systematic, pattern of offending ▪ Aimed at broader audience to coerce or intimidate ▪ Extremist group affiliation or extremist paraphernalia e.g., United Talmud Torah elementary school firebombing in Montreal in 2004 – prosecuted as Arson
	No	▪ Bias, prejudice or hate-based acts based on race, national or ethnic origin, language, colour, religion, sex, age, mental or physical disability, sexual orientation, or any other similar factor. ▪ Spontaneous, personal, retributive e.g., being the target of verbal or physical abuse or being assaulted because of one's sexual orientation.

3. Identifying Cases

Before such time as the collection and coding of empirical data can commence, there must be a clear understanding of the types of incident data that qualifies for inclusion and exclusion. Inclusion criteria will be influenced, in part, by the types of information on extremist crime that stakeholder groups would ideally like to have to service their needs better. For instance, the American Terrorism Study (ATS) only selects incidents on the basis of an indictment brought against an individual by the U.S. Department of Justice. By contrast, the ECDB does not code cases where charges were laid then dropped by police, but does include cases where charges were dropped by prosecutors. In the case of the latter, an incident is thought to have occurred that fits the definition of extremism, and that led to criminal proceedings, even if a jury subsequently acquits the defendant (Freilich and Chermak 2010, 20). This decision rule is a good example of the difference between seeking to identify and code instances of criminal violent extremism, as compared to the quite different goal of labelling individuals or groups as "extremists". If a defendant is acquitted, they cannot justifiably be said to be an extremist, which is, in any case, not the goal when creating an extremist crime database, but the incident in question might still fit the definition of violent criminal extremism; as such may be relevant to a database that is meant to capture such information. Each of the above examples directly affect which incidents are coded.

Other inclusion criteria will need to be considered for the prospective database. For example, should the database consider only those extremist acts committed in Canada? During what time period will acts have to have been committed to be included (e.g., 1990 to present). How will investigators deal with alleged crimes? For instance, the ECDB does not code allegations unless they refer to a specific act that occurred at a specific place and time that led to some sort of government response (see Annex D for a comparison of international database on key attributes).

Gaps and Inconsistencies

Table 3: Gaps and Inconsistencies when Identifying Cases

Incident Data	Included in Database	Not Included in Database
Inclusion criteria met	X	*Gap*
Inclusion criteria not met	*Inconsistency*	X

Adapted from Chermak et al. (2011, 213)

Table three above was adapted from Chermak et al. (2011, 213) based on gaps and inconsistencies they observed when reviewing existing terrorism-database sources. At times, they found that incidents that met the inclusion criteria for the database were missing from the database; whereas at other times, incident data was included that did not meet the inclusion criteria. Phrased differently, these are non-sampling errors that researchers should seek to minimize when identifying cases. Non-sampling error can arise at two different stages: when incidents are identified and/or in the way information is coded. Different coders may make different decisions about whether a suspect is a far-rightist, for example (216)(216)(216). In addition to situations where right incidents are missed or wrong incidents are included, incidents can be also be unsubstantiated, as described below:

> "True far-right homicide incidents may be missed for many different reasons, some of which include; a murder miscategorised by police, prosecutors, or medical examiners as a suicide or natural death, the far-right suspects were never identified as suspects in a homicide, suspects that were identified but were not tied to the far-right, information that did tie the suspect to the far-right was never reported to the media, or the media never incorporated an individual's far-right ideology into their articles, especially when the homicide was not ideologically motivated." (Chermak et al. 2011, 215-6)

The inconsistencies observed most often by Chermak et al. (2011) were databases that included lone wolves even though their criteria were only supposed to include groups or, as the case might be, ideological homicides. At other times, database sources missed the ideological crimes they were supposed to include. This paper has stressed the need for conceptual clarity which should limit the tendency for these types of problems to occur. Nonetheless, a rigorous process for quality control should be adopted. Several existing databases have already developed such processes (e.g., ECDB, the Institute for the Study of Violent Groups, etc.). It is therefore recommended that the relevant processes be sought from the curators of these databases to learn and benefit from their experience.

Chermak et al. (2011, 215) suggest creating an "error profile" to account for non-sampling errors. It is worth considering what a profile such as this would look like and the information it would contain. At a minimum, non-sampling errors should be documented so that users of the database are informed as to its limitations.

4. Searching for Cases

Pre-testing Phase

When developing the Global Terrorism Database, the investigators first developed a database codebook and web-based data entry interface, which was then pretested for data entry problems (LaFree and Dugan 2007, 186). A two-month pretest period was initiated in which the codebook was refined. It is recommended that sufficient time for pre-testing be undertaken when developing the Canadian database.

Lexicon

Once the inclusion criteria are established for the database, a uniform list of terms will need to be developed that will be used to search for potential cases. For example, words in general media searches to uncover right-wing extremist incidents for the U.S. ECDB include: Homicide and Klan, Homicide and militia, Homicide and sovereign citizen, Homicide and Aryan nations, Homicide and skinheads, Homicide and far rightist, Homicide and far right extremists. A similar combination of exhaustive terms will need to be developed for each type of extremism that is being explored by way of the data collection initiative.

Sources of Incident Data

The particular challenges associated with capturing data on terrorism-related offenses are well documented. There are three main sources for criminal incident data: official reports from law enforcement agencies (e.g., Uniform Crime Reporting surveys), victimization data and surveys, and “self-report” data from offenders. Official criminal statistics are problematic, since as LaFree (2012) describes, terrorists are often convicted for other offenses (e.g., weapons violations, money laundering, etc.). As Chermak et al. (2011) describe, Uniform Crime Reporting surveys were not designed to capture terrorism-related offenses, and researchers do not typically have access to primary (classified) data collected by intelligence agencies. Since victimization data rely on sampling methods, they are thought to be of little use for understanding terrorism-related offenses due to their extremely low incidence (LaFree 2012; LaFree and Dugan 2007). Also, victims who survive terrorist attacks are rarely able to provide details about terrorist offenders since most often, they are unfamiliar with them. In any case, the Canadian General Social Survey (GSS) Victimization survey is only conducted every five years and does not measure people’s experience of extremist crime. As LaFree (2012) acknowledges, self-report data from terrorism offenders is also lacking in many cases due to the fact that most researchers cannot gain access to interview convicted terrorists, and in any case, most terrorists refuse to be interviewed.

Any undertaking to collect data on extremist crime in Canada is expected to face similar challenges to those encountered when collecting terrorism-related incident data. For one, “extremism” does not violate Canada’s criminal code, and the code does not include a definition for violent criminal extremism. A Canadian-relevant list of data sources and search engines will have to be identified and mined for potential cases, which will then have to be judged to ensure they meet the criteria for inclusion in the database.

There are only very few official, Canadian sources of relevant incident data and not all of these sources can necessarily be made public. In 2004, the UCR 2.2 was created, at which time Statistics Canada began collecting police-reported hate crime data (Canadian Centre for Justice Statistics 2010). However, the UCR does not identify links between hate crimes and extremism. The homicide questionnaire represents another official law enforcement data source that is collected by Statistics Canada. The homicide survey has been administered since 1961, and has included a police officer's personal assessment of the apparent motive for the crime, and whether that motive relates to hate, along with a summary of the special circumstances related to the homicide (Statistics Canada 2010). Approval from Statistic's Canada would be needed before such time as these data sources could be accessed and additional coding of officers' assessments be undertaken. Another potential source of incident data are police forces from across the country. It is recommended that the Police Information and Statistics (POLIS) Committee of the Canadian Association of Chiefs of Police (CACP) be contacted. However, even if confidential access to data within Statistic's Canada or law enforcement agencies is permitted, it is highly unlikely that official data, in which the names of perpetrators, suspects or victims are known, could be made public, hence included in the database (see the Privacy section in this report).

Table 4: Search Engines Used for Uncovering Potential U.S. Extremist Crime Incidents

1. Lexis-Nexis
2. Proquest
3. Yahoo
4. Google
5. Copernic
6. News Library
7. Westlaw
8. Google Scholar (Articles & Legal Opinions)
9. Amazon
10. Google U.S. Government
11. Federation of American Scientists
12. Google Video
13. Center for the Study of Intelligence
14. Surf Wax
15. Dogpile
16. Mamma
17. Librarians' Internet Index
18. Scirus
19. All the Web
20. Google News
21. Google Blog
22. Homeland Security Digital Library
23. Vinelink
24. The inmate locator
25. Individual State Department of Corrections
26. Blackbookonline.info

Source: Chermak et al. (2011)

In all likelihood, data collection will need to rely on open sources of information for reasons of privacy. Many unofficial sources of incident data do exist that U.S. researchers, for instance, have come to rely upon for terrorism and extremism data (e.g., publically available, searchable materials, such as books, newspaper articles, official records, such court records, and magazines; Chermak et al. 2011). Those persons involved in searching and coding for the ECDB systematically search 26 web-engines to uncover information on extremist crimes, suspects, victims and groups (see Table 4). This list should be taken as a guide, revised and augmented based on their relevance to Canadian domestic extremist crime. The ECDB rely on other sources as well, such as scholarly reports and journals that include relevant case studies, chronologies and information. They also obtain information on extremist activities from watch-dog groups (e.g., the Southern Poverty Law Centre, the Anti-Defamation League, the Militia Watchdog Organization, the Centre for Democratic Renewal, and Political Resource Associates). These organizations are present on the Internet and their members often circulate reports, newspaper clippings and other documents. The extent to which there exist scholarly reports and journals and watch-dog groups reporting on Canadian extremist crime still needs to be explored.

One potentially very useful Canadian source for information is CanLii, which provides public access to court judgments from all jurisdictions (www.canlii.org).

Data Reliability

Procedures for ensuring the reliability of the data will be needed when developing the database. For instance, others have found that newspapers do not make consistent decisions about the definitions they use or will necessarily report on the same characteristics of people or events in their stories (Chermak et al. 2011, 194).

> "Ross's (1992) study of right-wing violence in Canada assembled a detailed chronology of events based upon material from the Toronto Reference Library, archival newspaper clippings from the intelligence branch of a police agency, files of three private organizations, published chronologies of violent political behavior in Canada, and newspaper clippings from major magazines." (Chermak et al. 2011, 195)

5. Coding Cases

Creating a set of variables and coding cases is probably the most complicated task thus far discussed. Once variables are created, these are not likely to change. The necessary time should be spent to get it right. Coding needs to be consistent, which can be challenging even if there is only one person who examines all prospective cases. Where multiple people are involved the process can quickly become a mess of inconsistency. Thus, a comprehensive set of protocols is needed to guide this activity, provide direction to "coders" and resolve ambiguities.

The coding of cases relies on a well-articulated set of inclusion and exclusion criteria. Then, a list of variables will need to be developed, along with the values associated with each and a clear description. This process will involve a number of decisions, including such things as how to track suspects when documenting prior and subsequent crimes, as well as how and when to create separate variables that will permit the greatest flexibility for those who will analyze the data (e.g., in a manner similar to how terrorism cases were coded in the GTD). A decision will also need to be made regarding the number of data points to capture, recognizing that with incident, suspect, and victim databases, the number of variables can quickly increase to a point where populating the data becomes too onerous and expensive.

It is recommended that a preliminary set of variables be created and disseminated to stakeholders so they might identify those deemed most relevant and important, with an eye to the future, to limit the overall amount of data being sought. A number of variables listed in the GTD and ECDB codebooks should probably be included in the Canadian database. We can benefit from their lessons learned. Defining, capturing and coding information in the same way will also permit ready comparisons between international, U.S. and Canadian incidence of extremist crime.

As much as other databases are probably already capturing data in ways that will be of interest to Canadian security intelligence and law enforcement agencies, other opportunities exist to explore synergies between the prospective database and existing law enforcement initiatives. For instance, the RCMP have created an attribute set for criminal extremism and terrorism that they use to complement their intelligence and analytical assessments of known violent criminal extremists and groups. Experts have been relied upon to assign weights to the different attributes based on their judgement of which attributes are most closely related to capability and intent to use violence. It is conceivable that variables could be created for each of the attributes, and the information collected as part of the database initiative. Doing so would permit an empirical examination of the different attributes, in terms of their relative and changing prevalence over time, as well as their relationship to outcome variables, such as the severity of violence against persons (representing one of the existing attributes), property damage, etc. With access to empirical data, the results of consultations with experts (i.e., expert judgements) could be validated and an assessment could be completed of the relative importance of the attributes. One issue, of course, will be the extent to which information on the attributes is readily available. But the first step is to review the set of attributes, and develop a list of variables, following which a pilot test can be undertaken to determine the extent to which and how readily data are available.

Privacy

Any data that is collected must respect and not violate the rights to privacy of any identifiable persons. Data collection that draws exclusively on information that is available through open sources largely obviates privacy concerns. The overview below becomes relevant primarily should the project also draw on or collate data held by government or private organizations.

Federally, personal information comes under: the Privacy Act 1983 applying to the federal public sector, and the Personal Information Protection and Electronic Documents Act 2004 (PIPEDA) which applies to commercial activities in the Atlantic Provinces, Ontario, Manitoba, Saskatchewan and the Territories. Quebec, Alberta and BC have their own laws in this regard, except in instances where PIPEDA applies to the federally regulated private sector and personal information collected in interprovincial and international transactions occurring within these provincial boundaries. Both the Privacy Act and PIPEDA are enforced by the Charter, largely through s.8 on the right to freedom from unreasonable search or seizure. Accordingly, violations of these rights are punishable under the criminal code. These regulations have been recently strengthened by mandatory Privacy Impact Assessments that monitor government agencies' performance in upholding these important privacy regulations when delivering services.

For the purposes of this project statutes that limit the use of personal information collected by the federal government are particularly important and catalogued in the Table 5 below. However, it is not particularly useful to sift through all 28 of the provincial privacy acts until the objective and the method of data collection have been finalized. Should a database end up being housed at a university, that province's privacy legislation may have to be perused to ensure compliance. Nonetheless, the relevant provincial acts are found in Annex E. Should these come into play, advice by proper legal counsel, alongside a review of applicable case law will likely be inevitable.

Privacy Act

The Privacy Act (PA) is the primary legislative document governing the collection, storage and disclosure of data collected by the Federal government. It ensures that the civil liberties guaranteed to Canadian citizens under the Charter are upheld by Federal bodies requiring the collection of personal information. For the purpose of this act, Personal Information is considered:

> "Personal information" means information about an identifiable individual that is recorded in any form including, without restricting the generality of the foregoing,
>
> *(a)* Information relating to the race, national or ethnic origin, colour, religion, age or marital status of the individual,
> *(b)* Information relating to the education or the medical, criminal or employment history of the individual or information relating to financial transactions in which the individual has been involved,
> *(c)* Any identifying number, symbol or other particular assigned to the individual,
> *(d)* The address, fingerprints or blood type of the individual,
> *(e)* the personal opinions or views of the individual except where they are about another individual or about a proposal for a grant, an award or a prize to be made to

another individual by a government institution or a part of a government institution specified in the regulations,
(f) Correspondence sent to a government institution by the individual that is implicitly or explicitly of a private or confidential nature, and replies to such correspondence that would reveal the contents of the original correspondence,
(g) The views or opinions of another individual about the individual,
(h) The views or opinions of another individual about a proposal for a grant, an award or a prize to be made to the individual by an institution or a part of an institution referred to in paragraph (e) but excluding the name of the other individual where it appears with the views or opinions of the other individual, and (i) the name of the individual where it appears with other personal information relating to the individual or where the disclosure of the name itself would reveal information about the individual.

Even within the government, *the use and disclosure of this information must directly relate to the purpose for which it was originally collected.* The only exception to this rule is under s. 8 (2) of the Privacy act where the agency can collect information from a secondary source where direct collection "would defeat the purpose or prejudice the use for which information is collected." This is particularly relevant for the purposes of this research, since it is unlikely that those actors being entered into the database for the purpose of social network analysis would willingly divulge incriminating evidence. In those instances where event-centric data is collected from publically available sources, where no minors are implicated in any criminal activity, collection of data would not be subject to the Privacy Act. Likewise data collected on persons when that data has been submitted to a national library or museum is not subject to regulation by the Privacy Act. The only other instances where data can be disclosed without individual consent are as follows:

Section 8 (1) & (2).

- For the reasons the information was obtained.
- For a purpose that is consistent with the purpose for which the information was obtained.
- For any purpose in accordance with an Act of Parliament.
- To comply with subpoenas or warrants issued by a court or person or body of jurisdiction to compel the production of information.

These exceptions are detailed further in the chart below.

Personal Information Protection and Electronic Documents Act

If this project is to be a commercial enterprise, then it would also be subject to regulation by PIPEDA. The only exception would be in those provinces that have legislation that is substantially similar to PIPEDA, in which case the project would still be subject to the same constraints, just under different legislation. PIPEDA essentially extends extant privacy legislation to secure the exchange of information as technological advances increase ease of communication of said information. It ensures that the collection and disclosure of this information by private entities conforms to privacy legislation. PIPEDA does not apply to any government agency that is already regulated by the 1983 Privacy Act. Companies must only collect information without individual consent or knowledge if:

<u>**Sec. 2**</u>

(*a*) The collection is clearly in the interests of the individual and consent cannot be obtained in a timely way;
(*b*) It is reasonable to expect that the collection with the knowledge or consent of the individual would compromise the availability or the accuracy of the information and the collection is reasonable for purposes related to investigating a breach of an agreement or a contravention of the laws of Canada or a province;
(*c*) The collection is solely for journalistic, artistic or literary purposes;
(*d*) The information is publicly available and is specified by the regulations; or
(*e*) The collection is made for the purpose of making a disclosure

----

(2) For the purpose of clause 4.3 of Schedule 1, and despite the note that accompanies that clause, an organization may, without the knowledge or consent of the individual, use personal information only if
(*a*) in the course of its activities, the organization becomes aware of information that it has reasonable grounds to believe could be useful in the investigation of a contravention of the laws of Canada, a province or a foreign jurisdiction that has been, is being or is about to be committed, and the information is used for the purpose of investigating that contravention
(*b*) it is used for the purpose of acting in respect of an emergency that threatens the life, health or security of an individual;
(*c*) it is used for statistical, or scholarly study or research, purposes that cannot be achieved without using the information, the information is used in a manner that will ensure its confidentiality, it is impracticable to obtain consent and the organization informs the Commissioner of the use before the information is used.

There is some flexibility in the collection of data without individual consent if it can be proven that the collection of this data is:

a) in the interest of national security;
b) *for the purpose of a scholarly study*;
c) The permission of the Privacy Commissioner is granted prior to data collection.

Gaining access to this information presents an entirely different challenge; however, if the above conditions are met the collection of this data would be in compliance with the statute. PIPEDA grants any citizen the right to file a claim against an enterprise s/he feels to be in violation of the act. This is of consequence for the project as stipulated below (Table 5). Still, these considerations only apply if this is to be a commercial enterprise.

Table 5: Privacy Legislation Considerations

Legislation	Primary Issue	Implication	What Can be Done?	How?
Federal Privacy Act	The Federal Government (FG) is not allowed to disclosure personal information it collects without consent from individuals	Could be difficult to use information collected by the FG, therefore project organizers would be required to collect data that is already available yet inaccessible	Use information collected for purposes similar to the goals of the database Comply with a legislative act that grants additional powers to studies being conducted in the interest of national defence	Focus on data collected for the purpose of national security Find a legislative act that coincides with our purposes It may be possible to make a case that it is a matter of national defence in which case it then it would be allowed under the Access to Information Act. Information submitted in a national library or museum can be used freely
	The FG may not grant access to information gained by a provincial government without that province's consent	If the FG grants access to certain information, the 28 different provincial privacy acts may apply	There is no way around this. But it is not immediately obvious how provincial data may be immediately necessary or relevant	Use data that is collected by provinces will require examination of provincial legislation
PIPEDA	Regulates private entities collecting data by electronic means	If this is to be a private enterprise then this may constrain barriers to data collection	Best addressed with the Privacy Commissioner directly to ensure compliance	There is some room for leniency in scholarly undertakings, particularly if they aid national defence and permission is granted by the Privacy

				Commissioner
	Individual(s) can file complaints against organizations if that individual feels the organization is not in compliance If the Commissioner has any reason to believe that the project is being conducted in a manner that does not comply with the act, s/he may audit the project	At best this could stall the collection of data, and at worst it could stop the project all together	Since there is no way to stop a valid complaint, the collection, disclosure and storage of personal information is not beyond reproach	The complaint will either be ruled invalid by the commissioner, in which case there is no issue, or the commissioner will determine the complaint to be valid and the project would be subject to an audit, the consequences of which could be the cessation of the project, or even conferring damages to the plaintiff.

Other Privacy Considerations

There is another consideration regarding privacy that warrants consideration. It involves the extent in which identified individuals are associated with alleged crimes in the database. Other databases, (e.g., ECDB) includes the names of suspects who are associated with alleged incidents even where charges were dropped by prosecutors or the suspect was found to be innocent by a jury. Obviously, the goal of the database is to capture incidents that fit the definition or inclusion criteria for violent criminal extremism. The intent – similar to the ECDB – is not to label individuals or groups as "criminals" or "extremists". Still, it is unclear whether this approach has Canadian privacy implications. Unfortunately, colleagues at the Department of Justice are not in a position to provide legal advice on this issue at this time; as such, it is still considered a risk. Despite the focus of database being incidents not individuals, conceivably, an individual who committed an alleged crime, but who was not convicted of that crime or for whom charges were subsequently dropped, could sue for damages if their name is associated with defamatory content. While this does not appear to have been an issue for the ECDB, it is recommended that strategies be considered and legal advice be obtained about how best to mitigate against such a likelihood.

Definition of an Incident

There are particular challenges involving the definition of an "incident" that will need to be overcome when developing the Canadian database. Both the ECDB Codebook and Uniform Crime Reporting (UCR) Incident-Based Survey offer some useful guidance. For instance, the ECDB investigators clearly note, "an incident may contain more than one crime" (Freilich and

Chermak 2010, 23). According to the UCR report, a “criminal incident” can also involve several victims and several accused persons (Canadian Centre for Justice Statistics 2010). “Incidents are usually distinct”, in the ECDB, "if they occur at different times (temporally distinct) in different locations (spatially distinct) involve different victims and are not linked to earlier acts that were necessary, i.e., must occur, for the subsequent act to occur.” (Freilich and Chermak 2010, 24). The following examples of one incident in the ECDB are given: (a) A shoots B & C simultaneously; (b) A shoots B & C in the same room (at the same time). By contrast, “situations that involve different victims, different suspects, and occur at different times and in different places are also usually distinct incidents.” (ibid).

For the UCR, the primary rule that determines the number of incidents appears based on the type of violation and consistency surrounding the elements of the crime. Fundamentally different types of criminal violations are coded as separate incidents (e.g., traffic and non-traffic violations).Where actions are interrelated, however, they can be coded as a single incident, with one the consequence of the other (e.g., a person commits murder in a building then sets fire to the building in order to cover up the crime). However, the fact that criminal violations occur over time does not mean that they should necessarily be coded as separate incidents if enough elements of the crime are the same and if all of the actions come to the attention of police at the same time (e.g., a person breaks into a cottage several times over several weeks). In cases where a person robs a bank, for instance, then proceeds to break into a car – these should be separate incidents. According to the UCR report, “violations can be tied together because they either happened in a sequential manner, they repeat over time, or they are all part of a larger case.” (Canadian Centre for Justice Statistics 2010, 21). Table 6 refers to the specific rules that are given to police when identifying incidents for the UCR survey.

Table 6: Definition of an Incident from the Uniform Crime Reporting Incident-Based Survey

Two or more violations of the law (and their related victims and accused persons) are grouped into the same unique incident if and only if they are committed by the same person or group of persons and if they are either:

1. part of simultaneous or sequential actions that occur at the same place (not repeated actions over a long period of time but actions committed simultaneously or in sequence in a short period of time at the same place); or

2. part of interrelated actions over a short period of time, that is, actions where one action leads to the other or where one is the consequence of the other(s); or

3. when a violent action is repeated over a period of time and all the violations only come to the attention of the police at one point in time; or

4. when a series of similar crimes, committed at the same location by the same individual(s), come to the attention of the police at a given time.

Reproduced from: (Canadian Centre for Justice Statistics 2010, 21)

Researchers for the ECDB and UCR acknowledge that situations can be tricky and the rules governing when to group violations together into one incident can be confusing and even appear contradictory. It is, therefore, recommended that all of these situations be reviewed, a list of examples created, and a comparable set of rules be adopted for use when coding incidents for the Canadian database.

Relevant Variables

The ECDB includes several variables that are used to identify cases: an incident ID, master-file identifier, relational ID, as well as variables that permit relational ties to related suspects and victims (Table 7). Clearly, some form of identification of cases will be needed to distinguish them and to be able to, for instance, identify and track suspects' criminal history and map their network of connections. As to whether this is the best approach for tracking incidents, suspects and victims warrants further consideration, and a discussion with the person(s) responsible for developing the relational database. Being that there is a separate initiative under the CRTI project to examine how best to track criminal behaviour in Canada over time, it is recommended that researchers seek guidance from the responsible persons.

Table 7: Variables for Coding Discrete Incidents in the ECDB

Variable Name	**Values**	**Description**
Incident ID	Numeric	[ECDB] List the case identification number based on the coder's personal identification number.
Master-file Identifier		[ECDB] List master-file identification number. If listing more than one number, separate with a semicolon.
Relational ID	Numeric	Case ID number and Master ID number (no space between numbers)
Coder's Name	Masked	
Why discrete incident	String	Why is the incident discrete?
Related Suspects	Numeric	List the case ID numbers for all suspects related to the incident
Related Victims	Numeric	List the case ID numbers for all victims related to the incident

Source: Freilich and Chermak (2010, 26-7)

Individuals, Groups and Organizations

Understanding what constitutes a single incident poses a challenge when collecting and coding data for the database. Another challenge involves distinguishing individual, group and organizational-level involvement in violent extremism. Implicit in the discussion thus far, is that the database will collect and code individual-level data on domestic violent extremism. However, there are benefits to collecting data that would permit subsequent analyses at the group- and organizational-level. For instance, (Asal, Pate, and Schulzke 2012, in press) completed a quantitative analysis of factors associated with the use of violence by extremist organizations in the Middle East. Since many acts of political violence are thought to be committed by members of extremist organizations, it is important to understand whether there are organizational factors that might explain which organizations are more or less likely to engage in political violence as well as the tipping points that might affect an organization's propensity towards violence.

Retrospectivity

An issue that will need to be resolved is how to handle incidents of wrongdoing that were committed in the past (e.g., prior to the enactment of current anti-terrorism legislation). If a past offense meets the criteria for inclusion in the database, then it should be captured and coded accordingly. However, to the extent that data collection relies on open sources, as others have noted (LaFree 2012, 46), there is an issue with the decreasing extensiveness of open source data over time. That is, the databases will likely undercount total events occurring farther back in time. This will pose a methodological challenge when deciding how far back in time to try and collect data. There may be insufficient data available to identify and correctly code cases for inclusion in the database. Findings will also be distorted and will need to be calibrated if the database undercounts past incidents.

Another issue that will need to be considered when relying on open sources for data collection involves what is referred to as "publicity effects" Chermak et al. (2011, 210). Higher as compared to lower profile incidents tend to be overrepresented in the media. While higher profile incidents provide multiple data sources that can be used to verify the accuracy of the data, greater effort will likely need to be expended to capture more obscure and less publicized data points.

Automated or Manual Coding

There is a question as to whether computer algorithms can be used to augment or replace people for purposes of identifying and capturing information for a database. Algorithms have become reasonably good at identifying people and places (so-called Named Entity Recognition), but at present, they cannot be solely relied upon to determine if an incident meets the inclusion criteria for the database. Whether an incident can be coded as violent, politically-motivated extremism, for instance, requires a trained and knowledgeable person in charge of coding activities. Nor are algorithms particularly effective for dealing with semantic information. Different sources of information will misspell names, use only initials or short forms, which pose additional challenges when using algorithms. Similarly, algorithms can identify dates but cannot readily distinguish between different conventions (e.g., whether "3/2/2012" refers to February or March). In most instances, human background knowledge is necessary, which means that coding can be time-consuming.

Despite the limitations of algorithms, there is a possibility that automated approaches could support and expedite the work of a human coder. Algorithms could be used to process a document initially and create a record by tagging the important parts with low-level tags such as the names of individuals, places, targets, dates, and times; as well as strings for other text. A subsequent step would still be needed to code the tagged data, but automating the initial capture of information into a record could hasten the process of reviewing, assessing and coding the incident data.

Here is an example of a way media source data can be automatically captured:

> *April 5 2004: Firebombing of the United Talmud Torah elementary school in Montreal. Attack against Jewish Canadians. No injuries as school closed for Passover. Fire act of hatred, a bid to destroy children's learning centre in retaliation of Israel's policy towards Palestinians. Fire hurled into library. Perpetrator(s) unknown.*
>
> <date coding=2004/04/05>April 5 2004</date>:<action> Firebombing</action> of the<location> United Talmud Torah elementary school</location> in<city> Montreal</city>. Attack against <target> Jewish Canadians</target>. No injuries as school closed for Passover. Fire act of hatred, a bid to destroy children's learning centre in retaliation of Israel's policy towards Palestinians. Fire hurled into library. Perpetrator(s) <perp>unknown</perp>.

Following the automated extraction and compilation of potential incident data, a subsequent step could be to create a database record from the document. Other automatic tools exist (e.g., database front-ends) that use tag sets as inputs, parsing each document, extracting the information within each tag to a database record field. Though, given some of the inherent challenges and limitations that were previously referred to, it may be still be necessary for a human coder to review each tagged record before such time as it is coded and transferred into a database record. It is, therefore, recommended that automated tools be identified and explored that might greatly expedite the initial search and coding of rudimentary incident data.

6. Data Storage & Access

This document has continually referred to the creation of a *database* on Canadian extremist crime. Yet, various options exist for storing data, the first of which is not a database at all, but rather a format, such as a text file or a spreadsheet. In terms of databases, there are also different options, varying from open-source to commercial.

The benefit of a text or spreadsheet format for storing data is that it can be easily shared and accessed using a wide range of tools, including those that researchers may develop themselves. The ability to create and process queries does require greater sophistication. A database is the logical format, but commercial databases are the most expensive by an order of magnitude. They can hold much larger volumes of data than open-source tools, but they also use proprietary formats to represent the data, which means that analysts typically requires the extraction of tables and/or conversion of data to an accessible format.

Another consideration when selecting a medium for storing the data is the extent to which end-users (e.g., government, academia) would prefer access to the data via the Internet, and whether such access should include ability to manipulate the data (e.g., slice and dice the data, display graphs, etc.). It is recommended that database options be explored that would lend themselves so such a capability, if so desired.

Who stores the data is another question that will need to be addressed. Among the factors that will, no doubt, influence the decision is sustainability. One option is an academic Centre that already manages similar datasets. Various locations will need to be identified and assessed.

7. Conclusion

Much of the initial effort when creating a database on extremist crime will be to construct, test and refine a “codebook”. While this paper has identified some key issues and steps that warrant further consideration, there is much work to be done. For instance, the ECDB Codebook is 310 pages long. It contains, in some cases, less information than what is presented here, and, in other respects, substantially more information. Much of the additional information corresponds to a set of well-articulated protocols that are intended to guide a team of investigators involved in identifying, searching and coding for extremist criminal behaviour. This paper has argued for a preliminary step as well, which serves as a foundation for everything that follows: the creation of very clearly defined concepts. Unless sufficient time is spent defining and clarifying what is meant by concepts, such as terrorism or extremism, everything that follows will be cast into doubt. Concepts must be clearly defined and there must be a high degree of transparency surrounding their meaning. A database on extremist crime is only useful if those who are subsequently involved in analyzing and reporting on the data clearly understand what the data represents (e.g., what types of data are included and excluded) and are fully aware of its limitations. This is the one area in which an improvement could be made to the ECDB Codebook. Despite all of the information it contains, questions exist concerning some of the key concepts and data that are being captured.

When initiatives such as this one are proposed, oftentimes, there are so many steps associated with gaining approval, once monies are obtained, there is tremendous pressure to begin data collection. While the desire to get on with things is natural, it is nevertheless recommended that sufficient time and effort be spent defining terms, and creating protocols that will help to ensure a rigorous approach to data collection, once it begins, and a high degree of public confidence in the quality of the database. Considering that a database such as the one proposed will be around for a long time, it just makes sense to spend the time at the beginning to get things right.

The steps, while numerous, are ultimately quite logical. Concepts need to be defined and inclusion criteria developed. A set of inclusion criteria are necessary before an exhaustive set of search terms can be created, and a comprehensive list of sources need to be identified before searches can be undertaken. Open-source searches are necessary to identify cases, but those cases cannot be coded until a list of variables and a relational database are created. A pilot will be necessary to check for errors before such time as the data collection phase can commence; whereas, a quality control process will also be needed to ensure data collection proceeds smoothly and uniformly and gaps and inconsistencies are minimized.

What follows are a series of recommendations that stem from this report. These recommendations are merely suggestive. They intend to set the stage by providing readers with a “methodological primer” of sorts. Options and recommendations are made for defining relevant concepts, identifying, searching, coding and storing cases for the prospective database. Given how complicated it is to create an extremist crime database, it is hoped that this paper will alert interested parties to some of the many methodological issues inherent in the undertaking.

8. Recommendations

(1) The database is intended to capture Canadian domestic extremist crime, but the actual scope of the initiative still needs to be determined. While "violent extremism" is a concept that is often used interchangeably with "terrorism", it is a broader phenomenon with terrorism representing a subset. It is recommended that the concept of "extremism" be conceptualized to illuminate the potential scope of the data initiative. Also, what constitutes "domestic" criminal activity also needs to be defined. For instance, attacks can be planned and preparations made in Canada but carried out elsewhere. Extremist crimes can also carried out, internationally, against Canadian interests or targets.

(2) This paper has proposed a conceptualization of "political extremism" (see Annex C). Subject matter experts should be sought who can critique the typology. The framework warrants theoretical, practical and empirical scrutiny, in so far as it may provide a useful way of conceptualizing and illustrating the spectrum of criminal extremist behaviour. As well, it is recommended that other conceptualizations be similarly identified and assessed.

(3) Canadian terrorism legislation should to be used to define what constitutes "terrorism". It is recommended that a condensed and simplified version of "terrorist activity" based on section 83.01(1)(b) be created in a manner similar to what was done by the U.S. National Counterterrorism Centre in order to permit them to compile an annual database on terrorist incidents, under the rubric of the Worldwide Incidents Tracking System (WITS).

(a) The following is an example of a simplified definition based on Canadian law that might be used for purposes of discussion and refinement at a meeting of experts:

Terrorism: A criminal act, committed by non-state actors for political, religious or ideological reasons, with the intention of political intimidation, subversion or compelling a government or organization to do or refrain from doing any act and that either threatens to cause or actually causes death or serious bodily harm, endangers life, causes a serious risk to the health and safety of a population, causes substantial property damage that is likely to result in harm, and/or causes serious interference or disruption of an essential service, facility or system.

(4) It is recommended that definitions and inclusion criteria be specific enough to resolve ambiguities and minimize theoretical gaps and inconsistencies when collecting data.

(a) The following are examples of possible inclusion criteria based on the proposed definition of "terrorism" above, as well as the criteria that were created for the GTD:

i) The incident must be intentional – the result of a conscious calculation.
ii) The act must be committed for political, religious or ideological reasons.
iii) It must threaten to cause or actually causes death or serious bodily harm, endanger life, cause serious risk to the health and safety of a population,

causes substantial property damage that is likely to result in harm, and/or serious interference or disruption of an essential service, facility or system.

iv) There must be evidence of an intention to intimidate a population or compel a government or organization to do or refrain from doing any act.

v) The perpetrators of the incidents must by sub-national actors.

Note. The Global Terrorism Database refers to "political, economic, religious or social goals", and refers to a communicative aspect, where perpetrators seek convey a message to a larger audience(s) than the immediate victims. It also includes an additional criterion based on definitions of (non)combatants.

(5) Data collection should not privilege one form of violent extremism to the exclusion of other forms; unless of course, a particular form is believed to have significantly greater incidence or resources are such that a narrower focus is believed necessary.

(6) Ensure that the definitions, inclusion criteria and variables that are created for the Canadian database permit valid comparisons, possibly also the sharing of data with other databases (e.g., U.S. Extremist Crime Database, Global Terrorism Database, etc.).

(a) Even where definitions vary, it is recommended that data be structured in a way that will permit users to apply their own definitions, similar to what was done for the Global Terrorism Database. For instance, data can be coded using the above inclusion criteria in a way that allows users to filter the data set based on their own definitions.

(7) Examine ways to capture acts of hate that are motivated by extremist ideology.

(a) Seek to identify acts of hatred that serve a broader, political, religious or ideological purpose, objective or cause and that intends or serves to intimidate segments of the public with regard to their security (s. 83.01 (1b.i) *Canadian Criminal Code*).

(b) Acts of hate might also be viewed as criminal extremism or even terrorism when they are deliberately committed by individuals or members of groups or entities, and when they cause, e.g., death or serious bodily harm, serious risk to health and safety, substantial property damage or serious interference with private or essential services.

(c) The database should seek to differentiate between spontaneous, personal or retributive attacks and those representing deliberate and/or systemic acts of hate by individuals, groups or entities that is directed as a segment of the population. Hate crimes comprising the latter should be considered for inclusion in the database.

Note. This is the approach that has been taken by the Global Terrorism Database. Hate crimes are viewed as terrorism if they target a broader audience, and are coercive; that is, aimed at attaining a political, economic, religious or social goal. By contrast, acts of hate that are instrumental, retributive or personal are excluded.

(8) It is recommended that a small contract be arranged with the Criminal Justice Statistics Division (CCJS) at Statistics Canada to code law enforcement officers' narrative description in the Homicide Survey Incident Questionnaire to see how many cases, if any,

fit a definition of extremist crime. While the data could not be publically released nor integrated into the database, this analysis has not been completed, and this and other historical analyses may help to further an understanding criminal extremism in Canada.

(9) A rigorous quality control process will need to be adapted or developed to ensure that gaps and inconsistencies in data collection are minimized.

(a) Contact the curators of existing, international databases that have already developed quality control processes (e.g., Extremist Crime Database, the Institute for the Study of Violent Groups, etc.), to seek to obtain and adapt their established processes.

(b) Consider ways to document non-sampling errors in order that users of the database can be informed as to its limitations. Examine and consider adopting the method used by Chermak et al. (2011) to create an "error profile" when coding data.

(10) A uniform list of search terms will need to be created to support data collection activities. These terms should be consistent and exhaustive in order to minimize gaps in collection.

(11) A Canadian list of data sources and search engines will have to be identified. Begin with the sources listed in Table 6 and adapt it to the Canadian context.

(a) Investigate the existence of Canadian scholarly reports, chronologies and watch-dog groups who report on historical cases of actual or suspected extremist crimes.

i) Incorporate the chronology of Canadian criminal extremist incidents (1970 to 2004) that was created by RCMP, Criminal Extremism Analysis Section.

ii) Incorporate the chronology of Terrorism incidents (1960-1989) that was created by the National Security Coordination Centre (Kellett, Beanlands, and Deacon 1991).

(12) A preliminary set of variables should be created and disseminated to stakeholders to seek agreement on those deemed most relevant and important in order that the total number of data points be kept to a reasonable number.

(a) Collaborate with the RCMP Centre for Criminal Intelligence, Research and Innovation on their attribute set for criminal extremism/terrorism. Explore ways to create variables and collect data based on the attributes in order to validate the framework and generate analytical insights.

(13) Using the ECDB Codebook as a guide, it is recommended that a similar Canadian Codebook be created with a comprehensive set of definitions, guidelines and protocols for use by those involved in identifying, coding as well as analyzing the incident data.

(14) It is recommended that sufficient time be allotted to pre-testing the Canadian database to test and refine the Canadian Codebook, once developed.

(15) Any data that is collected – despite being in the open domain – must be coded and stored in a way that respects and does not violate the right to privacy of identifiable individuals.

(a) A database such as this one will capture *incidents* that fit the definition or inclusion criteria for violent criminal extremism. The goal is not to label individuals or groups as "criminals" or "extremists". Still, it is recommended that legal advice be obtained and strategies adopted for how to mitigate against such a likelihood that an individual who committed an alleged crime, but who was not convicted of that crime or for whom charges were dropped, could sue for being associated with defamatory content.

(16) It is recommended that automated tools be identified and assessed that might greatly expedite the initial search and coding of rudimentary incident data via open sources.

(17) Identify and evaluate open-source and commercial database packages for their ability to permit distributed access to the database via the Internet, as well as the ability of users to slice-and-dice and download the data via online sources.

(18) Explore suitable options for data warehousing that address issues of privacy and sustainability. Warehousing will likely have to be done outside of government. Assess the suitability of Centres located at existing institutions who manage similar datasets.

9. References

Asal, Victor, Amy Pate, and Marcus Schulzke. 2012. Why Do Some Organizations Kill While Others Do Not: An Examination of Middle Eastern Organizations. Unpublished draft.

B'nai Brith Canada. 2005. A Review of Canada's Anti-Terrorism Act. The House of Commons Subcommittee on Public Safety and National Security of the Standing Committee on Justice, Human Rights, Public Safety and Emergency Preparedness and to The Senate of Canada Special Committee on the Anti-Terrorism Act: B'nai Brith Canada National Office.

Backes, Uwe. 2007. "Meaning and Forms of Political Extremism." *Central European Political Studies Review* no. IX (4):242-62.

Canadian Centre for Justice Statistics. 2010. Uniform Crime Reporting Incident-Based Survey. edited by Policing Services Program. Ottawa: Statistic's Canada.

Canadian Security Intelligence Service. 2010. Public Report 2009 / 2010. edited by Canadian Security Intelligence Service. Ottawa: Government of Canada.

Chermak, Steven M., Joshua D. Freilich, William S. Parkin, and James P. Lynch. 2011. "American Terrorism and Extremist Crime Data Sources and Selectivity Bias: An Investigation Focusing on Homicide Events Committed by Far-Right Extremists." *Journal of Quantitative Criminology* no. 28 (1):191-218. doi: 10.1007/s10940-011-9156-4.

Department of Justice. *The Anti-terrorism Act: Definition of Terrorist Activity*. Department of Justice 2008. Available from http://www.justice.gc.ca/antiter/sheetfiche/terrordefp2-terreurdefp2-eng.asp.

Freilich, Joshua D., and Steven M. Chermak. 2010. U.S. Extremist Crime Database (ECDB): Codebook & Additional Project Documentation

Green, Donald P., Laurence H. McFalls, and Jennifer K. Smith. 2001. "Hate Crime: An Emergent Research Agenda." *Annual Review of Sociology* no. 27:479-504.

Kellett, Anthony, Bruce Beanlands, and James Deacon. 1991. Terrorism in Canada, 1960-1989. edited by National Security Coordination Centre. Ottawa: Ministry of the Solicitor General of Canada.

LaFree, Gary. 2012. "Generating Terrorism Event Databases: Results from the Global Terrorism Database, 1970 to 2008." In *Evidence-Based Counterterrorism Policy,*, edited by C. Lum and L.W. Kennedy, 41-64. New York: Springer Science+Business Media.

LaFree, Gary, and Laura Dugan. 2007. "Introducing the Global Terrorism Database." *Terrorism and Political Violence* no. 19 (2):181-204.

National Consortium for the Study of Terrorism and Responses to Terrorism (START). 2011. Global Terrorism Database: GTD Variables & Inclusion Criteria. Maryland, USA: University of Maryland.

———. 2012a. Global Terrorism Database Codebook: Inclusion Criteria and Variables. Maryland: University of Maryland.

———. *Global Terrorism Database: Data Collection Methodology*. University of Maryland 2012b. Available from http://www.start.umd.edu/gtd/using-gtd/.

Statistics Canada. 2010. Homicide Survey: Incident Questionnaire. edited by Canadian Centre for Justice Statistics. Ottawa: Statistics Canada.

The National Counterterrorism Centre. 2012. 2011 Report on Terrorism. Washington, DC: Office of the Director of National Intelligence.

United Nations General Assembly. 2004. "Follow-up to the outcome of the Millennium Summit." no. A/59/565.

United Nations Security Council. 2004. Resolution 1566. In *S/RES/1566 (2004)*, edited by United Nations Security Council.

10. Annex A: Criminal Code Definitions and Legislation

Hate Propaganda Legislation

“hate propaganda” means any writing, sign or visible representation that advocates or promotes genocide or the communication of which by any person would constitute an offence under section 319;

Public incitement of hatred

319. (1) Everyone who, by communicating statements in any public place, incites hatred against any identifiable group where such incitement is likely to lead to a breach of the peace is guilty of

(a) an indictable offence and is liable to imprisonment for a term not exceeding two years; or
(b) an offence punishable on summary conviction.

Willful promotion of hatred

319. (2) Everyone who, by communicating statements, other than in private conversation, willfully promotes hatred against any identifiable group is guilty of

(a) an indictable offence and is liable to imprisonment for a term not exceeding two years; or
(b) an offence punishable on summary conviction.

Defences

319. (3) No person shall be convicted of an offence under subsection (2)

(a) if he establishes that the statements communicated were true;
(b) if, in good faith, the person expressed or attempted to establish by an argument an opinion on a religious subject or an opinion based on a belief in a religious text;
(c) if the statements were relevant to any subject of public interest, the discussion of which was for the public benefit, and if on reasonable grounds he believed them to be true; or
(d) if, in good faith, he intended to point out, for the purpose of removal, matters producing or tending to produce feelings of hatred toward an identifiable group in Canada.

Hate Crime Provisions

430. (4.1) Everyone who commits mischief in relation to property that is a building, structure or part thereof that is primarily used for religious worship, including a church, mosque, synagogue or temple, or an object associated with religious worship located in or on the grounds of such a building or structure, or a cemetery, if the commission of the mischief is motivated by bias, prejudice or hate based on religion, race, colour or national or ethnic origin,

(a) is guilty of an indictable offence and liable to imprisonment for a term not exceeding ten years; or
(b) is guilty of an offence punishable on summary conviction and liable to imprisonment for a term not exceeding eighteen months.

718.2 A court that imposes a sentence shall also take into consideration the following principles:

(a) a sentence should be increased or reduced to account for any relevant aggravating or mitigating circumstances relating to the offence or the offender, and, without limiting the generality of the foregoing,
(b) evidence that the offence was motivated by bias, prejudice or hate based on race, national or ethnic origin, language, colour, religion, sex, age, mental or physical disability, sexual orientation, or any other similar factor.

Terrorism Offenses in the Criminal Code

“terrorism offence” means

(a) an offence under any of sections 83.02 to 83.04 or 83.18 to 83.23,
(b) an indictable offence under this or any other Act of Parliament committed for the benefit of, at the direction of or in association with a terrorist group,
(c) an indictable offence under this or any other Act of Parliament where the act or omission constituting the offence also constitutes a terrorist activity, or
(d) a conspiracy or an attempt to commit, or being an accessory after the fact in relation to, or any counseling in relation to, an offence referred to in paragraph (a), (b) or (c);

“terrorist activity” has the same meaning as in subsection 83.01(1);

“terrorist group” has the same meaning as in subsection 83.01(1);

“terrorist activity” means

(a) an act or omission that is committed in or outside Canada and that, if committed in Canada, is one of the following offences:

i. the offences referred to in subsection 7(2) that implement the Convention for the Suppression of Unlawful Seizure of Aircraft, signed at The Hague on December 16, 1970,
ii. the offences referred to in subsection 7(2) that implement the Convention for the Suppression of Unlawful Acts against the Safety of Civil Aviation, signed at Montreal on September 23, 1971,
iii. the offences referred to in subsection 7(3) that implement the Convention on the Prevention and Punishment of Crimes against Internationally Protected Persons, including Diplomatic Agents, adopted by the General Assembly of the United Nations on December 14, 1973,
iv. the offences referred to in subsection 7(3.1) that implement the International Convention against the Taking of Hostages, adopted by the General Assembly of the United Nations on December 17, 1979,
v. the offences referred to in subsection 7(3.4) or (3.6) that implement the Convention on the Physical Protection of Nuclear Material, done at Vienna and New York on March 3, 1980,
vi. the offences referred to in subsection 7(2) that implement the Protocol for the Suppression of Unlawful Acts of Violence at Airports Serving International Civil Aviation, supplementary to the Convention for the Suppression of Unlawful Acts against the Safety of Civil Aviation, signed at Montreal on February 24, 1988,
vii. the offences referred to in subsection 7(2.1) that implement the Convention for the Suppression of Unlawful Acts against the Safety of Maritime Navigation, done at Rome on March 10, 1988,
viii. the offences referred to in subsection 7(2.1) or (2.2) that implement the Protocol for the Suppression of Unlawful Acts against the Safety of Fixed Platforms Located on the Continental Shelf, done at Rome on March 10, 1988,
ix. the offences referred to in subsection 7(3.72) that implement the International Convention for the Suppression of Terrorist Bombings, adopted by the General Assembly of the United Nations on December 15, 1997, and
x. the offences referred to in subsection 7(3.73) that implement the International Convention for the Suppression of the Financing of Terrorism, adopted by the General Assembly of the United Nations on December 9, 1999, or

(b) an act or omission, in or outside Canada,

i. that is committed

A. in whole or in part for a political, religious or ideological purpose, objective or cause, and
B. in whole or in part with the intention of intimidating the public, or a segment of the public, with regard to its security, including its economic security, or compelling a person, a government or a domestic or an international organization to do or to refrain from

doing any act, whether the public or the person, government or organization is inside or outside Canada, and

ii. that intentionally

A. causes death or serious bodily harm to a person by the use of violence,
B. endangers a person's life,
C. causes a serious risk to the health or safety of the public or any segment of the public,
D. causes substantial property damage, whether to public or private property, if causing such damage is likely to result in the conduct or harm referred to in any of clauses (A) to (C), or
E. causes serious interference with or serious disruption of an essential service, facility or system, whether public or private, other than as a result of advocacy, protest, dissent or stoppage of work that is not intended to result in the conduct or harm referred to in any of clauses (A) to (C),
F. and includes a conspiracy, attempt or threat to commit any such act or omission, or being an accessory after the fact or counseling in relation to any such act or omission, but, for greater certainty, does not include an act or omission that is committed during an armed conflict and that, at the time and in the place of its commission, is in accordance with customary international law or conventional international law applicable to the conflict, or the activities undertaken by military forces of a state in the exercise of their official duties, to the extent that those activities are governed by other rules of international law.

"terrorist group" means

(a) an entity that has as one of its purposes or activities facilitating or carrying out any terrorist activity, or
(b) a listed entity, and includes an association of such entities.

(1.1) For greater certainty, the expression of a political, religious or ideological thought, belief or opinion does not come within paragraph (b) of the definition "terrorist activity" in subsection (1) unless it constitutes an act or omission that satisfies the criteria of that paragraph.

(1.2) For greater certainty, a suicide bombing is an act that comes within paragraph (a) or (b) of the definition "terrorist activity" in subsection (1) if it satisfies the criteria of that paragraph.

(2) For the purposes of this Part, facilitation shall be construed in accordance with subsection 83.19(2).

Financing of Terrorism

provisions s. 83.02 to 83.04 have been excluded for the purposes of this report

Participating, Facilitating, Instructing and Harbouring

83.18 (1) Everyone who knowingly participates in or contributes to, directly or indirectly, any activity of a terrorist group for the purpose of enhancing the ability of any terrorist group to facilitate or carry out a terrorist activity is guilty of an indictable offence and liable to imprisonment for a term not exceeding ten years.

Marginal note: Prosecution
(2) An offence may be committed under subsection (1) whether or not

(a) a terrorist group actually facilitates or carries out a terrorist activity;
(b) the participation or contribution of the accused actually enhances the ability of a terrorist group to facilitate or carry out a terrorist activity; or
(c) the accused knows the specific nature of any terrorist activity that may be facilitated or carried out by a terrorist group.

Marginal note: Meaning of participating or contributing
(3) Participating in or contributing to an activity of a terrorist group includes

(a) providing, receiving or recruiting a person to receive training;
(b) providing or offering to provide a skill or an expertise for the benefit of, at the direction of or in association with a terrorist group;
(c) recruiting a person in order to facilitate or commit

i. a terrorism offence, or
ii. an act or omission outside Canada that, if committed in Canada, would be a terrorism offence;

(d) entering or remaining in any country for the benefit of, at the direction of or in association with a terrorist group; and
(e) making oneself, in response to instructions from any of the persons who constitute a terrorist group, available to facilitate or commit

i. a terrorism offence, or
ii. an act or omission outside Canada that, if committed in Canada, would be a terrorism offence.

Marginal note: Factors
(4) In determining whether an accused participates in or contributes to any activity of a terrorist group, the court may consider, among other factors, whether the accused
(a) uses a name, word, symbol or other representation that identifies, or is associated with, the terrorist group;
(b) frequently associates with any of the persons who constitute the terrorist group;
(c) receives any benefit from the terrorist group; or

(d) repeatedly engages in activities at the instruction of any of the persons who constitute the terrorist group.

Marginal Note: Facilitating terrorist activity
83.19 (1) Everyone who knowingly facilitates a terrorist activity is guilty of an indictable offence and liable to imprisonment for a term not exceeding fourteen years.

Marginal note: Facilitation
(2) For the purposes of this Part, a terrorist activity is facilitated whether or not

(a) the facilitator knows that a particular terrorist activity is facilitated;
(b) any particular terrorist activity was foreseen or planned at the time it was facilitated; or
(c) any terrorist activity was actually carried out.

2001, c. 41, s. 4.

Marginal note: Commission of offence for terrorist group
83.2 Every one who commits an indictable offence under this or any other Act of Parliament for the benefit of, at the direction of or in association with a terrorist group is guilty of an indictable offence and liable to imprisonment for life.
2001, c. 41, s. 4.

Marginal note: Instructing to carry out activity for terrorist group
83.21 (1) Every person who knowingly instructs, directly or indirectly, any person to carry out any activity for the benefit of, at the direction of or in association with a terrorist group, for the purpose of enhancing the ability of any terrorist group to facilitate or carry out a terrorist activity, is guilty of an indictable offence and liable to imprisonment for life.

Marginal note: Prosecution
(2) An offence may be committed under subsection (1) whether or not

(a) the activity that the accused instructs to be carried out is actually carried out;
(b) the accused instructs a particular person to carry out the activity referred to in paragraph (*a*);
(c) the accused knows the identity of the person whom the accused instructs to carry out the activity referred to in paragraph (*a*);
(d) the person whom the accused instructs to carry out the activity referred to in paragraph (*a*) knows that it is to be carried out for the benefit of, at the direction of or in association with a terrorist group;
(e) a terrorist group actually facilitates or carries out a terrorist activity;
(f) the activity referred to in paragraph (*a*) actually enhances the ability of a terrorist group to facilitate or carry out a terrorist activity; or
(g) the accused knows the specific nature of any terrorist activity that may be facilitated or carried out by a terrorist group.

2001, c. 41, s. 4.

Marginal note: Instructing to carry out terrorist activity
83.22 (1) Every person who knowingly instructs, directly or indirectly, any person to carry out a terrorist activity is guilty of an indictable offence and liable to imprisonment for life.
Marginal note: Prosecution

(2) An offence may be committed under subsection (1) whether or not

(a) the terrorist activity is actually carried out;
(b) the accused instructs a particular person to carry out the terrorist activity;
(c) the accused knows the identity of the person whom the accused instructs to carry out the terrorist activity; or
(d) the person whom the accused instructs to carry out the terrorist activity knows that it is a terrorist activity.

Harbouring or concealing

83.23 Every one who knowingly harbours or conceals any person whom he or she knows to be a person who has carried out or is likely to carry out a terrorist activity, for the purpose of enabling the person to facilitate or carry out any terrorist activity, is guilty of an indictable offence and liable to imprisonment for a term not exceeding ten years.

2001, c. 41, s. 4.

Hoax Regarding Terrorist Activity

83.231 (1) Every one commits an offence who, without lawful excuse and with intent to cause any person to fear death, bodily harm, substantial damage to property or serious interference with the lawful use or operation of property,

(a) conveys or causes or procures to be conveyed information that, in all the circumstances, is likely to cause a reasonable apprehension that terrorist activity is occurring or will occur, without believing the information to be true; or
(b) commits an act that, in all the circumstances, is likely to cause a reasonable apprehension that terrorist activity is occurring or will occur, without believing that such activity is occurring or will occur.

Marginal note: Punishment

(2) Everyone who commits an offence under subsection (1) is guilty of

(a) an indictable offence and liable to imprisonment for a term not exceeding five years; or
(b) an offence punishable on summary conviction.

Marginal note: Causing bodily harm

(3) Everyone who commits an offence under subsection (1) and thereby causes bodily harm to any other person is guilty of

(a) an indictable offence and liable to imprisonment for a term not exceeding ten years; or
(b) an offence punishable on summary conviction and liable to imprisonment for a term not exceeding eighteen months.

Marginal note: Causing death

(4) Everyone who commits an offence under subsection (1) and thereby causes the death of any other person is guilty of an indictable offence and liable to imprisonment for life.

2004, c. 15, s. 32.

Annex B: U.S. Extremist Crime Database

The following is reproduced from the ECDB Codebook (Freilich and Chermak 2010, 21-3).

The **far-right** is composed of individuals or groups that subscribe to aspects of the following ideals: They are fiercely nationalistic (as opposed to universal and international in orientation), anti-global, suspicious of centralized federal authority, reverent of individual liberty (especially their right to own guns, be free of taxes), believe in conspiracy theories that involve a grave threat to national sovereignty and/or personal liberty and a belief that one's personal and/or national "way of life" is under attack and is either already lost or that the threat is imminent (sometimes such beliefs are amorphous and vague, but for some the threat is from a specific ethnic, racial, or religious group), and a belief in the need to be prepared for an attack either by participating in or supporting the need for paramilitary preparations and training or survivalism.

The **Islamic Jihadist** movement is composed of individuals or groups that subscribe to aspects of the following ideals:

- Only acceptance of the Islamic faith promotes human dignity as well as affirms God's authority;
- Rejection of the traditional Muslim respect for "People of the Book," i.e., Christians & Jews;
- "Jihad" (defined as to struggle in the path of God in the example of the Prophet Muhammad & his early companions)" is a defining belief in Islam. This belief includes the "lesser Jihad" that endorses violence against a corrupt other;
- the Islamic faith and or one's people are oppressed and under attack in both "local and nominally Muslim" Middle-Eastern/North African/Asian governments that are corrupt & authoritarian, as well as in non-Islamic nations (e.g., Israel/Palestine, Russia//Chechnya; India/Kashmir, etc) that occupy indigenous Islamic populations (an argument for political & military mobilization);
- the West in general & the U.S. in particular supports the corruption, oppression & humiliation of Islam, and exploits the region's resources;
- the culture of the West in general & the U.S. in particular (e.g., gay-rights, feminism, sexual permissiveness, alcohol abuse, racism, etc.) has a corrosive effect on social & religious values;
- the people of the West in general and the US in particular are responsible for the actions of their governments and culture (NOTE: this is an important element that distinguishes jihadists from other Muslims critical of Western states because it could justify the killing of innocents);
- it is a religious obligation is to promote a violent Islamic revolution to combat this assault on Islam, oppression, corruption & the values of the West by targeting nonbelievers (both Muslims and non-Muslims);
- Jihad will remain an individual obligation until all lands that were once Muslim (e.g., Andalusia- Southern Spain, Palestine, Philippines, etc.) are returned & Islam again reigns supreme in those countries;
- Islamic law- Sharia- provides the ideal blueprint for a modern Muslim society and should be implemented in all "Muslim" countries by force

NOTE: Global jihadists are most concerned with combating the West in general & the United States in particular, while local jihadists are focused on a specific conflict such as Somalia; Russia/Chechnya; India/Kashmir; Israel/Palestine; China/Uighur; Philippines/Moro, etc.

Secular Arab nationalists are composed of individuals or groups that subscribe to aspects of the following ideals:

- the suspect's nation (either Muslim or Middle Eastern) that he identifies with is either oppressed by a "local usurper" Middle-Eastern/North African/Asian government that is corrupt & authoritarian, or the nation is occupied and/or under attack from the West in general or the United States in particular;
- the West in general & the U.S. in particular supports the corruption, oppression & humiliation of this nation and exploits its resources;
- the people of the West in general and the US in particular are responsible for the actions of their governments and culture;
- Action must be taken to combat this assault, oppression, & corruption;
- The goal is true independence from the West in general & the United States in particular.

Environmental and animal rights extremists are individuals or groups that subscribe to aspects of the following ideals:

- Support for biodiversity and bio-centric equality (i.e., that humans are no greater than any other form of life and have no legitimate claim to dominate earth);
- the earth and/or animals are in imminent danger;
- the government and /or parts of society such as corporations are responsible for this danger;
- this danger will ultimately result in the destruction of the modern environment and/or whole species;
- the political system is incapable and/or unwilling to fix the crisis by taking actions to preserve American wilderness, protect the environment and support biological diversity;
- there is a need to defend the environment and/or animals.

NOTE: Environmental rights extremists (primarily) are most focused on the environment while animal rights extremists (primarily) are most concerned with the rights of animals.

Annex C: Conceptualizing Extremism

It is difficult to think about creating a database of extremist crime without first confronting and addressing the conceptual confusion that surrounds the concept of “extremism”. Ideally, an initiative such as this one should be guided by theory. Simple, empirical definitions of different types of extremism can be created, as was done with the Extremist Crime Database, for instance, but these are likely to create theoretical problems if the concept is not well conceptualized. It is therefore recommended that time be taken, either at the outset of this project, or some later date, to review existing, relevant conceptual frameworks, and to adopt one that provides a theoretical basis for understanding, identifying and categorizing different types of criminal extremist activity.

This Annex will focus on one such framework developed by Backes (2007), which regards political extremism to be the antithesis of constitutional democracy. Political extremism represents “ideologies/movements which aim at the elimination of the constitutional state or the exclusion of parts of the population from assuring essential basic rights” (252) or both. Backes (2007) separates the dimensions of democracy and constitutionalism into four ideal types that may provide a useful way of conceptualizing “political extremism” (see Table 8); hence, defining its various criminal manifestations (e.g., where such acts also involve violence, planned violence or the threat of violence) and establishing inclusion criteria to support data collection activities.

Table 8: (Anti-)Democracy and (Anti-)Constitutionalism Combined into Four Ideal Type Forms

	(Anti-)Constitutionalism	
(Anti-) Democracy	(1) Democratic Anti-constitutionalism	(2) Constitutional Anti-democratism
	(3) Anti-democratic Anti-constitutionalism	(4) Democratic Constitutionalism

Source: Backes (2007, 251)

Technically, the fourth type (i.e., Democratic Constitutionalism) in Table 8 is only exclusively the antithesis of the third type (i.e., Anti-democracy Anti-constitutionalism). By also viewing quadrants one and two as extremism implies the existence of a continuum of political ideologies that are more or less extreme, which is a contradiction in terms. By definition, the “extreme” point is the one furthest from the centre. Still, as Backes recognizes, to solely focus on political extremism as representing, Anti-democracy Anti-constitutionalism would ignore political ideologies or movements that negate either of the two dimensions. A democratic constitutional state requires both dimensions, according to Backes. By including all four quadrants in the typology, one can differentiate between political ideologies that involve either a rejection of civil equality (i.e., fundamental human equality) or civil liberty (i.e., the power-controlled institutional structure of the modern constitutional state) or both.

If there is a missing dimension to Backes' typology in Table 8, it involves its one-sided focus on political ideologies that negate either of the two dimensions of constitutional democracy. Clearly, there can be an extreme in either direction to democracy and constitutionalism. If one considers the normative characteristics of modern-day, constitutional democracy as occupying the central region of a two-dimensional political space, two extreme dimensions become apparent for each of the two axes (Figure 1). Recognizing this failing, Backes adapts his framework to include the two extreme poles of democracy, which is "extreme egalitarianism" on the one end, and "anti-egalitarianism" on the other; and the two extremes of constitutionalism, one being "anarachic", which implies the absolute freedom of the individual and complete lack of national order, compared to the opposite extreme, being "totalitarianism" or what is complete subservience to the state. The space that is revealed is thought to provide a complete portrait of forms of political extremism.

The typology in Figure 1 represents four ideal types and can be used to derive an understanding of different forms of political extremism. It can be used to identify and search for real world examples that fall within its different quadrants. One can also look to existing forms of extremism and examine whether they fit within the typology. For instance, the ECDB refers to a limited set of what is referred to as ideological, extremist crimes in Annex B that appear to fit within the typology. Still, it is recommended that the typology be validated by subject matter experts, and definitions be created for the other forms of extremism that fall within the four quadrants.

Based on the ECDB definitions in Annex B, one can argue that the far-right extremists so-defined largely fall within the political extremes of quadrants one or two of the "Constitutionalism" axis in Figure 1 given their vehement support for individual liberty (e.g., their right to own guns and be free of taxes), and their suspicion, at times outright rejection of centralized federal authority. While some might fall within quadrant one, it is likely that many more would fall within quadrant two, given the fear that also often surrounds members of certain ethnic, racial or religious groups.

By contrast, animal- or environmental-rights extremists assert that animals have identical rights, in the case of the former, and in the case of the latter that all living things have inherent value. Representing extreme egalitarian views, both types of extremism would probably fall along the "Democratism" axis (quadrants one or three in Figure 1). Those extremists who also reject the absence of government control, hence the current political order for its inability or unwillingness to protect animals or preserve ecological value, would likely fall in the "Anti-Constitutionalism" axes (quadrant three).

Figure 1 is useful for casting light on the political sphere, but as the Canadian *Criminal Code* definition of a terrorist act reveals, extremist behaviour can be motivated by fundamentalist views of religion. While fundamentalism is obviously related to both egalitarianism and the state, its ideological basis is thought to be distinct in other respects; thus, Backes introduces a third "fundamentalism" axis which has as its extremes, "enmity towards religion", on the one hand, and "theocracy" on the other, which he combines into a three-dimensional depiction involving constitutionalism, democracy and fundamentalism (Figure 2).

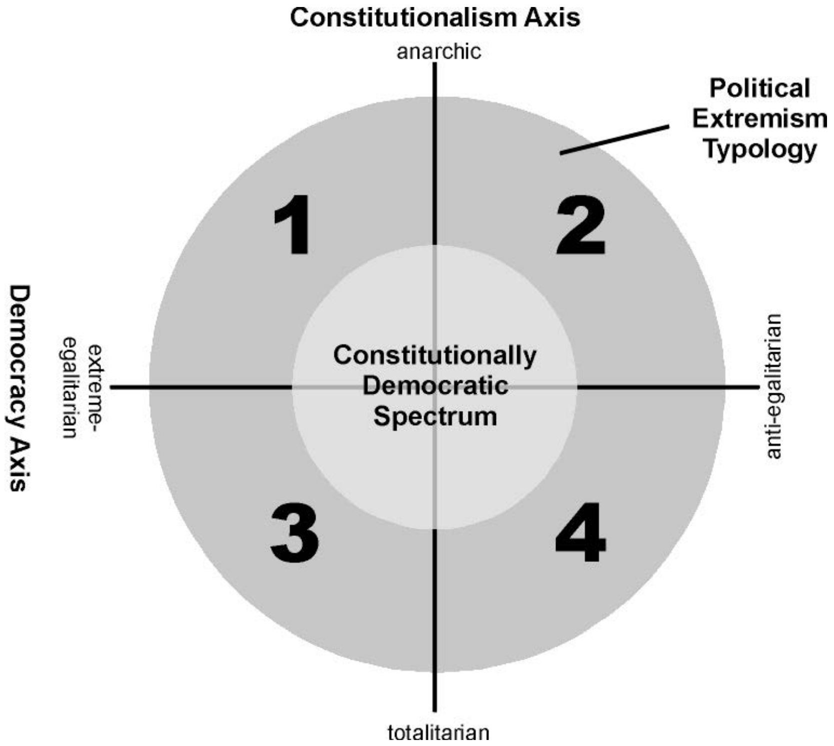

Figure 1: Forms of Political Extremism in a Two-Dimensional Political Space

Source: Backes (2007, 254), adapted from Bobbio, Norberto (1996): Left and Right. The Significance of a Political Distinction, Chicago, University of Chicago Press.

Backes' depiction warrants greater theoretical and practical scrutiny, in so far as it may provide a useful way of conceptualizing and illustrating the spectrum of criminal extremist behaviour for purposes of developing a database. Thus, it is recommended that greater time and effort be spent contemplating and validating his typologies so that there is a clear understanding of the various types of extremist behaviours that exist, and are to be considered for data collection. For the purposes of constructing a database it is, ultimately, important to ensure that the typology captures all forms of political extremism, such that clear definitions can be developed and data collection can be undertaken uniformly. There are many different past and current manifestations of political extremism, in Canada. There is no good reason, in our view, why a database should privilege one form of violent extremism to the exclusion of other forms; unless, of course, a particular form is believed to have significantly greater or lesser incidence than others, and resources are such that a targeted data collection strategy is necessary. Once there is conceptual clarity concerning the focus of inquiry, it is recommended that inclusion and exclusion criteria be clearly articulated to ensure that cases are identified and categorized correctly and consistently.

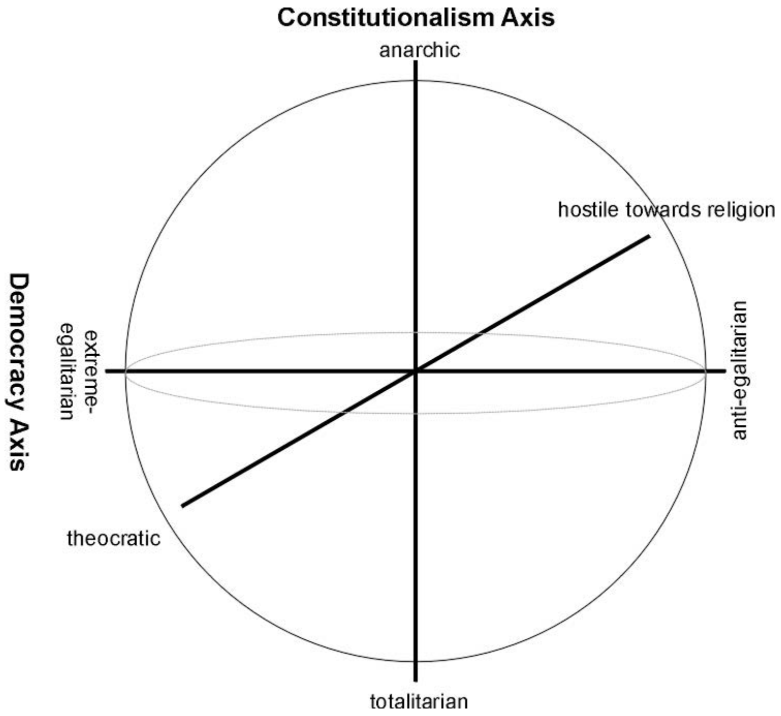

Figure 2: Forms of Political Extremism in a Three-Dimensional Sphere

Source: Backes (2007, 256)

Annex D: Comparison of International Database

1) Global Terrorism Database (GTD), START, University of Maryland	
Intent Purpose of database	Data is coded for geospatial analysis - "temporal changes in the spatial distribution of incidents, and to test models of diffusion" (LaFree & Dugan 2007, 198)
Geographic Scope National or transnational	Domestic (USA) and international
Definitions Used Broad definitions	“The threatened or actual use of illegal force and violence by a non-state actor to attain political, economic, religious or social goal through fear, coercion or intimidation” (Schmidt 296)
Inclusion Criteria More specific criteria to determine what qualifies as coding	For an incident to be included in the GTD all of the following (3) attributes must be present: Incident must be Intentional, violent and perpetrated by subnational actors. Additionally 2 of the following criteria must also be present: the act must be aimed at attaining a political, economic, religious or social goal; must be evidence of an intention to coerce or convey a message to a larger audience; outside the context of legitimate warfare activities
Coverage Years Included	1990–1992; 1994-2008 Note: Because the GTD recently applied the latter data collection criteria to the 1970-1997 data, the data now form a complete series from 1970 to the present Note: The GTD does not have 1993 data (LaFree and Dugan 2007; Chermak et al. 2011)
Data Holdings Quantity of data included in database	Open sources in multiple languages
Data Sources Where data is obtained (e.g., open sources)	Open sources in multiple languages
Variables A list of all, or those that are unique when compared to other databases	120 variables are locations, method of attack, date of the incident, responsible entity, and the number of casualties.
Data Access How and where data is made available and to whom	Openly available to research and policy communities.
2) Rick Ross Internet Archives for the Study of Destructive Cults Controversial Groups and Movements	
Intent Purpose of database	To study destructive cults, controversial groups and movements and to provide a broad range of information and services easily accessible to the public for assistance and educational purposes (Website.)
Geographic Scope National or transnational	Predominantly North America, but international news sources are also referenced.

Definitions Used Broad definitions	No rigorous definitions are applied; articles referring to 'controversial' groups are included in the repository.
Inclusion Criteria More specific criteria to determine what qualifies as coding	Not defined, but it appears to be group/cult driven. That is, he posts any events, including crimes that have been committed by various cults/groups (such as skin heads).
Coverage Years Included	Timeframe not indicated on the website, but appears to be 1990–2008
Data Holdings Quantity of data included in database	
Data Sources Where data is obtained (e.g., open sources)	
Variables A list of all, or those that are unique when compared to other databases	
Data Access How and where data is made available and to whom	Openly accessible and web-based

3) American Terrorism Study (ATS) conducted in cooperation with the FBI's Terrorist Research and Analytical Center

Intent Purpose of database	Smith and Damphousse (2002), "The primary goal of the ATS was to create an empirical database from which criminological theories and governmental policies could be effectively evaluated." The dataset focuses on terrorism behaviors with a focus on pre-attack planning and preparation
Geographic Scope National or transnational	United States of America
Definitions Used Broad definitions	Relies on legal definitions (either the FBI conventional definition or the Attorney General's regulatory definition if it is applied)
Inclusion Criteria More specific criteria to determine what qualifies as coding	It includes persons indicted federally as a result of an investigation under the FBI's Counterterrorism Program. Study selects data based on the type of indictments brought against individuals by the United States Department of Justice.
Coverage Years Included	1980–1989; 1990–1996; 1997–2002 *Began in 1988 Timeframe: 1990–2008 Note: The ATS has not completely collected all their terrorism court cases from 2004 to 2008 & they may be missing some people. Source: Chermak et al. 2011
Data Holdings Quantity of data	276 court cases, 9,633 indictments, 706 indicted, 71 terrorist groups, 1,097 unique persons (Circa 2009)

included in database	
Data Sources Where data is obtained (e.g., open sources)	Researchers were provided lists of persons indicted, then traveled to federal courthouses to collect data from trial transcripts and docket information.
Variables A list of all, or those that are unique when compared to other databases	Each of the five datasets includes information on approx. 80 variables in four major categories: (1) demographic info, (2) information about the terrorist group to which the individual belongs, (3) prosecution and defense data, and (4) count/case outcome and sentencing data.
Data Access How and where data is made available and to whom	Openly available, however given the preponderance of personal information contained in the ATS, the Federal Bureau of Investigation's Office of General Counsel approves the release of data.
4) Anti-Defamation League; Militia watch-group:	
Intent Purpose of database	The Anti-Defamation League (ADL) fights anti-Semitism and all forms of bigotry in the U.S. and abroad through information, education, legislation, and advocacy. ADL serves as a resource for government, media, law enforcement, educators and the public.
Geographic Scope National or transnational	
Definitions Used Broad definitions	
Inclusion Criteria More specific criteria to determine what qualifies as coding	"…include(s) ideologically motivated and non- ideological homicides, bias-motivated homicides, as well as homicides committed by lone actors and/or those that were prosecuted on the state-level." (Chermak et al. 2011, 205)
Coverage Years Included	
Data Holdings Quantity of data included in database	
Data Sources Where data is obtained (e.g., open sources)	
Variables A list of all, or those that are unique when compared to other databases	
Data Access How and where data is made available	

and to whom	
5) B'Nai Brith Canada	
Intent Purpose of database	Monitor anti-Semitism and hate crimes against minority groups in Canada; social education; lobby policy-makers to enact policies that will suppress anti-Semitism
Geographic Scope National or transnational	Canada - by regions; Ontario (with particular attention to the Greater Toronto Area) and Quebec (with particular attention to Montreal)
Definitions Used Broad definitions	"Racism and bigotry in this country, as expressed in attacks of harassment, vandalism and violence against individual Jews and community institutions" (Website, 2011 Audit).
Inclusion Criteria More specific criteria to determine what qualifies as coding	Extremist who committed anti-Semitic crimes, incidents involve harassment, vandalism or violence from 1996-2006
Coverage Years Included	2007(?) - present; past 30 years audit has been published
Data Holdings Quantity of data included in database	As a snapshot, 1,297 incidents were reported in 2011 and 1,306 incidents were reported in 2010.
Data Sources Where data is obtained (e.g., open sources)	Victim reporting; presumably news and police reports; Anti-Hate Desk tracks hate crimes against Canadian minorities, focused on anti-Semitic incidents.
Variables A list of all, or those that are unique when compared to other databases	Vandalism, harassment, violence/ assault, targets or location of incidents (e.g. synagogue, workplace, schools, online, etc.),
Data Access How and where data is made available and to whom	Yearly 'audit' report released to public via internet site in both English and French.
6) Database of U.S. Extremist Crime (ECDB)	
Intent Purpose of database	Violent crimes committed by far right extremists
Geographic Scope National or transnational	This database covers only crimes committed in the US, including crimes committed in detention facilities
Definitions Used Broad definitions	This database covers only crimes committed in the US, including crimes committed in detention facilities

Inclusion Criteria More specific criteria to determine what qualifies as coding	Includes homicides, attempted homicides, and incidents where the victim was killed or committed suicide
Coverage Years Included	Systematic collection of open-source data on non-violent and violent criminal behavior associated with far right-wing extremist groups, including data on event, perpetrator, and victim
Data Holdings Quantity of data included in database	1990-2008
Data Sources Where data is obtained (e.g., open sources)	Includes over 4,000 incidents of violent rightist extremism
Variables A list of all, or those that are unique when compared to other databases	Includes five different sources: Existing databases, official sources, scholarly and journalistic accounts, watch-group reports, systemic media searches
Data Access How and where data is made available and to whom	Open access web site on which it is hosted also allows spatial representation of all event data. Also allows users to manipulate data and control for variables

7) Chicago Project on Suicide Terrorism (CPOST) Robert A. Pape, Director University of Chicago

Intent Purpose of database	The Chicago Project's main activities focus on core international security challenges: such as the causes and solutions to terrorism, the dynamics of martyrdom, the consequences of nuclear proliferation, and the analytic premises of grand strategy
Geographic Scope National or transnational	International
Definitions Used Broad definitions	Captures terrorists events in which the death of the attacker is inherent or assumed (suicide attacks)
Inclusion Criteria More specific criteria to determine what qualifies as coding	". . .information on an attack must be available from multiple sources" Pape as cited in Wade 2007
Coverage Years Included	1981-2011 (additional years to be added)
Data Holdings Quantity of data included in database	
Data Sources Where data is obtained	Open source news media

(e.g., open sources)	
Variables A list of all, or those that are unique when compared to other databases	Year, location, group, campaign, target type, weapon and gender
Data Access How and where data is made available and to whom	Openly accessible and web-based;
8) International Terrorism: Attributes of Terrorist Events (ITERATE)	
Intent Purpose of database	Primarily concerned with international terrorism and designed for the US policymaking community
Geographic Scope National or transnational	International
Definitions Used Broad definitions	The use, or threat of use, of anxiety-inducing violence for political purposes by any individual or group, whether acting for or in opposition to established government authority, when such action is intended to influence the attitudes and behavior of a target group wider than the immediate victims, and when...its ramifications transcend national boundaries (Mickolus, Sandler and Murdock 1989).
Inclusion Criteria More specific criteria to determine what qualifies as coding	The Common File codifies terrorist activities by venue, type of incident, originating groups and their affiliations, characteristics of victims, and fatalities. The Fate of Terrorists File describes terrorist participants, their nationalities, and post-event outcomes. The Hostage File contains information on hostage events, demands and ransom, terrorist and negotiator behaviors, characteristics of negotiations, length and outcome of events, and nationalities involved. The Skyjack File includes information on aircraft and airlines involved, locations, duration and outcome of incidents, and number of victims.
Coverage Years Included	Common File: 1968-2007; Hostage File: 1968-2007; Fate File: 1968-1987; Skyjack File: 1968-1987 (circa 2008)
Data Holdings Quantity of data included in database	10,837 (as of 2007)
Data Sources Where data is obtained (e.g., open sources)	Open-source news media; "Originally, ITERATE was developed from two Rand chronologies and from press accounts in The New York Times, The Washington Post, and other media. " (Schmid & Jongman 1988, 145)
Variables A list of all, or those that are unique when compared to other databases	Up to 144 variables, basic markers such as the date of an incident, type of attack, casualty numbers, location, organization name (if applicable) are captured. Common File has 42 variables
Data Access How and where data is made available and to whom	Subscription-based; available electronically on CDs via Vineyard software

9) Institute for the Study of Violent Groups (ISVG) University of New Haven, Directed by Daniel Mabrey. Originally developed by Richard Ward at the College of Criminal Justice at Sam Houston State U in 2002	
Intent Purpose of database	Seeks to aggregate open-source information at the greatest level of detail on extremism, terrorism and criminality for output using visualization or analysis. ISVG has a specific focus on violent groups and organized crime, charting violent groups/individuals and their attacks.
Geographic Scope National or transnational	Global focus on international terrorism/subsidiary VKB focuses on domestic extremism (US). Data is geospatially enabled to track the spread of a group's activity across city/states etc.
Definitions Used Broad definitions	Expansive, includes all extremist, terrorist and criminal activity by all terrorist groups, events and individuals
Inclusion Criteria More specific criteria to determine what qualifies as coding	These inclusion criteria are amongst the least restrictive in modern terrorism databases because it covers events, groups and individuals. Furthermore it does not limit for the legitimacy of the target like WITS, GTD or ITERATE, whether the attack was domestic or international like ITERATE or whether secondary sources can corroborate like GTD.
Coverage Years Included	2002-Present, includes all priority 1 data, priority 2 data is recorded and stored electronically for future coding efforts and special projects
Data Holdings Quantity of data included in database	Database “houses more than 4.5 million records on more than 205,000 incidents, 3,800 groups and 35,000 profiles dating back to 2002 with special collections going back to 1970. It also includes a historical record of approx. 40,000 IED events” (I2 Group 2011)
Data Sources Where data is obtained (e.g., open sources)	Articles are identified based on an extant list of sources. Open-source only resources that are widely available to the public and nothing that has any level of secrecy classification
Variables A list of all, or those that are unique when compared to other databases	This database uses an event based schema divided into approx. 1,500 variables-- the most of any dataset. By recording each event in exhaustive minutiae the ISVG is able to arrange data by variables to this extent. Includes information on the events, groups, individuals, and locations identified as pertinent to the incident
Data Access How and where data is made available and to whom	The ISVG is not made accessible to public users, nor is it sold commercially. It is only available to US government sponsored initiatives and organizations. Funded by DOD. The i2 Analyst Notebook can be used to display the links between entities
10) RAND/Memorial Institute for the Prevention of Terrorism-Terrorism Knowledge Base (RAND/MIPT-TKB)	
Intent Purpose of database	No longer in existence. Data used to populate the Global Terrorism Database (GTD)
Geographic Scope National or transnational	International and domestic (American) terrorism events
Definitions Used Broad definitions	To be determined pending full inclusion into START database

Inclusion Criteria More specific criteria to determine what qualifies as coding	Includes MIPT data and research on global terrorism incidents, terrorism related court cases and terrorist groups and leaders. It is amongst the more interactive of American terrorism databases, providing: maps, key biographical information, graphs and summaries. Proved invaluable for those researching terrorism.
Coverage Years Included	1997 – 2004
Data Holdings Quantity of data included in database	Historical data including 29,000 incident profiles, 900 group files and 1,200 leader profiles. Also included a legal database of hundreds of indictments and case profiles
Data Sources Where data is obtained (e.g., open sources)	Relied on MIPT's internal library, comprised of databases and external research on 40 years of terrorism history
Variables A list of all, or those that are unique when compared to other databases	TBD pending full inclusion into START database
Data Access How and where data is made available and to whom	Completely open to anyone in the government or academic community
11) RAND/MIPT Terrorist Incident Database is a precursor to the RAND Database of Terrorism Incidents (RDWTI) continues and covers 1972 – present, though only data until 2009 is posted online. See http://www.rand.org/nsrd/projects/terrorism-incidents.html for more information.	
Intent Purpose of database	To satisfy data requirements for MIPT's primary goal of researching social and political causes of terrorism. In March 2008, the RAND/MIPT data was transferred from the National Memorial Institute for the Prevention of Terrorism to the National Consortium for the Study of Terrorism and Responses to Terrorism (START)
Geographic Scope National or transnational	
Definitions Used Broad definitions	Terrorism is defined by the nature of the act, not by the identity of the perpetrators or the nature of the cause. Terrorism is violence, or the threat of violence, calculated to create an atmosphere of fear and alarm. These acts are designed to coerce others...
Inclusion Criteria More specific criteria to determine what qualifies as coding	
Coverage Years Included	
Data Holdings Quantity of data included in database	
Data Sources	

Where data is obtained (e.g., open sources)	
Variables A list of all, or those that are unique when compared to other databases	
Data Access How and where data is made available and to whom	

12) Southern Poverty Law Center

Intent Purpose of database	As a repository of domestic terrorism, the SPLC keeps a list of “Active Patriot” and “Nativist Extremist” groups . The focus is on right-wing extremism in the United States of America.
Geographic Scope National or transnational	United States
Definitions Used Broad definitions	
Inclusion Criteria More specific criteria to determine what qualifies as coding	Neo-Nazis, Klansmen, white nationalists, neo-Confederates, skinheads, black separatists and border vigilantes.
Coverage Years Included	
Data Holdings Quantity of data included in database	
Data Sources Where data is obtained (e.g., open sources)	
Variables A list of all, or those that are unique when compared to other databases	
Data Access How and where data is made available and to whom	

13) Canadian Disaster Database (CDD)

Intent Purpose of database	The Canadian Disaster Database is an interactive event-centric database populated by the Canadian Federal Government's Department of Public Safety for public use
Geographic Scope National or transnational	Covers Canadian and international events that directly affect Canadians
Definitions Used Broad definitions	"a social phenomenon that results when a hazard intersects with a vulnerable community in a way that exceeds or overwhelms the community's ability to cope and may cause serious harm to the safety, health, welfare, property or environment of people; may be triggered by a naturally occurring phenomenon which has its origins within the geophysical or biological environment or by human action or error, whether malicious or unintentional, including technological failures, accidents and terrorist acts" *PS Emergency Management Framework for Canada*
Inclusion Criteria More specific criteria to determine what qualifies as coding	Must satisfy the previous definition and 1 or more of the following criteria: -10 or more people killed -100 or more people affected/injured/infected/evacuated or homeless -an appeal for national/international assistance -historical significance -significant damage/interruption of normal processes such that the community affected cannot recover on its own *Public Safety Canada*
Coverage Years Included	1900-2012
Data Holdings Quantity of data included in database	900 incidents excluding war
Data Sources Where data is obtained (e.g., open sources)	Both governmental and non-governmental sources
Variables A list of all, or those that are unique when compared to other databases	16 different variables including event location, year, fatalities and federal institution costs
Data Access How and where data is made available and to whom	Open Access

14) Canadian Legal Information Institute (CANLii Database)
Law Societies of Upper Canada

Intent Purpose of database	CANLii refers to a non-profit organization which aims to make Canadian law freely accessible to all Canadians. CANLii's primary tool for enabling access is an extensively populated database containing case law and legislation in both Canadian Federal and Provincial courts and legislatures.

Geographic Scope National or transnational	Includes cases in lower courts as well as courts of appeal, and consolidated legislative regulations and statutes.
Definitions Used Broad definitions	N/A
Inclusion Criteria More specific criteria to determine what qualifies as coding	Any case in any of Canada's provincial, federal or legislative bodies
Coverage Years Included	Varies widely depending on court. For example SCC decisions are catalogued from 1907 on, while coverage of Ontario's court of appeal begins in 1994.
Data Holdings Quantity of data included in database	Approx. 1,072,485 court decisions and 14,983 legislative decisions across 200 different collections
Data Sources Where data is obtained (e.g., open sources)	Populated by Lexum Inc. answerable to the Federation of Law Societies of Canada
Variables A list of all, or those that are unique when compared to other databases	Users can limit search by full text, statute name, case name, citation, docket number, decision date or scope
Data Access How and where data is made available and to whom	Open Access

Annex E: Applicable Provincial Privacy Legislation

Alberta

- *Freedom of Information and Protection of Privacy Act:*
  http://www.canlii.org/ab/laws/sta/f-25/20060718/whole.html

- *Health Information Act:*
  http://www.canlii.org/ab/laws/sta/h-5/20060718/whole.html

- *Personal Information Protection Act*:
  http://www.canlii.org/ab/laws/sta/p-6.5/20060718/whole.html
  (Legislation has been declared "substantially similar" to PIPEDA)

British Columbia

- *Freedom of Information and Protection of Privacy Act:*
  http://www.qp.gov.bc.ca/statreg/stat/F/96165_01.htm

- *Personal Information Protection Act:*
  http://www.qp.gov.bc.ca/statreg/stat/P/03063_01.htm
  (Legislation has been declared "substantially similar" to PIPEDA)

- *Privacy Act:*
  http://www.qp.gov.bc.ca/statreg/stat/P/96373_01.htm

- *Bill 24 — 2008: E-Health (Personal Health Information Access and Protection of Privacy) Act* (as passed Third Reading on May 29, 2008):
  http://www.leg.bc.ca/38th4th/3rd_read/gov24-3.htm

Manitoba

- *Privacy Act:*
  http://web2.gov.mb.ca/laws/statutes/ccsm/p125e.php

- *Freedom of Information and Protection of Privacy Act*:
  http://web2.gov.mb.ca/laws/statutes/ccsm/f175e.php
  (c)

- *Personal Health Information Act:*
  http://web2.gov.mb.ca/laws/statutes/ccsm/p033-5e.php

New Brunswick

- *Protection of Personal Information Act:*
  http://www.gnb.ca/0062/acts/acts/p-19-1.htm

Newfoundland and Labrador

- *Access to Information and Protection of Privacy Act:*
  http://www.assembly.nl.ca/Legislation/sr/statutes/a01-1.htm

- *Privacy Act*
  http://www.assembly.nl.ca/Legislation/sr/statutes/p22.htm

- *Personal Health Information Act* (To be proclaimed):
  http://assembly.nl.ca/Legislation/sr/statutes/p07-01.htm

Nova Scotia

- *Freedom of Information and Protection of Privacy Act:*
  http://www.canlii.org/ns/laws/sta/1993c.5/20060718/whole.html

Ontario

- *Freedom of Information and Protection of Privacy Act:*
  http://www.e-laws.gov.on.ca/html/statutes/english/elaws_statutes_90f31_e.htm

- *Personal Health Information Protection Act:*
  http://www.e-laws.gov.on.ca/html/statutes/english/elaws_statutes_04p03_e.htm
  (Legislation has been declared "substantially similar" to PIPEDA, with respect to health information custodians)

- *Municipal Freedom of Information and Protection of Privacy Act:*
  http://www.e-laws.gov.on.ca/html/statutes/english/elaws_statutes_90m56_e.htm

Prince Edward Island

- *Freedom of Information and Protection of Privacy Act:*
  http://www.gov.pe.ca/law/statutes/pdf/f-15_01.pdf

Québec

- *An Act Respecting the Protection of Personal Information in the Private Sector*:
  http://www.canlii.org/qc/laws/sta/p-39.1/20060614/whole.html
  (Legislation has been declared "substantially similar" to PIPEDA)

- *An Act Respecting Access to Documents held by Public Bodies and the Protection of Public*
  Information:
  http://www.canlii.org/qc/laws/sta/a-2.1/20060614/whole.html

Saskatchewan

- *Freedom of Information and Protection of Privacy Act:*
  http://www.qp.gov.sk.ca/documents/English/Statutes/Statutes/F22-01.pdf

- *Health Information Protection Act:*
  http://www.canlii.org/sk/laws/sta/h-0.021/20060614/whole.html

- *Local Authority Freedom of Information and Protection of Privacy Act*
  http://www.canlii.org/sk/laws/sta/l-27.1/20060614/whole.html

- *Privacy Act*
  http://www.canlii.org/sk/laws/sta/p-24/20060614/whole.html

Northwest Territories

- *Access to Information and Protection of Privacy Act:*
  http://www.canlii.org/nt/laws/sta/1994c.20/20060718/whole.html

Nunavut

- *Access to Information and Protection of Privacy Act:*
  http://canlii.org/nu/laws/sta/1994c.20/20070904/whole.html

Yukon

- *Access to Information and Protection of Privacy Act:*
  http://www.canlii.org/yk/laws/sta/1/20060728/whole.html

List of symbols/abbreviations/acronyms/initialisms

ATS	American Terrorism Study
CCJS	Centre for Criminal Justice Statistics at Statistics Canada
CRTI	Chemical, Biological, Radiological-Nuclear and Explosive (CBRNE) Research and Technology Initiative
DND	Department of National Defence
DRDC	Defence Research & Development Canada
CACP	Canadian Association of Chiefs of Police
CSIS	Canadian Security Intelligence Service
ECDB	The U.S. Extremist Crime Database
GSS	General Social Survey
GTD	Global Terrorism Database
IHL	International Humanitarian Law
PIPEDA	Personal Information Protection and Electronic Documents Act 2004
POLIS	Police Information and Statistics Committee of CACP
PA	The Privacy Act
START	National Consortium for the Study of Terrorism and Responses to Terrorism
UNSCR	United Nations Security Council
UCR	Uniform Crime Reporting
U.S.C.	United States Law Code
WITS	Worldwide Incidents Tracking System

DOCUMENT CONTROL DATA

(Security classification of title, body of abstract and indexing annotation must be entered when the overall document is classified)

1. ORIGINATOR (The name and address of the organization preparing the document. Organizations for whom the document was prepared, e.g. Centre sponsoring a contractor's report, or tasking agency, are entered in section 8.)

DRDC Centre for Security Science
Defence R&D Canada
222 Nepean St. 11th Floor
Ottawa, ON Canada K1A 0K2

2. SECURITY CLASSIFICATION (Overall security classification of the document including special warning terms if applicable.)

UNCLASSIFIED
NON-CONTROLLED GOODS
DMC-A
REVIEW: GCEC JUNE 2010

3. TITLE (The complete document title as indicated on the title page. Its classification should be indicated by the appropriate abbreviation (S, C or U) in parentheses after the title.)

Canadian Extremist Crime Database: Methodological Primer

4. AUTHORS (last name, followed by initials – ranks, titles, etc. not to be used)

Norton, S. and Leuprecht, C

5. DATE OF PUBLICATION (Month and year of publication of document.)

May 2013

6a. NO. OF PAGES (Total containing information, including Annexes, Appendices, etc.)

85

6b. NO. OF REFS (Total cited in document.)

09

7. DESCRIPTIVE NOTES (The category of the document, e.g. technical report, technical note or memorandum. If appropriate, enter the type of report, e.g. interim, progress, summary, annual or final. Give the inclusive dates when a specific reporting period is covered.)

Technical Memorandum

8. SPONSORING ACTIVITY (The name of the department project office or laboratory sponsoring the research and development – include address.)

Centre for Security Science
Defence R&D Canada
222 Nepean St. 11th Floor
Ottawa, ON Canada K1A 0K2

9a. PROJECT OR GRANT NO. (If appropriate, the applicable research and development project or grant number under which the document was written. Please specify whether project or grant.)

9b. CONTRACT NO. (If appropriate, the applicable number under which the document was written.)

10a. ORIGINATOR'S DOCUMENT NUMBER (The official document number by which the document is identified by the originating activity. This number must be unique to this document.)

DRDC CSS TM 2013-004

10b. OTHER DOCUMENT NO(s). (Any other numbers which may be assigned this document either by the originator or by the sponsor.)

11. DOCUMENT AVAILABILITY (Any limitations on further dissemination of the document, other than those imposed by security classification.)

Unlimited

12. DOCUMENT ANNOUNCEMENT (Any limitation to the bibliographic announcement of this document. This will normally correspond to the Document Availability (11). However, where further distribution (beyond the audience specified in (11) is possible, a wider announcement audience may be selected.))

Unlimited

13. ABSTRACT (A brief and factual summary of the document. It may also appear elsewhere in the body of the document itself. It is highly desirable that the abstract of classified documents be unclassified. Each paragraph of the abstract shall begin with an indication of the security classification of the information in the paragraph (unless the document itself is unclassified) represented as (S), (C), (R), or (U). It is not necessary to include here abstracts in both official languages unless the text is bilingual.)

This paper addresses the need for an historical, Canadian, national incident database on criminal extremism, and highlights methodological issues and challenges inherent in its development. While the contents are suggestive, 18 recommendations are enumerated that should be of interest to policy advisors, subject-matter-experts and those researchers who, ultimately, will be responsible for creating the database. Creating a Canadian database on domestic extremist crime is thought to be a useful undertaking, as there can be many benefits. However, as this report makes clear, creating a useful and beneficial tool that stands the test of time is a complicated task and considerable undertaking that requires much forethought.

14. KEYWORDS, DESCRIPTORS or IDENTIFIERS (Technically meaningful terms or short phrases that characterize a document and could be helpful in cataloguing the document. They should be selected so that no security classification is required. Identifiers, such as equipment model designation, trade name, military project code name, geographic location may also be included. If possible keywords should be selected from a published thesaurus, e.g. Thesaurus of Engineering and Scientific Terms (TEST) and that thesaurus identified. If it is not possible to select indexing terms which are Unclassified, the classification of each should be indicated as with the title.)

Violent Extremism; Incident Database; Canadian; Domestic Extremist Crime