ATAC
ASYMMETRIC THREATS ANALYSIS CENTER

Criminal Chemical, Biological, Radiological, and Nuclear (CBRN) Event Database

Codebook

June 30, 2024

Version 1.04

(For Criminal CBRN Event Database v1.0+)

Citing This Database: Sin, Steve S., and Markus K. Binder. *Criminal Chemical, Biological, Radiological, and Nuclear (CRIM CBRN) Event Database, Version 1.0,* Unconventional Weapons & Technology Division (UWT), National Consortium for the Study of Terrorism and Responses to Terrorism (START). Asymmetric Threats Analysis Center (ATAC), University of Maryland. College Park, MD. June 30, 2024. https://cbrn.umd.edu.

START NATIONAL CONSORTIUM FOR THE STUDY OF TERRORISM AND RESPONSES TO TERRORISM | UWT UNCONVENTIONAL WEAPONS AND TECHNOLOGY

UNIVERSITY OF MARYLAND

Contents

I. Criminal Chemical, Biological, Radiological, and Nuclear (CRIM CBRN) Event Database Introductory Material

A. Data Sourcing

The Criminal CBRN Event Database is compiled solely and exclusively from publicly accessible open-source materials. At no point has Criminal CBRN event data collection utilized restricted access governmental materials or non-publicly available grey literature. At no point has the Criminal CBRN Event Database utilized interviews, or any other form of direct contact, with individuals involved in investigating the events that may be recorded within the database.

B. Criminal CBRN Event Database Handling of Personally Identifiable Information (PII) Statement

The Criminal CBRN Database is an event-level database. It is structured to exclude specific individual and group identifying information[1] (e.g., name, date of birth, etc.) that are considered personally identifying information (PII)[2]. No individual threat actor/alleged threat actor is identified within the database. Where the actions of an individual threat actor/alleged threat actor are recorded in the database, they are done so in association within the context of genericized threat actor/alleged threat actor categories such as "Lone Actor" or "Small Unaffiliated Cell." Individual threat actors/alleged threat actors are not distinguished in any manner (other than their categories) and the database does not include any PII.

Although the Criminal CBRN Database itself does not contain any PII, the research staff may encounter threat actor/alleged threat actor PII (for example, name of an individual) through open sources during the course of the research. For these occurrences, the research staff stores such open-source material and any other relevant research records in a designated folder located on START's encrypted drive that only the research team members have access to. The research team only accesses these source materials and research records to extract relevant non-PII data to populate the database. Once the research staff has completed the extraction, the source materials and all relevant research records are then placed in an encrypted records archive folder, which only the principal investigator and the START CBRN data collection manager have access to, and retained for the duration of the project in compliance with

[1] NISTIR 8053, dated October 2015, states, "'identifying information' is used to denote information that identifies individuals. Therefore, identifying information is personal information, but personal information is not necessarily identifying information." (NISTIR 8053, Page 3)

[2] The term "PII," as defined in OMB Memorandum M-07-1616 refers to information that can be used to distinguish or trace an individual's identity, either alone or when combined with other personal or identifying information that is linked or linkable to a specific individual.

the University of Maryland Human Research Protection Policies and Procedures 3.013, "Research Records Retention and Security."[3] Upon the expiration of the retention period, all source materials and research records are purged from START/University of Maryland system. This allows the Criminal CBRN Event Database to maintain its integrity as an anonymized[4] database.

C. Inclusion Criteria

In order to consider an event for inclusion in the Criminal CBRN Event Database, *all four* of the following attributes must be present:

1. **Criminality without Ideology**
   Events of a purely criminal nature in which there is no ideological motive. This encompasses the following:
   a) The motivation is purely financial gain without a greater ideological motive;
   b) The target is a personal relation or acquaintance. Includes instances in which CBRN materials are employed to kill or injure a spouse, family member, friend, business partner, or other personal acquaintance purely because of a personal or professional grudge;
   c) The target is an unrelated or unknown individual, or individuals, killed or injured by CBRN agents or materials used by the threat actor/alleged threat actor in the course of actions directly associated with their efforts to kill or injure a spouse, family member, friend, business partner, or other personal acquaintance purely because of a personal or professional grudge.
   d) Instances of the use of CBRN agents or materials to cause harm driven by personal obsessions or mental illness

2. **Intent**
   The event must be intentional rather than inadvertent. The event must result from a conscious calculation on the part of a threat actor/alleged threat actor.

3. **Violence**
   The event must entail some level of violence, planned violence, or threat of violence, including property violence.

4. **Non-State Actors**
   The threat actor/alleged threat actor must be an individual or group operating independently from the state. Threat actors receiving support in the form of

[3] The most current version of the UMD HRPPP 3.013 is dated December 5, 2017, reviewed September 16, 2020.

[4] ISO/TS 25237:2008(E), "Health Informatics – Pseudonymization," and NISTIR 8053 defines anonymization as a "process that removes the association between the identifying dataset and the data subject. …it does not provide a means by which the information may be linked to the same person across multiple data records or information systems."

materials or training from a state may still be included provided the state is not exercising direct operational control over the threat actor's/alleged threat actor's planning or operations.

D. Exclusion Criteria

1. **Terrorism**
   If the event is ideologically motivated and accordingly aimed at attaining an ideological, political, economic, religious, or social goal the event should not be considered for inclusion in the Criminal CBRN Event Database. [Note: Individual actors associated with radical ideological movements may still engage in criminal acts that are not themselves ideologically motivated. The individual threat actor / alleged threat actor's associations are insufficient on their own to justify exclusion of an event].

2. **Hoaxes**
   If it is absolutely clear that the threat actor/alleged threat actor never thought they had an actual agent and was never attempting/plotting to acquire one, the event is purely a hoax and will not be included. Likewise, if a threat was made regarding the use of an agent related to a specific date that has since passed without incident and there is no evidence of an ongoing plot to carry out the threat, the event is not a real threat and will not be included.

3. **Corporate Malfeasance**
   If the harm is a direct result of a commercial entity engaging in intentional substitution of ingredients, neglecting quality control, or otherwise generally failing to exercise due care and diligence, for reasons of cost-cutting or other profit-seeking motives, the event will not be included in the dataset.

4. **State Actors**
   Incidents that are unambiguously carried out by the forces of a recognized state, including acts of conventional warfare or covert action will not be included in the database.

E. Case Framing

When considering the inclusion criteria all variables are coded as if an attack took place/would have taken place.[5] Uncertainty based on event details portrayed by sources is captured in the Source Discrepancy and/or Source Doubt variables.

[5] For example, if the threat actor(s)/alleged threat actor(s) had only formulated a proto-plot when they were interdicted by the authorities, and the research team was able to ascertain from open source reporting that a government facility would have been the target of the eventual attack, then the research team would code the Target Type of this event as "government facility."

Uncertainty concerning the event as a whole is captured in Inherent Event Uncertainty and/or Inherent Attack Uncertainty variables. Event variables are coded based on positive and neutral sources only[6].

F. Discrepancy/Doubt Evaluation

Each of the variables in this section is coded for each of the incident variables in the dataset. In the database, these variables are named with "Dis" or "Do" in front of the event variable that they apply to. For example, the variable that records whether there is/are discrepancy/discrepancies in the event type is named "Dis_ETYPE" in the database. Likewise, the variable that records whether there is a doubt about the event type is named "Do_ETYPE." By providing a variable-by-variable measure that shows corroboration or discrepancy between sources, when analyzing a particular variable, users have the option to include only those cases upon which multiple sources concur.

1. Source Discrepancy

(Dis_x)
Categorical Variable

If two (or more) sources have a discrepancy in the information for a particular variable, that variable will be flagged. In order to select between which discrepancies to code, the most recent information will be used for reasonably credible sources that are over four years apart. A reasonably credible source is defined as a source where the competence level of the source author is assessed to be generally competent[7] or fully competent[8] AND that the source is assessed to be potentially objective[9] or highly objective[10]. Competent articles published after the period surrounding the immediate aftermath of an event (i.e., sources

[6] A source is considered "positive" if it portrays the case as a CBRN event. The source is "neutral" if it portrays the event as taking place but does not discriminate between the event being CBRN or non-CBRN; or if the source is contextual and does not directly discuss the event.

[7] General competency means that the author/institution publishing the source is regarded as competent (extrinsic evaluation) and the source document itself shows a prima facie level of competence (intrinsic evaluation). However, the author/institution does not cover the subject matter area on a regular basis.

[8] Full competency means that the author and institution publishing it have proven or researched competence in the geographical and substantive domain on which they are reporting. It is usually either a primary source or a secondary source with extensive details. If it is a new source/author, coder must consider the history and reputation of the author and institution.

[9] A source is assessed as potentially objective when the author and/or institution publishing it have demonstrated bias in some cases, but not others. For example, a newspaper that is generally measured in its approach to reporting but is known on occasion to take a very pro-Israeli (or pro-Palestinian) stance on the Israeli-Palestinian issue.

[10] A source is assessed as fully objective when neither the author nor the institution publishing it has a known or documented bias. To code 'HIGH' without prior knowledge of the author/publisher, coder must research the history and reputation of the author and institution. Furthermore, the document itself shows no overt or easily recognizable signs of bias.

with some temporal distance from the event) are more likely to have more robust data on such variables as the number of fatalities and the threat actor/alleged threat actor. If the sources come from the same time period, the information supported by the majority of reasonably credible sources will be used. If the discrepancy is between only two sources within the same time period, the information from the source with highest assessment for source competence and objectivity of all reasonably credible sources will be used.

If a variable is unknown and therefore coded "-99", Source Discrepancy = "0".

If a variable is not applicable and therefore coded as "-77" or N/A (dependent upon field type), Source Discrepancy = "-77".

Note: The act of coding discrepancy is based on positive and neutral independent sources. This means that a source must portray an event as taking place for its discrepancy on details to be taken into context. (Discrepancy on whether the event and/or attack took place is captured in the **<Event Uncertainty>** and/or **<Attack Uncertainty>** variables.)

NB: If the source discrepancy is solely based on sources from different time periods, source discrepancy should be coded as "0". For instance, if the sources from the week of the event all report 7 casualties and sources from a month later report 15 casualties, there is no source discrepancy in the final coding.

0 = No Source Discrepancy

1 = Source Discrepancy

2. Source Doubt

(Do_x)
Categorical Variable

For every variable in the database, if only one source provides the information for that particular variable, that variable entry will be coded as having doubt.

If there is more than one source and a variable is unknown and therefore coded "-99", Source Doubt = 0.

If a variable is not applicable and therefore coded as "-77" or N/A (dependent upon field type), Source Discrepancy = -77.

Note: If several 'inherited[11]' sources provide information for a variable, but only one 'independent' source provides that information, source doubt still exists.

[11] "Inherited" source means the source is republishing information that has already been published in another source at an earlier date/time. For example, if media outlet A publishes a story about a CBRN event and media outlet B repackages and publishes the same event, then media outlet B's story is an "inherited" source.

Source doubt is coded on positive and neutral independent sources.

0 = No Source Doubt
More than one source provides the information for the variable in question.

1 = Source Doubt
Only one source provides the information for the variable in question.

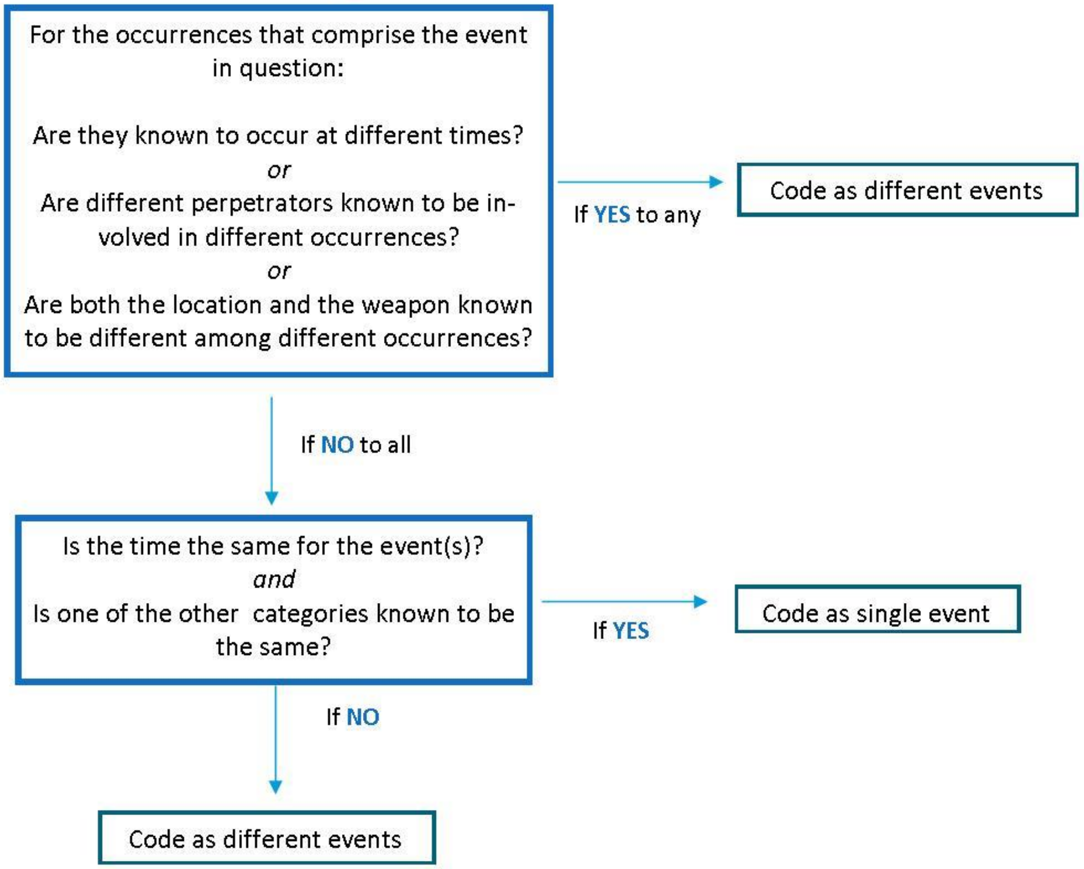
G. Missing Data

Throughout the database the code "-66" indicates that the field has not yet been coded for a particular variable but may be coded in future iterations of the database if information becomes available.

H. Single Event Determination

Consider these four notional variables: **[time]**, **[actor]**, **[location]** ***and*** **[weapon]**. If the time plus one of the other variables are known to be the same for multiple occurrences within an event, then code the event as a single event. Otherwise, code as different events. See the decision path on page 8 for detailed information.

Single Event Decision Path



For the occurrences that comprise the event in question:

Are they known to occur at different times?
or
Are different perpetrators known to be involved in different occurrences?
or
Are both the location and the weapon known to be different among different occurrences?

If **YES** to any → Code as different events

If **NO** to all ↓

Is the time the same for the event(s)?
and
Is one of the other categories known to be the same?

If **YES** → Code as single event

If **NO** ↓

Code as different events

The definitions below provide the parameters for each case variable being determined to be the same within an event.

Time: Actions taking place within the same calendar day or within twelve hours are regarded as occuring at the same time. All based on the standard time at the location.

Perpetrator: Individuals working together, part of the same organization, or collaborating organizations are regarded as the same perpetrator.

Weapon: Any combined agents and delivery mechanisms that are the same are regarded as the same weapon.

Location: Actions occurring in the same city are regarded as occurring at the same location.

II. Database Variables

A. Case Identifiers

1. CRIM ID

(CRIM_ID)
Numeric Variable

The CRIM ID is the primary event identifier. Events from the Criminal CBRN database have a "C" plus twelve-digit ID number.

- First: Always a C.
- Then: The eight-digit date formatted as "yyyymmdd". The date used here should be the most specific date from among the Attack, Discovery, and Plot dates. If more than one date has the same level of specificity, use the dates in their preferred order: Attack date > Discovery date > Plot date.
- Then: Two zeroes formatted as "00".
- Finally: The two-digit incident number for the given day which will be "01" unless there is more than one incident occurring on the same date.

For instance, an event in the Criminal CBRN database occurring on 25 July 1993 would be numbered as "C199307250001". An additional event recorded for the same day would be "C199307250002". The next event recorded for that day would be "C199307250003", etc. Events with no Attack, Discovery, or Plot date will be coded as C000000000001, followed by C000000000002, etc. For cases where only the year is known, the CRIM ID would be "C199300000001." If only the month and year is known, then the CRIM ID would be "C199307000001." If new sources provide better date information, the CRIM ID should be altered to reflect this new information.

2. CRIM ID Source

(CRIM_ID_SRC)
Categorical Variable

Indicates which date the **<CRIM ID>** references.

1 = Attack

2 = Discovery

3 = Plot

3. Target ID

*(TARGET*_ID)*
Numeric Variable

A unique identifier for each discrete target. This variable is simply a sequential number for each target included for each event generated for record keeping purposes. It is possible that an event recorded in the database may involve multiple targets. The Criminal CBRN Database will record up to five (5) actual or potential targets per event. The **<Target ID>** is recorded in the applicable fields.

For events with multiple targets, each Target Location will be assigned a unique **<Target ID>** number. The Target ID field is replicated and distinguished by the addition of a number inserted into the field variable name (e.g., TARGET1_ID / TARGET2_ID / etc.) represented in the codebook as TARGET*_ID where "*" will be replaced by a number ranging from 1-5.

4. ADP Date

(ADPDATE)
Numeric Variable

This variable records the year of the attack/discovery/plot, in that order of precedence if specific year is available for each and they are different.

5. ADP Country

(ADPCOUNTRY)
Categorical Variable

This variable records the country in which the threat actor/alleged threat actor associated with the recorded event mounted an attack, or was plotting to mount an attack where this is known. Values will reflect **<T1-TCOUNTRY>**. For events where there is no assigned value for **<T1-TCOUNTRY>** the **<DCOUNTRY>** value will be used.

B. Event Date

There are three categories of date recorded within the database. All three are recorded in the same way as outlined in section II.B.4 below.

Note that there is no field for Target Date. This information is captured by **<Attack Date>**.

1. Attack Date

<Attack Date> is defined as the date that an attack took place or would have taken place based on sources. If the event involves a plot with a known planned day of attack that was not carried out, the date of the planned attack should still be coded. If no attack date (or planned attack date) is known, this variable is left blank. If no planned **<Attack Date>** is known from available sources for an event that did not progress to the point of **<Attempted Use of Agent>** or **<Use of Agent**> **<Attack Date>** should be coded as "-77".

Dates change at local midnight in accord with standard Western usage.

2. Discovery Date

<Discovery Date> is defined as the date when authorities initially learned of the CBRN plot based on **publicly reported source materials**. It is acknowledged that there is potential for introduced inaccuracy in this field due to intentional misrepresentation of plot discovery dates by authorities in order to protect methods and/or sources.

Every event will have a **<Discovery Date>**, as by definition our knowledge of the event necessitates discovery.

For instance, if authorities start following a group in February but do not discover the CBRN plot until overhearing a conversation in April, the **<Discovery Date>** would be in April.

For events that are coded as plots or proto-plots the discovery date is not necessarily the interdiction date. For instance, if police started surveillance because they had identified a CBRN plot, that then led to subsequent arrests, the arrest date(s) will **not** be the **<Discovery Date>.** because the CBRN plot had been previously detected.

However, if the authorities started surveilling the threat actor(s)/alleged threat actor(s) because they had become aware of activities of interest to law enforcement or intelligence agencies, and subsequently arrested or otherwise intervened against the threat actor(s)/alleged threat actor(s), and only then discovered that the threat actor(s)/alleged threat actor(s) were planning a CBRN attack, then the arrest date would be the **<Discovery Date>.**

Additionally, it is also possible that the CBRN element of a threat actor(s)/alleged threat actor(s) activities may only be discovered subsequent to arrest in the course of interrogation days or weeks later. In this case **<Discovery Date>** is potentially after authorities intervened to disrupt the activity.

Additionally, if a previously unknown threat actor/alleged threat actor is arrested while crossing a border with a CBRN agent, then the arrest date would be the **<Discovery Date>.**

For events coded as an attack the **<Discovery Date>** will most commonly be the same as the Attack Date. However, exceptions may exist when:

- The CBRN plot was discovered prior to the attack occurring, but authorities were nevertheless ineffective in preventing it.
- The attack utilized high-latency agents such as certain biological agents (e.g., if the attack is carried out using a biological agent that has an incubation period of one month, and a large number of people get sick on a X date, then the **<Attack Date>** would be recorded as one month earlier than the **Discovery Date>**).

3. Plot Date

<Plot Date> is defined as when the threat actor(s)/alleged threat actor(s) initially started planning the specific event. Often, only a year can be deciphered for this variable.

4. Date formatting and coding

If a field is not coded with specific date information, whether due to it being non-applicable, or simply unknown, the field (for example, **<ADATE>**) should be coded as Not Applicable "-77" or Unknown "-99" as appropriate. In such instances Doubt and Discrepancy for the particular variable should be coded as Not Applicable "-77".

a) Date

(ADATE; DDATE; PDATE)
Date Variable

This field records the full date the attack/discovery/plot occurred. The date is recorded as an eight-digit number formatted as YYYYMMDD. Leave all the date fields blank as appropriate based upon the discussion in Section II.B.1-3 above, or if no date information is known.

If a portion of the date is known, use zeros as place fillers for the unknown portions. For instance, if an event took place on an unknown day during August 1998, the attack date would be listed as 19980800.

b) **Year**
(AYEAR; DYEAR; PYEAR)
Numeric Variable

This field contains the year in which the attack/discovery/plot occurred. In the case of event(s) occurring over an extended period, the field will record the year when the event was initiated. If the date is completely unknown, this variable will be recorded as "0". However, if another portion of the date is known, while the year is unknown, this will be recorded as "0".

c) **Month**
(AMONTH; DMONTH; PMONTH)
Numeric Variable

This field contains the number of the month in which the attack/discovery/plot occurred. In the case of event(s) occurring over an extended period, the field will record the month when the event was initiated. If the date is completely unknown, this variable will be recorded as "0". However, if another portion of the date is known, while the month is unknown, this will be recorded as "0".

d) **Day**
(ADAY; DDAY; PDAY)
Numeric Variable

This field contains the numeric day of the month on which the attack/discovery/plot occurred. In the case of event(s) occurring over an extended period, the field will record the day when the event was initiated. If the date is completely unknown, this variable will be recorded as "0". However, if another portion of the date is known, while the month is unknown, this will be recorded as "0".

e) **Approximate Date**
(APPROX_ADATE; APPROX_DDATE; APPROX_PDATE)
Text Variable

Whenever the exact date of the event is not known or remains unclear, this field is used to record the approximate date of the event. All words in phrases should be capitalized. For instance, "Early January" or "Late 1998".

- If an event occurred in June 1993 and the *day* of the event is not known, then the value for **<Day>** will be “0” and the value for **<Approximate Date>** will be “June 1993”.

- If an event occurred in the first half of 1993 and the month and day are not known, then the values for **<Day>** and **<Month>** will both be “0” and the value for **<Approximate Date>** will be “First Half of 1993”.

This field should also be used to note additional specific date information such as the time of day the event occurred. All words in phrases should be capitalized. For instance, “Around Dawn” or “After Dinner”. Exact times should be in local time according to the location of the attack/discovery/plot and formatted in a numeric 12-hour two-cycle day with the abbreviations AM/PM capitalized. For instance, “12:15 PM” or “9:21 AM”.

C. Event Location

1. Discovery Location

<Discovery Location> is the location where authorities initially learned about the CBRN plot. For instance, if a threat actor/alleged threat actor is in South Africa, but intelligence authorities in London intercept emails and discover a CBRN plot, the **<Discovery Location>** would be London.

Every event will have a **<Discovery Location>**, as our knowledge of the event necessitates discovery. If an attack occurs (**<Attempted Use of Agent>** or **<Use of Agent**>- see II.D.2. below), the **<Discovery Location>** variables will be coded as per II.B.2 above.

2. Plot Location

<Plot Location> is defined as the location where the threat actor(s)/alleged threat actor(s) initially started planning the specific event. By definition, every case has a **<Plot Location>**, even if it is unknown. Often, only a country can be deciphered for this variable.

3. Target Location

<Target Location> is defined as the specific location where the threat actor(s)/alleged threat actor(s) mounted or intended to mount an attack.

Some events will have multiple targets, each of which are coded separately in the appropriate Target fields (see section II.J). If there are multiple target locations, each should be coded as a unique entry, regardless of whether the **<Entity Name>** or **<Specific Target>** is the same. For instance, attacks on villagers in three separate villages would be coded as three unique targets. Each **<Target Location>** will be assigned a unique **<Target ID>** number as described in Section II.A.3.

4. Location formatting and coding

This section describes the procedures for coding location. The values and procedures outlined below apply equally to **<Plot Location>**, **<Discovery Location>**, and **<Target Location>**.

a) Country

(DCOUNTRY; PCOUNTRY; TCOUNTRY)
Categorical Variable

This field identifies the *sovereign country* where the event occurred. When an event occurred in international waters or airspace, the country of departure is listed as the country of the event. If the departure point is not identified, the event is coded as “901”[12] which indicates “International”. If an event took place at a military base or embassy on foreign soil, it is coded as occurring in the country containing the embassy or military base.

In cases where the country in which an event occurred cannot be identified, it is coded as “905”, which indicates “Unknown”. By definition, most cases have at least a potential **<Target Country>**, even if no information is known about it. However, in cases where **<Intent to Use>** has been coded as “0” which indicates “No” and **<Entity Name>** has been coded as “None”, TARGET variables will be coded as N/A or “-77” for this event. In the case where the **<Attack Date>** is the same as the **<Discovery Date>** the **<Discovery Country>** will be coded identically to the **<Target Country>**.

By definition, every case has a <**Plot Country>**, even when it is unknown, and therefore it cannot be coded as “-77”.

(1) ISO-3166 Country Codes

This field identifies the *sovereign country* where the event occurred using the ISO-3166-1 numeric system. (Three-digit numeric codes).

(a) Dissolutions and Unifications

Because the political circumstances of many countries have changed over time, in a number of cases countries that represented the location of criminal events no longer exist. Examples include West Germany, the USSR, and Yugoslavia. In these cases, the country name for the year the event occurred is recorded. As an example, a June 1990 attack in Bonn would be recorded as taking place in West Germany (FRG). An otherwise identical attack in 1991 would be recorded as taking place in Germany.

The following change dates apply:

GENERAL:

- Eritrea – Independence: 24 May 1993;
- Germany – Unification: 3 October 1990;
- Timor-Leste – Independence: 20 May 2002;
- South Sudan – Independence: 9 July 2011.

BREAKUP OF CZECHOSLOVAKIA:

- Czech Republic – Independence: 1 January 1993;
- Slovakia – Independence: 1 January 1993.

[12] The ISO 3166-1 standard reserves the sequence 900-999 as user-assigned codes. These may be assigned as needed by an end user. Glossary for ISO 3166, https://www.iso.org/glossary-for-iso-3166.html

BREAKUP OF UNION OF SOVIET SOCIALIST REPUBLICS (USSR):

- Russian Federation – Independence: 24 August 1991;
- Armenia – Independence: 21 September 1991;
- Azerbaijan – Independence: 30 August 1991;
- Belarus – Independence: 25 August 1991;
- Estonia – Independence: 17 September 1991;
- Georgia – Independence: 9 April 1991;
- Kazakhstan – Independence: 16 December 1991;
- Kyrgyzstan – Independence: 31 August 1991;
- Latvia – Independence: 21 August 1991;
- Lithuania – Independence: 17 September 1991;
- Moldova – Independence: 27 August 1991;
- Tajikistan – Independence: 9 September 1991;
- Turkmenistan – Independence: 27 October 1991;
- Ukraine – Independence: 24 August 1991;
- Uzbekistan – Independence: 1 September 1991;
- USSR – Terminates: 26 December 1991 – 5 January 1992.

BREAKUP OF YUGOSLAVIA:

- Bosnia and Herzegovina – Independence: 11 April 1992;
- Croatia – Independence: 25 June 1991;
- Kosovo – Independence: 17 February 2008;
- Macedonia – Independence: 8 September 1991;
- Montenegro – Independence: 3 June 2006;
- Serbia – Independence: 3 June 2006;
- Slovenia – Independence: 1 January 1992;
- Yugoslavia (FRY) – Independence: 27 April 1992;
- Yugoslavia (FRY) – Becomes Serbia-Montenegro: 4 February 2003.

b) Separate Entity/Territory

(ASEP_ENTITY; DSEP_ENTITY; PSEP_ENTITY; TSEP_ENTITY)
Text Variable

This field identifies territories claimed by other states, non-self-governing territories, or other disputed/special territories. Code the de-jure state as the primary entity under Country and code the separate entity in this field. In the case where the separate entity in which an event occurred cannot be identified, either because the country where an event occurred cannot be identified or because it is unknown whether an event in a given country occurred within a separate entity, it is coded as "-99" which indicates "Unknown". If no separate entity applies to this record the variable should be coded as “-77” which indicates “Not Applicable”.

c) **Province/State**
(DPROV_STATE; PPROV_STATE; TPROV_STATE)
Text Variable

This field identifies the primary administrative subunit of the country where the event occurred. The name should be listed without a modifier such as “Province”, unless the modifier is unique to that specific subunit, such as the “’District of’ Columbia”. For instance, “Al-Anbar Governorate” would be listed simply as “Al-Anbar”. Spelling should conform to ISO 3166-1 (*Codes for the representation of names of countries and their subdivisions – Part 2: Country codes)* https://www.iso.org/obp/ui/#search. If there are multiple provinces, they should be listed alphabetically separated by a semi-colon for Discovery Province and Plot Province. Because there is a unique entry for each target, there will not be multiple Target Provinces in a single entry. In the case where the province in which an event occurred cannot be identified, it is coded as “Unknown”. If Country is coded as “-77” which indicates “Not Applicable” or “901” which indicates “International”, province will be coded as “Not Applicable”.

d) **City**
(DCITY; PCITY; TCITY)
Text Variable

This field contains the name of the city in which the event occurred. Spelling should conform to the principal usage in ISO 3166-2 (*Codes for the representation of names of countries and their subdivisions – Part 2: Country codes*) https://www.iso.org/obp/ui/#search. If there are multiple cities, they should be listed alphabetically separated by a semi-colon for **<Discovery City>** and **<Plot City>**. Because there is a unique entry for each Target Location (see section II.J), there will not be multiple Target Cities in a single entry. In the case where the city in which an event occurred cannot be identified, it is coded as “Unknown”. If Country is coded as “-77” which indicates “Not Applicable” or “901” which indicates “International”, City will be coded as “Not Applicable”.

e) **City Latitude and Longitude**
(DCITY_LATITUDE; DCITY_LONGITUDE; PCITY_LATITUDE; PCITY_LONGITUDE; TCITY_LATITUDE; TCITY_LONGITUDE)
Numeric Variable

These fields contain the latitude and longitude of cities listed in the City variable. This variable is calculated using https://www.latlong.net/. Enter the city in the search box and the application provides the latitude and longitude for the center of the city. The coordinates should be recorded as decimal degrees with five decimal places. For Discovery City Latitude and Longitude, Plot City Latitude and Longitude and Target City Latitude and Longitude, these fields allow for the coordinates of up to three city locations to be included (*DCITY_LATITUDE1; DCITY_LONGITUDE1; DCITY_LATITUDE2; DCITY_LONGITUDE2; DCITY_LATITUDE3; DCITY_LONGITUDE3; PCITY_LATITUDE1; PCITY_LONGITUDE1; PCITY_LATITUDE2; PCITY_LONGITUDE2; PCITY_LATITUDE3; PCITY_LONGITUDE3; TCITY_LATITUDE1; TCITY_LONGITUDE1*). If multiple city locations are provided, list the coordinates in the order the cities are listed in the City variable. Because there is a unique entry for each target, there will not be multiple Target Cities in a single entry. If no city is listed or the coordinates cannot be identified, this variable will be blank.

f) **Vicinity**
(DVICINITY; PVICINITY; TVICINITY)
Categorical Variable

1 = “Yes”
The event occurred outside of the formal boundaries of the city or town but in a nearby area closer to the city than any other notable town or city.

0 = “No”
The event occurred in the city itself.

-99 = “Unknown”
Although the city is known, it is not known whether the event occurred in the vicinity of the city in question or in the city itself.

-77 = “Not Applicable”
If City is coded as “Unknown” or “Not Applicable”, Vicinity will be coded as “Not Applicable”.

g) **Location Description**
(DLOCATION; PLOCATION; TLOCATION)
Text Variable

This field specifies any additional information about the location of the event not captured by the other location variables. This might take the form of general location details which fall outside the definition of the other location variables. For instance, an event where sources do not give a specific city location in New York state, but they do specify a campground in Saratoga

County. Ideally, the information in this field will add greater specificity to the other location variables by identifying neighborhoods, official building names, or other specific location information. For instance, the event took place at "the New York Stock Exchange" or at "Fatima Zohra High School" or "5 miles northeast of Bangkok" or "Near the mango tree in the center of town".

If there are multiple specific locations, they should be listed alphabetically separated by a semi-colon for Discovery Location Description and Plot Location Description.[13] If there are multiple specific locations in multiple locations identified in the Province/State or City variables, they would be listed with the modifier "in X Province" or "in X City". For instance, "Water Treatment Plants in New York; Water Treatment Plants in New Jersey" or "Grocery Stores in Edmonton; Grocery Stores in Vancouver". Because there is a unique entry for each target, there will not be multiple Target Location Descriptions in a single entry. If Country is coded as "-77", which indicates "Not Applicable", Location Description will be coded as "Not Applicable". If Country is not coded as "-77" and there is no additional location information, Location Description should be coded as "Unknown".

If possible, additional research should be done to provide the maximum level of location detail, such as official names, addresses, etc. For instance, if sources note that the office of the Prime Minister of Pakistan was the location of the attack, the official building name and address should be identified for the date the event occurred. Multiple pieces of location information should be listed from most specific to least specific separated by commas. For instance, "Office of the Prime Minister, Prime Minister's Secretariat, 44000 block of Constitution Avenue" or "Sai Yeung Choi Street South in front of Ginza Plaza, Mong Kok District" or "Pui Ching Middle School, 20 Pui Ching Road". The first word of long descriptive phrases should be capitalized and they should end without a period. For instance, "Campgrounds in Saratoga County" or "Salad bars and buffets in hotels and restaurants" or "25 miles south of Alice Springs" or "Metal bench at the northeast corner of North Washington Street and West Main Avenue". All words in short phrases which name a specific thing or place should be capitalized. For instance, "Aum Shinrikyo Hideout" or "Border Crossing Station" or "Military Checkpoint" or "Water Treatment Plant". Abbreviations should not be used.

[13] As previously noted above (c.f.: Section II.C.4 & II.A.4) Target Locations are individually coded rather than aggregated as described here for Plot Location and Discovery Location. Therefore, no Target Location will require the use of semi-colons.

NOTE: UNDER NO CIRCUMSTANCES WHATSOEVER should this field include or record any information that can be deemed as identifying information as defined by NISTIR 8053; "identifying information" denotes information that identifies individuals. (NIST Internal Report 8053, Page 3)

h) Location Description Latitude and Longitude

(DLOCATION_LATITUDE; DLOCATION_LONGITUDE; PLOCATION_LATITUDE; PLOCATION_LONGITUDE; TLOCATION_LATITUDE; TLOCATION_LONGITUDE)
Numeric Variable

These fields contain the latitude and longitude of locations listed in the Location Description variable. This variable is calculated using Google Maps or some comparable geospatial software and should reflect the approximate latitude and longitude of the specific location center. The coordinates should be recorded as decimal degrees with five decimal places. For Discovery Location Description Latitude and Longitude, Plot Location Description Latitude and Longitude, these fields allow for the coordinates of up to three city locations to be included (*DLOCATION_LATITUDE1; DLOCATION_LONGITUDE1; DLOCATION_LATITUDE2; DLOCATION_LONGITUDE2; DLOCATION_LATITUDE3; DLOCATION_LONGITUDE3; PLOCATION_LATITUDE1; PLOCATION_LONGITUDE1; PLOCATION_LATITUDE2; PLOCATION_LONGITUDE2; PLOCATION_LATITUDE3; PLOCATION_LONGITUDE3*).

If multiple specific locations are provided, list the coordinates in the order the specific locations are listed in the Location Description variable.

NOTE: Because there is a unique entry for each target, there will not be multiple Target Location Descriptions in a single entry (see section II.J).

NOTE: If no specific location is listed or the coordinates cannot be identified, this variable will be left blank.

NOTE: UNDER NO CIRCUMSTANCES WHATSOEVER should this field include or record any information that can be deemed as identifying information as defined by NISTIR 8053; "identifying information" denotes information that identifies individuals. (NIST Internal Report 8053, Page 3)

D. Event Characteristics

1. Event Type

(EVENT_TYPE)
Categorical Variable

This set of variables code for the **highest event level** applicable to any agent/weapon involved in the specific event.

All variables in this section are coded with "1" for yes and "0" for no depending on whether the condition applies.

a) Protoplot

(EV_TY_PROTOPLOT)

Sources do not present any evidence of an actual plot but rather mention events that may lay the groundwork for an actual plot. For instance, the discovery of a chemical weapons manual or knowledge of a criminal group hiring a scientist with a weapons' specialty would be coded as a protoplot.

b) Plot

(EV_TY_PLOT)

There is evidence that the threat actor(s)/alleged threat actor(s) seriously considered acquiring and using CBRN materials as a weapon, but when those involved in the plot have not (yet) made an attempt to acquire the agent and do not have the agent in their possession.

Note: If a case is coded as a plot, most variables should be coded as if the event took place as intended. For instance, code the intended targets and event date if precise information is provided on intended target(s) and/or intended attack date. However, the number of casualties/injuries and progression should be coded based on what actually took place.

c) Attempted Acquisition

(EV_TY_ATT_ACQ)

There is evidence that the threat actor(s)/alleged threat actor(s) attempted to acquire CBRN agents/materials for use as a weapon but is not reported to have succeeded. "Attempted acquisition" includes the attempted (but unsuccessful or abandoned) acquisition of either raw materials or an intact CBRN weapon. If a threat actor/alleged threat actor possesses radiological materials but threatens to create and use a nuclear weapon, it should be coded as an "attempted acquisition." If a threat actor/alleged threat actor has the components (e.g., chemical reactants) needed for an agent, but has not made or historically used that agent, the event is coded as attempted acquisition. If the sole threat actor/alleged threat actor involved in an event is the intended recipient of an agent/weapon that was intercepted *en route*, the case may need to be coded as "attempted acquisition" and framed with the intended recipient threat actor/alleged threat actor as the threat actor/alleged threat actor.

d) **Possession of a Non-Weaponized Agent**
(EV_TY_POSS_NONWEAP)

There is evidence the threat actor(s)/alleged threat actor(s) succeeded in acquiring and possessing a CBRN agent, but this agent does not constitute a weapon (in most cases, it will *not* be in a deliverable form, i.e., will lack an effective delivery mechanism for the intended attack). In cases where a threat actor/alleged threat actor has the components required to produce an agent *that the threat actor/alleged threat actor has historically made or used*, in many contexts it can be regarded as possession of a non-weaponized agent (as opposed to attempted acquisition) if no delivery mechanism is apparent.

e) **Possession of a Weapon**
(EV_TY_POSS_WEAP)

There is evidence the threat actor(s)/alleged threat actor(s) possessed both the agent and a delivery mechanism in a form that either constitutes a viable weapon or can easily be assembled into such a weapon at the time of reporting. The completed weapon may be quite crude, such as radioactive material the threat actor/alleged threat actor plans to leave in a building, as long as there is evidence the threat actor/alleged threat actor intends to use the weapon in this crude form.

In cases where a threat actor/alleged threat actor intends to release an agent from an existing facility/storage/transport, there must be evidence the threat actor/alleged threat actor possesses the knowledge and materials to capably attempt the attack. For example, if an actor with plans to attack a chemical plant possesses conventional explosives, the case would only be coded as a "possession of a weapon" if there is evidence, such as building plans or a security guard schedule, that shows the attack is feasible for the threat actor/alleged threat actor to attempt.

f) **Threat with Possession**
(EV_TY_THREAT)

There is evidence that the threat actor(s)/alleged threat actor(s) both threatened to use a CBRN substance and actually had the weapon in their possession at the time of the threat. See **<Possession of a Weapon>** above for discussion of what does, and does not, constitute "possession."

In cases where an agent is distributed in such a way that it was clearly not meant to cause harm (e.g., a sealed vial of a chemical agent in the mail is sent to lend credibility to a threat actor's/alleged threat actor's threat), they are coded as "threat with possession." Even in the absence of an explicit threat, the distribution to a particular target of an agent in such a way that harm is clearly not intended can constitute an implied threat and be coded as **<Threat with Possession>**. In cases of threat with possession involving water supply as the delivery mechanism, the decision between coding as plot, possession of a non-weaponized agent, or threat with possession is based on the level of event development and should be discussed with a supervisor.

g) **Attempted Use of Agent**
(EV_TY_ATT_USE)

There is evidence the threat actor(s)/alleged threat actor(s) attempted to employ or disseminate a CBRN agent/material with the intent to cause harm but **no agent/material was released**.

h) **Use of Agent**
(EV_TY_USE)

There is evidence the threat actor(s)/alleged threat actor(s) employed or disseminated a CBRN substance in the commission of an attack. If a small amount of agent/material was used, **even if no harm was caused**, it should be coded as **<Use of Agent>** unless there is proof the event was not meant to cause harm (See **<Threat with Possession>** above). If a CBRN agent/material or weapon was employed to test its effectiveness as part of a larger plot and there is no evidence that the target was selected to attain an ideological, political, economic, religious, or social goal or to coerce, intimidate, or convey some other message to a larger audience than the immediate victims, then do not code as **<Use of Agent>**.

2. Evidence of Intent to Use (No Attempted Use)
(INTENT)
Categorical Variable

This field only applies to cases where **<Event Type>** is coded as **<Attempted Acquisition>**, **<Possession of a Non-Weaponized Agent>**, or **<Possession of a Weapon>**. Cases with all other Event Types should be coded as "Not Applicable".

Attempted acquisition, or even possession of an agent by a threat actor/alleged threat actor does not automatically indicate the existence of intent to use. The phenomenon of individuals obtaining illegal items out of pure curiosity is well-known.

1 = "Yes"
Sources show some explicit evidence that the threat actor/alleged threat actor was actively planning to use the weapon and/or agent in question in a CBRN attack or CBRN threat at some point in the future. This includes cases where no specific plot has been articulated. In some cases, the nature and/or motivation of the threat actor/alleged threat actor may be sufficient evidence of intent to use the weapon and/or agent.

0 = "No"
There is no evidence of any extant or potential plot or threat related to the weapon and/or agent in question. For instance, finding only cyanide capsules on the person of a threat actor/alleged threat actor that typically carries cyanide capsules to induce suicide upon capture would be considered as having no intent to use since the general intent for such capsules is for intragroup suicide. Other common instances include: 1) smuggling cases with no known potential end user and no evidence of any extant or potential plot or threat related to the weapon and/or agent in question; or 2) the discovery of CBRN materials (i.e., a chemical weapons manual), agents, and/or weapons with no evidence of any extant or potential plot or threat; or 3) the threat actor/alleged threat actor may have acquired the agent some years earlier with intent to use it but then abandoned the effort in which case the agent is a legacy of an abandoned plot; or 4) the agent or material were produced purely for sale to others.

-99 = “Unknown”

-77 = “Not Applicable”

3. **Heightened Interest**
(HEIGHT_INTEREST)
Categorical Variable

1 = "Yes"
The event is of **<heightened interest>**. **<Heightened interest>** is defined as an event that fulfills at least one of the following three criteria:

i. The event resulted in at least five total casualties (injuries and/or fatalities).
ii. The event involved a CBRN agent that is classed as a warfare agent.
   - For a chemical agent this includes: mustard, lewisite, nerve agents (cyclosarin, sarin, soman, tabun, VX, VR, and Novichok agents), arsine,

BZ, chlorine, cyanogen chloride, phosgene, diphogene, phosgene oxime, phenyldichorarsine, adamsite, and hydrogen cyanide.

- A biological agent must be a traditional warfare agent and in a weaponizable form. Examples include the agents that cause anthrax, smallpox, plague, tularemia, glanders, Q-fever, brucellosis, viral hemorrhagic fevers, VEE, botulism, foot and mouth disease, and aflatoxin.
- Nuclear agents (i.e., fissile materials or weapons containing these) are always of heightened interest (if **<Event Type>** is coded as **<Attempted Acquisition>** or higher).

iii. The event involved either the use of or a plot to create a weaponization of the agent in at least a moderately sophisticated manner as discussed in **<Sophistication Level of Attack>** (see Section II.D.14 below).

0 = "No"
The event does not meet the **<Heightened Interest>** criteria.

-99 = "Unknown"
The sources do not provide enough evidence to determine whether the case would be of **<Heightened Interest>**.

4. Compound Event

(COMPOUND)
Categorical Variable

In cases coded as a single event that consists of multiple components (see Single Event Determination section above for more information), then "Yes" is selected to denote that the particular attack was part of a "compound" event. For example, a single threat actor/alleged threat actor mailing 20 letters with anthrax on the same day would be a "compound event."

Only events classified with **<Event Type>** as "Use of Agent," "Attempted Use of Agent," and "Threat with Possession" can be coded as a compound event. All other event types should be coded as "No."

1 = "Yes"
The attack is a compound event.

0 = "No"
The attack is not a compound event.

-99 = "Unknown"
Based on the source information, a case cannot be coded as either a "1" or a "0."

5. **Compound Event Occurrences**
(NCOMPOUND)
Numeric Variable

Provide the number of occurrences in a compound event.

-77 = "Not Applicable"
Applies to all events coded with a **<Compound Event>** of "0".

6. **No Progression**
(*NO_PRO_**)
Categorical Variable; Textual Variable

Note: This set of variables codes for known information about why a plot did not progress to the level of Use of Agent.

***All variables in this section are coded with "1" for yes and "0" for no depending on whether the condition applies*.**

a) **Not Applicable**
(NO_PRO_NOT_APPLICABLE)

Applies to all events coded as Attempted Use of Agent or Use of Agent for **<EVENT_TYPE>**. (Coding of "1" for **<EV_TY_ATT_USE>** or **<EV_TY_USE>**).

b) **Interdiction**
(NO_PRO_INTERDICT)

Law enforcement / intelligence discovered the plot, resulting in the progress of the event being halted as a result of action by law enforcement / intelligence agencies. Includes apprehension.

If this variable is positively coded ensure that appropriate coding is provided in the derivative INTERDICTION fields.

c) **Abandonment of Plot**
(NO_PRO_ABANDONED)

Based on available source information the threat actor/alleged threat actorabandoned the CBRN plot prior to reaching the point of Use of An Agent in favor of pursuing conventional weapons or for other reasons.

If this variable is positively coded ensure that appropriate coding is provided in **<ABANDON_FTAVW>** and **<ABANDON_CONV>**.

d) **Unknown**
(NO_PRO_UNKNOWN)

Available evidence indicates that the plot definitely did not progress to the level of Use of Agent but does not provide sufficient data to determine the reasons.

7. Manner of Interdiction

Note: This set of variables provides additional detail for those events in which **<No Progression>** is coded positively for <NO_PRO_INTERDICT>. Use highest level of coding that applies. This may not be the initial interdiction method. It is acknowledged that there may be some ambiguity in selection of the appropriate value.

***All variables in this section are coded with "1" for yes and "0" for no depending on whether the condition applies*. If "a <INTERDICT_NO_APPLI> is positively coded then "b" through "i" should be coded as "-77."**

a) **Not Applicable**
(INTERDICT_NO_APPLI)

The event was coded as any value other than "Interdiction" in the **<No Progression>** set of variables.

b) **Unknown**
(INTERDICT_UNK)

The means by which the plot was discovered and interdicted are unknown but the event was unambiguously the subject of interdiction**.**

c) **Informant**
(INTERDICT_INFORM)

The plot/acquisition was revealed to law enforcement, military, or intelligence agencies through the action of an informant external to the cell engaged in the actual plot. Typical informants may be neighbors, spouses, coworkers, rival threat actors.

This entry is distinct from an undercover investigation, with special attention given to considerations such as the role of a cell member. Informants alert authorities to the plotting but do not participate in the gathering of evidence or in efforts to draw the threat actor into more advanced criminal activity.

d) **Chance Discovery**
(INTERDICT_CHANCE)

Law enforcement, military, or intelligence discovered the plot without the use of a routine search, investigation, or sting operation. Can include discovery through the investigation of a similar plot/acquisition. For example, an individual is arrested for robbery and offers details about a CBRN attack plot in exchange for a lesser sentence. Or, a car is pulled over for speeding and a CBRN agent is found.

e) **Routine Search**
(INTERDICT_ROUTINE)

The plot/acquisition was noticed during a routine search not focused on the specific event. Includes checkpoints. For the purposes of coding, an example of the difference between chance discovery and routine search can be demonstrated with the distinction between random and systematic stopping of vehicles. Where an enforcement official has discretion in the choice of whether or not to pick out and stop individual vehicles subsequent discovery and interdiction is "chance." In instances where all vehicles are being stopped at a permanent or temporary checkpoint this would be a "routine search."

f) **Probable Cause Search**
(INTERDICT_PROB_CAUSE)

The plot/acquisition was discovered while investigators were conducting a formal search related to a specific event. For instance, if the home of a suspected criminal is searched and CBRN agents are found, it is a probable cause search.

g) **Surveillance Investigation**
(INTERDICT_SURVEIL)

Law enforcement or intelligence ran an investigation focused on the plot/investigation at hand. Includes surveillance but not undercover operations.

h) **Undercover Investigation**
(INTERDICT_UCOVER)

Involves an undercover law enforcement officer or turned group member gathering evidence of threat actor/alleged threat actor wrongdoing. Does not include a sting operation.

i) **Sting Operation**
(INTERDICT_STING)

An undercover agent offers some type of bait such as (fake) weapons or contacts. The threat actor/alleged threat actor must take the bait for the operation to be successful.

8. CBRN Specific

(*CBRN_SPECIFIC*)
Categorical Variable

Note: This field is only coded for those events in which **<No Progression>** is coded as "Interdiction". For all other events code as not applicable "-77"

1 = "Yes"
The manner of interdiction is CBRN specific.

0 = "No"
The manner of interdiction is not CBRN specific.

9. Abandoned Plot – Failure to Achieve Viable Weapon

(*ABANDON_FTAVW*)
Categorical Variable

This variable provides additional detail for those events in which **<No Progression>** is coded positively for **<Abandonment of Plot>.**

Note: This field is only coded for those events in which **<Abandonment of Plot>** is coded as "Yes". For all other events code as not applicable "-77"

Note: This field should not be positively coded for events in which **<Event Type>** is coded positively for **<Possession of a Weapon>** or higher.

1 = "Yes"
The threat actor abandoned their CBRN efforts recorded in this event because they were unable to acquire or prepare a viable weapon.

0 = "No"
The threat actor abandoned the recorded CBRN effort for reasons other than their Failure to Achieve Viable Weapon.

10. Abandoned Plot – Unknown Reason

(*ABANDON_UNK*)
Categorical Variable

This variable provides additional detail for those events in which **<No Progression>** is coded positively for **<Abandonment of Plot>.**

Note: This field is only coded for those events in which **<Abandonment of Plot>** is coded as "Yes". For all other events code as not applicable "-77"

1 = "Yes"
The threat actor is known to have abandoned their CBRN efforts recorded in this event but the reason is unknown.

0 = "No"
The reason that the threat actor abandoned the recorded CBRN effort is known.

11. **Abandoned Plot – Other CBRN**
(*ABANDON_OTHER*)
Categorical Variable

This variable provides additional detail for those events in which **<No Progression>** is coded positively for **<Abandonment of Plot>.**

Note: This field is only coded for those events in which **<Abandonment of Plot>** is coded as "Yes". For all other events code as not applicable "-77"

1 = "Yes"
The threat actor abandoned the specific CBRN plot recorded in this record in favor of a different CBRN effort.

0 = "No"
The threat actor did not pursue an alternative CBRN plot subsequent to their abandonment of the plot recorded in this record.

Note: When coding "Yes" for this variable it would be typical to expect an additional event to be recorded in the database that is linked to "this" record.

12. **Abandoned Plot – Subsequent Conventional**
(*ABANDON_CONV*)
Categorical Variable

This variable provides additional detail for those events in which **<No Progression>** is coded positively for **<Abandonment of Plot>.**

Note: This field is only coded for those events in which **<Abandonment of Plot>** is coded as "Yes". For all other events code as not applicable "-77"

1 = "Yes"
The threat actor abandoned their CBRN efforts recorded in this event in favor of a subsequent conventional attack using such weapons as explosives or firearms. There is no requirement that the conventional plot was successfully developed or executed.

0 = "No"
The threat actor did not pursue a conventional plot subsequent to their abandonment of their CBRN efforts.

13. **International Interdiction Collaboration**
(*INTLLAW_INVOLVE*)

Categorical Variable

Note: This field is only coded for those events in which **<No Progression>** is coded as "Interdiction". For all other events code as not applicable "-77"

1 = "Yes"
Sources state that international law enforcement aided in interdiction. May include information sharing or joint missions. May include another state's law enforcement/military/intelligence or an intergovernmental institution.

0 = "No"
Sources do not state any aid from international law enforcement.

14. Apprehended - None
(*APPREHENSION_NONE*)
Categorical Variable

1 = "Yes"
None of the individual threat actors directly associated with the event recorded in the database, where the primary threat actor was an autonomous cell or formal group, were apprehended.

Where the threat actor directly associated with the event recorded in the database was a single individual and that individual was not apprehended.

0 = "No"
Sources portray apprehension of at least one or more individual threat actors directly associated with the event recorded in the database, where the primary threat actor was an autonomous cell or formal group, were apprehended.

Where the threat actor directly associated with the event recorded in the database was a single individual and that individual was apprehended.

15. Apprehended – Some
(*APPREHENSION_SOME*)
Categorical Variable

1 = "Yes"
At least one, though not all, of the individual threat actors directly associated with the event recorded in the database, where the primary threat actor was an autonomous cell or formal group, were apprehended.

0 = "No"
Sources do not portray any apprehension of more than one but less than all individual threat actors directly associated with the event recorded in the

database.

List in case notes the number of apprehended threat actors. Threat actors killed in the course of an interdiction are not considered apprehended but their number should be noted in Case Notes. Apprehension does not have to be immediate but must be at least partially related to the specific event.

16. Apprehended – All

(*APPREHENSION_ALL*)
Categorical Variable

1 = "Yes"
All of the individual threat actors directly associated with the event recorded in the database, where the primary threat actor was an autonomous cell or formal group, were apprehended.

Where the threat actor directly associated with the event recorded in the database was a single individual and that individual was apprehended.

0 = "No"
Sources do not portray apprehension of all of the threat actors.

List in case notes the number of apprehended threat actors. Threat actors killed in the interdiction are not considered apprehended but their number should be recorded in Case Notes. Apprehension does not have to be immediate but must be at least partially related to the specific event.

Where the threat actor directly associated with the event recorded in the database was a single individual, that individual was not apprehended.

17. Sophistication Level of Attack

(*ATTACK_SOPHISTICATION*)
Categorical Variable

The sophistication level of the event is based on both the sophistication of the intended agent and delivery method. If the agent and delivery fall under different categories, code for the highest level.

All variables in this section are coded with "1" for yes and "0" for no depending on whether the condition applies.

***a)* Unknown Sophistication**
(ATT_SOPH_UNK)

The level of sophistication of the agent/delivery device/attack cannot be determined.

b) **Low Sophistication**
(ATT_SOPH_LOW)

No complex CBRN agent was produced or used. Also involves a relatively simple delivery method. For example, a plot or attack that involves leaving an unmodified radiological source in a location or contaminating drinking water with raw sewage.

c) **Medium Sophistication**
(ATT_SOPH_MED)

This includes the acquisition of a readymade CBR weapon where the use is fairly straightforward. Also includes large scale production of relatively simple CBR agents or standard explosives used in combination with simple technical CBR agents.

d) **High Sophistication**
(ATT_SOPH_HIGH)

The attack used a sophisticated agent and/or delivery method. The attack involves either specialists/access to specialized knowledge or acquired agents. The attack involves either delivery or production of a warfare agent. For example, high sophistication would include any nuclear attack, or complex explosives (involving any remotely controlled attack or attack involving simultaneous (non-suicide) explosions or timers) with a simple CBRN agent. Other aspects of the attack could indicate high sophistication, such as the state of the safety or containment systems that protect threat actors/alleged threat actors from an agent.

18. Facility/Storage/Transport of Existing Agent
(FACILITY_ATTACK)
Categorical Variable

1 = "Yes"
The threat actor/alleged threat actor attacked an entity[14] that contained CBRN agents/materials with plans to release that agent. For example, using conventional explosives to release chemicals in a transport truck or an attack on a nuclear reactor.

0 = "No"
The threat actor/alleged threat actor did not intentionally attempt to release an

[14] In this instance "entity" can include a factory or chemical plant engaged in chemical production processes, or a storage vessel for hazardous chemicals at any location, or a vehicle such as a train, ship, or truck, engaged in the transportation of a hazardous chemical.

agent not in their possession.

-99 = "Unknown"

19. Hostages

(HOSTAGES)
Categorical Variable

1 = "Yes"
The event reportedly involved an attempt to take hostages or the actual taking of hostages. This usually refers to an act whose primary objective is to obtain political or other concessions in return for the release of prisoners (hostages), although can also include cases where hostages are taken on an impromptu basis. Includes cases where the event occurs and usually plays out at the target location with little or no intention to hold the hostages for an extended period in a separate clandestine location, as well as cases where the threat actor/alleged threat actor intends to move and hold the hostages in a clandestine location. The victims can be selected beforehand.

0 = "No"
Sources do not report any hostages being taken or attempts to do so.

20. Assassination

(ASSASSINATION)
Categorical Variable

1 = "Yes"
The event reportedly involved an assassination, an attempted assassination, or a planned assassination. This is defined as an act whose primary objective is to kill one or more specific, usually prominent individuals. Usually carried out on persons of some note, such as high-ranking military officers, government officials, celebrities, CEOs, etc. Not to include attacks on non-specific members of a targeted group. The killing of a police officer would not be an assassination unless there is reason to believe the attackers singled out a particular officer for assassination.

0 = "No"
There was no report of assassination.

-99 = "Unknown"

21. Explosive Involved

(EXPLOSIVE)
Categorical Variable

1 = "Yes"
The attack involved explosives related to the CBRN attack/plot. This includes explosives used as the delivery mechanism and explosives used in coordination with a CBRN attack.

0 = "No"
The CBRN plot/attack did not use an explosive. Sources do not mention any explosives being found or any intention to use explosives in the attack.

-99 = "Unknown"
If explosives are found with a CBRN agent but sources do not confirm the explosives were going to be used with the CBRN agent.

22. Indiscriminate Attack

(INDISCRIM)
Categorical Variable

1 = "Yes"
In an indiscriminate attack, there is no evidence of any efforts made to limit the focus of an attack. For example, any agent being released in a crowded market.

0 = "No"
In a discriminate attack, there is some evidence of an effort made to limit the effect of an attack to a specific set of structures and/or individuals. For example, a grenade thrown in or at a police station or a church is assumed to be targeted.

-99 = "Unknown"
Most cases should be coded as "Yes" or "No." However, some plots may not provide enough information to make this determination.

23. Source Derived Validity

(*VALIDITY*)
Categorical Variable

Cumulative evidence that an event actually occurred. This variable verifies whether the event actually took place and whether that event really constituted a CBRN attack based on corroboration between multiple independent sources. The variable is coded once for each case.

Note: A source is regarded as independent of another source if it does not share the same original authorship and does not rely on the same original source material.

Additionally, if you have multiple sources from the same institution (such as the New York Times or Associated Press), only the most recent source counts as an independent source. Code the others as "Inherited" and link them to the most recent source.

NOTE: For the sake of **<Source Derived Validity>** two sources displaying the same bias will not be regarded as independent. However, sources with the same bias are still considered independent for the sake of discrepancy and doubt.

All variables in this section are coded with "1" for yes and "0" for no depending on whether the condition applies.

a) **Validity Unknown**
(VALID_UNK)

Sources are unknown.

b) **Validity Not Obtained**
(VALID_NOT_OBT)

Source(s) exist but have not been obtained, so the variable cannot be calculated, since it is not possible to assess which have objectivity or competence.[15] This includes cases where a source has been obtained but is in a foreign language that could not be translated.

c) **Validity Single**
(VALID_SINGLE)

A single source or multiple non-independent sources are used.

d) **Validity Two Independent Sources**
(VALID_TWO)

Two independent sources are used. It should be noted that two sources displaying the same specific bias will not be regarded as independent.

e) **Validity Three Plus Independent; Two With Competing Bias**
(VALID_THREE_PLUS)

Three or more independent sources are used; or two independent sources with competing biases are used.

24. Inherent Event Uncertainty

(UNCERT_EVENT)
Categorical Variable

Some events are clouded by inherent uncertainty over whether the CBRN event

[15] This is most likely to occur with cases derived from pre-existing datasets such as the Monterey WMDT. Due to changes over time in coverage by organizations such as Lexis-Nexis sources that were available at the time an event was recorded in the Monterey WMDT may not have been available at a later date.

occurred (i.e., unrelated to the reliability or number of sources). Based on conflicting reports or uncertain reports, it is uncertain whether the CBRN event took place. This variable pertains only to whether the CBRN event occurred, not the details of an event.

All variables in this section are coded with "1" for yes and "0" for no depending on whether the condition applies.

a) **No Event Uncertainty – None**
(UNCERT_EVENT_NONE)

Certainty exists that the event took place or was planned to take place.

b) **Some Event Uncertainty**
(UNCERT_EVENT_NONE)

Most observers believe the event occurred, but uncertainty exists.

c) **Considerable Event Uncertainty**
(UNCERT_EVENT_CONSID)

Most observers believe the event did not occur but some maintain that it did.

25. Inherent Attack Uncertainty

(UNCERT_ATTACK)
Categorical Variable

Some events are clouded by inherent uncertainty over whether the event was an attack (i.e., unrelated to the reliability or number of sources). These usually reflect the situation where the reporting is undisputed, but the larger question with respect to whether an event was actually an attack or was an accident or natural event is uncertain. This variable pertains only to whether the event was an attack, not the details of the event.

All variables in this section are coded with "1" for yes and "0" for no depending on whether the condition applies.

a) **No Attack Uncertainty - None**
(UNCERT_ATTACK_NONE)

Certainty exists that the event was an attack or planned attack.

b) **Some Attack Uncertainty**
(UNCERT_EVENT_NONE)

Most observers believe that the event was an attack or planned attack, but uncertainty exists.

c) Considerable Attack Uncertainty

(UNCERT_ATTACK_CONSID)

The event was most likely an accident or the result of natural causes, but the possibility has been raised that it was an attack.

E. Attack

This section of the database includes a number of fields that are described in section II.B.1 (Attack Date) above. The only fields discussed in this section of the codebook are those not separately discussed previously.

1. Warning Before Attack

(*ATTACK_WARNING*)
Categorical Variable

1 = "Yes"
The threat actor/alleged threat actor or another non law enforcement group/individual provided some kind of warning to the public, media, or law enforcement *before the attack took place*. Includes anonymous tips. Must be event specific.

0 = "No"
Sources did not portray any warning.

-77 = "Not Applicable"
Applies to all events not coded with an **<Event Type>** of **<Attempted Use of Agent>** or **<Use of Agent>**.

2. Claim of Responsibility After the Attack

(*ATTACK_RESPONSIBILITY*)
Categorical Variable

1 = "Yes"
Sources state that a single threat actor/alleged threat actor or multiple threat actors/alleged threat actors claimed responsibility for the attack.

0 = "No"
Sources do not state that anyone claimed responsibility for the attack. Includes instances where no attack took place.

-77 = "Not Applicable"
Applies to all events not coded with an **<Event Type>** of **<Attempted Use of Agent>** or **<Use of Agent>**.

3. Known Insiders Used

(*INSIDERS*)
Categorical Variable

1 = "Yes"
According to sources, insiders (such as a security guard at a chemical plant)

willingly or under duress assisted in the plot, attempt, or attack. This also includes a group member becoming employed on the inside for the purpose of the plot. An insider is someone with access to materials/equipment for the weapon/target.

0 = "No"
Sources do not portray assistance from insiders.

F. Plot

This section of the database includes a number of fields that are described in section II.B.3 (Plot Date) and II.C.2 (Plot Location) above.

G. Event Consequences

These variables assess the direct consequences of an event. Where possible, CBRN vs. non-CBRN casualties in the same event are clearly differentiated.

Only events coded as **<Event Type>** Attempted Use of Agent or Use of Agent (see section II.D.2.) can list casualty numbers.

For all cases that are coded as **<Event Type> <Unknown>** or below **<Attempted Use of Agent>** the entire event consequences section, with the exception of appropriate identifiers, should be coded as -77 for fields II.G.1. - II.G.18.

For **<Event Type> <Attempted Use of Agent>** or **<Use of Agent>**, if sources do not confirm zero casualties and the specific number is not reported, enter "-99" to indicate an unknown value. If sources do not discern between CBRN and non-CBRN inflicted casualties and injuries, enter "-99" to indicate an unknown value for these categories, only coding total casualties and injuries.

Where several independent sources report different numbers of casualties, the database will usually reflect the number given by the most recent source.

Where there are several "most recent" sources published around the same time, then the majority figure will be used. Where there is no majority figure among independent, equally credible sources, the database will record the lowest proffered fatality figure, unless there is clear reason to do otherwise.

1. Total Number of Fatalities

(TKILL)
Numeric Variable

This field records the total number of all individuals who died as a direct result of the CBRN event including both threat actor(s)/alleged threat actor(s) and victims, from any and all causes.

2. Total Number of Injuries

(TWOUND)
Numeric Variable

This field records the number of confirmed non-fatal injuries experienced as a direct result of the CBRN event including both threat actor(s)/alleged threat actor(s) and victims, from any and all causes.

3. Total Number of non-CBRN Fatalities

(NKILL)
Numeric Variable

This field records the number of individuals who died as a direct result of anything in the event except the CBRN agent (e.g., security personnel shot and killed during the deployment of the CBRN agent). Includes both threat actor(s)/alleged threat actor(s) and victims.

4. **Total Number of non-CBRN Injuries**
(NWOUND)
Numeric Variable

This field records the number of confirmed non-fatal injuries experienced by individuals caused by anything in the event except the CBRN agent. Includes both threat actor(s)/alleged threat actor(s) and victims.

5. **Total Number of CBRN Fatalities**
(CBRN_KILL)
Numeric Variable

This field records the number of individuals who died as a direct result of use of the CBRN agent/material employed in the event. Includes both threat actor(s)/alleged threat actor(s) and victims.

6. **Total Number of CBRN Injuries**
(CBRN_WOUND)
Numeric Variable

This field records the number of confirmed non-fatal injuries experienced by individuals directly caused by use of the CBRN agent/material employed in the event. Includes both threat actor(s)/alleged threat actor(s) and victims.

7. **Total Number of Fatalities - Victim**
(TVICTIM_KILL)
Numeric Variable

This field records the number of all victims who died as a direct result of the event from any and all causes.

8. **Total Number of Injuries - Victim**
(TVICTIM_WOUND)
Numeric Variable

This field records the number of confirmed non-fatal injuries experienced by victims as a direct result of the event from any and all causes.

9. **Total Number of non-CBRN Fatalities - Victim**
(NVICTIM_KILL)
Numeric Variable

This field records the number of all victims who died as a direct result of anything in the event except the CBRN agent (e.g.: explosives, shooting).

10. **Total Number of non-CBRN Injuries - Victim**
(NVICTIM_WOUND)
Numeric Variable

This field records the number of confirmed non-fatal injuries experienced by victims caused by anything in the event except the CBRN agent.

11. **Total Number of CBRN Fatalities - Victim**
(NCBRN_VICTIM_KILL)
Numeric Variable

This field records the number of total confirmed fatalities of all victims who died as a result of use of the CBRN agent/material employed in the event.

12. **Total Number of CBRN Injuries - Victim**
(NCBRN_VICTIM_WOUND)
Numeric Variable

This field records the number of confirmed non-fatal injuries experienced by victims caused by use of the CBRN agent/material employed in the event.

13. **Total Number of Fatalities - Actor**
(TPERP_KILL)
Numeric Variable

This field records the number of threat actors/alleged threat actors who died as a direct result of the event from any and all causes.

14. **Total Number of Injuries - Actor**
(TPERP_WOUND)
Numeric Variable

This field records the number of confirmed non-fatal injuries experienced by threat actors/alleged threat actors as a direct result of the event from any and all causes.

15. **Total Number of non-CBRN Fatalities - Actor**
(NPERP_KILL)
Numeric Variable

This field records the number of total confirmed threat actor/alleged threat actor fatalities for the event who died as a direct result of anything in the event except the CBRN agent.

16. **Total Number of non-CBRN Injuries - Actor**
    (NPERP_WOUND)
    Numeric Variable

    This field records the number of confirmed threat actor/alleged threat actor non-fatal injuries caused by anything in the event except the CBRN agent.

17. **Total Number of CBRN Fatalities - Actor**
    (NCBRN_PERP_KILL)
    Numeric Variable

    This field records the number of total confirmed threat actor/alleged threat actor fatalities as a direct result of the use of the CBRN agent/material employed in the event.

18. **Total Number of CBRN Injuries - Actor**
    (NCBRN_PERP_WOUND)
    Numeric Variable

    This field records the number of confirmed threat actor/alleged threat actor non-fatal injuries experienced as a direct result of the use of the CBRN agent/material employed in the event.

H. Event Agent

CBRN weapons are those being used for the toxic physiological effects on victims (or, in the case of nuclear weapons, the kinetic, thermal and toxic effects). The agent/weapon coded is the agent/weapon intended for use in the event (protoplot through attack). Other information is coded in **<Weapons Detail>**. For instance, if a group has acquired potassium cyanide but intends to use hydrogen cyanide, only hydrogen cyanide would be coded as the specific weapon.

Events can record multiple agent type values. This is more common in the case of the event type **<Protoplot>** where the threat actor/alleged threat actor has not yet narrowed down their choices prior to interdiction or abandonment of their CBRN efforts. However, sufficient information may be present in sources to discern the early stages of planning in the case of an event that progressed to the point of **<Attempted Use of Agent>** or **<Use of Agent>**. In these instances, it is appropriate to record all agent types explored by the threat actor/alleged threat actor.

If a case does not involve a particular type of agent (e.g.: chemical agent) categorical variable fields should be coded "-77" and related text variables coded "N/A".

1. Chemical Agent

(CHEM)
Categorical Variable

1 = "Yes"
The event reportedly involved a **<Chemical Agent>**. A chemical agent is gaseous, liquid, or solid matter that produces chemical reactions and toxic effects on the human body. Chemical agents include military grade or highly toxic industrial chemicals. Also, all reported "poisons" are treated as "chemical" unless sources provide evidence to the contrary.

The chemical designation includes plans and components that lead to the creation of chemical agents.

0 = "No"
There was no report of a chemical agent.

Note on chemical agents: Gas/propane/petroleum/liquid explosive bomb/acids: If chemicals in the possession of, or sought by, a threat actor/alleged threat actor were being used for, or intended for use for, the purposes of ignition, explosion, corrosive effects, etc. (i.e., for any reason other than to have toxic physiological effects on victims), they are not considered CBRN. Explosive materials intended to support the dissemination of a CBRN agent/material are not, however, exclusionary.

2. **Specific Chemical Agent**
   (SCHEM_AGENT)
   Text Variable

   This field contains the name of the specific chemical agent used. If the specific agent is unknown, code this field using the most specific unknown agent name possible based on the sources utilizing the options listed in the SAGENT Codes (e.g.: "Unknown Chemical").

   In the event that there are multiple chemical agents associated with the event, list each agent separated by a semi-colon. List multiple chemical agents in alphabetical order adhering to the agent names specified in the Specific Agent Codes listed in Section III.A.1.

3. **Biological Agent**
   (BIO)
   Categorical Variable

   1 = "Yes"
   The event reportedly involved a biological agent. A biological agent is a cultivated micro-organism (or product of a living organism) that causes damage to biological material. Agents can include bacteria, viruses, prions, fungi, and biological toxins. (Toxins should also be positively coded in the toxin variable.)

   The biological designation includes plans and components that lead to the creation of biological agents.

   0 = "No"
   There was no report of a biological agent.

4. **Specific Biological Agent**
   (SBIO_AGENT)
   Text Variable

   This field contains the name of the specific biological agent or toxin used. The scientific name should be used if known. Enter "Unknown" if not known.

   In the event that there are multiple biological agents associated with the event, list each agent separated by a semi-colon. List multiple biological agents in alphabetical order adhering to the agent names specified in the Specific Agent Codes listed in Section III.A.1.

5. **Toxin**
   (TOXIN)
   Categorical Variable

1 = "Yes"
The event reportedly involved a toxin. This variable is reported separately due to contention over whether toxins are biological or chemical agents. For the purposes of the Criminal CBRN Event database all biologically derived toxins are also treated as biological agents (e.g.: Botulinum toxin, Ricin, Cobra venom, etc.)

0 = "No"
There was no report of a toxin.

Note: If this variable is coded as a "1", then **<Biological Agent>** must be coded as a "1".

6. **Radiological Agent**
   (RAD)
   Categorical Variable

   1 = "Yes"
   The event reportedly involved a radiological agent capable of causing harmful ionizing radiation. All events involving radiological/nuclear material, to include plutonium or enriched uranium, are considered "radiological" unless (a) a source provides evidence to the contrary or (b) the threat actor/alleged threat actor is known to have nuclear aims (see Section II.H.8).

   The radiological designation includes plans and components that lead to the creation of radiological agents.

   0 = "No"
   There was no report of a radiological agent.

7. **Specific Radiological Agent**
   (SRAD_AGENT)
   Text Variable

   This field contains the name of the specific radiological agent used. Enter "Unknown" if not known.

   In the event that there are multiple radiological agents associated with the event, list each agent separated by a semi-colon. List multiple radiological agents in alphabetical order adhering to the agent names specified in the Specific Agent Codes listed in Section III.A.1.

8. **Nuclear Agent**
   (NUC)
   Categorical Variable

   1 = "Yes"

The event reportedly potentially involved a nuclear weapon (or attempts to obtain one). To code Special Nuclear Material (Weapons Grade Highly Enriched Uranium or plutonium) as a nuclear agent, sources or context must provide evidence that the threat actor/alleged threat actor intended to develop a gun-type or implosion mechanism. In order for non-nuclear material (such as low-enriched uranium) to be included as a nuclear agent, there must be some evidence of an intention to enrich the agent or otherwise produce a nuclear weapon. A contextual or source-based threat to use a nuclear weapon also is coded as a nuclear agent.

Note: Instances where the threat actor/alleged threat actor mistakenly believes that they have materials that are useful for the production of a nuclear device will be positively coded for this value. Especial care should be taken to ensure accurate notation of the **<Specific Nuclear Agent>** as this will be of great importance in assessing the level of threat represented by this particular event.

0 = "No"
There was no report of a nuclear agent.

9. **Specific Nuclear Agent**
(SNUC_AGENT)
Text Variable

This field contains the name of the specific nuclear agent used. Enter "Unknown" if not known.

In the event that there are multiple nuclear agents associated with the event, list each agent separated by a semi-colon. List multiple nuclear agents in alphabetical order adhering to the agent names specified in the Specific Agent Codes listed in Section III.A.1.

10. **Unknown Agent**
(UNKNOWN_AGENT)
Categorical Variable

1 = "Yes"
One or more of the agents involved are unknown agent types.

0 = "No"
All of the agents involved are known and specified in other variables.

11. **Specific Agent**
(SAGENT)
Categorical Variable

These variables record up to seven (*SAGENT_1; SAGENT_2; SAGENT_3; SAGENT_4; SAGENT_5; SAGENT_6; SAGENT_7*) CBRN agents using codes found in the Specific Agent Code Table (SAGENT Codes) of the Criminal CBRN Event database. Specific agents should be coded in the order in which they are listed in previous agent variables so that any chemical agents would be coded first in the order they are listed in the Specific Chemical Agent variable, followed by any biological agents and so on. For cases with less than seven specific agents code "-77" for N/A in this set's remaining variables.

Note: This variable is coded at the validation stage and should not be coded in earlier rounds of coding.

12. Delivery System Type

(DELIVERY)
Categorical Variable

This variable codes for known information detailing how the agent was, or was intended to be, delivered by the threat actor/alleged threat actor when mounting their planned attack. Multiple values may be coded positively.

All variables in this section are coded with "1" for yes and "0" for no depending on whether the condition applies.

a) Delivery Method Unknown

(DEL_UNK)

The threat actor/alleged threat actor intends to deliver the agent, but the delivery method is either unknown to the threat actor/alleged threat actor or unknown based on source information.

b) Not Intended For Delivery

(DEL_NOT_DEL)

The available evidence shows the threat actor/alleged threat actor never actually intended to deliver the agent. Often coded in cases where **<Intent to Use>** is negatively coded, but this depends on context.

c) Aerosol/Spray

(DEL_AEROSOL)

A delivery system that delivers an agent in the form of either an aerosol or spray. This would include a crop duster or drone spraying an agent, or a fixed sprayer device.

d) Casual/Personal/Direct Contact

(DEL_CONTACT)

Includes cases where the agent is intentionally delivered through close proximity or touch. "Casual/personal/direct contact" would include a threat actor/alleged threat actor purposefully: coughing towards a target while infected with plague, spraying a chemical at a target with a Windex bottle, or leaving a non-volatile agent on a doorknob.

e) Consumer Product Tampering

(DEL_PROD_TAM)

Includes cases where CBRN agents/materials are put into consumer products (incl. food/drink purchased in a store), provided the product packaging is apparently intact. Consumer product tampering includes cases where tampering takes place in the production facility. For example, yogurt injected with a chemical falls into this category if it is purchased in a seemingly sealed package. Consumer product tampering includes bottled water, if sealed.

f) Explosive Device

(DEL_EXPLO)

Any primary delivery device that consists of an explosive. Also includes instances where agents form an aerosol after the use of explosives.

g) Food/Drink

(DEL_FOOD_DRINK)

Food/drink includes the intentional placement of the agent in the victim's food or drink, but excludes cases categorized as consumer product tampering (see above). Includes poisoning in restaurants, mess halls and similar facilities. If the packaging/seal on a consumer product is obviously broken when presented to the intended victim (for instance, a previously opened bottle of soda served in a restaurant), it is regarded as "food/drink." An office water cooler would also be included.

h) Injection/Projectile

(DEL_INJECT_PROJECT)

This value implies a delivery by <u>controlled</u> trajectory that forcefully inserts an agent into a person. For example, a target is struck by a cyanide-laced bullet. Can also include threat actor(s)/alleged threat actor(s) utilizing items such as syringes.

i) Latent

(DEL_LATENT)

A latent delivery system includes any agent that is left out without forcing direct contact. For instance, leaving breakable vials of an agent on the floor intending for the target to step on the vials and release the agent, or any type of radiological emission device.

j) Mail/Letter/Package

(DEL_MAIL)

Any agent that is delivered by mail, letter, or package. In the case of a letter bomb, use this value and ensure that **<Explosive Involved>** is coded as "1".

k) Reaction Device

(DEL_REACT)

A reaction device method of delivery means that the device used in the event is designed to produce a chemical, physical or biological reaction in order to release a harmful agent. For instance, a canister of acid set to rupture into a container of cyanide salt.

l) Ventilation System

(DEL_VENT)

Ventilation system includes cases where victims would be indiscriminate and therefore excludes dispersing an agent through the air-conditioning system of a car, which is more accurately categorized as direct contact.

m) Water Supply

(DEL_WATER)

Water supply includes facilities of any size involving plumbing, from apartment buildings to cities, and wells. Can include bottled water if the source of the bottled water is a municipal water supply which is contaminated before bottling. Generally, if water supply is the delivery mechanism, it should not be the target of the attack; the target would be the individuals exposed to the tainted water.

n) Multiple Delivery Methods

(DEL_MULTIPLE)

Use this classification when the event involves multiple delivery system types in a single occurrence. Most likely to be appropriate to events at the **<Protoplot>** or **<Plot>** stage.

13. Specific Delivery System Type

(SDELIVERY)
Categorical Variable

These variables record up to four (*SDELIVERY_1; SDELIVERY_2; SDELIVERY_3; SDELIVERY_4*) delivery mechanisms using the codes found in the Specific Delivery Mechanism Table (SDELIVERY Codes) of the Criminal CBRN Event database, providing for 1) greater specificity than the Delivery System Type variable and 2) the identification of multiple delivery system types coded as “Multiple Delivery Methods” in the Delivery System Type variables**.** For cases with less than four specific delivery mechanisms code “-77” for N/A in the remaining variables in this set.

Note: This variable is coded at the validation stage using the Specific Delivery Mechanism Codes listed in Section III.A.2. and should not be coded in earlier rounds of coding.

I. Agent Acquisition

The following variables assess a threat actor's/alleged threat actor's acquisition, planned acquisition, or attempted acquisition of a ready-made weapon, ready-made CBRN agent, or the components of a CBRN agent. Method of acquisition is nonexclusive.

1. Barter

(*BARTER*)
Categorical Variable

1 = "Yes"
Based on source information, the threat actor/alleged threat actor bartered nonmonetary items or services to acquire the agent.

0 = "No"
Sources do not report acquisition through barter.

2. Bribery/Coercion

(*BRIBERY*)
Categorical Variable

1 = "Yes"
Based on source information, the threat actor/alleged threat actor bribed or coerced an individual/organization outside of the group for access to the agent. Bribery is based on paying for the ability to acquire an agent (e.g.: the threat actor/alleged threat actor pays off a security guard at a chemical plant). Coercion is using intimidation to create the opportunity to acquire an agent.

0 = "No"
Sources do not report acquisition through a bribe or coercion.

3. Facility

(*FACILITY*)
Categorical Variable

1 = "Yes"
This value includes instances where, according to source information, the threat actor/alleged threat actor used or planned to use the agent held by a facility in an attack without changing the location of the material.

0 = "No"
Sources do not report acquisition based on a facility attack.

4. Gift

(*GIFT*)

Categorical Variable

1 = “Yes”
Based on source information, the threat actor/alleged threat actor received the agent from another party outside of the group without using payment or coercion.

0 = “No”
Sources do not report acquisition through a received gift.

5. **Production**
   (*PRODUCTION*)
   Categorical Variable

   1 = “Yes”
   Based on source information, the event involves the threat actor/alleged threat actor producing some level of the agent or weapon in house.

   0 = “No”
   Sources do not report acquisition through in-house production.

6. **Purchase**
   (*PURCHASE*)
   Categorical Variable

   1 = “Yes”
   Based on source information, the threat actor/alleged threat actor bought the agent through a black or white market channel. Includes previously set up illicit networks.

   0 = “No”
   Sources do not report acquisition through purchase.

7. **Serendipity**
   (*SERENDIPITY*)
   Categorical Variable

   1 = “Yes”
   Based on source information, the event involves the threat actor/alleged threat actor acquiring the weapon or weapon components through an unplanned or unexpected opportunity.

   0 = “No”
   Sources do not report the threat actor/alleged threat actor acquiring the weapon or weapon components by an opportunity presenting itself.

8. **Theft**
   (*THEFT*)
   Categorical Variable

   1 = "Yes"
   Based on source information, theft includes instances where the threat actor/alleged threat actor acquired the agent through theft.

   0 = "No"
   Sources do not report acquisition through theft.

9. **Training**
   (*TRAINING*)
   Categorical Variable

   1 = "Yes"
   Based on source information, the event involves the threat actor/alleged threat actor participating in some semblance of training specific to the production, handling, and/or delivery of the agent and/or delivery mechanism. Examples can include working directly with specialists to develop the capabilities or taking related legitimate courses. Training can even include remote interaction through email; however, the correspondence must carry on beyond a few initial questions and involve a relationship with the trainer. May be associated with positive coding for **<Production>**.

   0 = "No"
   Sources do not report the threat actor/alleged threat actor being involved in any training that would lead to the in-house production of the agent or delivery mechanism.

10. **Unknown**
    (*UNKNOWN*)
    Categorical Variable

    1 = "Unknown"
    No sources provide information on agent acquisition.

    0 = "Known"
    At least one type of agent acquisition is known.

11. **Amount of Agent Material**
    (*AGENT_AMOUNT*)
    Text Variable

    This field is to include any known information about the amount of agent material possessed or intended to be used by the threat actor/alleged threat actor. Convert to metric scale; volume (for liquids) and weight (for solids). [http://www.google.com/landing/searchtips/#unitconversion]

If amount of material is known for multiple event-specific agents, list each agent's name and amount followed by a semicolon. Enter "Unknown" if not known.

However, if the amount of agent material is not listed in a standard metric in any of the sources, still include the nonstandard information. For instance, two canisters or several small vials.

12. Mechanism of Awareness

(*MECHANISM_AWARENESS*)
Categorical Variable

This variable notes how the threat actor/alleged threat actor initially became aware of the CBRN technology.

***All variables in this section are coded with "1" for yes and "0" for no depending on whether the condition applies*.**

a) Demonstration – Immediate Context

(MECHANISM_AWARENESS_DEMOI)

The threat actor/alleged threat actor became aware of the CBRN technology used by demonstration within his/their immediate network. Such direct user ties include immediate competition, or other VNSAs the group has close ties with.

b) Demonstration – Broad Context

(MECHANISM_AWARENESS_DEMOB)

The threat actor/alleged threat actor became aware of the CBRN technology due to a displayed use outside their immediate network. Such demonstrators may include non-connected VNSAs, Hollywood movies, or state actors using the specific CBRN technology.

c) Proselytization

(MECHANISM_AWARENESS_PROSELY)

The threat actor/alleged threat actor became aware of the CBRN technology when someone outside of the group actively advocated for the technology.

d) Self-Initiated Search

(MECHANISM_AWARENESS_SEARCH)

The threat actor/alleged threat actor pursued the agent and/or weapon in question as a result of a self-recognized need for the CBRN tactic at hand.

e) **Unknown Awareness Mechanism**
(MECHANISM_AWARENESS_UNK)

No sources found reference the mechanism by which the threat actor/alleged threat actor became aware of the CBRN technology planned or employed.

13. Minimum Number Acquired – Intended
(*MIN_NUM_ACQ_INTENDED*)
Numerical Variable

The minimum number of weapons that the threat actor/alleged threat actor wanted for the plot (intended). If the exact number is known, the min and max can be the same. Enter "-99" if unknown. List zero if known to be zero. Some agents and delivery mechanisms, including those involving poison and water supply, may not be applicable for this variable. If not explicit, "1" may be coded if there is positive **<Intent to Use>**.

14. Maximum Number Acquired – Intended
(*MAX_NUM_ACQ_INTENDED*)
Numerical Variable

The maximum number of weapons that the threat actor/alleged threat actor wanted for the plot (intended). If the exact number is known, the min and max can be the same. Enter "-99" if unknown. List zero if known to be zero. Some agents and delivery mechanisms, including those involving poison and water supply, may not be applicable for this variable.

15. Minimum Number Acquired – Actual
(*MIN_NUM_ACQ_ACTUAL*)
Numerical Variable

The minimum number of completed weapons (or weapons able to be completed) that the threat actor/alleged threat actor had acquired for that event. If the exact number is known, the min and max can be the same. Enter "-99" if unknown. List zero if known to be zero. Some agents and delivery mechanisms, including those involving poison and water supply, may not be applicable for this variable.

16. Maximum Number Acquired – Actual
(*MAX_NUM_ACQ_ACTUAL*)
Numerical Variable

The maximum number of completed weapons (or weapons able to be completed) that the threat actor/alleged threat actor had acquired for that event. If the exact number is known, the min and max can be the same. Enter “-99” if unknown. List zero if known to be zero. Some agents and delivery mechanisms, including those involving poison and water supply, may not be applicable for this variable.

J. Target

This section of the database includes a number of fields that are described in section II.C.3. (**<Target Location>**) above. The only fields discussed in this section of the codebook are those not separately discussed elsewhere.

Identifying targets is not always easy since violent actors may have multiple levels of intended target. Moreover, although criminals, unlike terrorists who by definition, aim their attacks at a minimum of two entirely different kinds of targets—an immediate (or direct) target, i.e., the victims or structures that suffer the actual physical assault (who are often selected for their symbolic or representative value); and the ultimate (or indirect) target, i.e., the wider audience(s) whose perceptions and behavior they hope to influence)—this does not mean that criminal actors may not also target a specific individual, or generic group of individuals, in order to produce a wider or more generalized effect. There are many instances where criminal actors are completely indifferent to the identity of the specific individuals injured or killed in their attacks as their focus is an institution which these individuals are employees or customers of.

For the purposes of the database, however, it is the **direct target** that is of principal concern in classifying the target in the Criminal CBRN Event Database. Even so, in order to ensure flexibility, for each event, more than one target of an attack can be identified in the database record. Thus, in cases with multiple targets, all variables in the Target Location section will be coded for each unique target. This is particularly relevant to events that did not progress beyond **<Protoplot>** or **<Plot>**.

The Criminal CBRN Event Database records up to five distinct targets for each event. For those cases with only a single target, or more than one but less than five, all un-used fields will be coded as -77.

All Target fields are replicated and distinguished by the addition of a number preceding the variable name (e.g., T1-TENTITY / T2-TENTITY / etc.) represented in the codebook as T* where "*" will be replaced by a number ranging from 1-5.

In some attacks, there may be both an intended target and an actual target. If a suicide bomber is stopped at a checkpoint on his way to attacking a market and detonates his device at the checkpoint, both the market (the intended target) and the checkpoint (the actual target) are coded. If a letter with a sealed vial of anthrax is sent to Bill Gates and the vial cracks in the mail and a postal employee becomes ill, Bill Gates is the intended target. In this example casualties would be coded as "0" for the **<Target ID>** describing Bill Gates, while the **<Target ID>** describing the postal employee would be coded as "1" casualty. The **<Target ID>** recording the postal employee would also be coded "0" to note that this was not the **<Intended Target>**.

1. **Entity Name: Name of Corporation/Agency**
   (T-TENTITY)*
   Text Variable

   This field identifies the name of the broad entity or class of which the **<Specific Target>** is a part. This variable can be coded regardless of **<Event Type>** so long as the target location is known. If the entity has an official name, the official name should be researched and entered here. For instance, an attack on Russian soldiers would be entered as "Armed Forces of the Russian Federation". Likewise, an attack on a U.S. Embassy in Kenya would be entered as "United States Department of State".

   If the **<Specific Target>** (see section II.I.2.) is part of an entity with no official name, then it should be designated according to the broad category of which the Specific Target is a part. For instance, an attack on British student workers would be entered as "Citizens of the United Kingdom" while an attack on the Prime Minister of Pakistan would be entered as "Government of Pakistan". Likewise, an attack against dams in France would be entered as "Dams in France" while an attack on abortion clinics in the United States would be entered as "Abortion Clinics in the United States". To ensure uniformity, the "Entity Name of Country X" or "Entity Name in Country X" formatting should be maintained where appropriate. An attack against private citizens where either an individual was specifically targeted irrespective of their membership in the broader population or where the Attack Location is coded as "-99" which indicates "Unknown", should be coded as "Civilians".

   If the **<Target Location>** is coded as "-99" which indicates "Unknown", then the **<Entity Name>** should be listed without a specific location modifier. If the Entity Name cannot be identified, the field should be coded as "Unknown".

   This field should not be coded as "Unknown" if a known **<Specific Target>** has been coded. However, a known Entity Name may still be coded if **<Specific Target>** has been coded as "Unknown." In cases where **<Evidence of Intent to Use>** has been coded as "0", Entity Name should be coded as "None".

2. **Specific Target**
   (*T*-TSPECIFIC*)
   Text Variable

   This is the specific person, building, installation, etc., that was targeted and is a part of the entity named above. (For example, if the U.S. Embassy in Country X was attacked the "Name of Entity" would be "U.S. Department of State" and the "Specific Target" would be "U.S. Embassy in Country X.") If multiple individuals that form part of the same entity are targeted, list each separated by a semicolon. If unknown code "Unknown".

Note: UNDER NO CIRCUMSTANCES WHATSOEVER should this field include or record any information that can be deemed as identifying information as defined by NISTIR 8053; "identifying information" denotes information that identifies individuals. (NIST Internal Report 8053, Page 3)

3. **Intended Target**
(*T*-TINTENDED*)
Categorical Variable

1 = "Yes"
The target recorded was the target that the threat actor/alleged threat actor intended to strike when they made their CBRN agent use attempt.

0 = "No"
The target recorded was not the target that the threat actor/alleged threat actor intended to strike when they made their CBRN agent use attempt.

-99 = "Unknown"
There is no, or insufficient, information available to determine whether the recorded target was the intended target.

K. Target Type

The target type section is coded as a subsidiary field of the TARGET entry (see section II.J)

All Target Type fields are replicated and distinguished by the addition of a number preceding the variable name represented in the codebook as T* where "*" will be replaced by a number ranging from 1-5 (e.g., T1-AGRICULTURE / T2-AGRICULTURE / etc.).

The target type is recorded utilizing the list below. Each target can be associated with multiple attributes that describe the type of target attacked. For example, a government-owned power station can be coded "1" for both "GOVERNMENT" and "UTILITIES". A single target may be comprised of multiple components and still be regarded as a single target, but the components must be connected functionally (i.e., several vehicles in a convoy or multiple buildings on the same base).

1. Agriculture

(*T*-AGRICULTURE*)
Categorical Variable

1 = "Yes"
Any attack on plants, animals, or personnel in an agricultural context. Including disruption to agricultural products prior to arrival at production facilities, such as a factory producing packaged vegetable products, or a meat packing plant.

0 = "No"
Sources do not report target as agriculture.

2. Aviation

(*T*-AVIATION*)
Categorical Variable

1 = "Yes"
An attack that is carried out either against an airplane or against an airport. Attacks against airline employees while on board are also included in this value.

Includes attacks conducted against airport business offices and executives. Attacks where airplanes were used to carry out the attack (such as three of the four 9/11 attacks) are not included.

0 = "No"
Sources do not report target as aviation.

3. **Business**
(*T*-BUSINESS*)
Categorical Variable

1 = "Yes"
Businesses are defined as individuals or organizations engaged in commercial or mercantile activity as a means of livelihood. Any attack on a business such as a restaurant, gas station, music store, bar, café, etc.

Includes attacks carried out against corporate offices or employees of firms like mining companies, or oil corporations. Furthermore, includes attacks conducted on business people or corporate officers. Also included in this value are chambers of commerce and cooperatives.

Does not include attacks carried out in public or quasi-public areas such as "business district or commercial area" (these attacks are captured under "Private Citizens and Property", see below). Does not include attacks where evidence exists that businesses were harmed only incidentally.

0 = "No"
Sources do not report target as a business.

4. **Educational Institution**
(*T*-EDUC_INSTITUTION*)
Categorical Variable

1 = "Yes"
Includes attacks against university professors, teaching staff and school buses. Moreover, include attacks against religious schools in this value.

If attacks involving students or faculty are not expressly directed against a school, university or other educational institution or are not carried out in an educational setting, they are coded as private citizens and property.

0 = "No"
Sources do not report target as an educational institution.

5. **Energy Utilities**
(*T*-ENER_UTILITIES*)
Categorical Variable

1 = "Yes"
This value pertains to facilities for the transmission or generation of energy. For example, power lines, oil pipelines, electrical transformers, high tension lines, gas and electric substations, are all included in this value. This value also

includes lampposts or streetlights.

Attacks on officers, employees or facilities of utility companies in the performance of their duties, or if evidence suggests they were targeted because of their connection to the utility are included.

0 = "No"
Sources do not report target as an energy utility.

6. **Government (General, Justice Administration, and Politics)**
(*T*-GOVERNMENT*)
Categorical Variable

1 = "Yes"
Any attack on a government building; government member, former members, including members of political parties, their convoys, or events sponsored by political parties; political movements; or a government-sponsored institution where the attack is expressly carried out to harm the government.

This value includes attacks on judges, public attorneys (e.g., prosecutors), courts and court systems, politicians, royalty, heads of state, government employees (unless police or military), intelligence agencies and spies.

0 = "No"
Sources do not report target as government.

7. **Government (Diplomatic)**
(*T*-DIPLOMATIC*)
Categorical Variable

1 = "Yes"
Attacks carried out against foreign missions, including embassies, consulates, etc.

This value includes cultural centers that have diplomatic functions, and attacks against diplomatic staff and their families and property.

0 = "No"
Sources do not report target as diplomatic.

8. **Journalists & Media**
(*T*-MEDIA*)
Categorical Variable

1 = "Yes"
Includes attacks on reporters, news assistants, photographers, publishers, as

well as attacks on media headquarters and offices.

0 = "No"
Sources do not report target as journalist or media.

9. **Maritime (Includes Ports and Maritime Facilities)**
(*T*-MARITIME*)
Categorical Variable

1 = "Yes"
Implies civilian maritime. Includes attacks against fishing ships, oil tankers, ferries, yachts, etc.

1 = "No"
Sources do not report target as maritime.

10. **Medical Facility**
(*T*-MEDICAL_FACILITY*)
Categorical Variable

1 = "Yes"
Attacks on medical facilities and medical employees when the attack takes place in the facility. Includes attacks on abortion facilities.

0 = "No"
Sources do not report target as a medical facility.

11. **Military**
(*T*-MILITARY*)
Categorical Variable

1 = "Yes"
Includes attacks against military (Army, Navy, Air Force, etc.) units, facilities, equipment, etc. This variable also includes attacks on recruiting sites and soldiers engaged in internal policing functions such as operating checkpoints or performing anti-narcotics activities. International peacekeepers deployed in support of a United Nations or other mandate also belong to this value.

Excludes attacks against non-government militia and guerrillas; these types of attacks are coded as "Violent Political Actors" see below.

0 = "No"
Sources do not report target as military.

12. **Monuments and National Icons**
(T-MONUMENT)*

Categorical Variable

1 = “Yes”
Includes attacks against national icons and monuments.

0 = “No”
Sources do not report target as a monument or national icon.

13. NGO

(*T*-NGO*)
Categorical Variable

1 = “Yes”
Includes attacks on offices and employees of non-governmental organizations (NGOs). NGOs here are defined as primarily large multinational non-governmental organizations. These include the Red Cross and Doctors Without Borders. Does not include labor unions, social clubs, student groups, political parties, and other non-NGO (such cases are mostly coded as “Other”, see below).

0 = “No”
Sources do not report target as an NGO.

14. Police

(*T*-POLICE*)
Categorical Variable

1 = “Yes”
For attacks on members of the civilian police force or associated police installations; this includes police boxes, patrols, headquarters, academies, vehicles, checkpoints, etc. This does not include military police which should be coded as “Military”.

0 = “No”
Sources do not report target as police.

15. Prisons

(*T*-PRISON*)
Categorical Variable

1 = “Yes”
Includes attacks against jails or prison facilities, or jail or prison staff or guards.

0 = “No”
Sources do not report target as a prison.

16. Private Citizens

(*T*-PRIVATE_CITIZEN*)
Categorical Variable

1 = "Yes"
For attacks on individuals. Also applies to attacks in public areas including markets, commercial streets, busy intersections, shopping centers, and pedestrian malls where the target focus is non-specific members of the general public or passers-by.

Also includes ambiguous cases where the target was a named private individual, or where the target/victim of an attack could be identified by name, age, occupation, gender or nationality. This value also includes ceremonial events, such as weddings and funerals.

If attacks on students are not expressly against a school, university or other educational institution or are not carried out in an educational setting, these attacks are coded using this value. Also, includes events involving political supporters as private citizens and property, provided that these supporters are not part of a government-sponsored event. Finally, this value includes police informers.

0 = "No"
Sources do not report target as private citizens.

17. Private Property

(*T*-PRIVATE_PROPERTY*)
Categorical Variable

1 = "Yes"
For attacks on private property as opposed to state-owned facilities.

0 = "No"
Sources do not report target as private property.

18. Private Security

(*T*-PRIVATE_SECURITY*)
Categorical Variable

1 = "Yes"
Includes attacks against private security guards.

0 = "No"
Sources do not report target as private security.

19. Religious Figures

(*T*-RELIG_FIGURE*)
Categorical Variable

1 = “Yes”
For attacks on religious leaders, (imams, priests, bishops, etc.) This value also includes attacks on organizations that are affiliated with religious entities.

Attacks on religious pilgrims (provided there is some evidence that they were attacked in this context) or missionaries are considered as religious figures.

0 = “No”
Sources do not report target as a religious figure.

20. Religious Institutions

(*T*-RELIG_INSTITUTION*)
Categorical Variable

1 = “Yes”
For attacks on religious institutions (mosques, churches), religious places or objects (shrines, relics, etc.).

0 = “No”
Sources do not report target as a religious institution.

21. Special Event

(*T*-SPECIAL_EVENT*)
Categorical Variable

1 = “Yes”
For attacks on special events such as an international meeting/conference, sports event, or concert. The World Cup, Olympics, a Sting concert, and the G8 meeting are all included in this category when the actual event is targeted (as opposed to only targeting a selected individual).

0 = “No”
Sources do not report target as a special event.

22. Telecommunications Infrastructure

(*T*-TELECOMMUNICATIONS*)
Categorical Variable

1 = “Yes”
For attacks on facilities and infrastructure for the transmission of information. More specifically this value includes targets like cell phone towers, telephone booths, television transmitters, internet hubs, radio, and microwave towers.

0 = "No"
Sources do not report target as telecommunications infrastructure.

23. Tourist

(*T*-TOURIST*)
Categorical Variable

1 = "Yes"
This value includes the targeting of tour buses, tourists, or "tours." Tourists are persons who travel primarily for the purposes of leisure or amusement. Government tourist offices are included in this value.

The attack must clearly target tourists, not just an assault on a business or transportation system used by tourists.

0 = "No"
Sources do not report target as tourist.

24. Transportation (Other Than Aviation)

(*T*-TRANSPORTATION*)
Categorical Variable

1 = "Yes"
Attacks on public transportation systems are included in this value. This can include efforts to assault public buses, minibuses, trains, metro/subways, highways (if the highway itself is the target of the attack), bridges, roads, etc.

Buses are assumed to be public transportation unless otherwise noted. Private commuter vehicles are not deemed to be public transportation unless evidence exists to the contrary.

0 = "No"
Sources do not report target as transportation.

25. Violent Political Actor(s)

(*T*-VIOLENT_ACTORS*)
Categorical Variable

1 = "Yes"
This value includes cases involving the targeting of terrorists, insurgents, militias, guerillas and other violent non-state political actors.

Terrorists or members of identified terrorist groups are included in this value. Membership is broadly defined and includes informants for terrorist groups but excludes former terrorists.

0 = “No”
Sources do not report target as violent political actor(s).

26. Other

(*T*-OTHER*)
Categorical Variable
This should only be used if no other category is deemed appropriate.

1 = “Yes”
For violent criminal acts committed against targets which do not fit into other categories.

0 = “No”
Target is coded in one of the other categories.

27. Unknown

(*T*-UNKNOWN*)
Categorical Variable

1 = “Yes”
If attack target is unknown.

0 = “No”
Sources do not report target as unknown.

28. None

(*T*-NONE*)
Categorical Variable

1 = “Yes”
If there is no attack target. If **<Intent to Use>** has been coded as “0”, which indicates “No”, **<Target Type>** should be coded as “None”.

0 = “No”
Sources clearly indicate that there was an intended target even if the type is unknown.

L. Event Actor

This section of the Criminal CBRN Event database records data associated with those group(s) and/or individual(s) associated with a specific recorded CBRN event. These individuals or organizations are referred to using the term "threat actor/alleged threat actor" or "event actor."

This section of the database will code a maximum of five discreet threat actor/alleged threat actor records per event. The need to code multiple threat actor/alleged threat actor records is generally limited to circumstances in which several independent groups are collaborating in order to mount an attack. As a general rule, events recorded in the Criminal CBRN Event Database will be undertaken by individuals.

The Criminal CBRN Event Database does not code individual identities of Lone Actors or members of threat actor/alleged threat actor groups.

In the case of an event with multiple threat actors/alleged threat actors (e.g., two criminal groups collaborating in an attack), all variables in the threat actor/alleged actor sections will be coded uniquely for each threat actor/alleged threat actor. If possible, code the separate threat actors/alleged threat actors in the order of importance to the plot.

The Criminal CBRN Event Database records non-state actor CBRN events. If the only threat actor/alleged threat actor associated with the recorded event is a state actor (such as Pakistan's Inter-Services Intelligence (ISI)), the case does not fit the definition of the database.

NOTE: Certain variables in this section, clearly indicated, are solely for internal use and function as research notes or aids for database coding. As such they should under no circumstances be publicly disseminated and should at all times be appropriately protected as instructed in section I.B of this codebook.

1. Event Actor ID

(EACTOR_ID_A)*
Numeric Variable

A unique identifier for each recorded event threat actor/alleged threat actor entry. This variable is simply a sequential number for each threat actor/alleged threat actor included for each event, generated for record keeping purposes and is not tied to the identity of particular threat actors/alleged threat actors. This field allows the recording of multiple threat actors/alleged threat actors per event if required. A threat actor/alleged threat actor is captured at the highest appropriate level as indicated by **<Actor Type>.** As an example, an event involving an **<autonomous cell>** comprised of 5 members would only be assigned a single **<E-Actor ID>**.

2. **Event Actor Known**
   (*EA_KNOWN_A**)
   Categorical Variable

   This variable indicates whether sources indicate that the threat actor associated with the recorded event was identified or not. The threat actor may have been identified through a self-claim, capture, intelligence or other means.

   1 = "Yes"
   Some or all of the threat actors, whether individuals or groups, associated with the recorded CBRN event were identified.

   0 = "No"
   No threat actors, whether individuals or groups, associated with the recorded CBRN event were identified in sources.

   NOTE: Where this variable is coded as "N" the ACTOR DB LINK variable should be coded as "-77" and no ACTOR DB entry should exist.

3. **Event Actor Group ID**
   (*EACTOR_ID_A**)
   Categorical Variable

   This field records the name of the formal group that carried out the attack as a predetermined numeric code. In order to ensure consistency in the usage of group names for the database, the Criminal CBRN Event database uses a standardized list of group names that have been established by project staff to serve as a reference for all subsequent entries. This list is available in the Actor Name (ANAME) codes resource.

   - For individual threat actors not connected to a group, code as “Individual.”
   - If the event threat actor is an unnamed, unaffiliated cell (2-10 people), code as “Unnamed Cell.”
   - If the threat actor/alleged threat actor is not listed in the sources, and accordingly negatively coded for **<EA_KNOWN>** list as “Unknown.”

   If a new group not currently recorded in the ANAME code resource is identified as a threat actor associated with an event recorded in the database, the new group should be brought to the attention of the database manager who will add the group to the ANAME codes resource as necessary.

4. Event Actor Doubt

(*EA-DOUBT_A**)
Categorical Variable

This variable does not look at whether the threat actor/alleged threat actor is known or unknown, but instead whether the identity of the threat actor(s) associated with the recorded event as provided in available sources is controversial in some way.

0 = Threat Actor/Alleged Threat Actor Identity Certain or Unknown
The threat actor(s) involved in the recorded event is either known with some degree of certainty or is completely unknown. It should be noted that threat actors are often unknown due to the covert nature of the event, a lack of adequate information, or for security reasons.

1 = Threat Actor/Alleged Threat Actor Identity Doubted
If any information concerning the identification of the threat actor/alleged threat actor associated with the recorded event is ambiguous, including if one suspects that the purported claims of responsibility have been intentionally manipulated, that government or other parties are disseminating disinformation, or if there are questions about the veracity or bona fides of the source providing information about the case, this variable is given a value of "1". Similarly, if there are only unverified allegations that certain parties were responsible for carrying out an act, or if the supposed threat actor/alleged threat actor were later acquitted during a trial, the threat actor/alleged threat actor implicated in the case is classified as "doubted".

Also list as doubted those cases where a reliable source mentions a potential suspect or if the government shows doubt in the suspect.

5. Event Actor Type - Unknown

(*EA_TYPE_UNK_A**)
Categorical Variable

This variable codes for whether or not the threat actor/alleged threat actor type has been identified.

1 = "Yes"
The threat actor type is not known based on available sources.

0 = "No"
The threat actor type is known based on available sources.

NOTE: If this variable is coded as "1" then **<EA_TYPE_INDV>**, **<EA_TYPE_AUTON>**, and **<EA_TYPE_FORMAL>** should all be coded as "-77".

6. **Event Actor Type - Individual**
   (EA_TYPE_INDV_A)*

The threat actor associated with the recorded event was an individual actor not operationally linked to any larger groups.

1 = "Yes"
The threat actor type is an individual actor based on available sources.

0 = "No"
The threat actor type is not an individual actor based on available sources.

NOTE: If the individual threat actor was operating under the direct operational control of a formal organization or in direct coordination with a small group of others, they are NOT an individual threat actor for the purposes of this database and should be recorded as either “autonomous cell” or “formal organization” as appropriate.

NOTE: If the individual threat actor was engaged in a primarily independent operation, and received **guidance or support** from, but was not under the direct operational control of, a formal organization **<EA-LINKED>** should be coded positively and the appropriate formal group ID should be recorded in **<LINKED_ENTITY>**.

7. **Event Actor Type – Autonomous Cell**
   (EA_TYPE_AUTON_A)*

The threat actor associated with the recorded event was an autonomous cell not operationally linked to any larger groups. An autonomous cell must have fewer than ten members (i.e., 2-9 members) and while they may be influenced by other organizations, they are not connected to other organizations.

1 = "Yes"
The threat actor type is an autonomous cell based on available sources.

0 = "No"
The threat actor type is not an autonomous cell based on available sources.

NOTE: If the cell was operating under the direct operational control of a formal organization, they are NOT an autonomous cell for the purposes of this database and should be recorded as a "formal organization".

NOTE: If the autonomous cell was engaged in a primarily independent operation, and received **guidance or support** from, but was not under the direct operational control of, a formal organization **<EA-LINKED>** should be coded positively and the appropriate formal group ID should be recorded in **<LINKED_ENTITY>**.

8. Event Actor Type – Formal Organization

(EA_TYPE_FORMAL_A)*

The threat actor associated with the recorded event was a formal organization. For the purposes of this database a formal organization is a group of 10 or more individuals operating together on a sustained basis, typically with a formal leadership structure, manifesto, recruitment, training, etc.

1 = "Yes"
The threat actor type is a formal organization based on available sources.

0 = "No"
The threat actor type is not a formal organization based on available sources.

9. Event Actor – Conventional Attacks

(EA_CONV_A)*

This field records whether the threat actor has also been associated with one or more acts of ideological violence using conventional weapons. This can include arson, bombs, firearms, stabbing/slashing attacks, vehicle ramming attacks, etc.

1 = "Yes"
The threat actor has, based on available sources, prior or subsequent to the recorded CBRN event, mounted, or engaged in plots for, attacks utilizing conventional weapons.

0 = "No"
The threat actor has not, based on available sources, prior or subsequent to the recorded CBRN event, mounted, or engaged in plots for, attacks utilizing conventional weapons. The threat actor has only engaged in plots or attacks utilizing CBRN weapons, agents, or materials.

10. Event Actor – Motive[16]

(EA_MOTIVE_*_A)*

This set of variables codes for known information about the primary criminal motivation of the threat actor associated with the recorded event.

Refer to the table in Section III.A.1 for details of field values.

NOTE: In the absence of any other information motivation should **NOT** be inferred from targeting choices.

[16] The values for this field, and the associated EA_SUBMOTIVE field are direct equivalents of the EA_IDEOLOGY field in the VNSA CBRN Event database.

11. Event Actor – Sub-Motive

(EA_SUBMOTIVE_A)*

This field records subsidiary divisions of the basic criminal character of the threat actor associated with the recorded event.

Refer to the table in Section III.A.1 for details of field values.

III. Appendix 1

A. Field Values

1. Specific Agent Codes

SPECIFIC AGENT NAME	CODE	SPECIFIC AGENT CODE	CODE
Acetic Acid (Concentrated)	100	Lewisite	134
Acetone	101	Mace	135
Aldrin	102	Malathion	136
Aluminum Powder	103	Mercuric Chloride	137
Ammoni/Ammoniac Acid	104	Mercury	138
Arsenic	105	Methanol	139
Atropine	106	Methomyl	140
Benzene	107	Methylene Blue	141
Brodifacoum	108	Mustard Gas	142
Bromine	109	Nicotine Sulfate	143
Butyric Acid	110	Nitric Acid	144
BZ	111	Nitrogen Mustard	145
Carbofuran	112	Osmium Tetroxide	146
Chlorine	113	Paraquat	147
Chloroform	114	Phenarsazine Chloride (Adamsite)	148
Chlorophenyl Silatrane	115	Phenol	149
Chloropicrin	116	Phosgene	150
Cobalt	117	Potassium Chloride	151
CS Gas	118	Potassium Cyanide	152
Diethylene Glycol	119	Sarin	153
Diisopropyl Fluorophosphate	120	Sodium Chlorate	154
Dimethyl Sulfoxide (DMSO)	121	Sodium Cyanide	155
Drano	122	Sodium Hydroxide	156
Endrin	123	Sodium Hypochlorite	157
Fluoroacetamide	124	Sodium Monofluroacetate	158
Halothane	125	Sulfur	159
Hexamine	126	Sulfuric Acid	160
Hydrazine	127	Tabun	161
Hydrochloric Acid	128	Talc	162
Hydrogen Cyanide	129	Tetraethylammonium Bromide (Tetranium)	163
Hydrogen Fluoride	130	Tetramethylene Disulfotetramine (TETS)	164
Hydrogen Peroxide	131	Vinegar	165
Ketamine	132	VX Nerve Agent	166
Lachrymatory Acid; Pepper Spray	133	Warfarin	167

SPECIFIC AGENT NAME	CODE	SPECIFIC AGENT CODE	CODE
Hydrogen Sulphide	168	Radium-226	306
Hydrogen Phosphide / Phosphine	169	Strontium-90	307
Vinyltrichlorosilane	170	Tellurium	308
Cypermethrin	171	Thorium-232	309
Abrin	200	Tritium	310
Aflatoxin	201	Uranium-235	311
Bacillus Anthracis	202	Uranium-238	312
Bacillus Licheniformis	203	Phosphorus-32	313
Bacillus Subtilis	204	Iodine-125	314
C. Botulinum Toxin	205	Unknown Biological	406
Cobra Venom	206	Unknown Chemical	407
Coxiella Burnetii	207	Unknown Nuclear	408
Digoxin	208	Unknown Radiological	409
Ebola	209	Unknown Acid	410
Escherichia Coli	210	Unknown Cyanide Salt	411
Foot and Mouth Virus (FMV)	211	Unknown Gas	412
Hepatitis C	212	Unknown Pesticides	413
Human Immunodeficiency Virus	213	Unknown Poisons	414
Influenza	214	Unknown Nerve Agent	415
Mycobacterium Tuberculosis	215	Sewage	420
Ricin	216	Cyanic Acid	421
Salmonella Typhi	217		
Salmonella Typhimurium	218		
Solanine	219		
Staphylococcus	220		
Strychnine	221		
Tetrodotoxin	222		
Vibrio Cholerae	223		
Yersinia Pestis	224		
F. Tularensis	225		
C. Tetani	226		
Epsilon Toxin	227		
SARS-CoV-2	228		
Americium-241	300		
Americium-242	301		
Cesium-137	302		
Iridium-192	303		
Monazite-Ce	304		
Plutonium-239	305		

2. Specific Delivery Mechanism Codes

CODE	SPECIFIC DELIVERY MECH
-99	Unknown
0	Not Intended for Delivery
1	Aerosol canister
2	Agent contaminated non-explosive weapon (knife, bullet etc.)
3	Latent
4	Contaminated Beverage Product
5	Contaminated Food Product
6	Contaminated Food/Drink
7	Contaminated Food/Drink (Restaurant)
8	Contaminated Pharmaceuticals or toiletries
9	Drop agent from airplane (or other flying objects)
10	Explosive rigged with CB agent
11	Facility attack (non-suicide)
12	Fan sprayer
13	Handheld sprayers (not aerosol canister) or directly throwing the agent
14	Injection of agent
15	Lotion, cream or other spreadable material
16	Mail
17	Nuclear Reaction Device
18	Radiological Dispersal Device
19	Reaction Device (Chemical/Biological)
20	Stationary aerosol dispersal device
21	Suicide bomb (non-vehicle)
22	Suicide facility attack
23	Vehicle based IED
24	Vehicle sprayer system
25	Ventilation/HVAC system
26	Water Supply

3. Motivation Codes

MOTIVE - TYPE		MOTIVE - SUBTYPE	
CODE		CODE	
1	Criminal	1	Extortion
		2	Grudge
		3	Personal / Idiosyncratic
		4	Profit
		5	Unknown
8	Unknown	60	Unknown

The motivation and motivation sub-type variables allow tracking of a threat actor/alleged threat actor's observed or declared motivation for carrying out the event leading to inclusion in this database. These do not describe the actor's motives for selecting a CBRN agent or weapon as opposed to a more conventional weapon. That is addressed elsewhere. Given the nature of the inclusion criteria these motivations are non-ideological in nature. As is the case with other elements of the database, care has been taken to ensure that there is no clash with the VNSA Actor or VNSA CBRN Event databases. The following sections describe in more detail the various values.

Some criminally motivated individuals or organizations will be driven by multiple factors in the preparation of their criminal acts while others may have very clear, simple, and direct motives. Any attempt to capture all of the potential nuances associated with each event, while better reflecting the diversity of human relations, would inevitably result in an excessively detailed schema with very few threat actors being captured in any particular category. Furthermore, in the absence of detailed, and honest, testimony, backed by confirmatory evidence, both of which are frequently unavailable in whole or in part, it can be extremely difficult to parse out the specific sub-motives of every actor. Accordingly, the Criminal CBRN Event Database has adopted an approach wherein the primary motive of the threat actor/alleged threat actor is identified and then presented. In the examples given above both would be represented as ethno-nationalists as their area of disagreement relates to policy approaches to be adopted subsequent to achieving their ethno-nationalist goals.

Both the motive and motive subtype variables are structured to allow room for expansion in the event that a need for greater detail in the motive sub-types or the motive fields is determined to exist.

a) Criminal

(EA_MOTIVE__CRIM_A)*

The threat actor's activities were motivated by criminal drivers such as profit, or personal factors such as rivalry, vengeance, obsessions.

This category can include individuals driven by the full-range of personal-idiosyncratic motivations or formal criminal organizations (such as the Russian Mafya, the Chinese Triads, and the Japanese Yakuza) whose primary goals are neither political nor ideological, but which instead engage in violent activities mainly in order to secure financial benefits, intimidate or eliminate competitors, or obtain revenge.

Appropriate use should be made of the **<EA_SUBIDEOLOGY>** field.

b) Unknown Motive

(EA_MOTIVE_UNKNOWN_A)*

The specific motive for the threat actor's activities is unknown, but available sources provide no indications pointing to ideology as a driver. If ideology is the primary driver for the threat actor/alleged threat actor's activities, then the event should not be recorded in the Criminal CBRN Event Database.