January 2025

ATAC
ASYMMETRIC THREATS ANALYSIS CENTER

Foundational Datasets

Global Chemical, Biological, Radiological, & Nuclear Data Suite & Portal

START
NATIONAL CONSORTIUM FOR THE STUDY OF TERRORISM AND RESPONSES TO TERRORISM

APPLIED RESEARCH LABORATORY FOR INTELLIGENCE AND SECURITY

UNIVERSITY OF MARYLAND

ABOUT THE AUTHORS

The author of this summary is Mr. Markus K. Binder, of the National Consortium for the Study of Terrorism and Responses to Terrorism (START), University of Maryland. Dr. Steve S. Sin, Ms. Alexandra Williams, Ms. Amanda Nagle, and Ms. Megan Rutter provided valuable assistance in the development of this report.

Questions about this report should be directed to Markus K. Binder at mkbinder@umd.edu.

ABOUT THE PROJECT

This report is part of the project, "Foundational Data: Global Chemical, Biological, Radiological, & Nuclear Data Suite & Portal," part of the Asymmetric Threat Analysis Center (ATAC), a joint program between START and UMD's Applied Research Lab for Intelligence and Security (ARLIS). ATAC is funded by the Department of Defense under award no. HQ003421F0481. Any opinions, findings, and conclusions or recommendations expressed in this report are those of the authors and do not necessarily reflect the views of the Department of Defense.

ABOUT START

The National Consortium for the Study of Terrorism and Responses to Terrorism (START) is a university-based research, education and training center comprised of an international network of scholars committed to the scientific study of terrorism, responses to terrorism and related phenomena. Led by the University of Maryland, START is a Department of Homeland Security Emeritus Center of Excellence that is supported by multiple federal agencies and departments. START uses state-of-the-art theories, methods and data from the social and behavioral sciences to improve understanding of the origins, dynamics and effects of terrorism; the effectiveness and impacts of counterterrorism and CVE; and other matters of global and national security. For more information, visit www.start.umd.edu or contact START at infostart@umd.edu.

ABOUT ARLIS

The Applied Research Laboratory for Intelligence and Security (ARLIS), based at the University of Maryland College Park, was established in 2018 under the sponsorship of the Office of the Under Secretary of Defense for Intelligence and Security (OUSD(I&S)). As a University-Affiliated Research Center (UARC), ARLIS' purpose is to be a long-term strategic asset for research and development in artificial intelligence, information engineering, and human systems. ARLIS builds robust analysis and trusted tools in the "human domain" through its dedicated multidisciplinary and interdisciplinary teams, grounded both in the technical state of the art and a direct understanding of the complex challenges faced by the defense security and intelligence enterprise. For more information, visit www.arlis.umd.edu/about-arlis or contact ARLIS at info@arlis.umd.edu.

CONTENTS

Executive Summary

This report describes one component of the larger Foundational Data research initiative. Over the course of two phases this effort entailed the updating of a number of existing databases describing aspects of the use of chemical, biological, radiological, and nuclear (CBRN) weapons by violent non-state actors (VNSA), the combination of a pair of previously separate pre-existing databases, the creation of a new prototype database dedicated to criminally motivated use of CBRN agents or materials, and the establishment of an online data portal providing public access to the full suite of START CBRN databases.

In addition to the above tasks the effort also extended to publication of in-house analyses of individual cases drawn from the database, and presentations derived from a broader assessment of elements of the data. Finally, START worked to make the databases accessible to outside researchers and government personnel to support academic research on terrorism and CBRN use, and the development of related public policy.

This report provides a basic description of the activities undertaken as part of this research effort before highlighting some core themes and insights drawn from the data speaking to VNSA CBRN threats and trends. Finally, the report will make some observations about what the available data suggests may be relevant future areas for research and analysis that can deepen understanding of the future VNSA CBRN threats.

Key accomplishments, insights, and some findings of this research effort are summarized below.

Key Insights

1. Military use of CW agents by insurgent groups is a recurring development of the past 40 years that has been demonstrating increasing levels of sophistication, both in terms of agents deployed and agent employment, over time.
2. Insurgent use or pursuit of CBRN agents is an under-studied phenomenon that has been counter-productively conflated with terrorist use for several decades.
3. VNSA threat actors generally lack significant chemical or biological skills or experience.
4. Sophisticated biological agent pursuit or use is extremely uncommon and limited to criminal activity involving insiders.
5. Abandoned and otherwise failed CBRN plots may be able to tell researchers and policymakers more about terrorist capabilities than successful attacks.
6. Criminal threat actors, some of whom have been conflated with ideological actors, are capable of undertaking attacks as, or more sophisticated as those mounted by ideological threat actors.

Recommendations

To support and sustain ongoing efforts to counter non-state actor pursuit and use of CBRN agents and weapons the following recommendations are offered:

- The START CBRN Data Suite should be sustained as a valuable public resource which supports relevant academic analysis while also supporting unclassified U.S. and other government outreach to partner nations and public-interest organizations.
- Conduct more research into military uses of CW by insurgent groups focusing on:
    - The impact of the use of relatively unsophisticated agents on the military operations (offensive and defensive) of state forces with limited resources for training or equipping forces to operate in a CBRN environment.
    - The resource requirements for an insurgent group to develop low-grade, but effective, CBR capabilities.
- Undertake more in-depth case studies of individual CBRN plots or attacks
- Undertake more research into the capabilities of criminal CBRN perpetrators.
    - The vast majority of ideologically motivated CBRN threat actors, including those that have successfully mounted attacks, have low technical capabilities or experience that align strongly with those of the majority of criminal actors
- Undertake research more tightly focused on terrorist weapon selection to develop a stronger understanding of processes and factors leading individual actors or groups to select CBRN over conventional weapons.
    - This research has the potential to be highly beneficial by expanding understanding of weapon selection more generally thereby providing potential gains in identifying interdiction and detection points.

Introduction

This report describes one component of the larger research initiative entitled Foundational Data for Asymmetric Threat Analysis. Over the course of two phases this effort entailed the updating of a number of existing databases describing aspects of the use of chemical, biological, radiological, and nuclear weapons by violent non-state actors, the combination of a pair of previously separate pre-existing databases, the creation of a new prototype database dedicated to criminally motivated use of CBRN agents or materials, and the establishment of an online data portal providing public access to the full suite of START CBRN databases.

In addition to the above tasks the effort also extended to publication of in-house analyses of individual cases drawn from the database, and presentations derived from a broader assessment of elements of the data. Finally, START worked to make the databases accessible to outside researchers and government personnel to support academic research on terrorism and CBRN use, and the development of related public policy.

This report provides a basic description of the activities undertaken as part of this research effort before highlighting some core themes and insights drawn from the data speaking to VNSA CBRN threats and trends. Finally, the report will make some observations about what the available data suggests may be relevant future areas for research and analysis that can deepen understanding of the future VNSA CBRN threats.

Note: All three of the databases reported upon as part of the CBRN Data Suite were compiled solely and exclusively from publicly accessible open-source materials. At no point has data collection utilized restricted-access governmental materials or non-publicly available grey literature. At no point has collection utilized interviews, or any other form of direct contact, with individuals involved in investigating the events that may be recorded within the database.

CBRN Data Suite Activities and Accomplishments

Research activity in support of the Foundational Data: Global Chemical, Biological, Radiological, & Nuclear Data Suite & Portal project was undertaken in two discreet phases

Phase One: Activities

In the first phase of the research effort, START executed three primary subtasks. These were:

1) Transition the pre-existing disparate datasets into a newly developed integrated Unconventional Weapons & Technology Global Chemical, Biological, Radiological, and Nuclear Data Suite (the CBRN Data Suite).
2) Bring the CBRN Data Suite up to date.
3) Develop and launch the Unconventional Weapons & Technology Global Chemical, Biological, Radiological, and Nuclear Data Suite Portal (the CBRN Data Portal).

Firstly, START revised the existing codebooks to simplify and coordinate the existing coding scheme and database structure for the two new datasets as a first step to establishment of the CBRN Data Suite. Steps were also taken to ensure compliance with contemporary standards for protection of personally identifiable information (PII)

Secondly, the pre-existing RANNSAD (radiological actors) and CABNSAD (chemical and biological actors) datasets were combined and revised utilizing the new coding schema for the CBRN Actor Database

Third, new collection was undertaken to continue to increase data holdings while preserving the currency of the datasets. New data was collected for both the Event and Actor databases for the period 2016 through to June 2022.

Fourth, research was undertaken to identify new data moving backwards in time to fill in any gaps in the previously collected data as well as identify any new cases that have come to light since the previous data collection cycle or that had been missed in previous research. This latter activity was necessary due to the not infrequent lag in publicization of relevant events, or data on associated individual actors. This effort covered the period back to January 2000.

Finally, the team undertook the development and implementation of a publicly accessible VNSA CBRN Data Portal to provide online access to the VNSA CBRN Event and Actor Databases.

Phase One: Accomplishments

1) Unified the CBRN Event and CBRN Actor Databases by eliminating divergent coding schemes for equivalent variables. The codebooks of both databases were carefully reviewed, and changes were made to both databases to ensure that where practical and appropriate identical coding was used.
    a. This has reduced workload by eliminating duplicative coding and reducing training requirements for personnel.
    b. The changes made represent an enhancement for researchers seeking to make use of both databases.
2) Combined and revised content from the pre-existing RANNSAD (radiological actors) and CABNSAD (chemical and biological actors) datasets utilizing the new coding schema for the CBRN Actor Database.
3) Updated the new CBRN Actor Database with new threat actor records based on new events added to the CBRN Event Database.
4) Developed and launched the Unconventional Weapons & Technology Global Chemical, Biological, Radiological, and Nuclear Data Suite Portal (the CBRN Data Portal).

Phase Two: Activities

In the second phase of the research effort, START executed four subtasks to bring additional value to end users.

First, new collection was undertaken to continue to increase data holdings while preserving the currency of the datasets. New data was collected for both the Event and Actor databases for the period May 2022 through to June 2024.

Second, research was undertaken to identify new data moving backwards in time to fill in any gaps in the previously collected data as well as identify any new cases that have come to light since the previous data collection cycle or that had missed in previous research. This latter activity was necessary due to lags in publicization of relevant events, or data on associated individual actors.

The third activity, comprising a major new effort, was the development of a non-ideologically motivated non-state actor CBRN event database to include associated data collection.

Fourth, the team undertook development and implementation of improvements to the first iteration of the VNSA CBRN Data Portal developed as part of the Phase One effort. These improvements addressed user interaction improvements and the development and implementation of additional data analytic and data visualization functionalities.

Finally, an ongoing effort was sustained for promotion of the newly available data portal via briefings and presentations to potential end-users and stakeholders in addition to responding to requests for information from U.S. Federal, State, and Local government agencies, U.S. and international academic researchers, and interested commercial businesses.

Phase Two: Accomplishments

1) Developed and launched the new prototype Criminal CBRN Event Database.
2) Updated the CBRN Event Database with new events for the period June 2022 to June 2024.
3) Updated the CBRN Actor Database with new threat actor records based on new events added to the CBRN Event Database and the Criminal CBRN Event Database.
4) Developed, trialed, implemented, and released user interaction improvements and additional data analytic and data visualization functionalities for the CBRN Data Portal.

A more detailed discussion of each of the databases included in the CBRN Data Suite follows below.

The VNSA CBRN Database

Overview

In its current form the VNSA Event Database records 593 distinct events across 106 variables covering the period 1990 to 2024. Events are recorded across a total of 65 countries, 41 of which were the target of attacks. Slightly more than 50 percent of all events, 298 of 593, were concentrated in the top five countries (USA, Iraq, Russia, Japan, and the United Kingdom) with the top 10 countries recording 68.5 percent of the events. Attacks were even more concentrated with the first 10 countries representing 76.1 percent of all attacks. Of the 65 countries recording events, the United States was the largest individually represented country with 21.1 percent of all events and 17.3 percent of all attacks.

Number of Attacks by Country		
Country	# Attacks	% of Total
USA	49	17.3%
Iraq	42	14.8%
Japan	27	9.5%
China	23	8.1%
Afghanistan	19	6.7%
Cambodia	16	5.6%
Russia	13	4.6%
Sri Lanka	9	3.2%
Colombia	9	3.2%
Syria	9	3.2%

Number of Events by Country		
Country	# Events	% of Total
U.S.A.	125	21.1%
Iraq	52	8.8%
Russia	50	8.4%
Japan	40	6.7%
U.K.	31	5.2%
Afghanistan	25	4.2%
China	24	4.0%
Israel	22	3.7%
Cambodia	19	3.2%
India	18	3.0%

Figure 1: Number of Events by Country

Chemical events dominate the dataset with 76.9 percent of all events involving at least one chemical agent, 22.3 percent of all events involving at least one biological agent, 9.6 percent of events involving radiological material, and 3 percent of events involving attempts to acquire nuclear materials. In 51 events, the threat actors explored both chemical and biological agents as part of their plotting. Of the biological events, 51 percent used or planned to use a toxin.

Confining the result solely to the 284 attacks or attempted attacks, 83.5 percent of events used a chemical agent while only 9.9 percent (28 events) employed a biological agent. No biological attack or attempted attack using anything other than a toxin has occurred since 2011. Radiological attacks or attempted attacks represent 1.7 percent of all events, with the last such event recorded as occurring in 2009.

A wide range of motivating ideologies have been associated with CBRN events with the breakdown illustrated in figure 2 below.

IDEOLOGY	ALL EVENTS	ATTACKS	SUCCESS %
Criminal[1]	43	12	27.9%
Ethnonationalist	126	56	44.4%
Islamist	199	70	35.2%
Sikh	3	0	0.0%
Cult	44	27	61.4%
Left Wing	41	28	68.3%
Right Wing	22	2	9.1%

[1] Some events suspected of being criminally motivated are included in the VNSA CBRN Event where, based on the details of targeting and surrounding context, there is reason to suspect that the motivation may have been, or included, an ideological element.

Anti-Abortion	22	22	100.0%
Animal Rights	11	8	72.7%
Environment	2	2	100.0%
Other	20	12	60.0%
Unknown	60	45	75.0%
	593	284	

Figure 2: Events by Ideology

For 519 events publicly accessible information is sufficient to determine the threat actor type associated with the event. The difference between these two sets of preceding figures is Individual actors represented 14.2 percent of all events while formal groups were 64.4 percent of the threat actors. Small autonomous cells, which are typically groups of 2-9 individuals acting in accord with an ideological motivation, but not under the direct operational control of a larger organization, accounted for 7.8 percent of all events. For the remaining 13.7 percent of events the threat actor type is unknown.

Of the 284 events involving an attempted or successful attack only 65 (31.3%) are known to have resulted in CBRN-related fatalities while 159 (56%) appear to have resulted in some CBRN injuries. However, in 28 of these events there is insufficient public information to determine the number of deaths caused by CBRN agents or materials, while in 38 events it is impossible to enumerate the number of individuals injured. Over the 35 years of attacks recorded in the database 546 individuals are known to have died from CBRN effects while at least 5,845 have been injured. However, given the number of unknowns the real numbers are likely higher.

Observations

Over the period studied the data shows that after rapidly increasing in frequency in the early 1990s, ideologically motivated CBRN events have been on a general downward trend since approximately 2000.[2] There are several years that diverge upward from this general trend, most notably 2005 and the period 2014 to 2017 while 2006 saw an anomalously low number of events. The last year in which more than 10 events of any type were recorded was 2017. Grouping the various event types into sub-categories can reveal some interesting patterns concealed within the overall trend.

[2] 1998 has an anomalously high total number of events reflecting the Chinese government reporting 22 events perpetrated by a single group that year. These events represent all but two of the total number of events reported by Chinese authorities for the entire period 1990 to 2024.

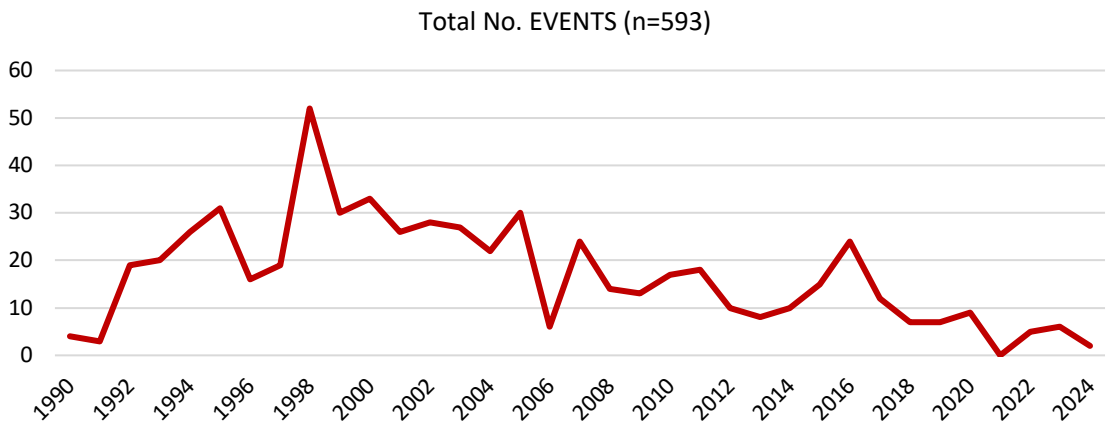

Figure 3: Total Number of Ideological CBRN Events by Year

Comparing plots that were abandoned or interdicted before progressing to an attack, so-called "non-attacks," with the pattern of events involving use or attempted use of an agent can be informative. In particular, it becomes clear that the number of attacks and the number of non-attacks is not closely aligned. Furthermore, it is also apparent that much of the "spikiness" of the data reflects surges and declines in the number of attacks while non-attacks vary less dramatically over time.

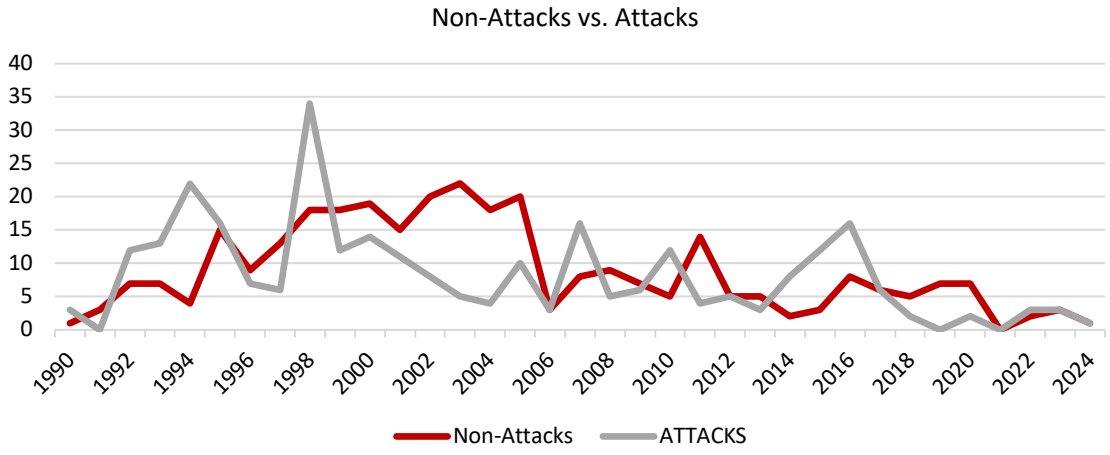

Figure 4: Non-Attacks vs. Attacks by Year

Apart from the large number of events reported out of China in 1998, which represents an exception from the overall pattern of events, there have been three distinct periods in which relatively high number of CBRN attacks took place. These are all clearly confined to specific geographic and ideological contexts. The first surge reflects the early 1990s activities of the Aum Shinrikyo cult in Japan. The second surge reflected the efforts of al-Qa'ida in Iraq in 2007. The final peak in activity resulted from the efforts of its successor organization, the so-called Islamic State in the period 2014 to 2017. A smaller surge in attacks in 2010 was concentrated in Afghanistan which saw nine of 12 total attacks for that year. Since 2021 all recorded attacks have occurred in Ukraine and Russia.

This last observation draws attention to a significant point which leaps out of the data: the salience of insurgency. At least 43 percent (122/284) of all attacks recorded in the database occurred in the immediate geographic and temporal context of an active insurgency with the active locations being Afghanistan, Cambodia, Colombia, Iraq, Russia, Sri Lanka, Syria, Türkiye, and Ukraine. Careful analysis of individual attacks in neighboring countries may increase these numbers. A clear association between insurgency and CW activity[3] may represent a significant future threat that warrants further detailed investigation, especially if recent examples are perceived to have demonstrated tactical or operational value in these weapons. Large, capable insurgent groups have repeatedly turned to consideration of CW agents over the last 40 years. Insurgent groups often have larger resources and a more stable operating environment that terrorist groups, potentially enabling them to pursue more advanced capabilities. As the process of globalization and industrialization increases global access to technical and personnel resources, the potential for U.S. or other national forces to encounter CBRN agents while engaged in irregular warfare activities is likely to increase over time.

The numbers of non-attacks underwent a fairly consistent pattern of annual increase from 1990 to 2005 after which there was a precipitous drop-off followed by periodic surges and declines. The first resurgence in activity covered the period 2008 to 2012, peaking in 2011 followed by a second revival of activity which lasted from 2015 to 2020, which was directly associated with the general expansion of external terrorist operations by the so-called Islamic State. This latter period saw 36 known abandoned or interdicted plots. These surges and declines appear to be aligned with enhanced enforcement efforts. Interestingly, both the surge and the decline in non-attacks lagged the increase and subsequent collapse of Islamic State attacks by one to two years.

The CBRN Event Database's inclusion of non-events, representing failed or abandoned plots introduces the potential to cast light on questions of terrorist intent, targeting choices, motivations, and perhaps most importantly, their capabilities that might be less visible if the database was solely focused upon successful attacks.

One noteworthy point that warrants further investigation is the observation that abandonment of a CBRN plot does not automatically result in abandonment of terrorist activity. Of the 32 CBRN plots known to have been abandoned by the involved threat actors 12 (37.5%) are confirmed to have resulted in a subsequent conventional plot. An especially complicated example was the series of plots in Sydney, Australia, directed by the Islamic State in 2017. Initial planning for a chemical attack was abandoned in favor of a failed attempt to place a concealed bomb on an aircraft after which the cell, under the direction of their Syria-based controller, pivoted back to attempting a chemical attack using hydrogen sulfide which was subsequently interdicted.[4] Another example is the 2016 case of a UK-based couple who initially planned a ricin attack before pivoting to attempting use of a TATP bomb.[5] It is possible, though not demonstrated, that there are significant numbers of additional events in which the perpetrators of successful conventional attacks explored the possibility of conducting a CBRN attack before

[3] There has been very little indication of significant BW or RN related effort by insurgent groups. Where interest has existed, it has tended to be purely exploratory in nature, operating at a very low level reflecting the limited technical resources available to the groups. Assessments of relative value may also be in play.

[4] Zammit, Andrew. (2020). Operation Silves: Inside the 2017 Islamic State Sydney Plane Plot. CTC Sentinel. 13(4) April. https://ctc.westpoint.edu/operation-silves-inside-the-2017-islamic-state-sydney-plane-plot/

[5] Casciani, Dominic. (2018). Derby terror plot: The online Casanova and his lover. BBC. January 8. https://www.bbc.com/news/uk-42370025

abandoning the effort. Research directed at this question might cast valuable light on factors contributing to plot abandonment, allowing governments to take actions to further complicate plot pursuit, potentially triggering CBRN plot abandonment, presuming that was determined to be an appropriate course of action.[6]

The VNSA CBRN Actor Database

Overview

The VNSA CBRN Actor Database is an actor (individual)-level database that brings together available open-source data on the demographic, educational, and experiential backgrounds of all identifiable individual non-state users and attempted users of CBRN weapons or devices. It includes details on the roles and motivations of the individual actors. The purpose of the database is to provide a resource that can contribute to understanding of the motives and capabilities of individual threat actors and how these relate to the pursuit and use (effective or not) of CBRN agents or materials. The database includes both ideologically and criminally motivated threat actors. Threat actors that have not been identified are as a matter of necessity excluded. Groups are not recorded as independent actors.

Many of the most interesting research questions potentially addressable by data recorded in this dataset encounter a problem with large proportions of "unknowns." Examples include educational background and prior experience with chemical or biological materials. This is an unavoidable consequence of the reliance upon open-source materials and the intentional avoidance of undertaking dedicated case studies of individual threat actors.[7]

Open sources such as newspaper accounts are often highly dependent upon material provided to them by public officials who are frequently uninterested in providing highly detailed biographical accounts of accused threat actors. Where non-official open sources do delve into biographical details this effort is frequently the purview of outlets with lower reputations for reliability. Official materials with the highest value for the database's purposes are often inaccessible for reasons of personally identifiable information (PII) or other privacy concerns. A particularly relevant example is pre-sentence reporting.

In its current form, the VNSA Actor Database records 541 distinct individuals across 50 variables over the period 1932 to 2024. Recorded actors conducted their activities in 47 known countries. Recorded threat actors are very unevenly distributed geographically with 34.6 percent (187) of individuals with known locations operating in the United States. The next most common locations are the United Kingdom with 7.8 percent (42) and Japan with 5.2 percent (28).

---

[6] It is conceivable that a government might determine that, given the risks of a CBRN vs conventional plot remaining undetected relative to the probability that such a plot would be successfully executed, it is beneficial to not take action that would divert threat actors from CBRN to conventional plots.

[7] Intensive case studies of individual threat actors that included interviews with incarcerated or released threat actors would have the potential to considerably enhance the value of the database but are outside the scope of the current research effort. The resource demands for such an effort would be substantial. More importantly there would be many important ethical issues surrounding human subject research that would need to be addressed before such research could be undertaken.

Threat actors most commonly pursued or used chemical agents, accounting for 76.9 percent (416) of threat actors. Biological agents were pursued or employed by 45.3 percent (245) of threat actors with slightly over half of them pursuing toxins. Radiological agents were rare with only 3.5 percent (19) of threat actors pursuing or employing this type of agent. Many threat actors explore multiple agent types before mounting an attack, or alternatively are associated with groups that engage in multiple attacks with different agents over a period of time, resulting in the total number of agents described being significantly higher than the number of actors recorded in the database. As an example, the Aum Shinrikyo group in Japan pursued both chemical and biological agents in the early 1990s.

Individual threat actors represent 34 percent (184) of those in the database with the remainder being either members of small autonomous cells (18.9%) or formal groups (47.1%). Ideology or motivation of the threat actors is described in figure 5 below.

IDEOLOGY	ALL ACTORS	INDIVIDUAL	CELL	GROUP
Criminal	178	136	36	6
Ethnonationalist	18	1	0	17
Islamist	168	11	42	115
Judaism	7	0	0	7
Sikh	9	0	0	9
Cult	46	0	0	46
Left Wing	23	1	0	22
Right Wing	56	12	13	31
Anti-Abortion	2	1	0	2
Animal Rights	2	0	0	2
Environment	0	0	0	0
Other	4	1	0	3
Unknown	27	21	6	0
	541	184	97	260

Figure 5: Events by Ideology

Level of educational achievement for individual threat actors is broken into four categories of less than high school (5), high-school education (38), some undergraduate education (51), and some post-graduate education (54). This category is unfortunately dominated by "unknowns (393). For those with identifiable educational and professional backgrounds the most common field is medical in nature, to include pharmacology. Microbiological and chemical engineering degrees are also prominent.

Observations

As noted above, the database is dominated by entries for individual threat actors active in the United States. Although language barriers might be anticipated to contribute to this effect these are, in practice, a relatively insignificant obstacle. Although it is possible that there are simply significantly more CBRN threat actors active in the United States than elsewhere it appears more likely that the primary source of this over-representation is the relative transparency of the U.S. justice system and associated public reporting. In many other countries public

reporting, or access to public records, is considerably more restrictive and individual threat actors may not be publicly identified at all.

Continued efforts to improve the comprehensiveness of entries for variables tracking threat actor education and prior experience with the agents or agent types that they pursued have the potential to make significant contributions to understanding of the level of prior expertise required to mount successful attacks, including attacks generating significant numbers of casualties. In this regard, it is noteworthy that 12 individual threat actors were able to execute plots that produced five or more fatalities, resulting in a total of 203 deaths, all of which were criminally motivated. Only one of these individuals was known to have an advanced education with the remainder assessed on the balance of the available public reporting as unlikely to have such.

The Criminal CBRN Event Database

Overview

In the course of conducting research for the CBRN Actor Database, the research team came across large numbers of purely criminal events, not all of which involved identified perpetrators. It was noted that many of these events generated, or had the potential to generate, numerous deaths or injuries. Due to their lack of an ideological component these events were excluded from all extant CBRN databases. However, many criminal threat actors employ the same agents as ideological threat actors, frequently with little or no regard for the potential to harm the public, or on occasion with the active intent to causing general harm. Notable agents employed have included chlorine, chloropicrin, and various toxins, not to mention a large range of other chemicals. The research team suspected that at a minimum there might be a significant overlap in terms of skills and capabilities, and access to resources between ideologically motivated lone actors and criminal actors that could be exploited to improve understanding of such phenomenon as acquisition pathways, targeting, and the potential for harm from the use of agents. In addition, it was noted that criminally motivated CBRN actions are more common for many of the threat actor types such as so-called disgruntled scientists, that have been a source of concern for CBRN-focused counter-terrorism researchers and officials.

Although the VNSA Event Database is designed so that it can include events that may possibly be criminal where there are indications of a potential ideological component, this can still result in significant CBRN events being excluded. As an example, four of the five toxin attacks targeting the U.S. President since 2012 have been unambiguously criminal in nature and are accordingly excluded from the VNSA Event Database. Simultaneously, due to their prominence and possibility of ideological elements, however open to question, some events are included in the VNSA Event Database that arguably would be much more appropriately recorded elsewhere.

The Criminal CBRN Event Database was developed as a phase 2 outgrowth of the VNSA Event Database on an experimental basis to explore the potential benefit of logging criminal events in addition to terrorist events. The Criminal Event Database has been established as a separate database from the current VNSA Event Database, but it was explicitly designed to be fully compatible with its progenitor. The database uses the same basic coding schema as the VNSA Event Database with the addition of a number of new field values to capture specific criminal activity details. The advantage of this approach was minimization of unnecessary effort in development of a new

database and ensuring future compatibility between the datasets. Taking this step also opens the potential for combining the two datasets in the future to provide a comprehensive Non-State CBRN Event Database.

Recognizing the limited resources available for this effort,[8] the initial iteration of the Criminal Event Database covers a limited period of time sufficient to support development and demonstrate its value for supporting research and analysis. Although the final volume of events recorded in the Criminal Event Database is significantly less than that of the VNSA Event Database, it represents a proportionately appropriate number for the period of effort and provides a robust foundation for future expansion.

In its current form the newly established Criminal Event Database records 71 distinct events across 106 variables primarily covering the period 2014 to 2023. A number of noteworthy outlier events are also included for the period 2005 to 2013, along with a single event for 2024. Events are very unevenly distributed geographically with 62 percent (44) of recorded events occurring in the United States. This disproportionate representation of the United States is likely a reflection of its relatively accessible court records and subsequent public reporting versus the relatively restricted nature of access to relevant records of criminal events in other nations and languages. It may be profitable for any follow-on activity to accept this constraint and initially explicitly limit itself to a focus on U.S.-based activity.

Chemical agents dominate the dataset with 62 percent of all events involving at least one chemical agent, 40.8 percent of all events involving at least one biological agent, and 2.8 percent of events involving radiological material. In three of the events the threat actors explored both chemical, biological, and radiological agents as part of their plotting. Of the biological events, all used or planned to use a toxin with ricin being the most common agent of choice at 69 percent followed by abrin at 20.7 percent. Confining the result solely to the 48 attacks or attempted attacks, 81.3 percent (39 events) used a chemical agent while only 18.7 percent (9 events) employed a biological agent.

Individual actors are the most common criminal threat actor, responsible for 87.3 percent of events. A single criminal organization was responsible for 7 percent (5) of all events. The 71 recorded events resulted in a minimum of 3,180 CBRN injuries and 64 deaths.

Observations

Preliminary analysis of the admittedly limited number of cases contained in the Criminal Event Database highlights several basic observations. Firstly, criminal actors are capable of inflicting large numbers of casualties. Troublingly, these large casualty counts are not always intentional, instead being the product of ignorance or indifference towards potential outcomes. It is worthwhile to note that the recorded casualty figures are undercounted as in a number of incidents no figures are publicly available for injuries.

Despite a lengthy trial, no indication was provided for the number of individuals injured in the course of the five deployments of chloropicrin in Hawaiian nightclubs by a criminal group from 2015 to 2017. Chloropicrin is a somewhat dangerous agent, especially in confined spaces, but it should be noted that the criminal organization

[8] Gathering data for the VNSA CBRN Event Database required approximately five years of initial effort followed by several years of additional effort for sustainment, to include the remodeling and updating undertaken as part of the currently reported activities.

involved also had access to the considerably more dangerous chemical agent Vikane through the termite fumigation company that was part of the overall criminal enterprise. It is not unreasonable to speculate upon the potential for an ideologically motivated actor to plan and execute an equivalent attack. The ease with which the organization was able to divert and deploy chloropicrin from legitimate uses should be concerning, as indeed should be their approach of burglarizing competing fumigation companies to supplement their stocks of chemicals.

The Hawaiian chloropicrin events highlight an additional element, the relatively high level of insider involvement. This insider involvement runs the gamut from simple diversion of materials, or the use of facilities and precursor chemicals, through to using insider access to mount an attack.

Although not directly equivalent to targeting terrorist events where targeted individuals are frequently chosen for their symbolic value to send a broader message, many of the recorded events involve individuals deploying chemical or biological agents against the public to indirectly punish or harm an employer or business rival. Attacks of this kind are much more likely to result in large numbers of casualties than attacks targeting specific individuals.

The research team anticipates that as it expands this database and undertakes more sophisticated analyses comparing criminal and ideological events further potentially valuable insights will be identified.

Conclusions and Recommendations

Over the course of the two phases the START CBRN Data Suite has been successfully expanded and updated in line with the original plan.

During the period of performance, the research team received numerous requests for access to the full dataset by government agency personnel, academic researchers, and commercial businesses as a result of being made aware of the CBRN Data Suite in the course of presentations by START personnel, by reading publications by START researchers or other researchers publishing using the databases, or through word of mouth. A list of the organizations is provided below.

U.S. State and Federal Agencies

Argonne National Laboratory	
DOD - Marine Corps	3rd Marine Div - CBRN Defense
Defense Threat Reduction Agency	Operations and Integration Directorate
Homeland Security and Emergency Management Agency	DC Fusion Center
New York City	Metropolitan Transportation Authority
Pacific Northwest National Laboratory (PNNL)	
U.S. Department of State	Office of WMD Terrorism
U.S. Secret Service	Technical Security Division
U.S. Air Force Air University	US National Guard CBRN Response Enterprise

International Governments and Organizations

Bundeswehr	
Interpol	Chemical & Explosives Terrorism Prevention Unit
NATO	Joint CBRN Defence Centre of Excellence
Spiez Laboratory	Organic Chemistry Branch
United Nations Office on Drugs and Crime (UNODC)	Terrorism Prevention Branch
World Health Organisation (WHO)	Biosecurity and Protection Unit

Commercial Businesses

Battelle	CBRNE Defense / CWMD Solutions
Emergent Biosolutions	
Fenix Insight	
International Security and Emergency Management Institute	
MIT Lincoln Laboratory	
RAND Corporation	
Tauria	

Educational Institutions

American Military University	
American Public University System	
California State University: Long Beach	
Forethought Institute	
Harvard Medical School	Disaster Medicine: Beth Israel Medical Center
Iowa State University	Industrial and Manufacturing Systems Engineering
Kings College London	Department of War Studies
Middlebury College	
Middlebury Institute of International Studies	Center on Terrorism, Extremism, and Counterterrorism (CTEC)
Missouri State University	
Oxford University	
Naval Postgraduate School	
Penn State University	
Troy University	
University of Central Missouri	Criminal Justice Department
University of East Anglia	
University of Health Sciences	CBRN Department
University of Nevada	
University of Rome	
University of Sydney	
Troy University	

CBRN Data Suite Publications and Presentations

START Publications

- Binder, Markus K. 'Tropical Nights, Burning Eyes: Chloropicrin in Hawaii'" in *CBNW Magazine* (8/24).
- Sin, Steve S. 'Emerging Biotechnology Capacity and Emerging Biosecurity Threats in Colombia and Chile.' in Susan Sim, Eric Hartunian, and Paul J. Milas (ed.s), "*Emerging Technologies and Terrorism: An American Perspective.*" U.S. Army War College Press. (4/24)
- Binder, Markus K. 'Pascale Ferrier and the Threat of "Bioterror"' in *CBNW Magazine* (11/23).
- Binder, Markus K. "CBRN Terrorism" for Oxford Research Encyclopedia of International Studies in collaboration with Dr. Gary Ackerman. 2023. https://doi.org/10.1093/acrefore/9780190846626.013.706
- Binder, Markus K. 'Novichok Terrorism: Prospect or Fever-Dream?' in *CBNW Magazine* (10/22).

External Publications

- Tin D, Cheng L, Shin H, et al. A Descriptive Analysis of the Use of Chemical, Biological, Radiological, and Nuclear Weapons by Violent Non-State Actors and the Modern-Day Environment of Threat. *Prehospital and Disaster Medicine.* 2023;38(3):395-400. doi:10.1017/S1049023X23000481

Presentations

- Binder, Markus K. Presentation to CBRNE Convergence 2024, "*Patters of Interdiction for CBRN Events: Can we gain insight into the effectiveness of interdiction approaches?*" Orlando, FL. October 30, 2024.
- Binder, Markus K. Presentation to NCT-USA 2024, "*Non-State CBRN Threats: Contextualizing the contemporary and future Non-State CBRN threat.*" Aberdeen, MD. September 4, 2024.
- Binder, Markus K. Presentation to CBRNE Convergence 2023, "*Significant Criminal CBRN Events: How different, if at all, is criminally motivated CBRN use from ideologically motivated use?*" Knoxville, TN. November 9, 2023.
- Binder, Markus K. Presentation to CBRNE Convergence 2022, "*CBRN Terrorist Motivations: What Do We Really Know? And What Don't We?*" Boston, MA. November 2, 2022.
- Binder, Markus K. Presentation to CBRNE Convergence 2021, *Bioterrorism: Conflated Concepts and an Inflated Reality*, Orlando, FL. November 4, 2021.

.

National Consortium for the Study of Terrorism and Responses to Terrorism (START)
University of Maryland, College Park, MD 20740
infostart@umd.edu
www.start.umd.edu