Models Assessing Terrorist Activities

DR. JAMES R. (BOB) JOHNSON AND DR ALEX POLYMENOPOULOS
ADB Consulting, LLC
2533 North Carson Street, Suite 5324
Carson City, Nevada 89706
UNITED STATES

Abstract: – Two models for estimating the levels of terrorist activities and threats to specific targets are described. They allow automated goal oriented collection and analysis of large amounts of data to generate a higher level of information than can be gained through a simple search. Studying interrelationships of model networks can help to increase confidence and provide a warning of increased terrorist activities.

Key words: model, terrorism, threat, assessment, knowledge discovery

1 Need for models

1-5 gigabytes [1] of textual materials are published daily containing pieces of information that report on terrorist activities and on pre-incident indicators occurring around the globe and in Greece. Analysts typically search small subsets of the total data published looking for hints and information, in their domain specialty area. It is only after an attack that subtle pieces of information show themselves as relevant indicators. As Vice President Cheney stated about September 11: *"If you put all those pieces together, I don't say you could have prevented September 11th, but there might have been some warning, had it been handled properly."* [2]

A model-based approach has many advantages over traditional methods. Each analyst has their own job focus, culture, business processes and life experiences which together act as biases on how the data are filtered. Such prejudices and information focuses could be minimized through the application of models. Models can be enhanced and capture the orthogonal information indicators that span the diverse nature of world events. Learning can be incorporated into models to expand their capabilities and minimize less significant conclusions. Sets of models can work together to present patterns that might otherwise go unnoticed. A large number of models on many topics can be graphically displayed. The triggered models, those that have data fitting the input requirements and mathematical relationships, can be marked. The resulting marked patterns would show a network of models that indicate specific threats or confirmed activities.

These models can be setup to operate automatically on data collected. The output of these models then provides the basis of a daily early warning report part of a daily situational report.

2 Model characteristics

Due to the extreme range of threats, methods used by terrorist groups and the variety of terrorist group behaviors, models must focus on a wide range of topics. However, they all have several characteristics in common. Models operate on data collected (usually text data), search for key words (names, places, events, and dates) and relationships between words. Models convert detected information into mathematical variables that can be operated upon and combined into useful metrics. The input parameters for these models are supplied by experts in given domains.

A key characteristic of a model approach is the ability is to link seemingly insignificant pieces of data into meaningful information. To accomplish this goal, models must initiate lateral exploration across diverse data sources. That is, look for indicators and events that are orthogonal to current thought. For example, analysts might be searching for terrorists transporting radiological materials through points of entry into the country. Such materials would be applicable for "dirty bombs". However, if the search was orthogonally extended to search for groups already in the country that had brought in such materials before the security infrastructure was in place that would improve detection. Another orthogonal search would look for indirect sources of funding such as drug trafficking or organized crime activities that could bring such materials into the country. Many lateral threads are instantiated in parallel.

In this paper, we talk about two types of models: 1) World Terrorism Metric [3] (WTM), which measures current terrorism activity and 2) Target Threat Assessment Model [4] which estimates threats by potential terrorist attacks. The WTM is an automated model that collects filters and combines indirect and direct measures of terrorist activities. The Target Threat Assessment Model combines input from a domain specialist with news to estimate the potential threats against locations or people.

3 World Terrorism Metric Model

The terrorist threat levels specified by the Department of Homeland Security (DHS) are meant to be warnings for all levels of government and the population. The DHS threat level seldom changes values without some very significant events.

The World Terrorism Metric (WTM) was developed to provide a continuous, daily assessment of the world terror level. The WTM provides an indicator of increased terrorist activities. It can induce analysts to increase awareness. Although computed daily, it could be computed more frequently, say every hour to provide more timely status. A corresponding metric could be developed for specific regions, countries, or types of organizations such as healthcare or building security.

The WTM is a weighted sum of news from major political, economic, news and terrorist reports collected using news from many Internet sources. The WTM has values ranging from about -35 to about +35, with negative values indicating low threat levels and positive values high threat levels. When the recently appointed leader of Iraq was assassinated, for example, the WTM value rapidly rose above 25, confirming an extremely high threat level. If proprietary data is available, then these sources could be applied to the input data stream as well.

The data is automatically collected and searched using a Perl script that gathers data and computes the WTM value using the model. Since all metric components comprising the WTM are stored, subsequent analysis can be performed on historically collected data.

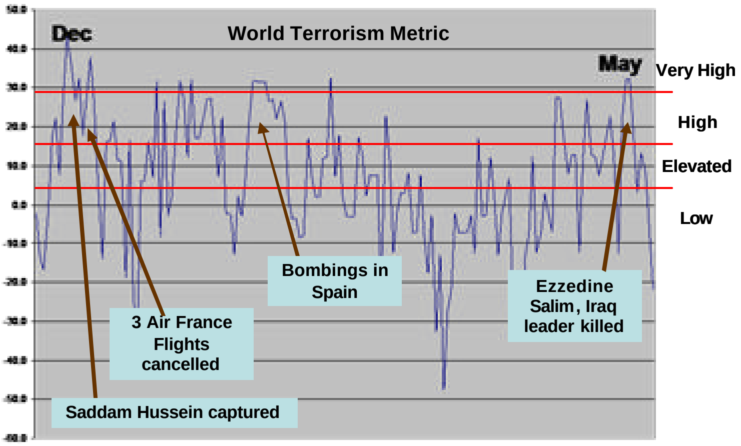


Fig 1. World Terrorism Metric from December 2003 to May 2004. Significant events are indicated in blue boxes.

Figure 1 shows the WTM plotted from December 2003 to May 2004. Thresholds for low, elevated, high and very high terrorist activity levels are marked by the horizontal lines. In cases where the WTM was very high, significant events are annotated.

3.1 WTM model components

Big events reported by the media and the Internet shape public perceptions. As an example, media reporting on the fact that no weapons of mass destruction have been found in Iraq has resulted in reduced American support for the "war on terrorism" and reduced support for the administration.

What sort of metric components are useful to monitor the world state and provide indicators of terrorist activities? Since media reporting has such a large impact, the selected metric components focus on news reporting on terrorism related activities and on economic indicators. Table 1 lists metric components that focus on the U.S. interests since most terrorist threats are against the U.S.

Table 1. Terrorism Metric components focused on the U.S. with primary area of measure

No.	Component	Measure
1	DOW Jones Average divided by 1000 sampled at the end of each trading day	Stock market behavior
2	Oil Prices per barrel divided by 3	Measure of supply and demand for energy source
3	VIX volatility index computed by the Chicago Board of Trade	Measure of uncertainty in options prices
4	Five-year note value multiplied by 10	Availability of Money
5	Number of terrorism related words in news stories	Global tension
6	Number of political related words in news stories	Global tension
7	Number of business related words in the news	Measure of democratic activities
8	Number of environmental disaster words in the news	Tension and stability measure
9	Number of words about nuclear, biological and chemical weapons in the news	Tension and stability measure
10	US Presidential cycle is modeled as a sinusoidal function where the ability to act is reduced in months close to an upcoming election	Ability to act

Other countries that are the targets of terrorism are Israel and any with significant presence, military or oil business in Muslim host nations such as Great Britain, Italy, Australia and Japan. Additional indicators that include threats against these countries are stock market indexes from those countries and news sources from these countries. Further, news sources from Muslim countries provide news of pre-incident indicators that are precursors to terrorism activities. The components in Table 1 serve as an example of a simple case for the WTM model.

For more robust capability, variances of economic variables show volatilities that are sensitive to terrorist attacks. Application of natural language processing extract linked relationships from published news.

Subjective measures such as the number of positive or negative news stories in each category further quantify the measure.

The components carry a certain level of information as measured by the standard deviation of the time data series. Natural language processing of the text from news stories allows interpretation of the text. For example, using data on Table 1 parameters from December 8, 2003 through 4 June 2004, standard deviations for the components were computed (Table 2).

Table 2. Averages and standard deviations of the WTM components for time series data collected and computed from December 8, 2003 through June 4, 2004.

Table 1 Component	Average Value	Standard Deviation
1	10.31	0.22
2	11.91	0.88
3	16.53	1.52
4	9.87	0.12
5	13.71	12.84
6	6.53	8.08
7	5.38	7.25
8	0.27	1.70
9	1.22	3.78

From Table 2, the ratio of the standard deviations to the averages is much lower (less than 0.1), than the word extractions (ratio > 1), for components based on the Dow Jones Industrial Average, oil prices, VIX and the five year note. Hence the variation in the news will cause greater sensitivity in the resulting WTM. Using the averages of the components, the WTM is +2.31.

For the economic indicators (components 1-4), if the ratio of the standard deviation to the average is taken as the measure of information, then the VIX and the oil indexes have the largest information content for the time period evaluated.

In this example, extraction of words is sensitive to the set of words searched. Terrorism related words (component 5) seem to occur with much more regularity than words about environmental disasters (component 8).

Each metric component is recorded daily. Analysis on each component and its behavior with terrorist activities can be used to refine weights as well as modify the components utilized.

3.2 Greek Version of the Metric – Terrorist Metric for Greece

A metric, similar to the WTM, can be defined for Greece. The Athens Stock Market index could be substituted for the Dow Jones Industrial Index. Further, Greek news web sites provide news on Greece and can be searched for the same words as in the World Terrorism Metric. The search could also be extended to search for words in Greek. The Prime Minister election timeline and impacts of political party politics would replace the U.S. Presidential election cycle. Interest rates for Greece can be substituted for the five-year note.

Additional components could be big events, such as the Athens Olympics. Proprietary data on economic indicators, criminal activities and arrests, involvement in NATO deployments, tension between Greece and surrounding states (Turkey, Balkan States), and the level of illegal emigrants could further localize and enhance the metric for Greece.

Each proposed component would need to be analyzed for correlations against actual terrorist activities in Greece or those that threaten Greek security. This analysis would result in proper definitions and weights associated with each component.

4 Target Threat Assessment Model

Targets at risk for terrorist attack include facilities, and people. A model of threats is valuable for positioning security resources. Such a model is quite complex due to a number of factors pertaining to terrorist group goals, accessibility of the target and the impact of an attack on the population, economy and government operations.

Developing targets model factors requires assessments from domain specialists as well as inclusion of news and information that provide indicators about potential terrorist actions. The Target Threat Assessment Model combines these two characteristics to provide a daily assessment and prioritization of threats for targets of interest.

4.1 Domain Specialist Assessment

Potential targets are important to terrorists for a variety of reasons. However, when actually planning a strike on a specific target, a terrorist or group of terrorists must go through an assessment process to evaluate the risks and potential for success. Domain specialists can go through the same process viewing the situation in the eyes of a terrorist. We employ the CARVER matrix [5] used by the US military as a foundation for target assessment. The CARVER acronym is defined by six measures for each target (Table 2).

Table 2. CARVER target assessment matrix components and their descriptions

Component	Description
Criticality	Criticality is a measure of the relative importance of the target, its importance to the functioning, well being and confidence of the population. Factors include: • Time – how rapidly taking out the target will affect operations or ability to respond or continue • Quantity – What percentage of the capability will be affected
Accessibility	Measure of how easily the target can be reached or infiltrated
Recuperability	Measure of the ability to recover if the target is destroyed
Vulnerability	Measure of the terrorist's expertise and means to destroy a target
Effect on the Population	Influence on the population if the target is destroyed
Recognizability	Degree to which the target can be recognized with respect to nearby objects or clutter

Using the CARVER rating for specific targets, governments can implement deterrence to reduce the "visibility" of a target. Multiple sources of the capability can be used to reduce the criticality and recouperability of the target. Security fences and guards can reduce the accessibility. Barriers and blast proof walls discourage terrorists by requiring more expertise and resources..

Governments can also publicize retaliation procedures to reduce the terrorist's willingness to attack specific targets.

4.2 Modulating the CARVER Ratings

These CARVER matrix components can be modulated by multiplying various modulating functions dependent on critical infrastructure information and published news about terrorist related activities pertaining to critical infrastructure categories.

Critical infrastructures (Fig 2) can be divided into fundamental and dependent resources. If terrorists can attack fundamental infrastructures, then the larger infrastructure can be affected.

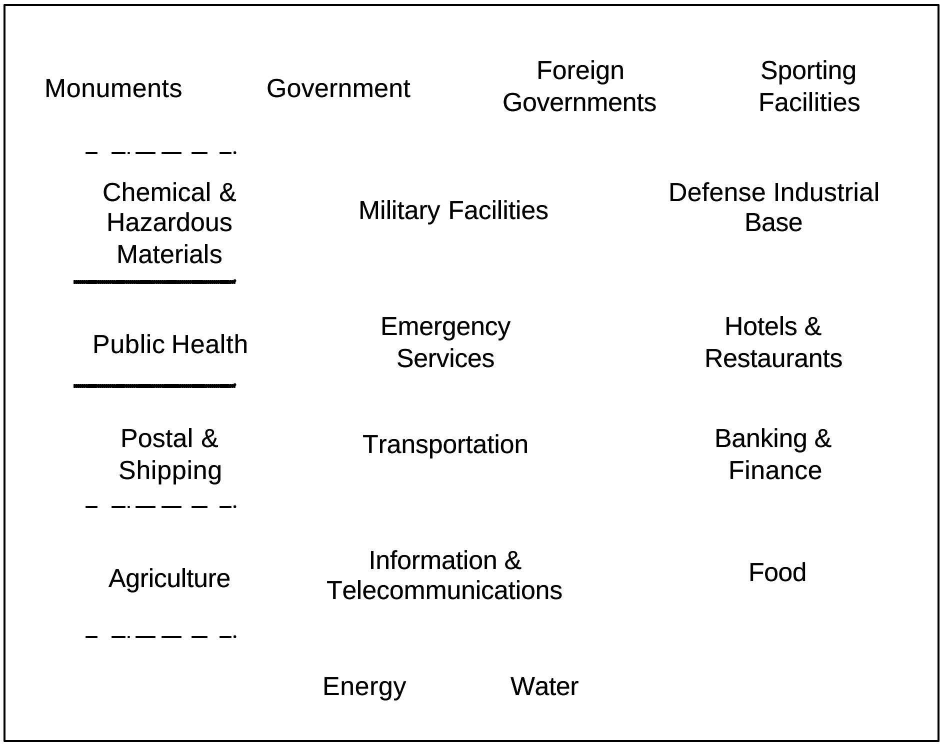


Fig 2.Critical infrastructure categories. Items in rows from the bottom show increased interrelationships and dependencies. Thus, if lower items are disrupted, the higher level items will be affected.

A Critical Relationship Matrix (CRM) is generated where the elements represent interrelationships between critical infrastructure categories. Each target is assigned to a critical infrastructure area. Linkages between these critical areas are used to refine the matrix. Government deterrents act as filters to reduce the CARVER ratings.

External dependencies represent target relationships through collaboration of nations or businesses or governments, and global threats issued by terrorist organizations. These are captured in a Global Dependency Database (GDD). The GDD is divided into two components: 1) those factors that are related to a target and 2) those factors that cross target boundaries or are global in nature. The target dependent GDD is attached to the target database. The global GDD structurally consists of lines of data with the factor(s) specified for a specific date or range of dates. In the current implementation, the global GDD is computed daily.

For example, a global factor is the release of an audio tape from Osama bin Laden urging terrorists to strike US targets during the Christmas holidays.

Finally, governments and businesses initiate deterrents and planned responses that can result in shifted focus away from particular targets to those that are more vulnerable. This data is captured in the target database. Published deterrents either reduce the visibility, vulnerability, accessibility or recognizability of a target, or reduce the time to recover or reduce the effects on the population if attacked. Deterrents are categorized by the following list:

- National and regional departments for Homeland Security
- Visible security forces
- Security barriers and sensors
- Cameras and other monitors at ports of entry
- Specialized detectors (dogs, sniffers, etc)
- Linked monitoring across all hospitals for biological agent outbreaks
- Command centers that proactively monitor for threats
- Communication's networks that improve response
- Strategically placed emergency response units
- Preparation of public notification alerts
- Extensive drills and exercises to educate emergency response teams
- Linkage between local response teams and military and coast guard units
- Intelligence capabilities to coordinate with other nations
- Procedures to effectively interrogate prisoners
- National Geospatial Information System mapping critical infrastructures, response teams and potential targets
- Coordinated evacuation plan
- Coordinated medical support from neighboring regions and states
- Trained special forces units to handle terrorism

Deterrents can be applied to single targets or groups of targets. Each deterrent is assigned weights (one for each CARVER parameter) that are applied to the existing CARVER matrix. The model is configured to allow multiple deterrents to be effective simultaneously. The weights for multiple deterrents are then multiplicative when applied to the CARVER values.

For example, the US Embassy in Athens is surrounded by a high metal fence, security cameras and guards. It is on a major road and has an entry gate on that road as well as the road intersecting that road. The building sits back about 15 meters from the fence. The embassy is very easy to see from the road.

Many US employees live near the embassy. To a terrorist, the US embassy represents a primary target. Additionally any US allies in the war against terrorism, as well as embassies of middle-eastern countries, are situated near the Greek Parliament and "White House" in Athens. Any potential targets, in the congested city of Athens, could severely stress the emergency response resources. Attacks on these targets could:

1. Provide a major message from al Qaeda;
2. Affect many hundreds of employees in each embassy as well as people in the neighboring areas;
3. Wreak havoc on a central area of Athens;
4. Severely stress medical emergency response;
5. Affect US and British security and intelligence coordination efforts for the Olympics for which the Greeks are dependent on;

On scales of 1 to 5, the CARVER measures for the US Embassy are assigned the following values:

Criticality:	5
Accessibility:	5
Recouperability:	3
Vulnerability:	4
Effect on Population:	5
Recognizability:	5
Total raw CARVER:	27

The Embassy is classified as a Foreign Government Building. There will be strong links to energy, water, computer and telecommunications, transportation, emergency services and public health. These dependencies will increase the target score.

4.3 CARVER modulation

Once the data has been collected, the mathematics for modulating the CARVER ratings and prioritizing the targets is carried out in the prioritization function (Fig 3).

The estimated reason for any threat is determined by looking for specific keywords in three diverse news sites (British, Greek and Australian). Six different sets of keywords are search. Each group is mapped into a threat category:

- General terrorist threat
- Political conflict
- Economic instability
- Environmental hazard
- WMD indicator
- Olympic security threat
- Specific target threat
- Terrorist group threat
- Intrusion threat
- Criminal threat

The CARVER ratings are first modulated by the target categories supplied by the domain specialist. There are mappings and weights assigned in a matrix for a number of critical infrastructures, including energy, water, information and telecommunications, agriculture, food supplies, postal and shipping, transportation, banking and finance, public health, emergency services, hotels and restaurants, chemical hazards, military, defense, monuments and historical buildings, government, foreign government and sporting. For a specific infrastructure category the infrastructure matrix modulates the CARVER ratings through a product of a weighted average of the matrix elements.

The modulated CARVER ratings at this point are independent of time. Temporal variations are taken into account through the use of news webcasts. News items, extracted daily, generate factors that are applied individually to each CARVER component. News is searched for word categories including but not limited to terrorism, weapons of mass destruction, Olympics, specific targets, terrorism groups.

The final CARVER rating for each target is computed as a sum of the individual components.

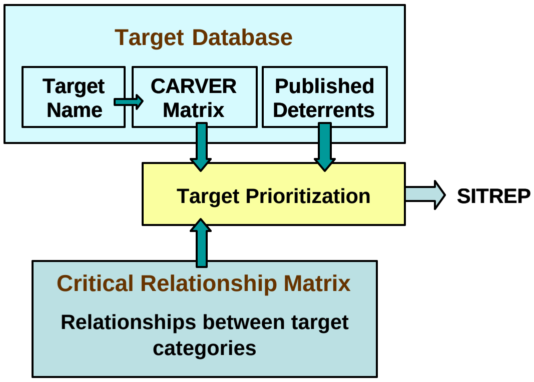
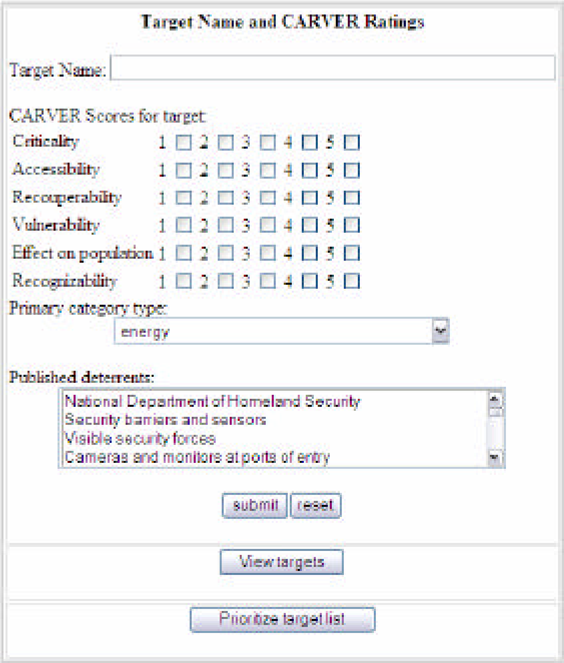


Fig 3. Data flow to modulate CARVER ratings and prioritize targets using the target database, the critical relationship matrix and the published deterrents. The output is provided to daily situational reports (SITREP).

4.4 Model Implementation

The model is implemented in Perl. There are two databases: one containing the Critical Relationship Matrix data and the other containing CARVER ratings for each individual target. Parameter input by domain experts is accomplished through a user interface (Fig 4). The Perl script accesses the databases, processes the data into final target ratings and sorts the targets based on the final ratings. The output of the sorted targets is written to a database for inclusion into a situational report. An example of the sorted threat output is shown in Figure 5.



Target Name and CARVER Ratings

Target Name:

CARVER Scores for target

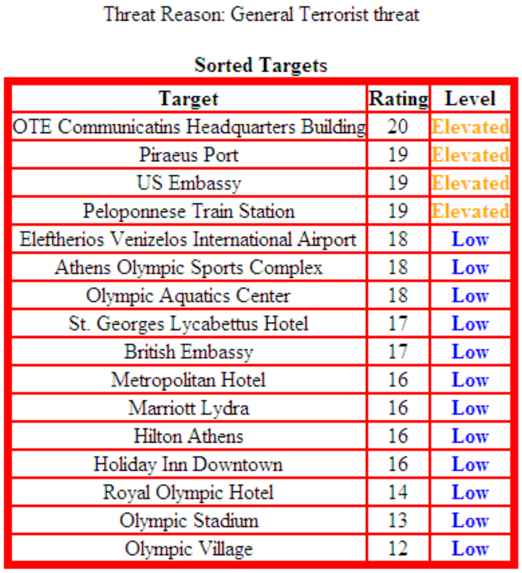
Criticality	1	□	2	□	3	□	4	□	5	□
Accessibility	1	□	2	□	3	□	4	□	5	□
Recouperability	1	□	2	□	3	□	4	□	5	□
Vulnerability	1	□	2	□	3	□	4	□	5	□
Effect on population	1	□	2	□	3	□	4	□	5	□
Recognizability	1	□	2	□	3	□	4	□	5	□

Primary category type: energy

Published deterrents:

National Department of Homeland Security
Security barriers and sensors
Visible security forces
Cameras and monitors at ports of entry

Fig 4. Data entry screen for the target data, raw CARVER ratings and published deterrents entered by domain specialists.



Threat Reason: General Terrorist threat

Sorted Targets

Target	Rating	Level
OTE Communicatins Headquarters Building	20	Elevated
Piraeus Port	19	Elevated
US Embassy	19	Elevated
Peloponnese Train Station	19	Elevated
Eleftherios Venizelos International Airport	18	Low
Athens Olympic Sports Complex	18	Low
Olympic Aquatics Center	18	Low
St. Georges Lycabettus Hotel	17	Low
British Embassy	17	Low
Metropolitan Hotel	16	Low
Marriott Lydra	16	Low
Hilton Athens	16	Low
Holiday Inn Downtown	16	Low
Royal Olympic Hotel	14	Low
Olympic Stadium	13	Low
Olympic Village	12	Low

Fig 5. Example output of target threat model, sorted by final score. Target classes include communications, transportation terminals, hotels, and Olympic facilities and venues.

At the top of the target threat output (Fig 4) is the reason for the threat (example, general terrorism threat). A table lists the targets currently included. Domain specialists can add new targets through the user interface. The threshold for low and elevated target threats is greater than 18.

4.5 Using the Models Together

Models can provide much more power when combined. The threats can be substantiated through the use of complementary models. Suppose the World Threat Metric and the Terrorism Threat for Greece show a very high level. Then the target threat assessment values can be increased. That means additional targets may increase their threat levels. Security forces can be deployed to enhance protection for those targets. We are researching methods for defining models such that their linkages yield additional actionable information.

5 Remarks

We have demonstrated that models can provide a level of information much more structured than raw data collected from a simple web search engine. In addition, models can extract critical information on single event occurrences.

Most knowledge discovery techniques are based on information extraction from databases [6][7]. In database search applications, the data is structured, bounded and potentially statistically uniform. Trends and statistical approaches can be applied. In contrast, searching for pre-incident indicators of terrorist events in open sources usually means looking for single event occurrences based on historical building blocks (e.g., types of targets attacks or methods used) or sequences of actions required to carry out an attack (e.g., biological weapons manufacturing and handling procedures).

Models and their integration into an operational network offer a solution to this problem. The models allow the data to be filtered and processed to produce more useful information that is of value to decision makers. Links between models help to enhance confidence or induce lateral evaluations of diverse and massive data.

These models typically incorporate input from domain experts and news from selected news sources.

6 References

[1] University of California at Berkeley, How much information? 2003, http://www.sims.berkeley.edu/research/projects/how-much-info-2003/execsum.htm

[2] CNN, "Cheney Blasts September 11 Critics.", 23 May 2002.

[3] James R.(Bob) Johnson, World Terrorism Metric, ADB Consulting Paper 2, Dec 2003.

[4] James R. (Bob) Johnson, Target Threat Assessment Model, ADB Consulting Paper 3, Jan 2004

[5] U.S. Army, JP 3-05.5, Appendix J, http://www.adtdl.army.mil/cgi-bin/atdl.dll/jt/3-05.5/3-05_5ak.htm

[6] Starlight Information Visualization System, Pacific Northwest National Laboratory, http://starlight.pnl.gov

[7] Han, J. and Kamber, M., Data Mining: Concepts and Techniques, Morgan Kaufman, 2001.