8th WSEAS CSCC (CSCC 2004)
Vouliagmeni (Suburb of Athens), Greece

Hotel ARMONIA: www.armonia.gr ,
1 Armonias str., 16671, Vouliagmeni, Athens, Greece

PLENARY LECTURE A': 08:00-08:45

1

Information Systems & Modeling for Counterterrorism

Dr. Alex Polymenopoulos
Principal Scientist
ADB Consulting, LLC

apolym@otenet.gr

8th WSEAS CSCC, Vouliagmeni, Athens, Greece

July 12th, 2004

Dear participants of the WSEAS Conference, Ladies and Gentlemen,

It gives me great pleasure to attend the 8th WSEAS Conference on Circuits, Systems, Communication and Computers. All the sessions are extremely important and that explains, why so many

distinguished experts from different countries and organizations have arrived to Athens for the occasion. I would especially like to thank Professor Mastorakis and WSEAS staff for their efforts to make this Conference possible.

This presentation along with it's associated papers which will follow in the Intelligent Systems session, would not have been possible without the excellent work, expertise, and insights of Dr. Bob Johnson, Chief Scientist of ADB Consulting and Dr. Kelley Stone, Director of Texas Homeland Security Department.

Let me take a moment, to briefly describe the two areas of our work. The first includes models we use to assess terrorist activities, and the other, a specific application that deals with an early warning system for bioterrorism also including modeling practices we have implemented in Texas, USA.

Models Assessing Terrorist Activities

Terrorism is a clear danger to the world. Terrorists launch attacks against population centers, economic and government infrastructures. They adapt to security and protective preparations continuously implemented. Sharing information, implementing deterrents and acquiring the ability to respond and manage incidents are key goals to protect populations and ways of life.

Conventional wisdom dicates that everything has changed because of September 11th and the subsequent anthrax attacks, and I think most of us know vulnerabilities still exist.

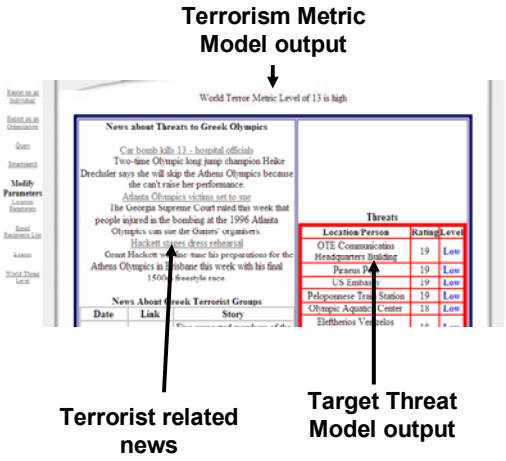
Defeating terrorism requires a more nimble intelligence apparatus that operates more actively within each country and makes use of advanced information technology. Data-mining and automated data-

analysis techniques are powerful tools for intelligence and law enforcement officials fighting terrorism.

3

Background

- ADB Consulting
  - Developed capabilities for analyzing large unstructured data sources (> 100 million files)
  - Automated Daily Situational Report capability implemented
- Models conceived and added to traditional methods
  - Structure collected data
  - Expand inquiries laterally across diverse disciplines
  - Focus information to support to decision makers



Example portion of a Daily Situational Report for threats on the Greek Olympics showing integrated model output

But these tools also generate controversy and concern. They make analysis of data—including private data—easier and more powerful. This can make private data more useful and attractive to the government. Data mining and data analysis are simply too valuable to prohibit, but they should not be embraced without guidelines and controls for their use. Policymakers must acquire an understanding of data-mining and automated data-analysis tools so that they can draft policy that encourages responsible use and sets parameters for that use.

Need for Models to Access Terrorist Activities

- Problem
  - Publish daily large text data volume: 1-5 Gigabytes of unstructured text materials
  - Search small subsets of data within specialty areas
  - Correlation not using raw data across domain specialties
  - Generate ad hoc hypotheses that are limited by analyst's knowledge base
- Advantages of model-based approach
  - Minimize prejudices, unbiased analysis of data
  - Allow what-if-then-else analyses
  - Look at data from orthogonal, structured viewpoints
  - Fit model parameters and learn from large data volumes
  - Integrate sets of models to provide a bigger and more complex picture than from a single model or analyst

1-5 gigabytes 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.

A model-based approach has many advantages over traditional methods. Each analyst has his 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, capturing 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 set up to operate automatically on data collected. The output of these models then provides the basis of a daily early warning report, which may be part of a daily situational report.

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 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, models should 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 useful 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.

5

Models:

- World Terrorism Metric (WTM), which measures current terrorism activity and
- Target Threat Assessment Model which estimates threats by potential terrorist attacks.

Example Models to be Discussed

	World Terrorism Metric Model	Target Threat Assessment Model
Automated data collection	√	√
Input by subject matter experts		√
Utilize news broadcasts	√	√
Assessment from terrorist viewpoint		√

The World Terrorism Metric (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.

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.

Model Definition

- Weighted sum of indicators that are collected automatically, daily
- Individual indicators are stored for subsequent analysis and refinement of the metric
- Threat levels for output are quantized to four levels
- Applicable for inclusion into web sites
- Could be computed at more frequent intervals, say every hour

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 a 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.

(More details will be presented in the presentation of the specific paper)

8

Selection of Components

- Example components are weighted for US threats
- Other components can be added or substituted to focus on another region (e.g., Greece)
  - Greek stock market indexes
  - Euro to Dollar ratio
  - Greek elections
  - Significant events such as the 2004 Olympics and World Cup
  - Criminal arrests and bombings
- Supplementary indicators can be identified that are sensitive to terrorist activities
  - Options put/call ratios
  - Activities of Islamic fund raising and religious centers
  - Issuing of videos from terrorist leaders

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.

9

Example WTM Components

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

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.

Targets at risk of 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.

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 used by the US military as a foundation for target assessment.

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

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:

10

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. The news is searched for word categories including but not limited to terrorism, weapons of mass destruction, Olympics, specific targets, terrorism groups.

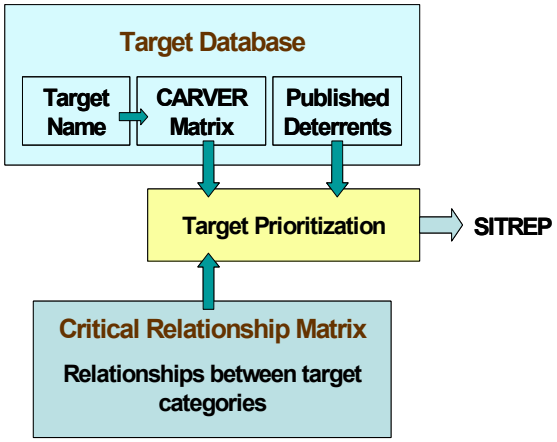
11

Model Description

- Utilizes the CARVER model in which subject matter experts can enter data about potential targets both buildings and people, from terrorist viewpoint
  - Criticality, recoverability, accessibility, recognizability, effect on population, vulnerability
- These parameters are modulated by other factors
  - Static
    - Nearness of targets to one another
    - Categories of targets and importance to economic, political, military etc
  - Dynamic
    - News and information about threats, targets, big events, etc
- Final scores are sorted by threat level
  - Thresholds used to specify High. Moderate or Low threats

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

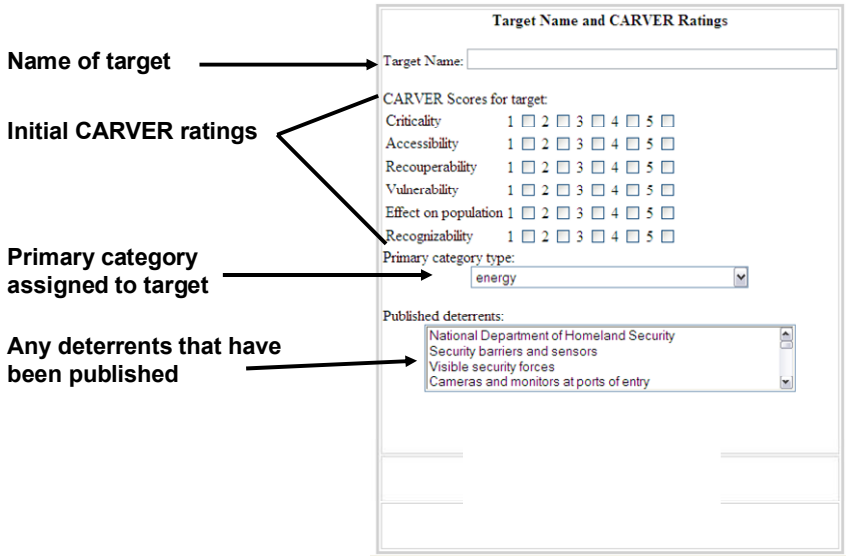
Data flow to modulate CARVER ratings and prioritize targets using the target database, the critical relationship matrix and the published deterrents. The output is provided to daily situational reports (SITREP). 12



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. 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 here:

13

Static Data Entry for Targets



At the top of the target threat output of the picture is the reason for the threat (e.g. general terrorism threat).

14

Prioritized Target List

Overall reason for threat → 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

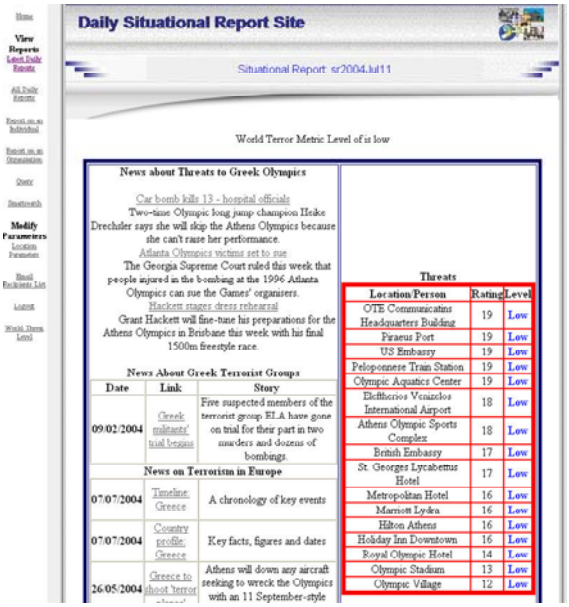
Name of Targets

Final prioritized rating

Quantized threat level

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.

15



Daily Situational Report Site

Situational Report: sr2004.jul11

World Terror Metric Level of is low

News about Threats to Greek Olympics

Car bomb kills 13 - hospital officials

Two-time Olympic long jump champion Heike Drechsler says she will skip the Athens Olympics because she can't raise her performance.

Atlanta Olympics victims set to sue

The Georgia Supreme Court ruled this week that people injured in the bombing at the 1996 Atlanta Olympics can sue the Games' organisers.

Hackett stages dress rehearsal

Grant Hackett will fine-tune his preparations for the Athens Olympics in Brisbane this week with his final 1500m freestyle race.

News About Greek Terrorist Groups

Date	Link	Story
09/02/2004	Greek militants' trial begins	Five suspected members of the terrorist group ELA have gone on trial for their part in two murders and dozens of bombings.

News on Terrorism in Europe

07/07/2004	Timeline: Greece	A chronology of key events
07/07/2004	Country profile: Greece	Key facts, figures and dates
26/05/2004	Greece to shoot 'terror	Athens will down any aircraft seeking to wreck the Olympics with an 11 September-style

Threats

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

16

Target Ratings Average, STD (June)

Target Name	Average	STD
OTE Communications Headquarters Building	18.7	1.59
Piraeus Port	18.3	1.45
US Embassy	18.3	1.53
Peloponnese Train Station	17.9	1.73
Olympic Aquatics Center	17.5	1.73
Eleftherios Venizelos International Airport	17.5	1.55
Athens Olympic Sports Complex	17.4	1.50
St. Georges Lycabettus Hotel	15.9	1.83
British Embassy	15.9	1.49
Metropolitan Hotel	15.3	1.87
Marriott Lydra	15.2	1.52
Hilton Athens	15.1	1.71
Holiday Inn Downtown	15.1	1.71
Royal Olympic Hotel	13.5	1.64
Olympic Stadium	12.1	1.16
Olympic Village	11.4	0.91

17

Analysis

- Absolute rating values do not change rapidly
- Re-ordering of targets primarily in the first decimal digit
- OTE Communications Headquarters, Piraeus Port and US Embassy always in the top three
- St. Georges Lycabettus Hotel has largest variance

Preparing for Bioterrorism through Widespread Information Sharing and Complex Modeling

The second part of my speech will cover an information technology application for early disease detection and for setting up linked prophylaxis clinics and emergency operations centers.

With any emergency public health scenario, hundreds of people could be affected before medical establishments discover the situation. An example of how fast a disease could go undetected is the SARS epidemic in Toronto where the city was shut down to visitors.

19

Goals

- Accelerated, semi-automated disease reporting
- Disease tracking and statistical analysis using models
- Coordinated emergency management alerting
- Coordinated response planning and monitoring
- Improved protection of citizens through early warning and guidance

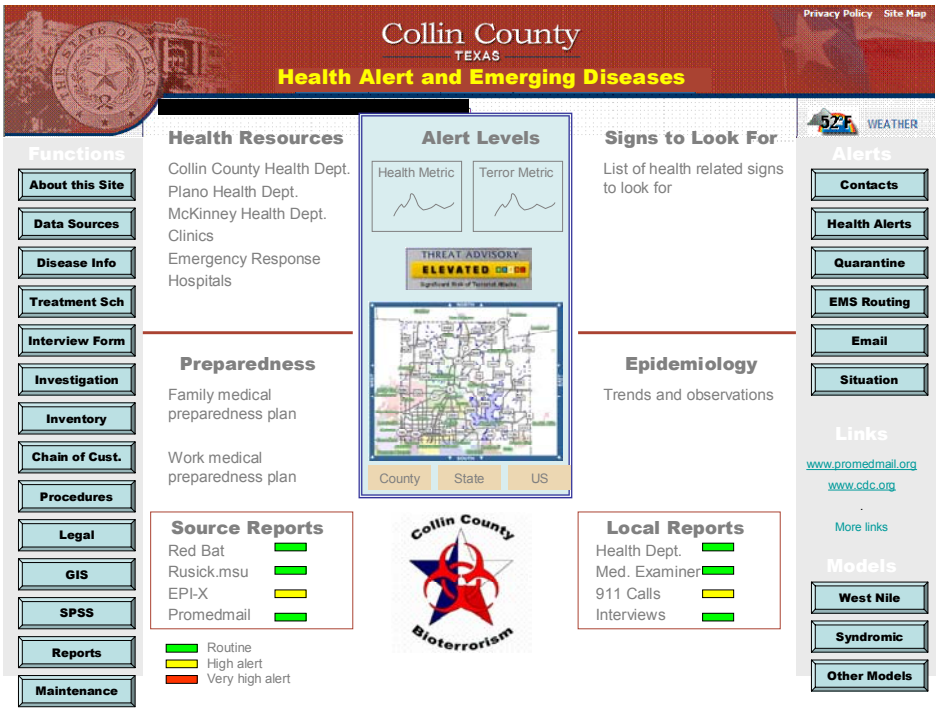
20

Improvement in Processes

Current		Proposed
Paper records	⟹	Digitized records
Patients and belongings not tracked	⟹	Tracking using bar codes through entire process
No scenarios	⟹	Scenarios used to develop procedures and training
Lack of bioterrorism training	⟹	Provide training and procedures for bioterrorism
Insufficient health coordination	⟹	Shared information and alerts between health professionals

Collin County, north of Dallas, Texas, has taken on these challenges by developing a strategic plan for creating working relationships with surrounding cities, counties, universities, businesses and State and Federal agencies. The primary focus there is on preventing

bioterrorism incidents using information sharing and modeling to provide early detection of possible events.



22

What is it?

- Secure web site managed by Collin County Health Department with Department of Homeland Security
- Collects emerging disease data from local and external sources
- Manages investigations to confirm cases
- Provides alerts and information to users and local population
- Accesses to treatment schedules, quarantine operations, evacuation planning
- Integrates information into Geospatial Information System to show where incidents and trends have occurred and locations of resources
- Coordinates emergency health response
- Provides daily public information bulletins in cases of outbreaks

23

Operational Concepts

- Routine
  - Continuous monitoring to detect disease outbreaks
  - Investigation input for confirmation of outbreaks
  - Preparedness through development of plans, procedures and draft public announcements
- Incident
  - Daily situational reporting of health incidents and treatments
  - Ingress/egress routing of EMS personnel
  - Coordination of medical resources
  - Public announcements
  - Evacuation maps for large incidents

Major hurdles addressed include:

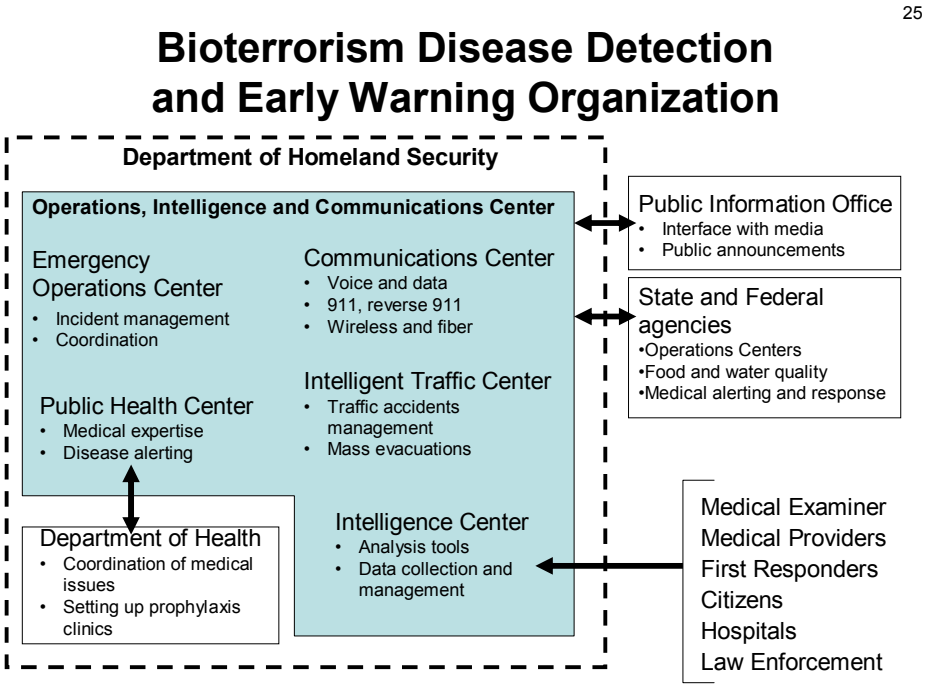
24

Major hurdles

- small Federal grants not aligned with County goals,
- gaps in collecting necessary health data to detect early indications of biological, chemical and nuclear incidents,
- lateral data collection and analysis for simulation, hypothesis and risk models to generate warnings of impending or possible terrorist attacks,
- identification of vulnerabilities and their dependencies to assess potential targets and consequences of attacks,
- early detection especially for biological attacks,
- real-time incident monitoring to coordinated responders and understand the unfolding of events, and
- sharing of data, information and maps.

Both detection and response require interoperable communications, real-time incident monitoring and integration and coordination of resources and decision support capabilities that operate over space and time as well as across participants. Developing a series of scenarios of possible attacks, or, incidents, is used to assess risks and generate courses of action.

25



The characteristics of this blueprint that integrates prevention, communications, early detection and decision support tools are illustrated here:

Characteristics and Attributes

26

Characteristic Category	Attributes
Focused on prevention and protection	• Develop preparations and courses of actions based on sets of scenarios (Proactive Preparation) • Continuous multimedia monitoring and collaboration of data that can lead to threat indicators (Proactive Monitoring) • Continuous daily situational reports • Vulnerability and dependency identification (Vulnerability Assessment) • Risk assessment and procedures for handling of risks linked to courses of action • Identify potential threats from analysis of terrorist profiles (Threat Profile Assessment) • Simulations and hypotheses that utilize observables to estimate threats
Interoperable, mobile communications	• Interoperable radio systems for first responders (Interoperable radios) • Interoperable IP-based wireless mobile systems linking radios and computer systems that travel with response teams (Interoperable, Mobile Networks) • Low profile transmitters that minimize potential terrorist disruptions • Redundant communications networks
Multidisciplinary monitoring and analysis	• Collect data from wide range of sources (Lateral Collection) • Analyze all media types (Multimedia Analysis) • Analyze using multidisciplinary teams and resources using lateral thinking and analysis techniques (Multidisciplinary Analysis)
Early warning solutions	• Daily situational reports tailored to decision timelines (Focused Reporting) • Health alerts input from Health Departments, World Health Organization and other agencies (Worldwide Alerts) • Terrorist threats against specific target types (Target Threats) • Real-time monitoring of incidents to measure how the incident is unfolding (Incident Rollout)
Geospatial information framework	• Geospatial referencing of data (Geospatial Referencing) • Interactive access to facilities, routing, and resources through maps (Interactive Maps) • Evacuation planning and action (Evacuation Planning) • Training reference (Training Reference)
Decision focusing models	• Models define types, formats and ranges of data for input and output (Data Defining Models) • Metrics of the quality of the information and algorithms to reduce uncertainties • Models come into play during specific circumstances (Model Patterns)

27

Healthcare Information Analysis

- Performed jointly by Intelligence Center, Public Health Center and the Health Department
- Data input via Healthcare Services web site
  - Secure access for each user group (Medical Examiner, Hospitals, Clinics, Medical Professionals, First Responders, etc)
  - Automated data from drinking water monitoring and food monitoring systems
- Data ingested into modeling software
  - Combination of models (Bayesian, rule-based)
  - Output most likely disease and recommended action
  - Compares to historical trends to detect anomalies
- Health Department carries out investigations
  - For bioterrorist related symptoms State and Federal agencies included in investigation
- Confirmed cases ingested into Center for Disease Control disease aberration software model for historical tracking
- Quarantine and prophylaxis actions taken as needed
- Public notices released through Public Information Office

28

System Functionality

Communications Services

- Interface with various Government agencies, emergency response and residents
- Maintain a 24x7 phone center
- Monitor deployed response teams
- Maintain a link to police 911 center

Investigator

- Investigate reports of food/water contamination
- Inspect restaurants/ issue permits
- Monitor water supply quality
- Work with health departments to understand contaminant and health threat
- Report findings to Analysis Group

Analysis Group

- Analyze data for trends and threats
- Maintain backup systems for facility
- Prepare alerts
- Support investigations with analyses and expertise
- Maintain databases on Biological and Chemical agents
- Detect, report and block network intrusions

Response Services

- Support Emergency Response Teams with technical information and expertise on food and water borne illnesses
- Prepare procedures and action plans pertaining to food/water protection
- Prepare public notices on procedures and plans

The system is organized around coordination centers. These centers can be built from scratch but more realistically can be virtual, utilizing existing facilities and resources thus helping to bring the new centers to an operational level quickly, while using minimal funding. These coordination centers are linked to emergency management organizations.

29

Coordination Centers and Functions

Coordination Center	*Functions*
Intelligence Center	• Headed by Collin County Director of Homeland Security • 24 x 7 continuous monitoring of threats • Verifies threats • Develops strategic plans such as evacuation plans, or mass casualty response plans • Issues alerts and public information to collaborating centers and outside organizations • Interfaces with politicians and Government organizations • Coordinates preparedness activities and exercises • Coordinated response • Coordinate communications resources • Intelligence data sharing across County, region, State and United States as necessary
Medical Coordination Center	• Headed by County Department of Health • Interfaces with area hospitals and out of area hospitals • Collects and monitors health threats and analyzes data for disease trends • Verifies health threats through case by case investigations • Interfaces with epidemiologists and clinics • Coordinates responses to mass casualties • Prepares public notices
Traffic Management Center	• Headed by Department of Traffic Management • Day-to-day management of traffic flow to minimize congestion • Coordinates response to traffic incidents and major chemical spills • Supports evacuation planning • Interfaces with Geospatial information System (GIS) Department to prepare ingress and egress routes for emergency response teams
Data Management Center	• Hosted by County GIS Department • Archive and manage databases • Serve out data and maps to other centers and organizations and public • Data sharing with surrounding regions, cities and State and Federal organizations
Private Sector Collaboration	• Develop associations of companies and businesses which exchange information on building vulnerability assessments and strengthening protection of infrastructures • Companies develop information that can be shared in times of crises • Companies work agreements to share information so that dependencies can be identified

Integration is a problem – for instance, most cities in the County use Motorola radios. The issue here is that how can cities inside Collin county communicate with emergency response groups that come from outside the County (especially Dallas County) where different radio systems are used?

In fact many cities and counties in the North Dallas region cannot directly communicate with each other. They must communicate through central switches and dispatcher units.

The solution which Collin County has adopted is to link all radio systems within the County to an Internet Protocol system allowing both voice and data information. This interface solution allows interoperability to external systems.

Collin County is utilizing high bandwidth fiber for high speed communications across County Government offices, and local hospitals. Links to hospitals across the State are also being negotiated and multiple networks will offer redundancy.

Collin County is also evaluating wireless technologies for widespread use. Wireless technologies provide interfaces with computer networks as well as existing radio systems such as Motorola's. They also operate from any vehicles responding to emergencies.

Wireless cameras and bio-sensors can be set up on fixed or moving positions and connected via a wireless network for remote monitoring of sensitive areas. This approach reduces the issues of laying cables and having video switches.

Of course all this equipment would be useless without models and hypotheses to test collected data for relationships. Without the need for much filtering involved, the models collect data for pattern identification, extraction of entities (names, places and organizations), and to classify structured and unstructured data.

Detection of emerging diseases caused by the outbreak of bioterrorist attacks is achieved through epidemiological monitoring and analysis. Data is collected from local hospitals, Medical Examiners, 911 calls, Federal and World Health Organization epidemic alerting sources and health departments. The Collin County Health Department

examines the data for trends and signatures of emerging diseases. They also perform validation of any threat by interviewing patients or investigating cases.

Analysts at the Intelligence Center take this information and initiate searches for possible correlations with possible terrorist activities. (Patient(s) recently entering the United States). Possible delivery mechanisms are investigated. Investigation of similar outbreaks is pursued.

Due to the dissimilar nature of data collected, its integration is accomplished using Bayesian models. A Bayesian network consists, in the bioterrorism case, of nodes corresponding to symptoms, possible diseases and methods of disease propagation. A probability table is associated with each node. Once specific symptoms are reported, the probability of specific diseases results from the model.

The data is correlated using simulations, models and GIS mapping tools to search for indicators and patterns. The data is also correlated with vulnerability and dependency databases to assess potential attacks against infrastructures such as water supplies, utilities, public buildings, and key businesses. Positive indicators are reported to law enforcement offices and federal agencies.

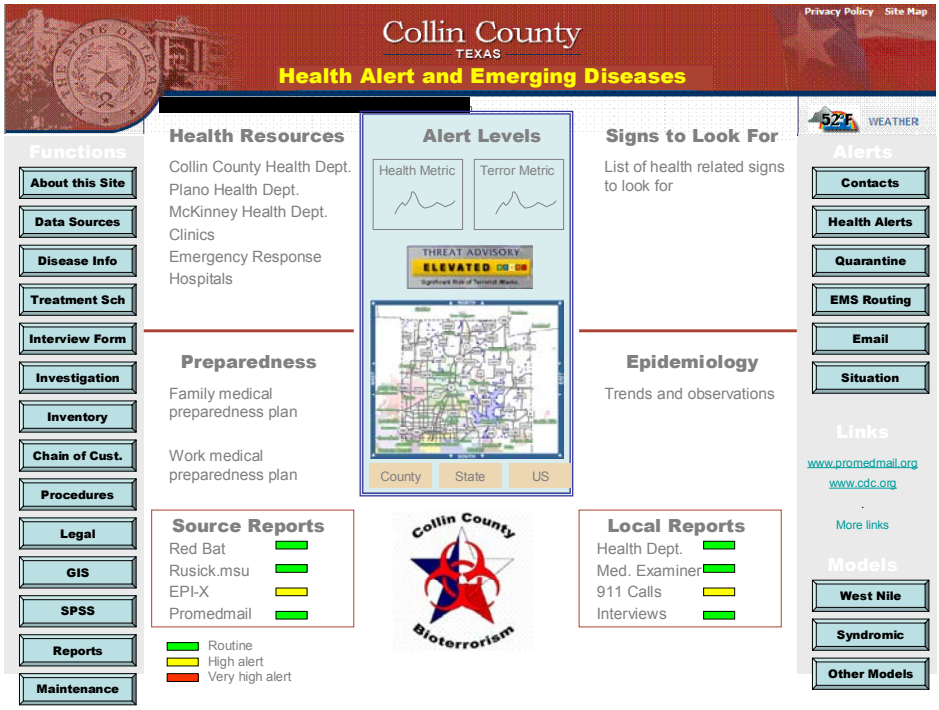
Also, an investigatory effort under way is to evaluate the potential of extracting information on threats from open and other sources. This approach utilizes the integration of four underlying software components: 1) data collection against selected types of web sites, 2)

indexing of collected files and other databases, 3) extraction on names and organizations and detailed reports on extracted items, and 4) information management and presentation for tailoring results to decision makers as well as integrating models to organize extracted information. Additional applications to display information in GIS formats, and visualization of complex data are added as an application/user interface layer on top of these four basic components.

In both terrorism and bioterrorism alert systems, the whole process described above all comes down to creating one thing – automated situation reports. The reports include lists of names and organizations with detailed reports and references, latest news about terrorism, prioritized target threats, important links as well as user annotations of new information that is immediately emailed to selected groups as the situation unfolds.

Requirements for the web site that the situation reports are based on, are still being refined prior to implementation. Two issues must be solved for adoption of the web site: 1) getting potential users to digitize their operational data, and 2) getting participants to use the web site on a daily basis as well as in times of crisis.

The web site will be accessible via web browser since this is the only quick and cost-effective approach that will give users' computers the capability to access the reports.



As for the web site itself, it has many access levels. Each user type (Fire Chiefs, First Responders, Health Departments, Hospitals, Medical Examiner, pathologists, and the public) will see a subset of functions tailored to their needs and access level. The information can also be tailored for a crisis level, reducing the amount of information during a crisis events to the utmost critical.

The Collin County Intelligence Center functions as the nerve center for the County,

- Interfacing with external organizations,
- Ensuring communications networks viability,
- Issuing public statements on the threat and its status,
- Coordinating evacuations,

- Coordinating responses and calls for regional, State and Federal assistance,
- Monitoring vulnerabilities, dependencies and determining possible targets,
- Generating GIS maps and products for dissemination,
- Running simulations and models to assess risks
- Determine options for decision makers

The geospatial information system (GIS) is the foundation for presenting information to participants and briefing the public and media.

GIS products include three dimensional (3-D) renderings of city areas to support emergency crew planning. Weather data is also rendered onto GIS maps and 3-D products. Finally, specialized model outputs such as plume spread, chemical spill drainage are represented in maps for understanding particular threats to the local population.

GIS is also interactive. Maps can be published electronically to computers and hand-held devices to allow emergency response personnel to point and click on specific intersections, buildings, and other features, and to retrieve the latest information about that location, or the latest events occurring there. Information can also be inserted into the GIS databases to inform other responders.

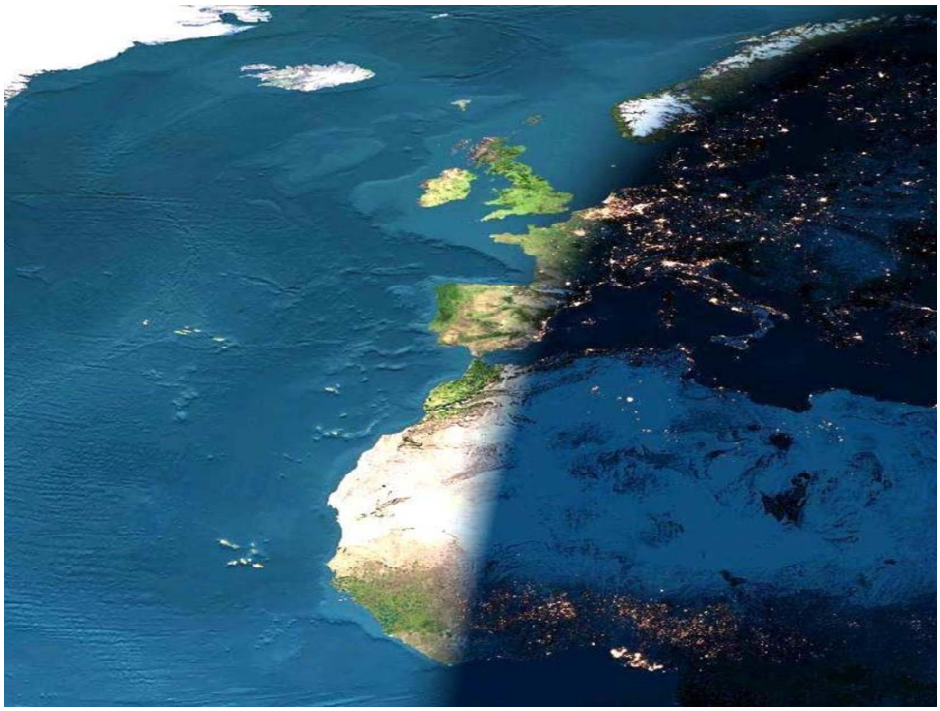
Medical bar code tagging technologies, can be used to tag mass casualty patients and their belongings so that medical personnel can view their status in real-time and view their location on GIS interactive maps. This same technology applies to equipment and resources as it moves around the County. Management of resources, and the logistics of getting the optimum resources to the right location, are enabled via GIS and tracking technologies.

Due to the complex interactions between the population, businesses, media and the crises that may arise, a table of consequences is constructed for each possible action taken by the first responders. Risks to the successful protection of the population are also tabulated against these actions. Critical infrastructures, their vulnerabilities and interdependencies, are taken into consideration. The continued functioning of basic infrastructures is critical to ongoing economic and living activities as well as to the recoverability of infrastructures damaged.

Simply building a system is not sufficient for assured protection. Education, training and procedures must be developed to ensure that stakeholders and participants understand their roles and responsibilities. The system should be tested and assessed at both the component and system levels.

The increased uncertainties caused by terrorists around the world, especially to western nations and large-scale sporting events (such as the Olympic Games or World Cup) make it imperative to develop

and implement capabilities to protect the population against such attacks. Such capabilities should be constricted with the types of disasters that occur from industrial accidents (e.g., chemical spills) and from natural disasters (e.g., earthquakes, tornadoes or hurricanes). Developing scenarios, models and procedures for non-terrorist related incidents, stakeholders can gain experience and confidence of their ability to minimize damage and loss of life when terrorist attacks occur. Continued infusion of technologies and process improvements will ensure that the best protection and preventative steps have been taken.



This light resonating from Athens, Greece, is the positive energy which beams off each, and every one of us here today. A universal omen perhaps, implying that a new future is to come, if we all work

together for the advancement of science and the prosperity of humanity.

Ladies and gentlemen,

It is needless to say that information technology can offer solutions that can help counterterrorism activities in several ways. To utilize the possibilities in the best possible way, a permanent interaction between theory and practice is needed. We all know that these two levels do not necessarily always meet. This conference shows that such an interaction is possible if we actively take up on the challenge.

Thank you very much.