Report #05-017

ASSESSMENT GUIDELINES FOR COUNTER TERRORISM

Hall, R.

CREATE REPORT
Under FEMA Grant EMW-2004-GR-0112

July 2, 2005

Center for Risk and Economic Analysis of Terrorism Events
University of Southern California
Los Angeles, California

DRAFT

Abstract

CREATE's (Center for Risk and Economic Analysis of Terrorism Events) is to improve our Nation's security through the advancement of risk and economic science in support of decisions to reduce the threats, vulnerabilities, and consequences or terrorism. CREATE accomplishes its mission through research and development of assessment methods and software, and through application of these tools to focused case studies, representing critical investment and policy decisions. This document describes a set of methods, models and procedures that comprise the CREATE Terrorism Modeling System (CTMS), which provides a systematic framework for conducting case studies, and which provides the foundation for the Risk Analyst Workbench (RAW) software tool. This report documents the methods used by CTMS to characterize threats and counter-measures, as well as the architecture adopted by the Risk Analyst Workbench (RAW) for supporting decisions in portfolio allocation, programmatic investments, targeted investments and acting on intelligence.

Acknowledgements

This material is based upon work supported by the United States Department of Homeland Security through the Center for Risk and Economic Analysis of Terrorism Events (CREATE) under grant number EMW-2004-GR-0112. Any opinions, findings, and conclusions or recommendations expressed herein are those of the author and do not necessarily reflect the views of the sponsors.

Table of Contents

1. INTRODUCTION

Terrorism is a criminal act that achieves political objectives through coercive attacks against ordinary people and their property. Major acts of terrorism against American interests have produced 4-5,000 fatalities over a period of roughly 20 years, beginning with the attacks in Beirut, Lebanon, of 1983. The majority of terrorist acts against Americans and their property have occurred outside our national borders. Nevertheless, the collection of domestic attacks at the World Trade Center, the Pentagon and in Pennsylvania on 9/11/2001 comprise more than half of the total fatalities, as well as more than half of the economic losses resulting from terrorism against America over this period.

Historically, the risk of death from terrorism has been small relative to many other causes. The single largest cause of death in the United States – heart disease – produces as many fatalities in an average two-day period as all major acts of terrorism produced against the United States in the 1983 – 2005 period. Homicides in the United States produce a comparable number of deaths in a 3-month period.

Despite the relatively low historical risk of terrorism-caused deaths, terrorism deserves special attention:

- The attacks on 9/11/2001 demonstrate that some terrorists have both the will and ability to commit massive attacks against our country, and that the potential exists for even more massive attacks than have occurred in the past.

- The coercive nature of terrorism can produce disproportionately large consequences relative to other human risks. These consequences include fear, avoidance of economic activities, economic disruptions and undesirable political outcomes.

- Unlike conflicts among nations, terrorism is an asymmetric threat, which cannot be readily countered through retaliation.

- The risk of terrorism is fundamentally adversarial and, therefore, actions that might be taken to protect against terrorism have the potential to induce behaviors that elevate the overall terrorist threat, or at least produce smaller than predicted gains.

CREATE's mission is to improve our nation's security through the advancement of risk and economic science in support of decisions to reduce the threats, vulnerabilities, and consequences of terrorism. CREATE accomplishes its mission through research and development of assessment methods and software, and through application of these tools to focused case studies, representing critical investment and policy decisions. Our goal is to develop and apply tools that identify and prioritize investments relative to the benefits that they produce (in the form of risk reduction), and with respect to their cost of implementation and operation. Just as importantly,

our goal is to develop and promote systematic methods of decision-making that result in coherent strategies for countering terrorist threats. This set of methods, models and procedures are encompassed in the CREATE Terrorism Modeling System (CTMS), as described in this document.

The remainder of this document is divided into five sections, covering these topics:

- CTMS general overview
- Terrorist threat classification
- Counter-measure Characterization
- Four-step modeling system
- Risk Analysis Workbench (RAW)
- Summary and conclusions

2. Overview of the CREATE Terrorism Modeling System

CTMS is both a methodology, and a software system, for assessing the risks and consequences of terrorism within the framework of economic analysis and structured decision-making. These are the essential elements of CTMS:

- Terrorism Threat Characterization (TTC) for problem definition and decision-making.
- Staircase model of terrorism intervention, which affords multiple opportunities to defeat a terrorist conspiracy, and considers feedback effects.
- Four-step modeling system, consisting of risk assessment, consequence assessment, emergency response and economic analysis.
- Integrated family of software tools, linked through the Risk Analyst Workbench (RAW) that utilizes a geographic-information-system (GIS) for data integration and display.

When fully developed, CTMS will support four classes of decision-making, as described below.

Portfolio Allocations: Distribution of a set budget among a set of alternative expenditures, such as allocation among drug development programs to counter biological weapons, federal grant allocations to states and localities, and funding distributions among alternative classes of threats or targets (e.g., comparing alternative infrastructure types or alternative weapon types). Portfolio allocation not only requires determination of whether an investment is worthwhile in its own right, but also whether it worthwhile relative to a set of alternative investments. Just as importantly in the case of terrorism, it also entails consideration of the interactive effects among investments, such as whether investments have complementary and synergistic benefits that exceed their individual benefits, and alternatively whether an investment in one area may have the counter productive effect of elevating the risk in other areas.

Programmatic Investments and Policies: Based on an identified threat and vulnerability, a programmatic decision addresses whether to broadly invest in measures to protect against a class of threats, such as whether to install counter-measures against missile threats on aircraft, whether to develop an information sharing program among law enforcement agencies or implement control measures on visitors to the United States. A programmatic investment may be achieved through regulations, budget allocations or policies that force or encourage participation among a range of organizations and individuals.

Targeted Investments: A targeted investment is intended to protect against threats at an individual location, such as installing a security barrier or monitoring equipment, employing security personnel or developing the capability to effectively respond to terrorist caused disasters. Targeted investment decisions are localized to the entity that would make the investment and reap the benefits from added protection.

Acting on Pieces of Intelligence: Based on a collection of evidence, a decision is needed as to whether to initiate an investigation, which could range from inspection of a cargo shipment or airline passenger to a criminal investigation of a suspected conspiracy. The decision amounts to determining whether the likelihood and significance of an illicit activity is sufficiently large to outweigh the likelihood and outcome of a false positive identification.

3. Terrorist Threat Characterization (TTC)

The CTMS methodology is intended to elicit consideration of the full spectrum of possibilities within a threat environment, with respect to the actions of both terrorists and counter terrorists. We begin this process by characterizing the threat. This step can be viewed as a problem definition phase that entails answering the general questions: "what are we concerned about happening." In the following section, we explore the subsequent question of "what can we do about this concern?" A concern could represent a set of terrorist objectives that might be achieved by any number of means. A concern could also represent a class of weapons, or possibly the actions of a particular group. By linking actions to concerns, our goal is to identify cost-effective strategies to counter terrorism.

Threat and Vulnerability

The threat characterization scopes the threats and defines a problem to be solved with a combination of four factors (Figure 1):

Weapons (e.g., a group of weapons that might be used in an attack)
Adversary Group or Tactic (e.g., a particular terrorist organization or a more general desire among terrorists to cause harm, for instance by attacking the viability and safety of air travel),
Targets (e.g., a set of nuclear power plants that need protection)
Scenarios The specific sequence of events associated with a terrorist attack, successful or otherwise.

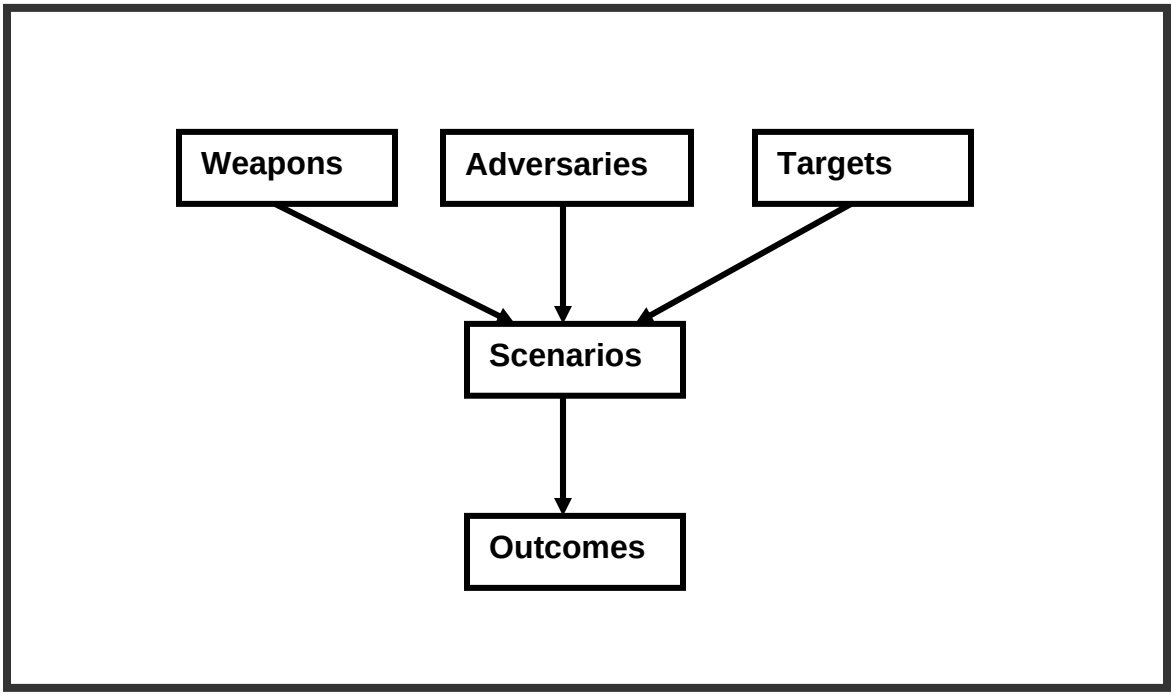


Figure 1. Terrorism Threat Characterization, Leading to Outcomes

Threats represent a collection of capabilities and intentions, whereas vulnerability represents the ease by which a threat can be executed. For simplicity, we view the combination of threat and vulnerability as simply the threat of a terrorist attack.

For the purpose of analysis, a threat should be sufficiently broad as to elicit a coherent and robust counter-terrorist strategy. It is best not to define an overly narrow threat, as the possibility of adaptation, on the part of terrorists, could be overlooked. To illustrate, the scope of a threat could be defined in the following way:

"*Protection against the shoot-down of domestic commercial aircraft in America by man portable, surface to air, infrared guided missiles,*"

which could lead to exploration of counter-measures designed to defeat an IR guided missile in the United States.

An alternative characterization could be this:

"*Protection against terrorists who wish to damage the economy, create fear and coerce changes in foreign policy by attacking commercial aircraft."*

This definition could lead to exploration of a much wider solution space, including measures designed to intervene against the positioning of many different types of weapons, and perhaps a greater emphasis on the adversaries than defeating a particular weapon.

The *CREATE Terrorism Threat Characterization System (CTTCS)* standardizes the description of threats with respect to four factors: (1) weapons, (2) adversaries, (3) targets and (4) scenarios. Each factor is associated with multiple attributes, which provide measures of loss potential (which might be viewed as either a threat or vulnerability). The intention of the CTCS is to elicit consideration of all important aspects of threats, and to help make effective comparisons to prioritize responses to threats. Initially we expect to provide a mechanism for experts to subjectively quantify the threat attributes, as will be described in a subsequent document. Eventually analytical tools or simulations could be used to quantify some attributes.

1. Weapons represent the means for inflicting damage. Terrorist weapons could be highly varied, ranging from weapons of mass destruction (such as biological and nuclear), to explosives, to cyber weapons. Weapons are classified according to the following attributes:.

- Nature of damage: degree to which weapon is capable of inflecting casualties and property damage.
    - Lethality/morbidity: degree to which weapon is capable of causing death and/or serious injury (physical or psychological), either through

the immediate effects of the weapon, or through the aftermath of property damage.
    - Property Scale: degree to which weapon is capable of causing property damage, to include causing property to be uninhabitable.
- Proliferation: sources for acquiring weapons (through purchase, theft or manufacture) and degree to which weapons are available to terrorist organizations
- Historical occurrence: whether there is a history of the weapon being used in terrorist acts, or other criminal acts
- Portability: size and signature of weapon and ease by which weapon can be transported and positioned without detection
- Versatility: Flexibility to use a weapon for a variety of purposes, and to use the weapon in a variety of environments.
- Sophistication: training required to acquire or construct, operate and maintain the weapon, and the number of people that would be needed to execute an attack.

2. Adversaries represent the individuals engaged in executing a terrorist attack. These are characterized by the following attributes:

- Persistence: degree to which individuals are motivated to execute attack in the presence of risk of apprehension or personal death or injury.
- Education and sophistication: degree to which individuals possess sufficient sophistication to successfully plan and execute attacks without capture.
- Commitment: degree to which individuals are committed to a terrorist conspiracy, and would not reveal the conspiracy to others.
- Mobility: degree to which individuals can move across borders without detection, including ability to acquire necessary documentation, and not arose suspicion.
- Motivation: a classification of terrorist organization according to its underlying motivations and intent.
- Scope and scale: size of organization, and geographic scope of its participants.

3. Targets represent the type of location where the attack occurs, as well as the opportunity and vulnerability for damage. Targets are classified according to the following attributes:

- Criticality: degree to which location is critical to the operation of the economy, or critical to the operation of the government.
- Human Occupation and Vulnerability: number of human occupants gathered in close proximity and their vulnerability to death or injury.
- Damage Vulnerability: degree to which target is vulnerable to damage in the event of a successful attack.

- Symbolism: degree to which the target has symbolic value, as represented by whether it is known worldwide, and whether it has iconic value to the American people.
- Protection: degree to which existing security around target can protect against the successful execution of an attack.

4. Scenario specifies a sequence of events associated with an individual terrorist attack or a series of terrorist attacks. Each of the attributes below could result from a randomized simulation of attacks.

- Event: a scenario is described by a suspected combination of weapons, targets and individuals.
- Success: a scenario may result in a successful attack on the part of terrorist, a failed attack, a false-alarm, or an intention deception (e.g., a hoax).
- Duration and dynamics: a scenario may have varying duration, and may entail a dynamic sequence of actions on the part of terrorist.
- Scope: a scenario may have varying geographic scope, and entail a set of attacks on geographically dispersed targets.

Terrorism Outcome

Outcomes represent the consequences of a terrorist event, which are measured in the form of human losses (fatalities and morbidities), financial losses, and symbolic losses (representing emotional consideration). These outcomes may be the intermediate steps of a terrorist group toward achieving political objectives.

- **Human Losses** can be the most devastating consequences of terrorism. Beyond the loss of loved ones, friends and workers through fatalities, illnesses and injuries -- such as severe burns, loss-of-limb, and loss of sight – fatalities and morbidities can be both life-changing and extraordinarily expensive to treat.
  - Fatalities: deaths resulting from the attack,
  - Morbidities: injuries or illnesses (physical or psychological) resulting from attack, accompanied by pain and suffering.
- **Financial Losses**
  - Direct property losses: immediate damage to property as a result of the attack
  - Indirect business losses: economic losses resulting from the dependence of economic activities on those entities that suffered immediate losses, including business interruption effects.
  - Costs of morbidities: costs of treating individuals who have suffered injuries or illness as a result of terrorism
  - Indirect morbidity costs: economic losses resulting from the inability of humans to continue their normal activities in the aftermath of an attack, resulting from either physical or psychological injuries.

- Response and recovery costs: costs of responding to terrorist events for the purpose of minimizing damages and minimizing injuries or fatalities.
- Costs of fear: economic costs due to the reluctance of individuals to engage in activities due to their increased fearfulness in the aftermath of a terrorist attack.

- **Symbolic Losses**
  - Emotional consequences: a subjective measurement of the emotional consequences of an attack, as determined in graphical imagery, symbolic value as a representation of American values, and identification with target.

As described in Appendix A, we propose a "*Terrorism Magnitude Scale*" (TMS) to represent the size of terrorist attacks. TMS is a base-10 logarithmic scale, with 1 representing an attack having minimal outcome, an 8 representing an attack with approximate maximal outcome (possibly a nuclear explosion in a major city), and a factor of 10 difference between consecutive numbers (e.g., a magnitude 4 event is 10 times worse than a magnitude 3 event). Logarithmic scaling provides a means to communicate outcomes from widely varying attacks, both those that occurred in the past and those that might occur in the future. Logarithmic scaling also enables order-of-magnitude comparisons, a useful feature because exact consequences are difficult to determine. Last, the scaling provides a familiar reference point, roughly comparable to the Richter scale for measuring earthquakes. It should be noted, however, that a Richter scale is not a measure of consequences (as we propose for TMS), but is instead a measure of the event that causes damage.

For illustration, the combined effect of the attacks on 9/11/2001 would be scored as follows on this 8-point scale:

Human:	5 = H
Financial:	6 = F
Symbolic:	6 = S

Because each additional point in the TMS corresponds to a magnitude 10 difference in outcome, the overall magnitude is approximated by the maximum of the three scaled attributes. Thus, we define the Simplified TMS (or STMS) as

$$STMS = \max\{H,F,S\}.$$

By this measure, 9/11 would be a category 6 event.

For contrast, the Oklahoma City bombing of 1995 would be scored as follows:

Human:	4
Financial:	3
Symbolic:	4

By the STMS, Oklahoma City would be a category 4 event, or a magnitude of about 1/100 of 9/11. A top of the scale event – category 8 attack – would be 100 or more times larger than 9/11, or 10,000 or more times larger than Oklahoma City.

4. Counter-Measure Characterization

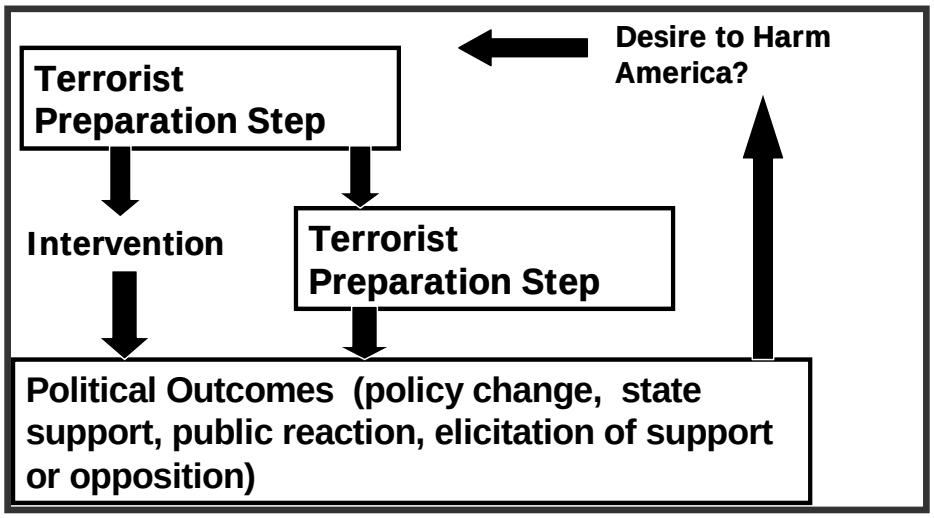
Counter measures represent the broad set of actions and investments used to reduce the likelihood of a terrorist action, or to reduce the adverse consequences of a terrorist action. Following the risk-based assessment approach, our goal is to identify those counter-measures that are effective against reducing the risk of terrorism, relative to their full life cycle costs. Effectiveness is measured by reduction in the likelihood of terrorist attacks, or reduction in the magnitude of terrorist attacks should they occur. Toward this end, a terrorist intervention strategy is described by these elements:

- Point of intervention relative to the steps of planning and executing an attack
- Direct costs associated with acquiring, operating and maintaining a counter-measure.
- Indirect costs or consequences associated with a counter-measure, to include efficiency losses due to delays and inconvenience, and efficiency gains due to improve technology.
- Human losses of counter-measure degree to which the counter-measure itself poses a risk of morbidity or fatality for humans, as could be the case in administering medications or vaccinations.
- Participants the set of organizations and individuals that would be participate in the implementation of a counter-measure.
- Effectiveness degree to which the intervention is known to change the likelihood of attacks (e.g., successful deterrence), likelihood of a successful attack, or outcome of an attack, and the set of threats for which a counter-measure is effective.

Staircase Model is a way to represent the point of intervention, as reflected in the sequence of steps followed by conspiracies in planning and executing terrorist attacks. These are the key features of the staircase model:

- Start to finish representation, beginning with the desire to harm America and ending with political outcomes.
- Feedback, accounting for the influence of terrorist actions, and interventions against terrorist actions, on the desire to harm America, and to join/form terrorist conspiracies
- Multiple intervention opportunities corresponding to the steps in planning and executing terrorist attacks.

Figure 2 illustrates a pair of steps in the stair case model. From the perspective of the terrorist conspiracy, success flows into a subsequent step. An intervention, on the other hand, flows out of the staircase. Either an intervention, or an actual terrorist attack, can lead to political outcomes, such as changes in policy, support or opposition of nations, or elicitation of public support, and all of these changes have some influence on the desire to harm America. Although not shown in the diagram, interventions can also lead to a change in tactics, which could



then create the need for alternate intervention strategies.Figure 2. Step Within Staircase Terrorist Intervention Model

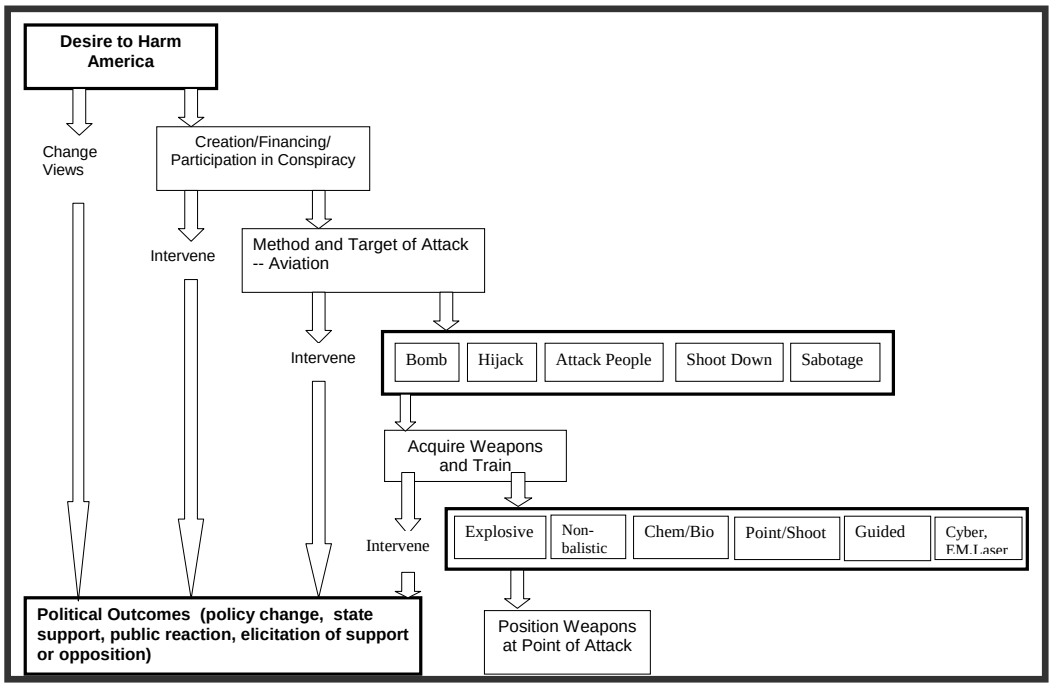


Figure 3a. Initiating Steps for Case of Aviation Attack

Although the staircase can vary from case to case, these are some of the key steps:

1. Desire to cause harm to America
2. Creation, financing and participation in conspiracies
3. Selection and planning for a method and target of attack
4. Acquisition and training for use of weapons
5. Positioning weapons at point of attack
6. Positioning perpetrators at point of attack
7. Synchronizing and executing attack
8. Defeat of counter-measures to attack
9. Immediate outcomes, in terms of damage and losses
10. Political outcomes
11. Feedback – particularly to desire to cause harm to America

The staircase is intended, in part, to highlight the importance of placing counter-terrorist strategies within the context of the full set of opportunities for intervention, as reflected in the above list of steps.

Figures 3a and 3b illustrate the staircase for terrorist threats to commercial aviation. In addition to the primary staircase steps, two additional boxes are shown to represent a step of options available to terrorists to cause harm to aviation, first with respect to a method of attack, and second with respect to a weapon of attack. The point here is to illustrate the need to be flexible to respond to a range of threats created by an adversary. In this regard, it is important to consider the underlying number of branches created by the choice of methods, targets and weapons. As one moves deeper in the staircase, the number of choices available to conspirators expands, making it increasingly difficult to defeat a terrorist attack. Thus, it may be more effective to focus on intervention in the initial steps -- particularly the formation of conspiracies -- than to focus on the later stages -- such as counter-measures designed to stop an attack once it has begun -- simply because the number of permutations is much smaller.

We use the staircase for the purpose generating ideas, both for how one might intervene against terrorists, and for anticipating how terrorist might respond to an intervention. It is also intended as a reminder that both interventions and terrorist actions must be considered within the environment of political outcomes, as this has been an underlying objective for the most catastrophic acts of terrorism in recent history.

Mapping Countermeasures to Threats A counter-measure's effectiveness should not be measured with respect to an individual threat, but rather with respect to a collection of threats, represented by multiple adversaries, weapons, targets and scenarios. A holistic approach is needed for two reasons: (1) to ensure that the solution is robust against a range of terrorist tactics and adaptations, and (2) to provide efficiency in the form of multiple uses for a counter measure.

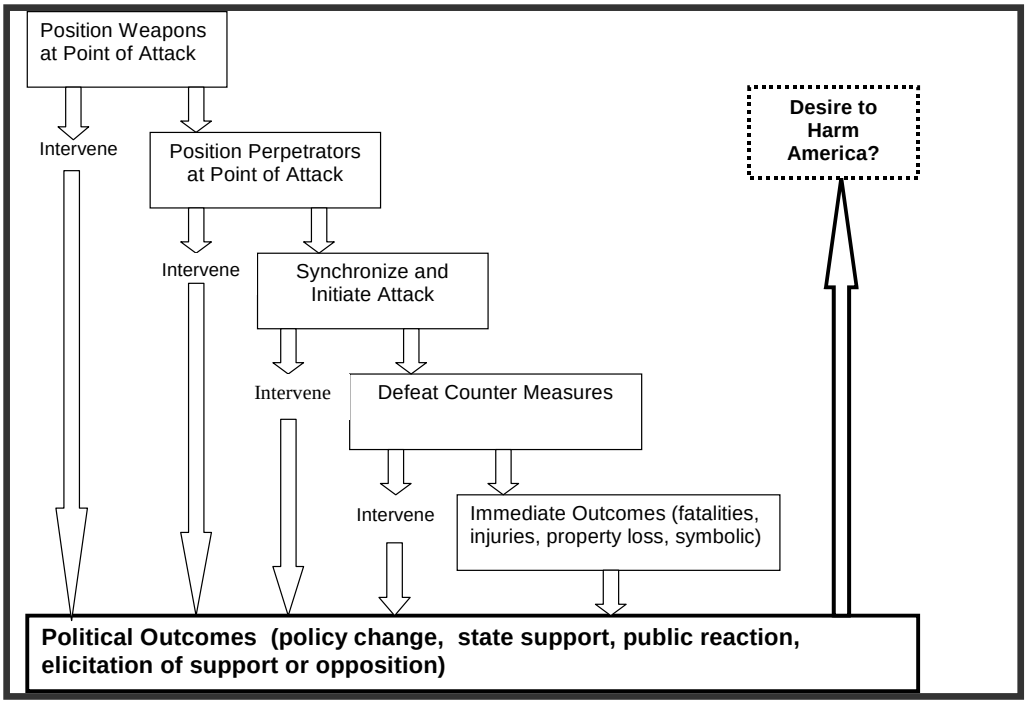


Figure 3b. Final Steps in Staircase Model

Counter measures can be evaluated by mapping the correspondence between individual threats and individual counter-measures. Relative effectiveness for each pairing of threat and counter-measure can then be explored, and solutions can be generated that cover the threat environment at minimal cost. An example of a preliminary assessment is provided in Table 1.[1]

[1] O'Sullivan, T. (2005). "External Terrorist Threats to Civilian Airliners: A Summary Risk Analysis of MANPADS, Other Ballistic Weapons Risks, Future Threats, and Possible Countermeasures Policies", CREATE Report.

TABLE 1: EXTERNAL THREATS TO AIRLINERS, VERSUS SELECT COUNTERMEASURES: GENERAL EFFECTIVENESS

	MANPADS Missile – Guidance System Type			Air or Ground Attack, Ballistic Weapons			Ground Attack
Countermeasure/ Survivability Measure	**Infrared (IR) or IR/Ultraviolet**	**Commnd- Line Of Sight (CLOS)**	**Laser Beam Rider (LBR)**	**Rocket-Propelled Grenade**	**Assault Weapons**	**Large-Caliber Sniper Rifle**	**Mortar Attack**
Aircraft-Based CM							
DIRCM*	Effective to Somewhat effective[2]	N/A	N/A	N/A	N/A	N/A	N/A
ATIRCM*	Effective to Somewhat effective[3]	N/A	N/A	N/A	N/A	N/A	N/A
Flares	- Same -	Some Effectiv	Ineffective?	N/A	N/A	N/A	N/A
Chaff	- Same -	Ineffective	Ineffective?	N/A	N/A	N/A	N/A
Non-reflec Paint or Anti-IR Gel coating	Some protection	If camouflage, some protect	N/A	N/A (some night protec)	N/A	N/A (or poss. night protection)	N/A
Pilot Survivability Flight Training	Some increase in survivab'ty (landing)	Some surviv. increase	Some surviv. increase	Some surviv. increase	Some surviv increase poss.	Some survivability increase (landing)	N/A
Aircraft redesign[4]	Poss. Some protect	Some protectn	Some protectn	Some protectn	Some protectn	Some protection	N/A
Airframe harden'g							
Titanium bathtub[5]	Pilot protection	Pilot protectn	Pilot protectn	Some protect	Protects pilots	Some pilot protectn	Some pilot protec
Fuel Tank Fire Suppression Syst.	Can reduce fire, increase time for safe landing	Reduce fire, allow time for safe landing	Reduce fire, allow time for safe landing	Reduce fire, allow time for safe landng	Reduce fire probability, allow landing	Reduce fire prob., allow more time for safe landing	Reduce fire prob. Allow safer pass. evacuation
Airport-Based CM							
Airport Perimeter Expansion	Small reduction in vulnerability	Small vulner. reduction	Small vulner. reduction	Poss. signific reductn vulner.	Poss. significnt vulner. reductn	*Significnt to Some* vulnerabil. reductn	*Some* vulnerabil. Reduction
Designated hardened Airports[6]	Some possible effectiveness	Some potentl effect	Some potentl effect	Effective	Some to Effective	Some to Effective	Some effect

*** DIRCM = Directed Infrared Countermeasures**

*** ATIRCM = Advanced Threat Infrared Countermeasure: Preemptive IR "lamp" transmitters not directed at specific missiles**

[2] Depends on the sophistication of both the MANPADS seeker and the directed infrared countermeasure.

[3] Not likely to be practical to deploy on civilian airliners, given the interference with ground communications systems, etc. More likely to be deployed some version of PLATO, aircraft-based airport perimeter IR protection system rather than on individual commercial jets. Overall effectiveness depends on the sophistication of both the MANPADS seeker and the infrared countermeasure.

[4] Particularly separation of or redundancy in critical systems needed in an emergency landing

[5] Protection for pilots, possibly critical instruments, similar to bullet-resistance "titanium bathtub" enclosure for pilots on A-10 attack aircraft.

[6] "Hardened" airports, in terms of increased security, possible permanent- or provision for temporary perimeter expansion, in the event of a confirmed first attack, to which to reroute airborne aircraft for safe landing in emergencies.

5. Four-step Modeling System

CTMS is implemented within CREATE's four-step modeling system, consisting of: (1) risk assessment, (2) consequence assessment, (3) emergency response and (4) economic assessment (Figure 4). As a whole, the modeling system is intended to support decision analysis with respect to such decisions as portfolio allocations, strategic or targeted investments, regulations or other counter-terrorism programs. The intent is to guide decision-making through structured analysis of terrorist intentions and capabilities, and cost-effectiveness of terrorist interventions.

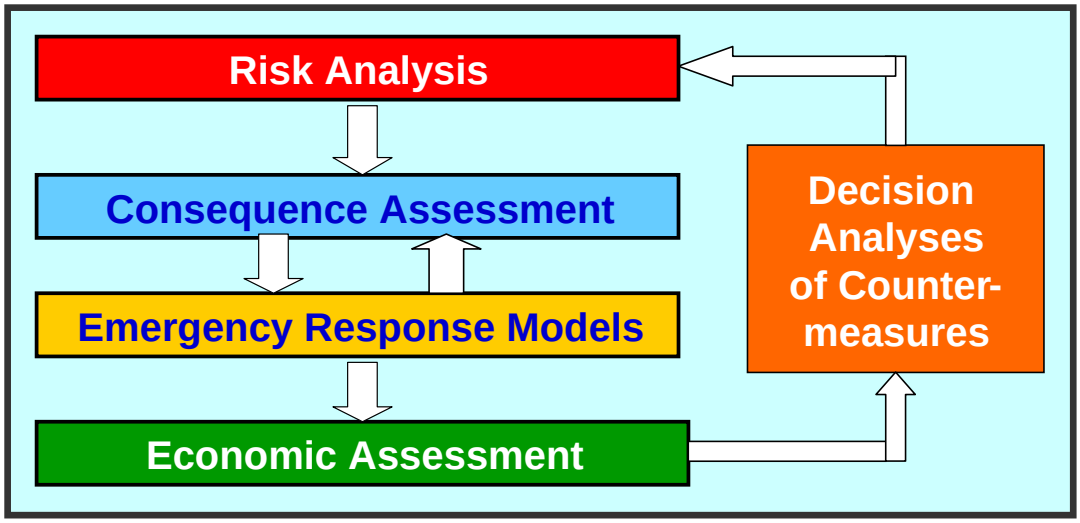


Figure 4. Four-Step Modeling Process

The four modeling steps are being programmed within an integrated modeling environment, built on the ESRI ArcGIS geographic-information-system (GIS). GIS is used because of its capability to represent catastrophic terrorism, which can inflict damage over large areas and is best modeled in a mapping environment. The GIS environment also enables outputs from one modeling step to be transferred as inputs to the next. For instance, a consequence scenario can feed into a disaster response. The modeling system is patterned off the HAZUS modeling system, developed by FEMA to evaluate natural disasters. Like the CREATE system, HAZUS is based on the ESRI platform.

1. Risk Analysis The four-step process is initiated by an assessment of the risk of terrorist attacks, beginning with a characterization of threats, as described in Section 3. Within the four-step process, risk analysis explicitly forces enumeration and comparison of the spectrum of potential threats and vulnerabilities, including scenarios by which threats might be executed, and which define consequence assessments. It is also our intent to capture the relative likelihood of alternate threats. From a software perspective, risk analysis is conducted within the Risk Analyst Workbench (RAW), under development, as described in the following section.

2. Consequence Assessment The second step represents the modeling of the outcomes from the terrorist scenarios generated in the risk assessment step. It provides the methodology for predicting consequences, as indicated by factors like exposure to the effects of weapons (accounting for human behavior in the aftermath of an attack), injuries, illnesses, loss of life, or immediate damage to property. The output of a consequence assessment provides a spatial distribution of outcomes by geographic location. Examples of consequence assessments include:

Plume Models Dispersion of plumes of toxic gasses coupled with models of human exposure, morbidity and lethality. Plume models account for such factors as point of release (indoor, outdoor, exact location), atmospheric conditions, the dispersion characteristics and toxicity of the gas, number of people occupying exposed region, and inhalation rates.

Disease Spread Models Representation of the contraction of diseases based on exposure to contagions, and spread from individual to individual, coupled with measures of lethality and morbidity.

Blast Models Prediction of damage to structures or property due to explosions, based on structure design, size of explosion and placement of explosion. A blast model may be coupled with data on human occupancy to predict injuries and fatalities.

Fire Models Prediction of the spread of fire based on flammability properties and fire suppression systems. A fire model may be coupled with data on human occupancy to predict injuries and fatalities.

CREATE will not develop consequence models, except in particular instances when a new model is needed to address a priority topic. Rather, CREATE will draw on publicly available models within an integrated modeling environment.

3. Emergency Response The third step represents the actions that occur after a disaster to minimize loss of human life or to minimize damage to property. It is based on input provided by consequence models, which define the location, nature and magnitude of a terrorist attack. The response may include dispatch of responders or emergency supplies, provision of emergency medical services, evacuation or distribution of relief supplies, such as food, water or clothing. An effective response strategy can reduce the consequences of a terrorist attack by reducing exposure to terrorist weapons (such as biological agents), increasing survival rates, or reducing damage in the case of fires or toxic plumes. CREATE's focus is on developing tools to assist in the optimal dispatch of emergency resources, and on prediction of terrorist outcomes that result from alternative response strategies.

4. Economics The final step of the four-step process models the economic losses associated with a terrorist attack, particularly indirect losses the occur in the form of

business disruptions or altered economic behavior. The economic assessment follows from the consequence assessments and emergency response models, which define the spatial extent, nature and magnitude of an attack. To date, CREATE's focus has been on enhancement and expansion of the Southern California Planning Model (SCPM), including extension to a national model. SCPM models location specific multi-sector interactions within the economy. It can, for instance, represent the change in economic activity in one location, in one sector, based on economic disruptions elsewhere, or based on infrastructure disruptions. CREATE is in the process of developing a family of economic models to measure a variety of economic impacts, accounting for the effects of terrorist incidents on economic behavior.

Decision Analysis The CTMS process as a whole supports analysis of portfolio allocations, strategic or targeted investments, regulations or other counter-terrorism programs. It is intended to assist decision makers in defining threats, exploring the space of alternative counter measures, and evaluating the specific consequences of threat scenarios. It is also intended to support the planning for response to terrorism. We anticipate that CTMS will be executed as an interactive tool that enables decision-makers to explore and compare alternatives, and to evaluate and prioritize alternative programs and investments. This would include multi-attribute comparisons alternative strategies, and an ability to generate a prioritized list of investments.

Collectively, the four-step modeling system provides these capabilities:

- Assess and compare terrorist threats, and to enumerate threat scenarios
- Evaluate and prioritize alternative investments for countering terrorist threats
- Predict outcomes for individual terrorist scenarios
- Plan for the response to terrorism, to mitigate damages

6. Risk Analyst Workbench

The Risk Analyst Workbench (RAW)[7] is a software tool that provides modeling and analysis capabilities for the risk analysis and decision analysis steps of CTMS. RAW also provides a mechanism for extracting data from external sources, building libraries of data for internal use and linking models to support other modeling steps. RAW guides the risk analyst through the steps of threat and counter-measure characterization, probability estimation, outcome definition, and scenario creation. It also provides tools for rating outcomes of threats, effectiveness of counter-measures, and prioritizing investments.

RAW Functionality

RAW will be executable in a classified, "official use only" or public environment. When security is needed, sensitive information, such as specific intelligence, may be restricted to authorized users. RAW is also being designed with the capability for networked analysis and distributed sharing of information, combined with information security when needed.

RAW is executed in the following steps:

1. Select problem type: Problems are divided into four broad classes: portfolios, programmatic investments and policies, targeted investments, and acting on intelligence.
2. Define Threat: A set of threats is defined according to the attributes of the CTTCS. The user is asked to rate a threat according to attributes mentioned in Section 3, either subjectively, or by calling on data or models to support the assessment. RAW then guides the user in the creation of threat scenarios.
3. Define Counter-Measures: The user inputs, or selects, a set of alternative counter-measures to associate with the threats.
4. Matrixing Counter-Measures and Threats: RAW guides the user in rating the effectiveness of counter-measures relative to a set of defined threats. RAW assists the user in identifying sets of counter-measures that are most effective against a spectrum of threats.
5. Probability Generation: RAW interviews the user, or a collection of participating experts, to elicit probability estimates for alternate threat scenarios. RAW also searches relevant databases to locate information to support probability estimates. Using game theory derived models, RAW estimates changes in probabilities resulting for intervention strategies, to produce estimates of incremental change in risk.
6. Evaluation Based on a selected set of interventions, RAW estimates effectiveness according to multiple outcome measures. When desired by the user, RAW calls consequence, emergency and economic models to estimate

[7] Orosz, M. (2005). "Risk Analyst Workbench Design and Architecture," CREATE Report.

outcome measures. RAW estimates effectiveness of interventions based on modeled scenarios, data libraries on prior analyses, and human judgments.

7. Exploration and Presentation: RAW provides a set of interactive graphical displays to explore and compare alternative interventions. Users can change intervention strategies and visualize cost-effectiveness. Graphical displays will include:

    - Display of terrorist scenarios and interventions in the staircase format
    - Matrices and networked diagrams showing the matching between threats and interventions
    - Icons showing relative effectiveness of interventions
    - Maps showing areas affected by threats and interventions.

RAW Architecture

RAW is an infrastructure/framework in which risk assessment models, risk scenarios, and data from a variety of sources can be accessed, analysis undertaken, and results cataloged. Each workstation has a common look-and-feel human computer interface that allows the analyst to characterize threats, define risk scenarios, select risk models to be used, specify input data locations and formats, and define how and where the results are displayed.

As illustrated in Figure 5a, RAW is a central-server based distributed system with one or more workstations (i.e., laptops, desktops, etc.,), each capable of on or off-line operations. RAW has access to both secure (e.g., classified, proprietary, etc.,) and non-secure (i.e., open) data and models (Figure 5b) that can be stored locally for off-line (stand-alone) operations.

Each RAW workstation contains the following capabilities/utilities.

- Scenario templates that guide the analyst in defining the risk scenario/event to be analyzed.
    - Create new scenarios from templates
        - Weapon selection(s)
            - Guided via a weapon to target feasibility matrix Target selection(s)
        - Adversary selection(s)
        - Counter-measure selection(s)
            - Guided via a counter-measure to threat matrix
        - Probability/feasibility of event(s) occurring
    - Create new scenarios from existing scenarios available either locally (to the workstation) or globally on the RAW distributed network
- Interfacing logic to existing risk assessment models available either locally or globally on the RAW distributed network
- Model interface to allow new models to be integrated into RAW

- Graphical interfaces to display results, alternatives, and current environment status
- Increased situational awareness through alert mechanisms that track data relevancy/currency
- Access to both secure/sensitive and non-secure/open data and models
- Data management services
    - Central-server based data archiving
    - Re-synchronization of data and status when off-line systems are brought back on-line (on the RAW distributed network)
    - Interfaces to non-RAW systems
        - XML
        - ODBC
    - Model parameter/interfacing configuration
    - Management of secure/non-secure data/models
    - Allow analyst to define access control list for proprietary scenarios, models, and assessment results and data

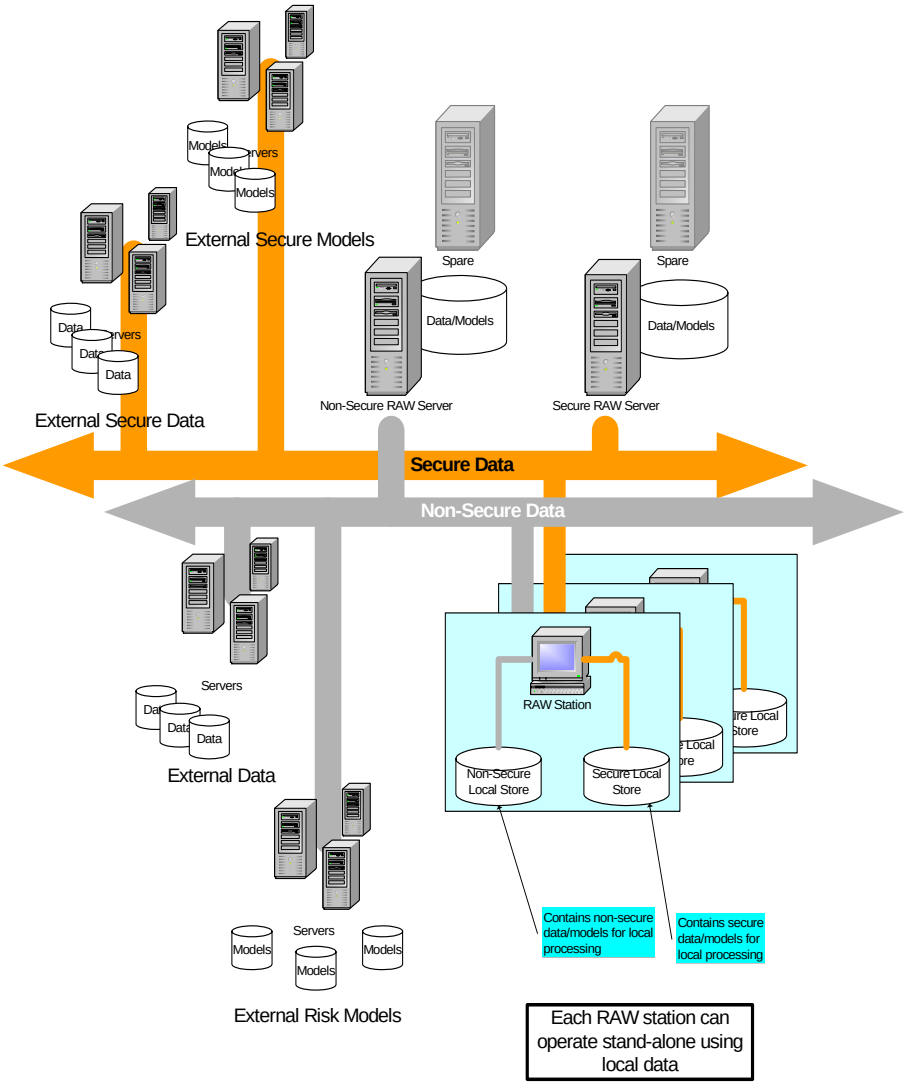


Figure 5a – RAW System Architecture

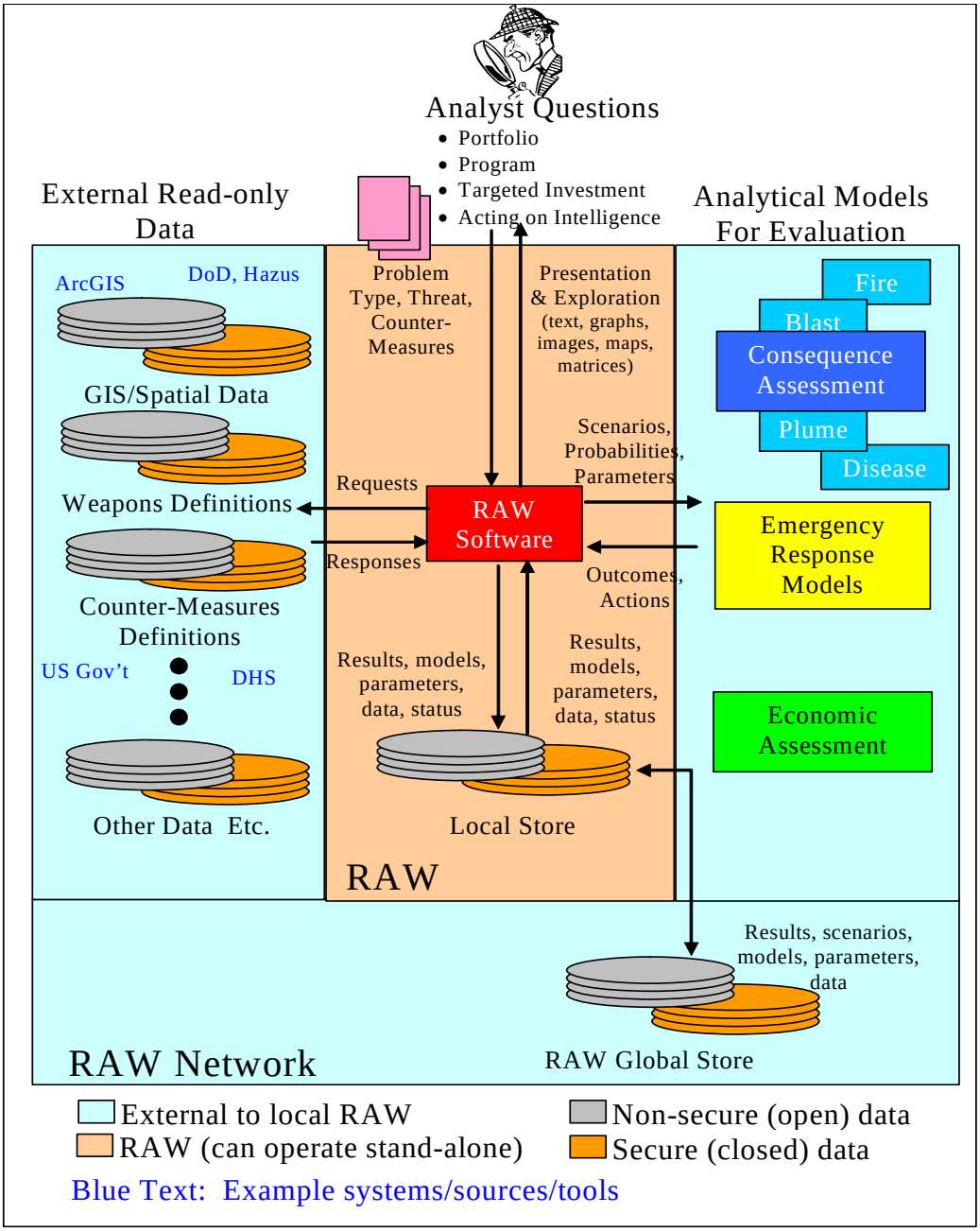


Figure 5b – System Interfaces for a Single RAW Workstation

CREATE Geographic Information Systems (GIS)

The CREATE Geographic Information System (GIS)[8] will provide tools for managing and displaying map-based data at each of the four steps in the modeling process, particularly as they related to managing data created and used by the analytical models in Figure 5b. As shown in Figure 6, the GIS will provide:

- Data management: spatial and non-spatial, multi-user, server connected and detached
- Spatial analysis tools
- Map display and production
- Integration with the CREATE Risk Analyst Workbench
- Integration with analytic software developed by CREATE research teams
- Integration with commercial and government off-the-shelf software

The CREATE GIS will be constructed on ESRI's ArcObjects software platform. ArcObjects is a collection of Microsoft COM objects and associated libraries, plus applications built from them. Extension of the GIS to other platforms will be considered for future releases if demand warrants.

Desktop. Data management via a database management system or as files will be supported. Where practical, code will be available as developer libraries or as server components, though this is expected to be quite limited at the first release. The CREATE Risk Analyst Workbench will function as a driver for creating scenarios for analysis by CREATE analytical software. RAW data will be available for mapping and possibly editing through the GIS, and RAW itself will have some limited map and spatial query functionality and access to spatial data sources (Table 2).

CREATE GIS will have access to the Risk Analyst Workbench data on weapons, individuals, countermeasures and targets. Other non-spatial data will also be accessible as tables.

The CREATE GIS will integrate analysis within the four-step analysis process, as illustrated in Figure 7. RAW is first used to create a threat scenario, which in the example represents a dirty bomb within the Port of Los Angeles. This leads to use of a consequence model to predict human exposure to the resulting plume. In the third step, emergency response is modeled through the distribution of medical supplies. In the last step, economic consequences are predicted for the region as a result of a port shutdown.

[8] Bowman, H. (2005). "CREATE Geographic Information System Design and Architecture", CREATE Report.

Table 2. Example Spatial Data Sources

ESRI Maps & Data
- United States - Census
- United States - Transportation
- United States - Hydrography
- United States - Landmarks
- United States - Other
- StreetMap USA Detailed Streets

FEMA HAZUS data:
- Building Occupancy
- Demographics at the block and tract level, including residential, school, and basic employment figures
- BuildingStock by use, construction, etc.
- Critical facilities: emergency, fire, police, schools, medical care
- Facilities of special concern: dams, hazmat, levees, military, nuclear
- Transportation facilities
- Agricultural land use
- Vehicle inventory

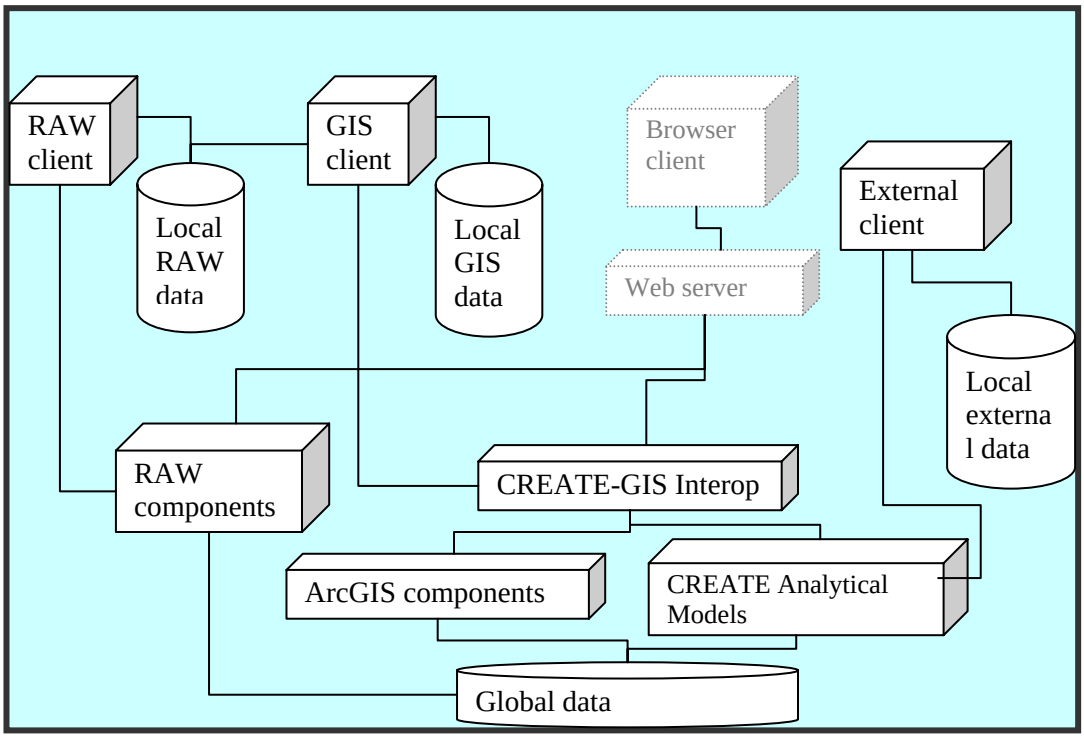


Figure 6. Architecture for Managing Spatial Data

Summary

To summarize, the vision of the Risk Analyst Workbench (RAW) is to provide an environment that assists the analyst in characterizing threats, generating threat scenarios, identifying appropriate counter-measures, and evaluating scenarios and decisions. RAW specifically supports risk analysis and decision analysis, and interfaces with analytical models and data sets to conduct evaluations. The overall goal is to help analysts evaluate a full spectrum of alternatives, both from the perspective of what a terrorist might do, and from the perspective of what might be done to counter the terrorist, and to use the evaluations to support effective decision-making.