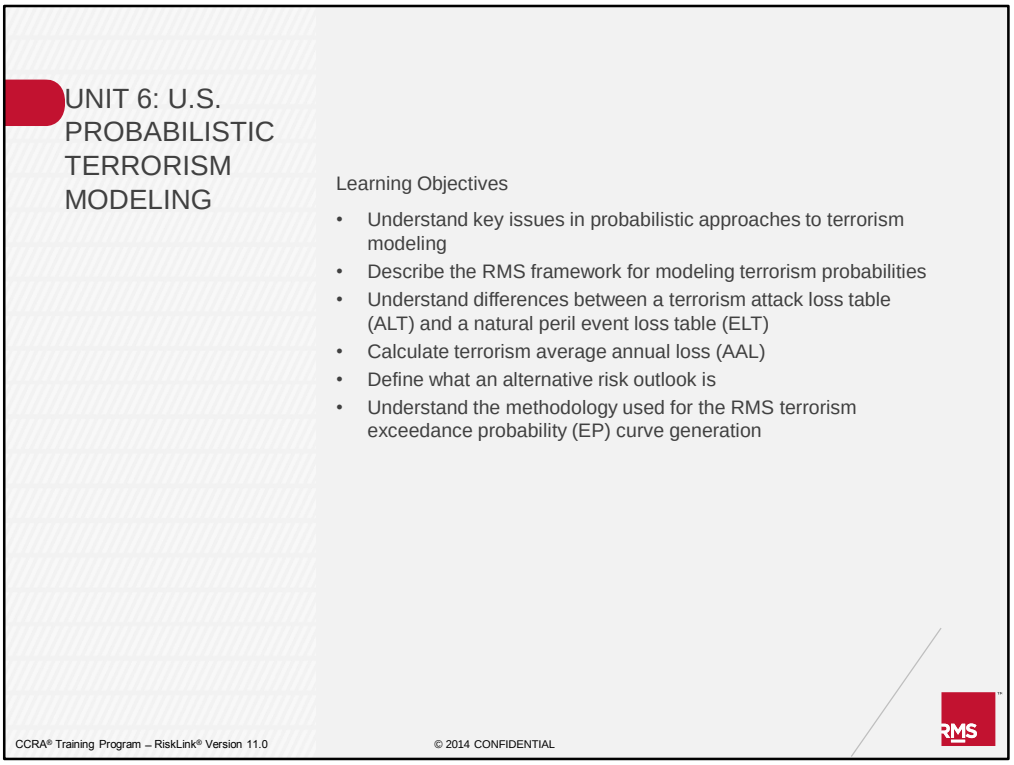
TERRORISM MODELING

UNIT 6

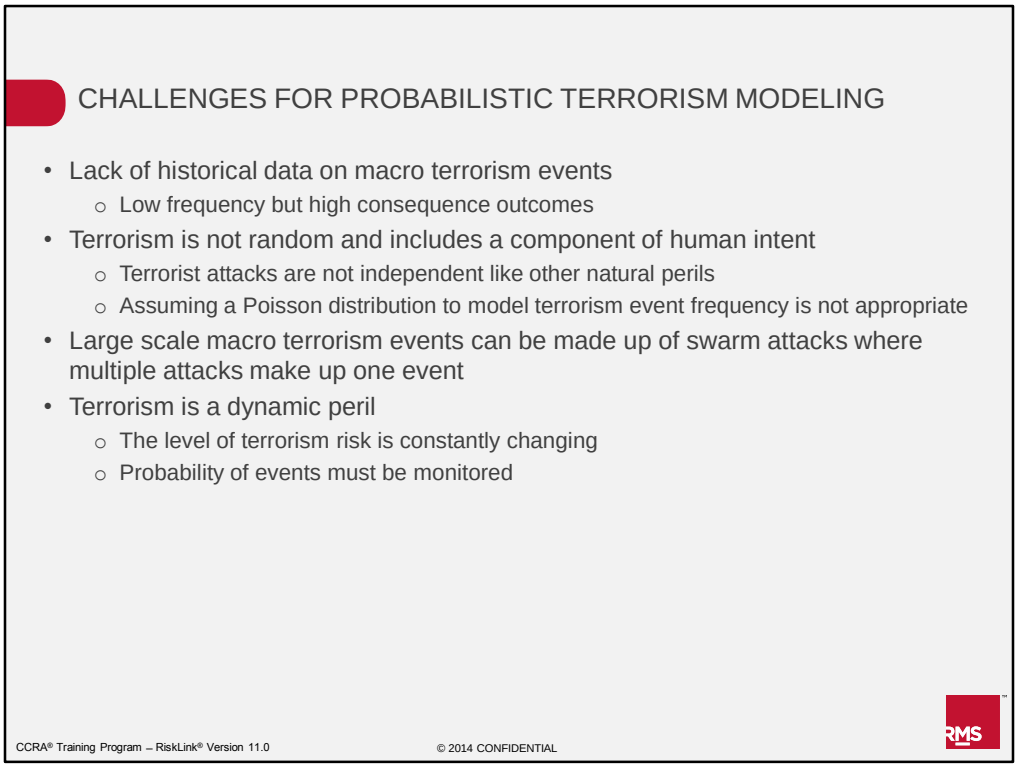
RMS® CCRA® Training Program

AGENDA

- Unit 1: Understanding Terrorism Risk
- Unit 2: Terrorism Modeling Overview
- Unit 3: Terrorism Hazard Module
- Unit 4: Terrorism Vulnerability Module
- Unit 5: Terrorism Financial Modeling
- **Unit 6: Probabilistic Terrorism Modeling**



At the end of this unit you should have a good understanding of each of the five learning objectives listed on this slide.



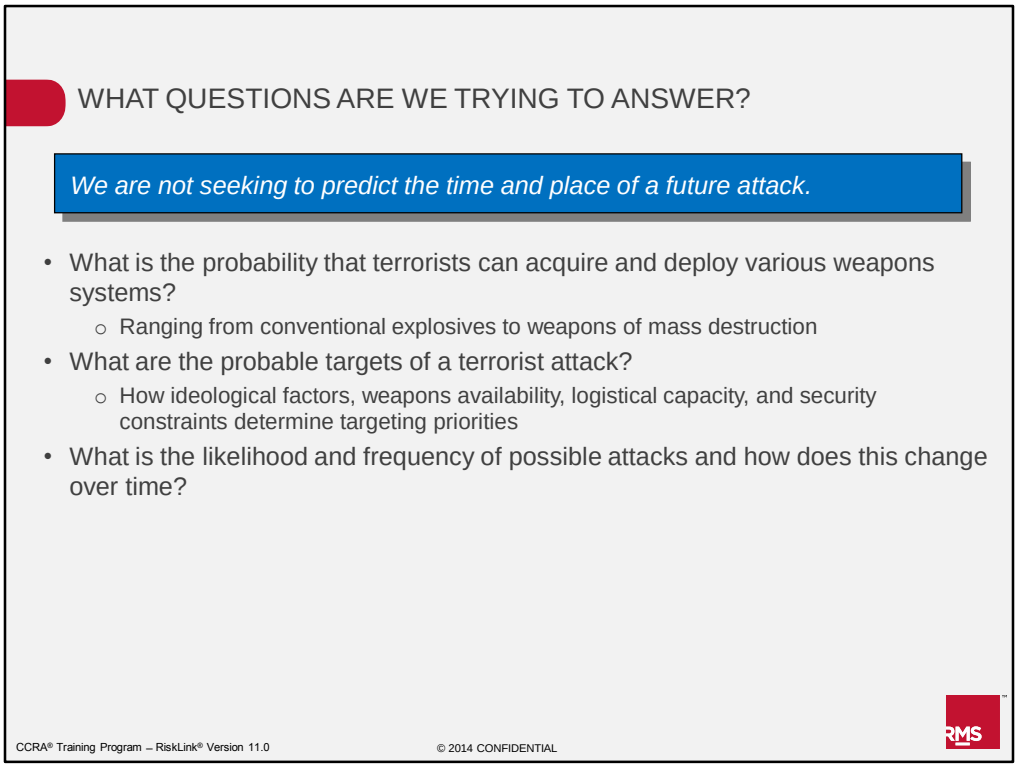
There are several challenges to developing a model to quantify terrorism risk probabilistically. To identify just a few:

- There is a **lack of historical data** on macro-scale terrorism events that can be used to model terrorism occurrence rates. Fortunately for Americans, macro-scale terrorism in the U.S. has a very low frequency. Unfortunately, the attacks of September 11, 2001 proved that though terrorism events may be infrequent, they have high consequence outcomes both economically and from a human casualty point of view.
- Since **terrorism events are not random** like earthquakes or hurricanes, it is not appropriate to assume, even with a reasonably large worldwide historical terrorism attack catalog to work with, that terrorist events are independent,. Therefore, traditional assumptions, such as using a Poisson distribution to model event frequency, is not an appropriate assumption for terrorism.

Other modeling challenges for terrorism include the fact that **large scale macro terrorism events can be made up of swarm attacks** where multiple attacks make up one event. This was illustrated by the Sept. 11 attacks where one event was made up of three successful attacks.

Finally, **terrorism is a dynamic peril** that requires constant monitoring. For instance, the war on terrorism as well as other factors such as increased security and counter terrorism measures can reduce the overall risk posed by terrorists. On the other hand, terrorist groups' planning, recruitment, and overall financing can increase risk. All of these changes can result in modified targeting patterns. Unlike earthquakes, where for the most part, faults and potential earthquakes on those faults can be identified and remain relatively static, changing targeting patterns and attack priorities require constant monitoring.

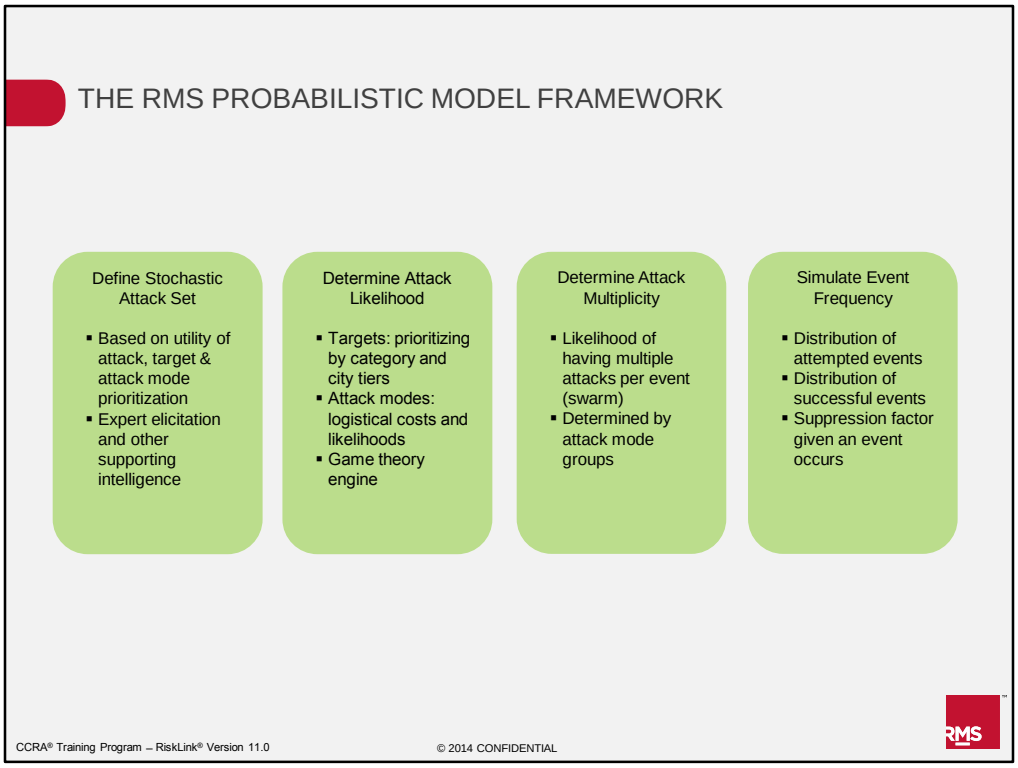
To address these challenges, RMS has developed a framework that incorporates methods to model the dynamic nature of terrorism risk, but also explicitly tackles the problem of how to model terrorism occurrence rates that are non-Poissonian in nature. The next few slides will highlight several terrorism modeling questions that RMS considered in developing a guiding framework for modeling probabilistic terrorism and will also introduce the RMS probabilistic model.



To start, we will look at the questions we are trying to answer in a probabilistic model for terrorism. First of all, we are not seeking to predict the time and place of a future attack but rather to develop a system to monitor how terrorism risk will manifest and change over time. Some of the key questions that RMS used to develop a framework to model terrorism probabilistically include:

- What is the probability that terrorists can acquire and deploy various weapons systems ranging from conventional explosives to weapons of mass destruction? This boils down to determining what the most likely attack weapons are.
- What are the most probable targets of a terrorist attack? This includes determining targeting priorities, including how terrorists' priorities are shaped by ideological factors, weapons availability, logistical capacity, and security constraints. We also consider probable insured losses across multiple lines of business for a given type of terrorist attack since terrorists would attempt to maximize the economic impact of an attack.
- What is the likelihood and frequency of possible attacks? How does this risk change over time?

These questions not only help RMS develop a framework to model terrorism, but also provide a structured way to engage experts in the field to elicit their input based on available intelligence.

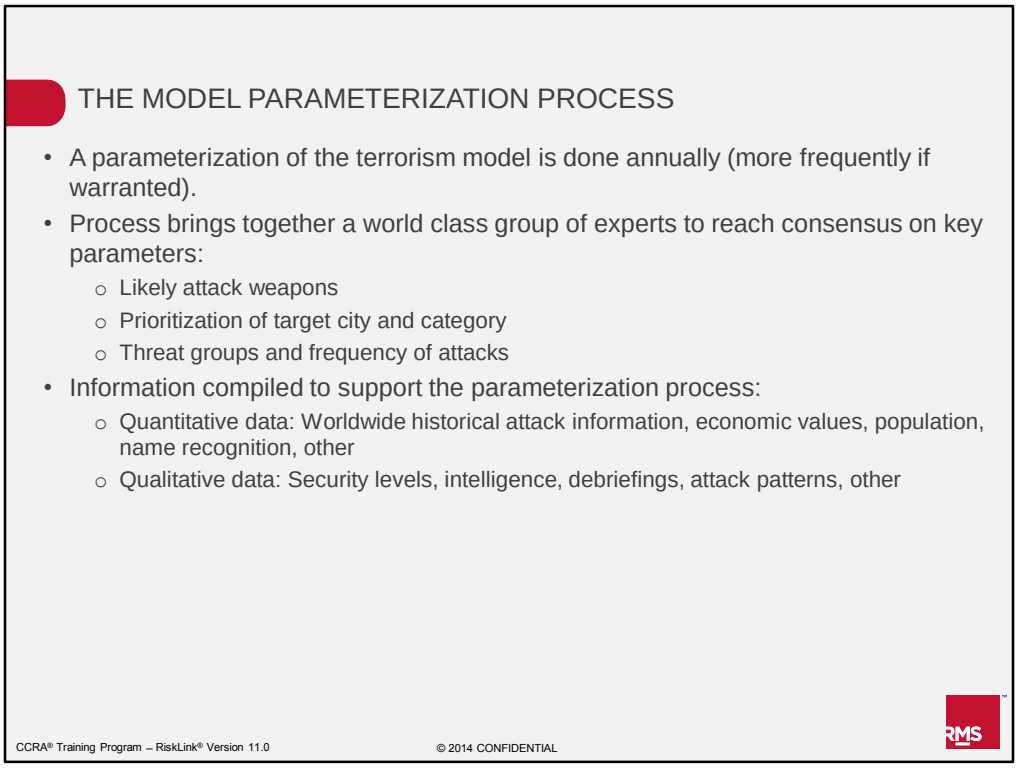


The RMS probabilistic model framework consists of four main components.

First, a stochastic attack set is defined. The stochastic attack set is developed based on quantitative input (including historical attack data) as well as qualitative input (including expert knowledge) to determine the most probable attack modes and targets from various terrorist threat groups. Next, for each attack in the stochastic attack set, we must determine the relative attack likelihoods -- or the conditional probability of each attack. Conditional probabilities are derived from concepts based on game theory as well as input from experts on attack and targeting patterns of terrorist groups. Note that **the conditional probability of an attack can be defined as the likelihood of the attack given that an attack occurs**.

Next, we determine the likelihood of having multiple attacks making up a single event (or a swarm event). Attack multiplicity distributions are derived based on input from experts on terrorist groups' ability to coordinate multiple attacks for a particular weapon type. Last, we model a terrorism event frequency distribution. Instead of using a Poisson distribution to model event frequency, RMS uses a control process that considers the likelihood of attempted attacks, success rates, as well as a suppression factor given heightened security after an event occurs.

We will get into each of these components in more detail in the following slides.



To fully develop each component of the probabilistic model, RMS has put together a process to regularly review parameters used in the model. The model parameterization process occurs annually and could occur more frequently if warranted by world affairs. The model parameterization brings together a world class group of experts to discuss what the most likely weapons, target cities, and target types are given the current threat environment. The team of experts also reach consensus on the ability of threat groups to attempt and successfully deploy such attacks to determine the frequency of attacks in the coming year.

Information used to support the parameterization process are both quantitative and qualitative. Some examples of the quantitative data used to support the process include:

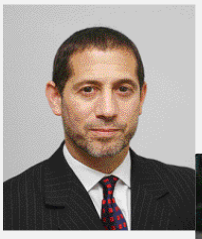
- A worldwide historical attack database that is used to calibrate the cities and target types that are most likely to be attacked
- Economic and demographic indicators to identify attacks that would cause the most harm in terms of property damage, human casualties, and economic disruption
- Data compiled on name recognition of targets by primary threat groups

Other qualitative data is also assessed including:

- The state of the security level in each country
- Intelligence on terrorism threat as relayed to RMS by its experts
- Observations of recent attack patterns by the primary terrorist threat groups

THREAT LEVEL EXPERTS

- Dr. Bruce Hoffman:
  - Professor, Security Studies Program, Georgetown University
- Dr. Rohan Gunaratna:
  - Head of the International Center for Political Violence and Terrorism Research (ICPVTR) at the S.Rajaratnam School of International Studies (RSIS), Singapore.
- Dr. Magnus Ranstorp:
  - Research Director, The Centre for Asymmetric Threat Studies at the Swedish National Defense College, Stockholm, Sweden.
- Dr. K. Jack Riley:
  - Director, RAND Public Safety and Justice, and co-Director of Center for Terrorism Risk Management Policy




CCRA® Training Program – RiskLink® Version 11.0 © 2014 CONFIDENTIAL

RMS works with a long list of experts to build all aspects of the terrorism model. The threat level update is the focus of four world renowned experts. The first three are academics who have made it their life's work to study.

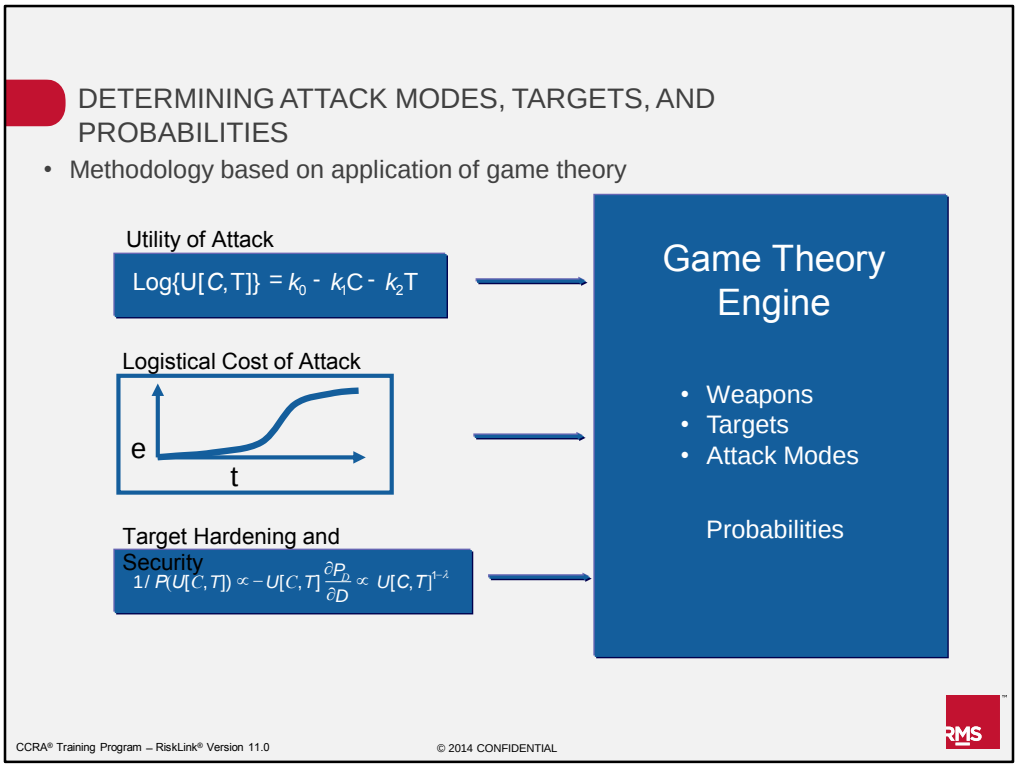
- Bruce Hoffman: One of the first to pursue terrorism from an academic standpoint, he is probably the most cited person in any terrorism book. He recently returned from Iraq where he was a consultant to the U.S. military forces.
- Rohan Gunaratna: Perhaps the world's leading authority on Al Qaeda. He is also a Sri Lankan interrogator of political prisoners. He spent a good deal of time in the Middle East, particularly pre-9/11, and he had an opportunity to interview many terrorists. He had access to many key sources of information not in the public domain, including the encyclopedia of Jihad and Al Qaeda training tapes.
- Magnus Ranstorp: He is the director of CSTPV at St. Andrews University, the most prestigious academic institution for terrorism study in the world. He is also the leading authority on Hizballah, and spends a great deal of time in the Middle East and throughout Europe.
- Jack Riley: He is a RAND security expert currently on the ground in Afghanistan.

The RMS main threat level experts are highly respected and world renowned in various fields of terrorism risk. These experts come from various think tanks and research organizations including:

- The Rand Corporation: A renowned think tank that has significant roots in advising both the U.S. government – specifically the U.S. military – as well as corporations in areas of national defense.
- The Institute of Defense and Strategic Studies in Singapore
- The Center for the Study of Terrorism and Political Violence at St. Andrew's University

In addition, RMS also has a broader set of experts that advise in modeling various weapon types, as well as their likelihood for being used. These include the following:

- Jane's Consultancy (an authority on weapon systems and attack technology)
- The Center for International Security and Cooperation at Stanford University
- The nuclear engineering department at UC Berkeley

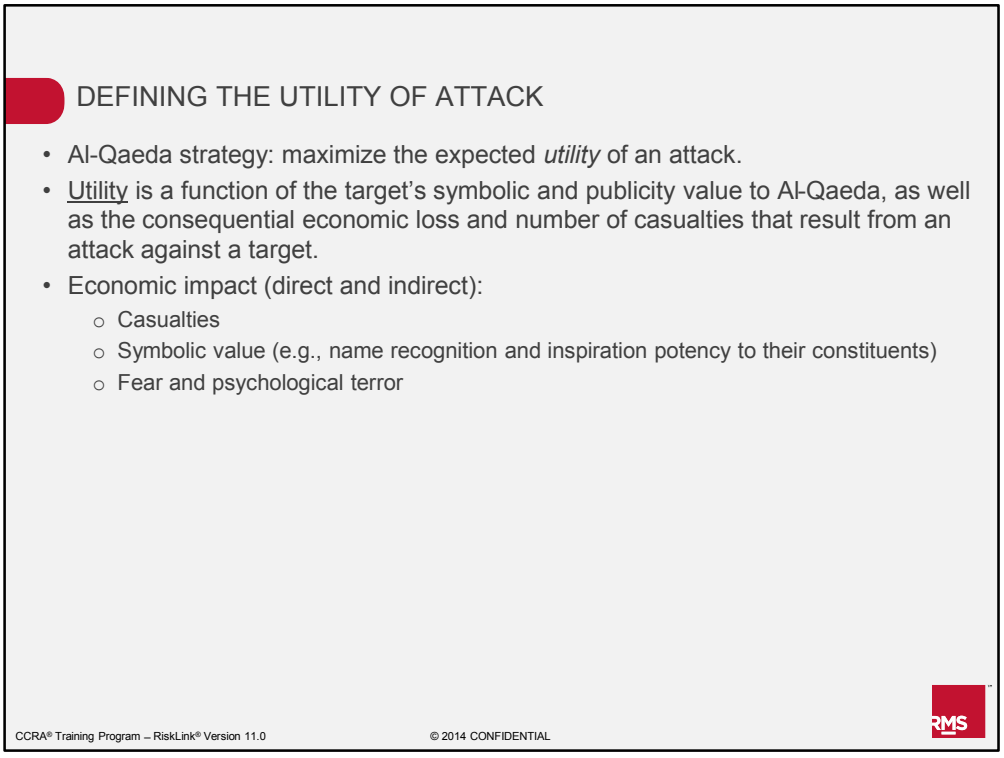


The next few slides discuss the framework RMS uses to determine the most probable targets and attack modes that are included in the RMS terrorism stochastic attack set as well as their relative likelihood – or the conditional probability of each attack. To reiterate, an attack conditional probability can be defined as the likelihood of the attack given that an attack occurs.

RMS uses the application of game theory concepts to quantify attack likelihoods. The main inputs to the RMS model include measurements of:

- The utility of an attack, which is a measure of a terrorist's desire to maximize the overall impact of an attack
- The logistical cost of an attack based on the skills, personnel, monetary cost, and time it would take to build the capability to deploy the weapon
- Target hardening and security, which has the opposing effects of decreasing the likelihood of attacks at the targets that are hardened, while at the same time shifting risk from one type of target to another

All of these inputs are considered both when building the stochastic attack set and determining individual attack conditional probabilities.



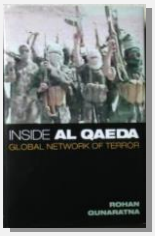
To define the most probable attacks and their likelihoods, RMS starts by looking at a terrorist group's attempt to maximize the utility of an attack.

In order to understand the utility of attack against a target, RMS must consider the threat posed by the Al-Qaeda network since it is the primary threat group for the countries modeled in the RMS Probabilistic Terrorism Model. In some sense, we need to get into the minds of terrorists to understand what their targeting and attack patterns will be. Threat experts have helped RMS understand that, for Al Qaeda, the utility of an attack is a function not only of a target's symbolic and publicity value but also its ability to cause large scale economic destruction and human casualties. Causing fear and other psychological terror is another goal for Al-Qaeda when considering the types of attacks to plan and attempt.

ATTACK UTILITY: TARGET PRIORITIZATION

"Al-Qaeda goes for symbolic, high prestige targets – *targets that matter.* Targets that inspire and influence other Muslims to go and take similar targets. The inspirational value is embedded in their targeting."

Dr. Rohan Gunaratna
Institute of Defence & Strategic Studies
Singapore



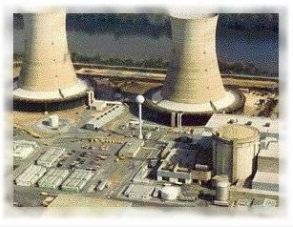
A major component of Al-Qaeda's attempt to maximize the utility of an attack is to focus on targets of prestige with high symbolic value – as seen by the September 11 attacks in 2001. One of RMS' threat experts, Rohan Gunaratna, who is a widely known expert on the Al-Qaeda terrorist network and author of the book "Inside Al-Qaeda," sums up Al-Qaeda's targeting priorities in this quote:

"Al-Qaeda goes for symbolic, high prestige targets – *targets that matter*. Targets that inspire and influence other Muslims to go and take similar targets. The inspirational value is embedded in their targeting."

Not only are targeting patterns determined by the ability to cause large scale destruction to property and people, but attacks on highly symbolic targets are also recruiting mechanisms to persuade other radical Muslims to join the Al-Qaeda cause.

FACTORS DETERMINING TARGET LIKELIHOOD

- Target utility
- Debriefings of operatives
- Historical attack patterns
- Known planned attacks
- Intelligence
- Local level of security
- Expert opinion



CCRA® Training Program – RiskLink® Version 11.0 © 2014 CONFIDENTIAL

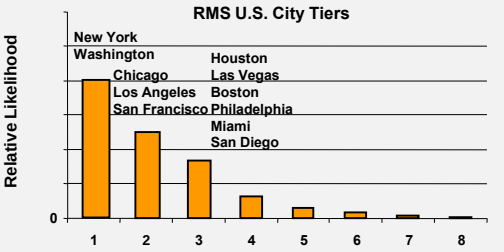
To model Al-Qaeda's targeting patterns, RMS looks at various factors to determine the most probable targets to model. These factors include target utility, debriefings of operatives, historical attack patterns, known planned attacks, intelligence, local level of security, and expert opinion. RMS uses these inputs to develop targeting priorities, or rankings, by both target categories and target cities.

Target rankings by category are determined by reviewing attack patterns, known planned attacks, intelligence reports, and debriefing of captured operatives.

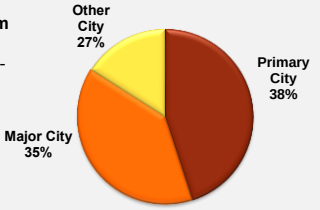
RMS target category rankings are shown in this slide. Targets that fall in the Tier 1 category, which include presidential and other key government offices, are the ones with the highest utility for Al-Qaeda. Tier 6, apartment buildings and so forth, would have a lower utility than categories listed in Tiers 1 through 5.

LIKELIHOOD OF TARGETING SPECIFIC CITIES

- Total population of city
- Economic importance – gross metropolitan product (GMP)
- Known intent to attack – attacks, attempted attacks
- Name recognition – the familiarity of city
- Radical Islamic activity & support – the presence of known radical Islamic organizations and movements in cities.
- Symbolic targets – the presence of symbolic targets or association with a symbolic site nearby.
- Level of anti-terrorism security



Macro Terrorism Attacks
Worldwide 2002-2010



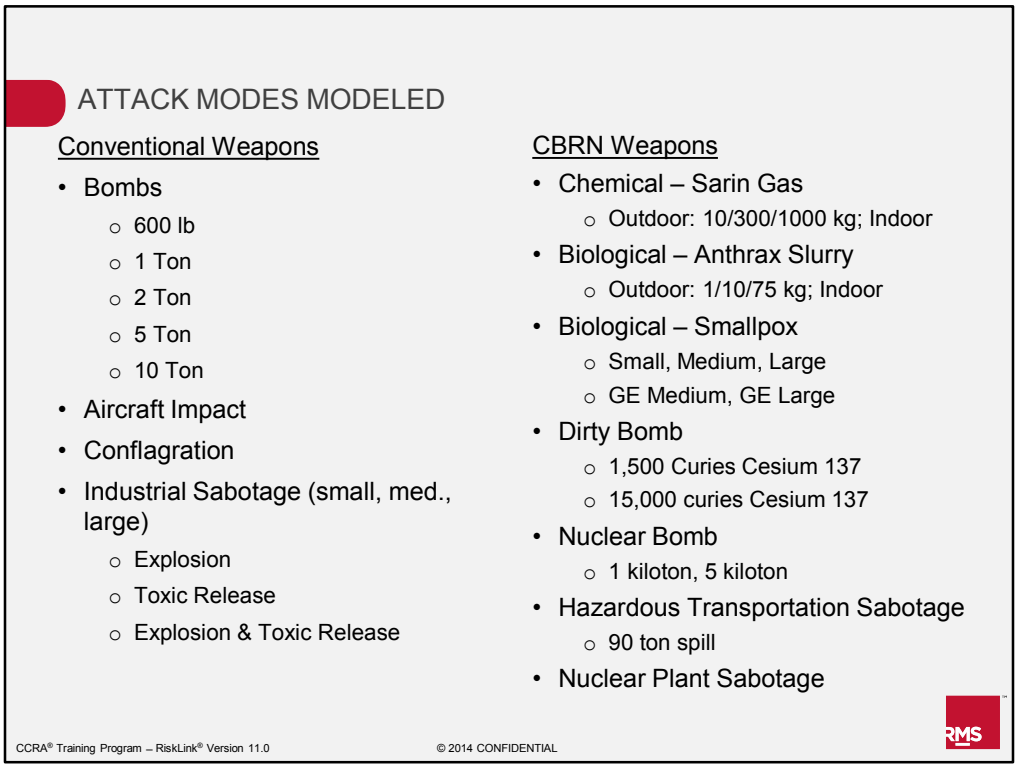
- Primary city is the capital city or major economic city in the country where the terrorist attack took place.
- Major city is one of the largest 5 cities by population in the country where the terrorist attack took place.
- Macro terrorist attack means a car bomb or worse.

CCRA® Training Program – RiskLink® Version 11.0 © 2014 CONFIDENTIAL

Target rankings by city are determined by reviewing name recognition in the Middle East, historical attack patterns, the ability to cause economic destruction and human casualties, as well as other relevant information available in intelligence reports and debriefings of captured operatives.

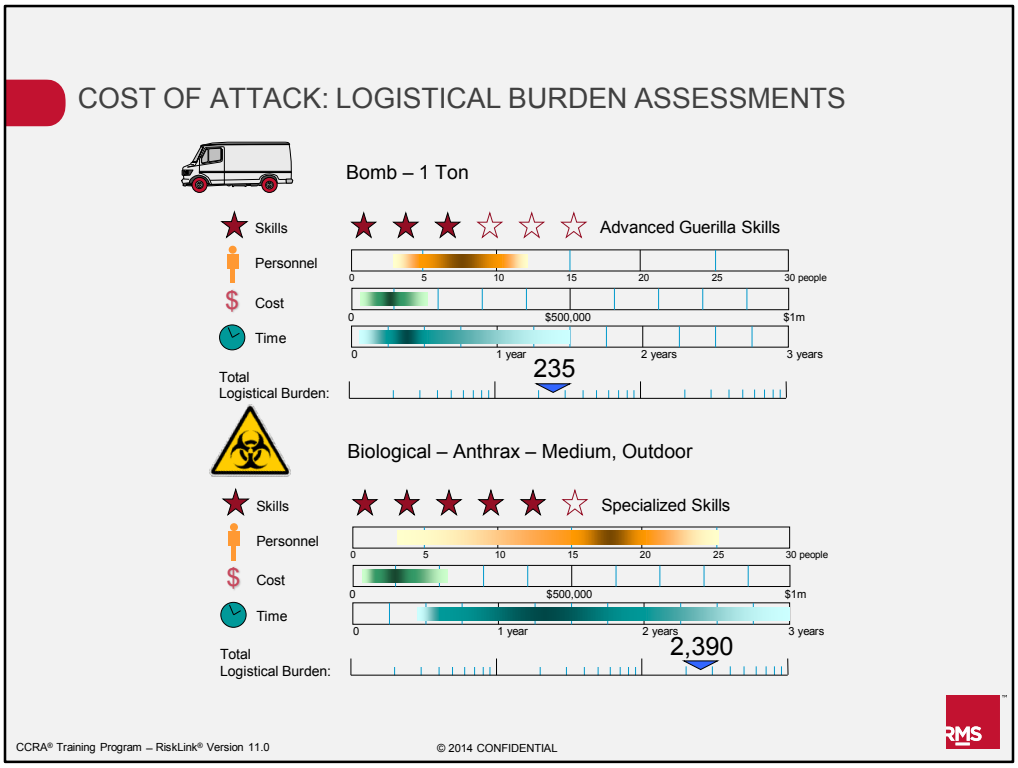
The chart at the top right of this slide shows RMS target city rankings for the U.S. for the 2012 Risk Outlook; New York and Washington D.C. are the most likely cities to be targeted while other major metropolitan centers fall into lower tiers. The chart at the bottom of the slide shows one calibration made against a catalog of historical worldwide attacks that illustrates that RMS modeled city tier likelihoods are similar to observed attack patterns that are categorized into: 1) primary cities, 2) major cities, and 3) elsewhere.

Targeting primary and major cities is just one example of how terrorist maximize the utility of the attack by considering higher profile targets in those cities.



Another factor RMS considers in developing attack likelihoods is to determine the most probable attack weapons that could be used against targets of significance. One main input used is to assess the overall cost it takes to acquire, develop, and deploy a particular weapon type.

This slide shows the list of attack modes that are included in the RMS terrorism model. This list of attack modes has been developed through many sessions with RMS experts to identify and understand the most probable weapons that the Al Qaeda network could deploy against potential targets. All of these attack modes are considered macro-scale terrorism events and considered in the model.



It is now known that the September 11 attacks took several years to plan. It was financially well-resourced but also required time, effort, and the right personnel to prepare and deploy the attack. To account for the fact that some weapon types are easier to acquire, develop, and deploy than others, RMS uses a logistical burden score that was developed with the guidance of experts from the Jane's Information Group to help measure the overall cost of a weapon type. The logistical burden is developed to capture the overall cost of the attack type using a combination of factors including the skill, personnel, monetary cost, and time it requires to acquire, develop, and deploy the attack weapon.

This slide shows an example of the logistical burden to deploy a 1-ton bomb and also illustrates that the 1-ton bomb logistical burden is an order of magnitude lower than the logistical burden to deploy a medium sized outdoor anthrax attack weapon. The logistical burden of an attack weapon is one input used to measure the relative likelihood of a particular attack based on the difficulty for Al Qaeda to successfully plan and attempt the attack.

ATTACK MODE PREFERENCES: MODELED VS. OBSERVED

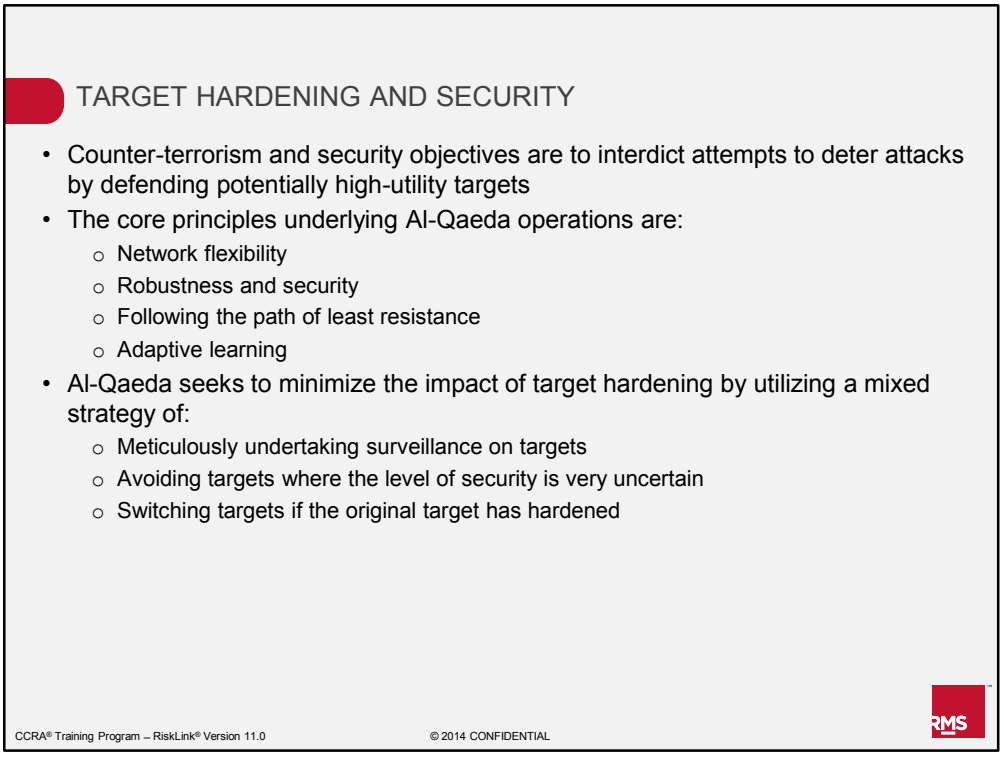
Macro Attacks Only

	Worldwide Observed 2002-2010
2 ton or larger Truck Bomb	1%
Truck Bomb	2%
Car Bomb (Less than 1 ton)	51%
Total Bombs	**54%**
CBRN	0%
Standoff Attacks	20%
Aircraft Impact & In Flight Explosion	0%
Armed Attack	23%
Sabotage of Infrastructure	2%
Conflagration Attack	1%

CCRA® Training Program – RiskLink® Version 11.0 © 2014 CONFIDENTIAL

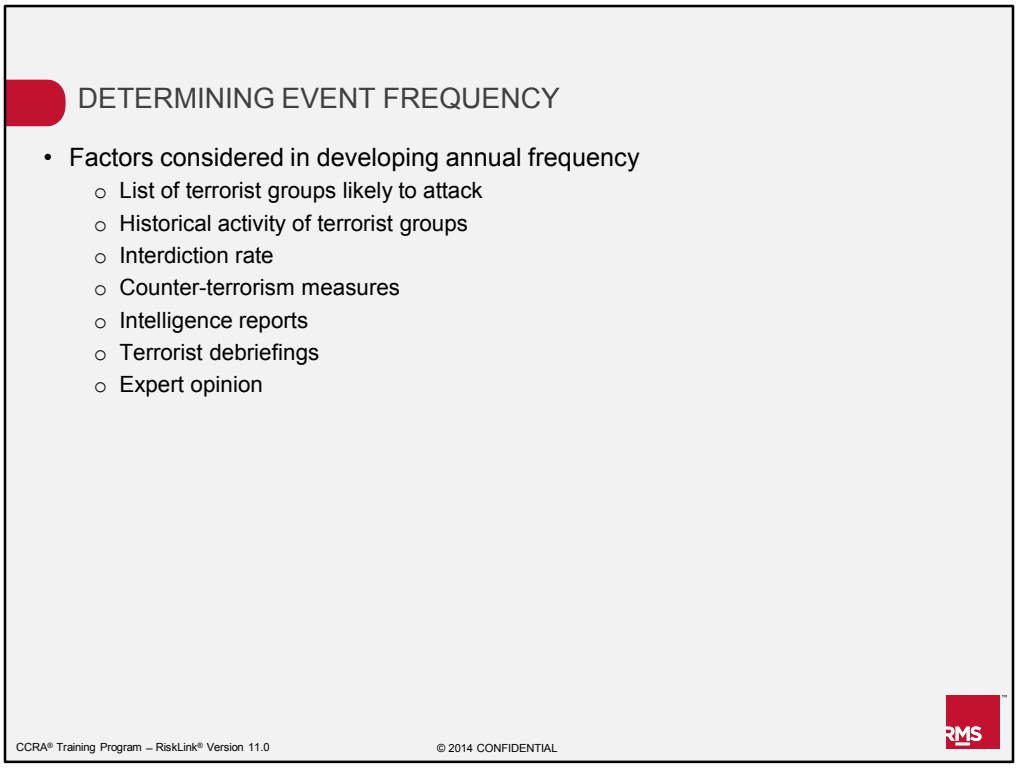
RMS uses the measurement of the logistical burden for various weapon types as a parameter to determine the relative likelihood of various types of attack modes. This slide illustrates the relative attack mode likelihoods that are used in the RMS terrorism model. Vehicle bombs have the largest likelihood of occurring, while CBRN (or chemical, biological, radiological, or nuclear) attacks have a low likelihood.

Note that surface to air and other stand off weapon attacks are not included in the RMS stochastic terrorism model which is one of the reasons why the sum of conditional probability for all RMS stochastic attacks does not sum to one.



Another game theory input to determine attack likelihoods is the state of the security environment. The goal for the U.S. is to deter attacks by enabling interdiction and disruption of attack preparation. While the U.S. hardens certain targets perceived to be at high risk, Al-Qaeda is an adaptive organization that attempts to minimize the impact of target hardening through surveillance on targets and ultimately target substitution. An increased security environment effectively hardens some targets to make attacks against them less likely while at the same time pushes the likelihood of attacks to other less secure targets.

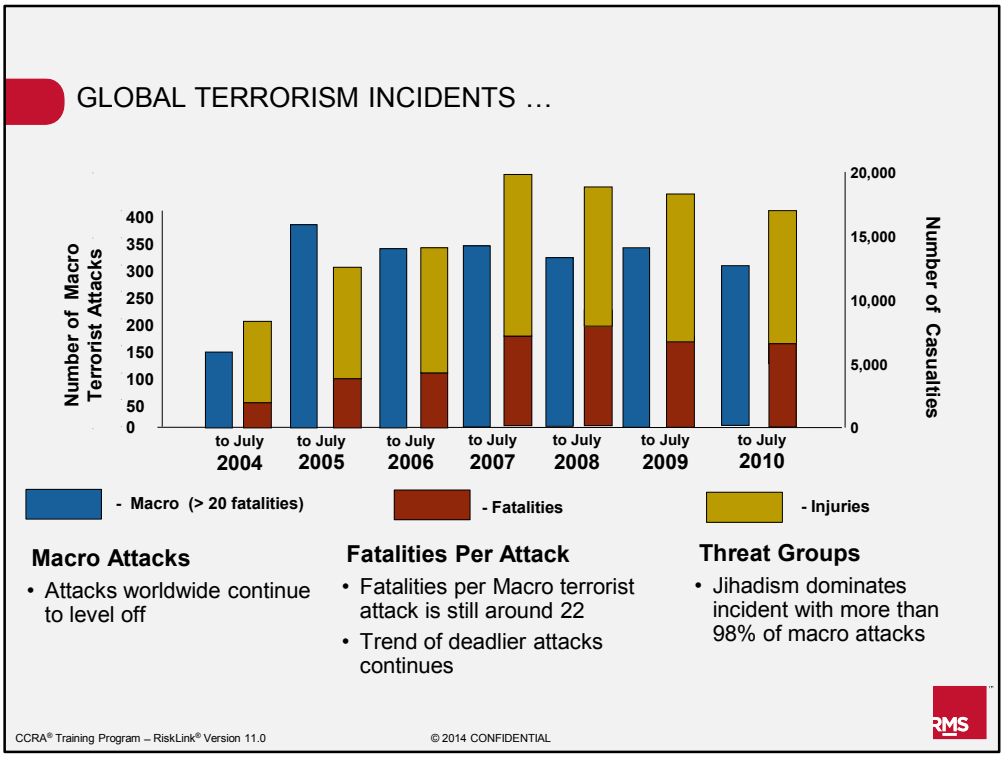
Jack Riley of RAND – a pre-eminent think-tank on homeland defense – is a key advisor to RMS on the state of the security environment, policy developments, and the issues that confront us as a nation about the funding and effectiveness of public deterrence. RMS encapsulates the issues of mission success versus target hardening through a utility optimization for a given set of target hardening situations. Utility optimization for the set of target hardening situations is the final input, in addition to the utility and logistical cost of an attack, that is considered when developing the conditional probabilities for each attack in the terrorism stochastic attack set.



Up to this point in this course, we have mainly focused on defining how the RMS stochastic attack set is developed and how conditional probabilities for each attack are determined. To switch gears, we will move on to the third component of the RMS probabilistic terrorism model framework, which is terrorism event frequency.

We have already mentioned in a previous slide that terrorism event frequency is not random, and thus, using a Poisson assumption (which relies on the underlying assumption that events are independent) to describe event frequency for terrorism is not appropriate. As an example, consider how the likelihood of having another successful Al-Qaeda terrorism event changed after September 11. Security measures to deter another event from occurring were high which illustrates how the occurrence of one event is able to affect the occurrence of the next. In general, this is different from earthquakes and hurricanes where the occurrence rates are more or less random and that the occurrence of one event does not affect the occurrence of the next event.

RMS explicitly models terrorism event frequency as a control process rather than a Poisson process. The control process RMS uses will be described in more detail in the following slides. To start the discussion, this slide lists some of the factors considered when developing a terrorism-specific event frequency, including a list of foreign groups likely to attack the U.S., historical activity of terrorist groups, interdiction rates in the U.S. and other developed countries, the current state of counter-terrorism measures in the U.S., intelligence reports, terrorist debriefings, and expert opinion.

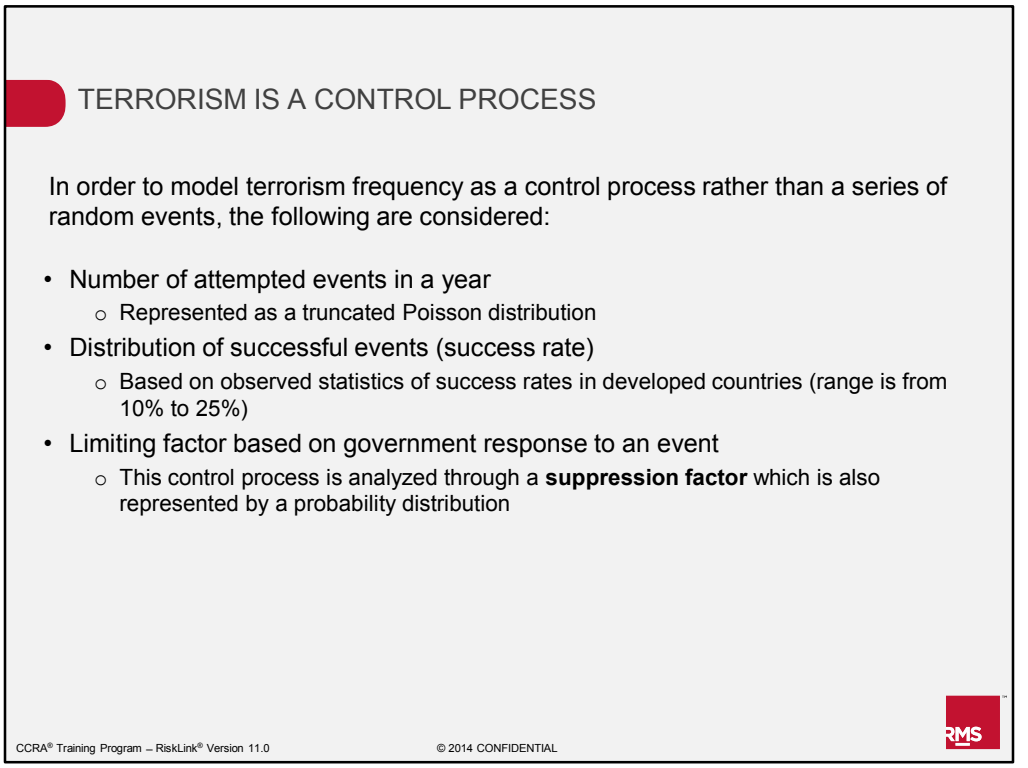


Assessing the number of terrorism incidents is a tremendous challenge, with hard data lagging events on the ground. However using the Jane's/RMS standardized terrorism event catalog that currently logs an average of 15 new events each day, we are able to get a good picture of how many terrorist incidents have been perpetuated.

Political violence by salafi-jihadi groups have increased around the globe. Despite the progress in Iraq, macro terrorism attacks perpetuated by salafi-jihadi have increased to more than 350 attacks globally compared to 336 in 2010. More ominously, there is a slow, steady increase in attacks and fatalities around the world outside of Iraq. In fact, many commentators have assessed that the flow of "foreign jihadi" to Iraq has diminished, but the consequence is that the would-be terrorists are now engaging in violence at home or perhaps in other regional theaters. Algeria, Afghanistan, Pakistan, Somalia, and Yemen all experienced terrorist attacks by groups imbued with the salafi-jihadi doctrine. These groups have conducted numerous attacks using Al Qaeda's hallmark of suicide bombings and improvised explosive devices (IEDs).

The variability of the number of casualties per attack has decreased, and at this juncture, the number of fatalities caused by each macro attack has leveled to about 22 fatalities per event.

Vehicle bombs remain the weapon of choice for terrorists, used in more than 52% of macro attacks worldwide during the past year. However, terrorists continue to increase the destructiveness of these conventional weapons by better targeting and techniques, expertise which is rapidly disseminated to cells operating in many different countries. The average number of people killed per vehicle bomb worldwide has doubled since 2004. Conventional weapons are expected to be used in future attacks, but in more destructive ways.



This slide illustrates the control process RMS uses to model terrorism frequency. In order to do this, RMS looks at three main components:

RMS starts by modeling how many attacks will be attempted.

To do this, RMS collects information on the number of terrorist operatives within each modeled country (or able to infiltrate each country) and the number of attempted attacks of previous years ranging from one to ten per year. RMS then estimates a mean number of attacks which is entered as a parameter into a truncated Poisson assumption to come up with a probability distribution of the number of attempted attacks.

Next, RMS looks at how many attempted attacks will succeed.

To do this, RMS looks at both counter-terrorism measures in place that attempt to disrupt attacks in preparation, as well as intelligence on each countries ability to penetrate into dissident groups and detect terrorist activity. RMS collects statistics of success rates in developed countries which range from around 10% to 25%. The success or interdiction rate is represented by a probability distribution of attack success rates.

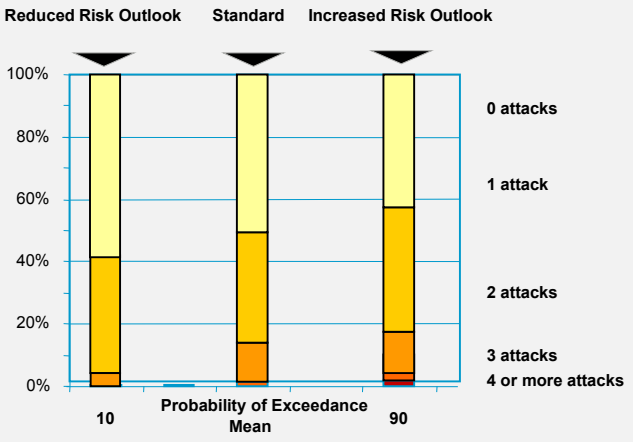
Finally, RMS considers a limiting factor to the number of attacks per year based on the fact that the government will respond and increased security will reduce the chance of a successive attack. This control process is analyzed through a suppression factor.

A suppression factor can be described as the political willpower and motivation of a country to fight terrorism activity recurrence. The suppression factor is a function of available resources as well as public tolerance to the temporary infringement of civil liberties. Experience shows that the post-9/11 response cut terrorism activity by approximately 45% the following year. RMS currently uses a suppression factor assumption similar to post-9/11 which is represented by a probability distribution.

SIMULATION OF TERRORISM MACRO ATTACK FREQUENCY

- A Monte Carlo simulation is used to derive the full probability distribution of the number of events
- 90% confidence limits used to model alternative risk outlooks

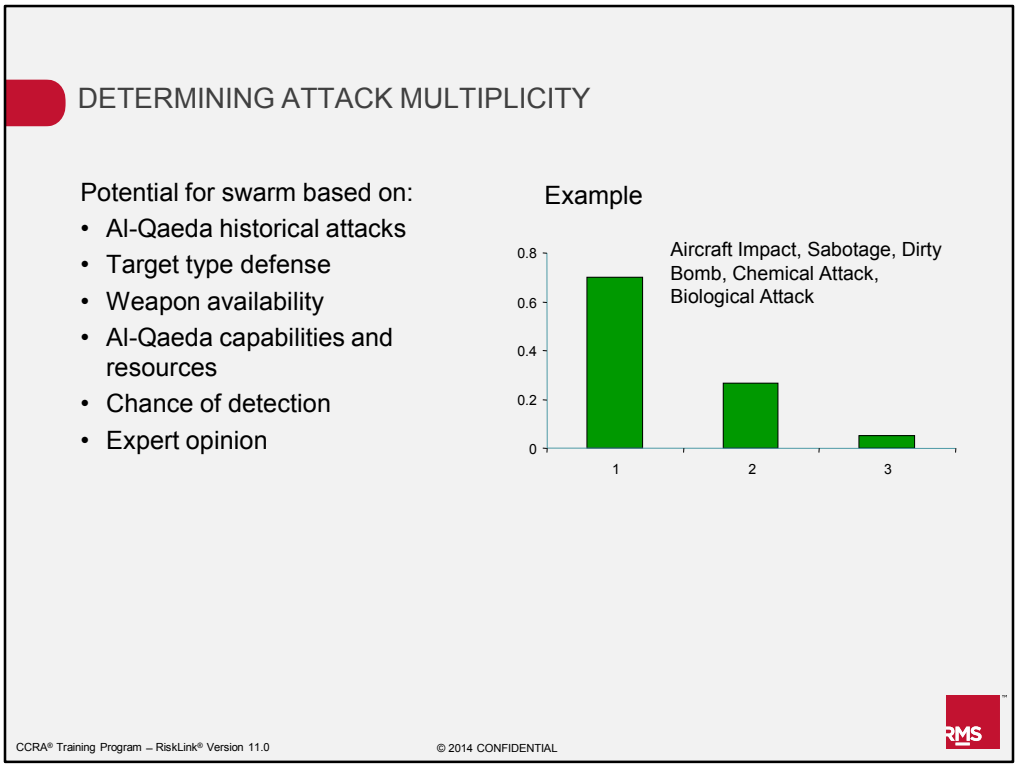
Example U.S.



CCRA® Training Program – RiskLink® Version 11.0

Probability distributions (described in the previous slide) for **the number of planned macro-terror attacks**, **the interdiction rate** achieved by security forces and the post-event counter-terrorism **suppression factor** are input to a Monte Carlo simulation to derive the full probability distribution of the number of successful events in a given year.

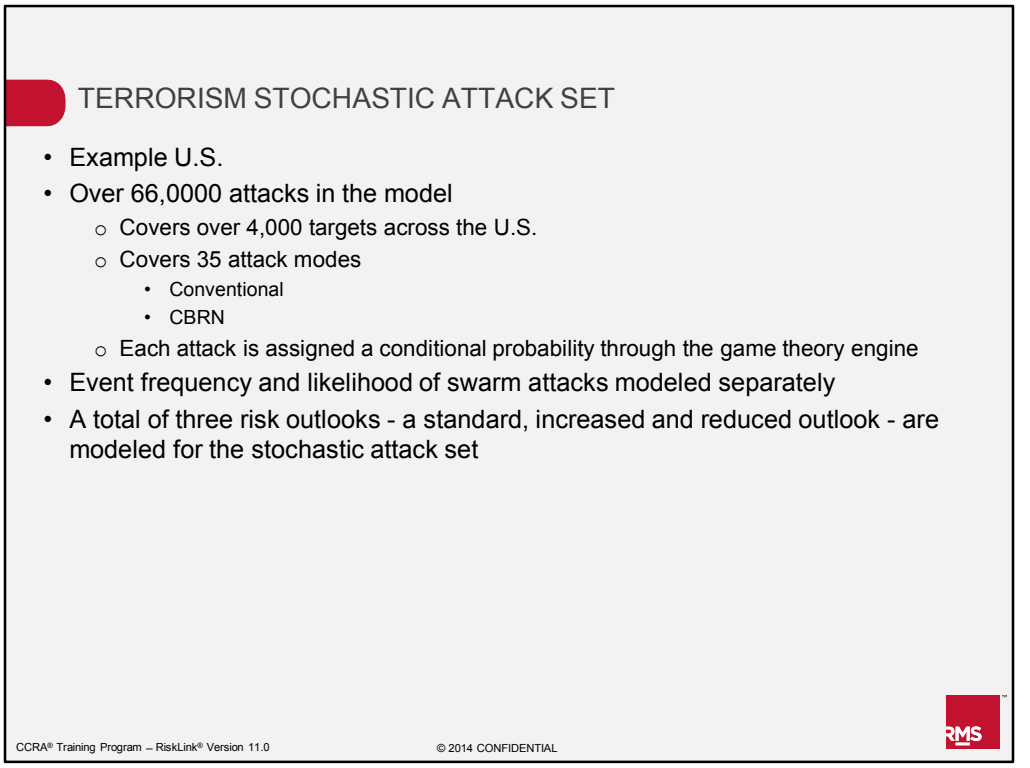
This simulation process also allows RMS to quantify the 90% confidence limits around the mean frequency distribution. The upper and lower 90% confidence limits are used to model the RMS increased and decreased risk outlooks for a given terrorism probabilistic model. The mean frequency is what is used in the RMS standard outlook for the year.



The last component of the RMS probabilistic terrorism model framework is the attack multiplicity or the potential for swarm attacks. The attack multiplicity can be defined as the likelihood (or distribution) of having multiple attacks make up a single terrorism event. Attack multiplicity distributions are determined based on historical attack patterns by Al Qaeda, target type defense, weapon availability including terrorists' capabilities and resources, the overall chance of detection, and expert opinion.

In the RMS model, attack multiplicity is modeled by attack group. For example, RMS models the possibility of having five bombs making up an event, but not the case where two bombs and one aircraft attack make up a single event. Currently, there are five distinct multiplicity distributions used in the RMS terrorism model:

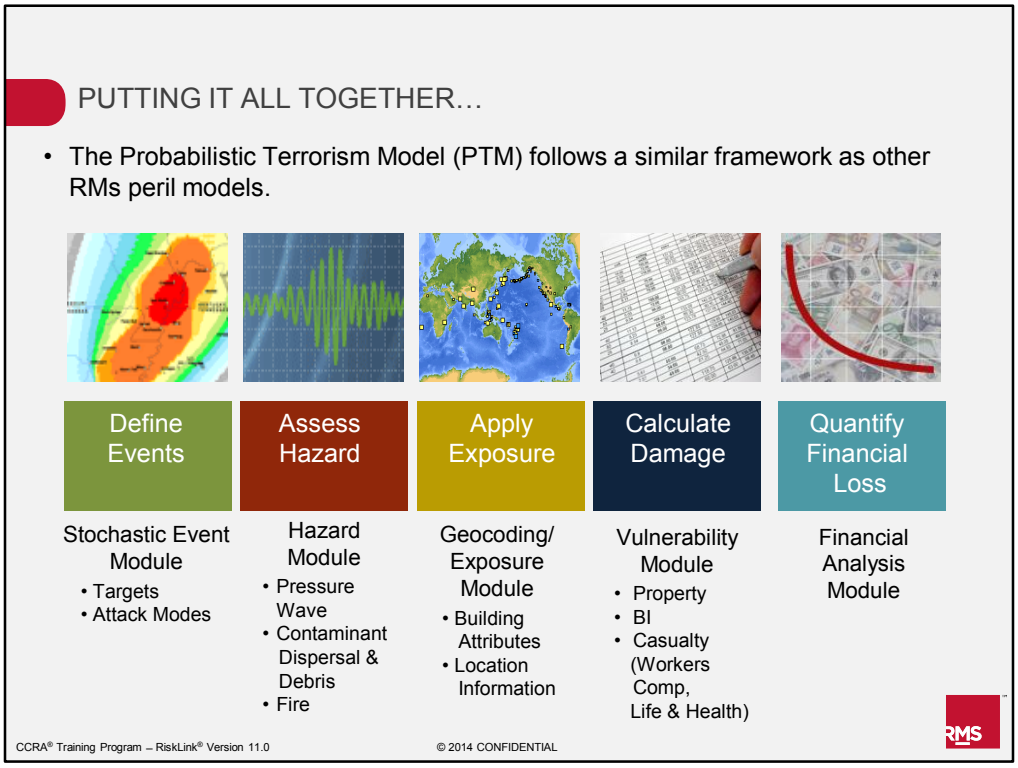
- 600lb conventional bombs (which have an average multiplicity of 3.17);
- Conventional bombs except 600lb (which have an average multiplicity of 1.7);
- Conflagration attacks (which have an average multiplicity of 1.95);
- Aircraft, sabotage, chemical, biological, radiological attacks (which have an average multiplicity of 1.4); and
- Nuclear bombs (which have an average multiplicity of 1)



The previous slides describe how a terrorism stochastic attack set along with three probabilistic components -- the attack conditional probabilities, event frequency and attack multiplicity -- are determined. The end result is a terrorism stochastic attack set and probabilistic inputs which form the building blocks to run an exceedance probability analysis in the RMS Probabilistic Terrorism Model (PTM) application.

For the U.S., the stochastic attack set contains over 66,000 unique individual attacks which are defined as RMS' best estimation of the most probable weapon types that could occur at the most probable targets. The stochastic attack set covers over 4,000 targets across the U.S. and includes 35 different attack modes.

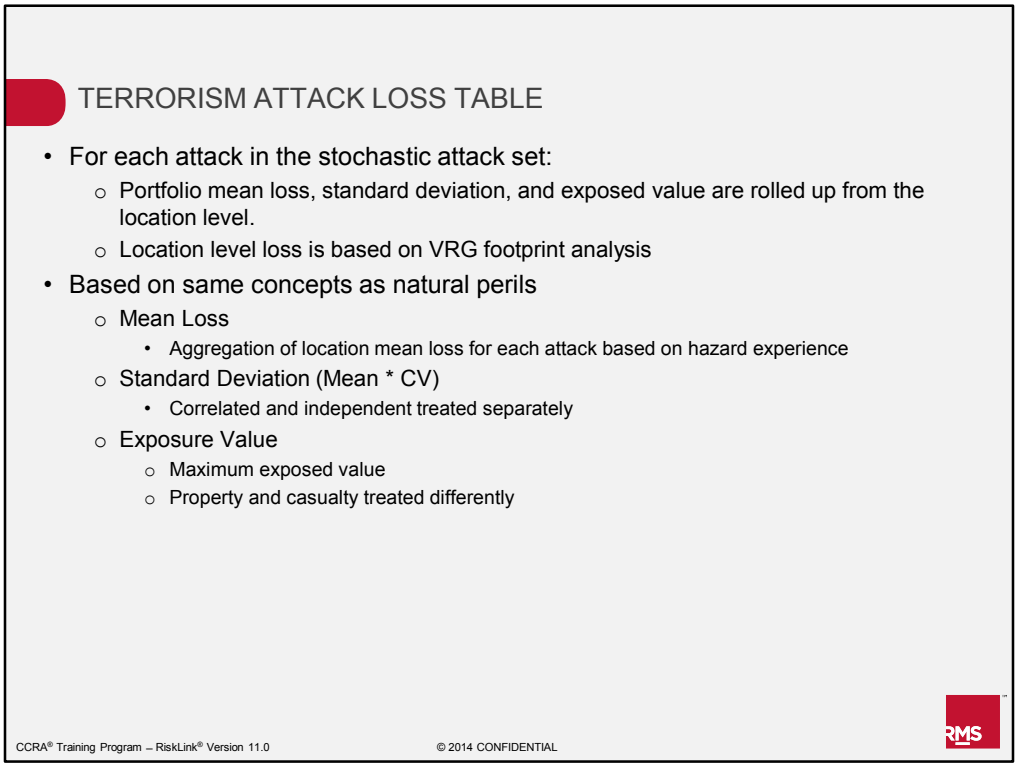
Each attack in the stochastic attack set is assigned a conditional probability using an approach that considers concepts from game theory. Event frequency and attack multiplicity distributions are modeled separately. In addition, RMS models a total of three alternative risk outlooks, or three distinct probabilistic models for a given stochastic attack set, to help users quantify uncertainty around the overall rate of terrorism event occurrence.



Now that we have established how RMS has built a stochastic terrorism attack set including a probabilistic model that considers both that terrorism events are not random and that multiple attacks can make up a single event, we can return to the familiar RMS framework for modeling probabilistic natural peril models.

As review, remember that the probabilistic terrorism follows the same process as natural perils starting with…

- The stochastic module which defines the terrorism attacks; to the…
- Hazard module that for each event determines the hazard footprint of the attack; to the…
- Exposure module that determines which locations in your portfolio are affected by the given hazard footprint; to the…
- Vulnerability module that determines a mean damage ratio (MDR) or mean casualty rate for the attack; finally, to the…
- Financial module that calculates a ground up loss and flows through financial structures to determine gross and net financial perspectives.



A terrorism attack loss table (ALT) is the equivalent of a natural peril model event loss table (ELT) but with a few key differences. This slide first focuses on the similarities between the ALT and ELT. The next slide emphasizes the important differences. Just as for natural perils, the attack loss table is made up of a collection of scenarios defined in the stochastic attack set. For each attack in the stochastic set, the portfolio mean loss, standard deviation (independent and correlated), and exposed value are rolled up from location level losses, standard deviation, and exposed values determined using a VRG analysis.

The portfolio mean loss is the aggregation (or sum) of the mean loss for each location. The standard deviation (SD) is quantified separately for the correlated and independent portions. Like natural perils, the correlated SD is summed for each location and the independent SD is the square root of the sum of the squares from the location level. For property, the exposed value is the sum of exposed values for each location. For casualty analyses, the exposed value is the sum of the number of people in a given injury level multiplied by the average benefit for that injury level.

DIFFERENCES BETWEEN THE ALT AND ELT

- The attack loss table (ALT) is a collection of individual scenario losses from the RMS terrorism stochastic attack set.
- Main difference between RMS ALT and ELT is the rate field.
  - Terrorism
    - "Rate" is a function of the conditional probability, average frequency, and average attack multiplicity, and follows a control process rather than a Poisson process.
    - Conditional probability (and not rate) is output to the RMS RDM.
    - Each attack in the ALT is NOT independent.
  - Natural perils
    - "Rate" is the event rate; assumption is that natural peril events are random and follow a Poisson distribution.
    - Each event is independent.

Attack Loss Table – Ground Up Loss

Event Id	Ground Up Mean Loss	Std Dev - Correlated	Std Dev - Independent	Exposed Value	Conditional Probability
A	1,000			100,000	0.025
B	500			100,000	0.050
C	2,000			100,000	0.005
D	100			100,000	0.100

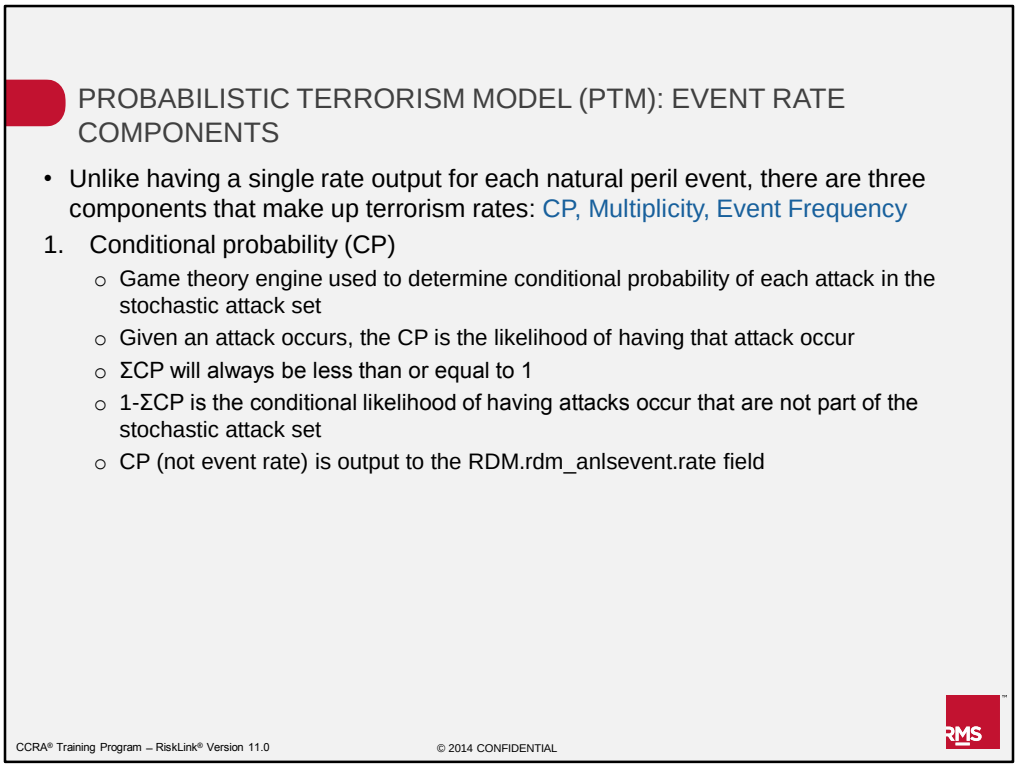
CCRA® Training Program – RiskLink® Version 11.0 © 2014 CONFIDENTIAL

The terrorism ALT has a few key differences when compared to the natural peril ELT, which are summed up in this slide.

The primary and most important difference between the ALT and ELT is what is output as the "rate" for each scenario in the stochastic set. For terrorism, a rate is defined as the product of several probabilistic components including the attack conditional probability, the average event frequency, and the average attack multiplicity. To reiterate an earlier slide in this unit, this is done in order to accommodate that terrorism frequencies are defined using a control process rather than a Poisson process.

Another key difference between the terrorism ALT and natural peril ELT is that each attack in the ALT is not independent. In other words, if an attack were to occur, it would have significant impact on the likelihood of future attacks occurring. By contrast, the occurrence of one earthquake event in San Francisco does not affect an event from occurring in Los Angeles. In other words, the events in a natural peril model are modeled as being completely independent of one another. This assumption is most important to consider when building an exceedance probability curve.

One important note for RMS product users is that the conditional probability, and not the rate, is output to the RMS RDM when you run a terrorism analysis.



The next few slides cover important information about each of the three RMS probabilistic terrorism model components that are used to calculate a terrorism event rate– conditional probability, multiplicity, frequency. To start, let us take a look at the attack conditional probability (CP).

The attack CP is generated using the game theory engine described earlier in this unit and is available for each attack in the stochastic attack set. To reiterate, **the CP can be defined as the probability of an attack given that the attack has occurred**. In theory the sum of the CP will always be less than or equal to one. In the RMS model, 1-sum(CP for all stochastic attacks) is the conditional likelihood of having an attack occur that is not covered by the attacks modeled in the stochastic attack set (for example, surface to air missiles are not included in the stochastic attack set).

As noted in the previous slide, CP, and not event rate, is output to the RMS RDM when you run a terrorism analysis.

PROBABILISTIC TERRORISM MODEL (PTM): EVENT RATE COMPONENTS (CONTINUED)

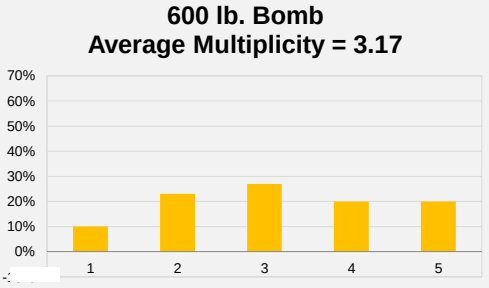
2. Multiplicity
   - Likelihood of having up to five attacks making up one swarm event (e.g. September 11, 2001 was one event made up of three successful attacks)
   - Multiplicity varies by attack group
   - Average Multiplicity (m_i)

$$m_i = \sum_{s=1}^{S} s_i * p(s_i)$$

Where…

s = # of attacks in a swarm event for attack (i)

p(s) = probability of having s attacks for attack (i) in a swarm event



CCRA® Training Program – RiskLink® Version 11.0 © 2014 CONFIDENTIAL

Another probabilistic terrorism model event rate component is the multiplicity distribution.

The multiplicity distribution is the likelihood of having up to five attacks making up one swarm event. The average multiplicity can be defined as the sum product of the possible number of attacks in the swarm and the probability of having that number of attacks in an event.

The multiplicity of attacks varies by attack groups. The full multiplicity distribution for the 600 lb. conventional bomb is shown in the graph on this slide. The average multiplicity for this attack mode computes to 3.17 in the terrorism model.

PROBABILISTIC TERRORISM MODEL (PTM): EVENT RATE COMPONENTS (CONTINUED)

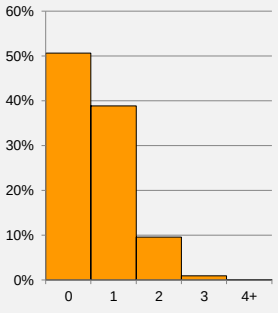
3. Event Frequency
   - Probability of having 0, 1, 2, 3, 4+ events in a year
   - Based on a simulation of: 1) probability of attempted events, 2) probability of success, 3) suppression factor given an event is successful
   - Average Frequency (f)

$$f = \sum_{n=0}^{N} n * p(n)$$

Where…

n = number of events in a year

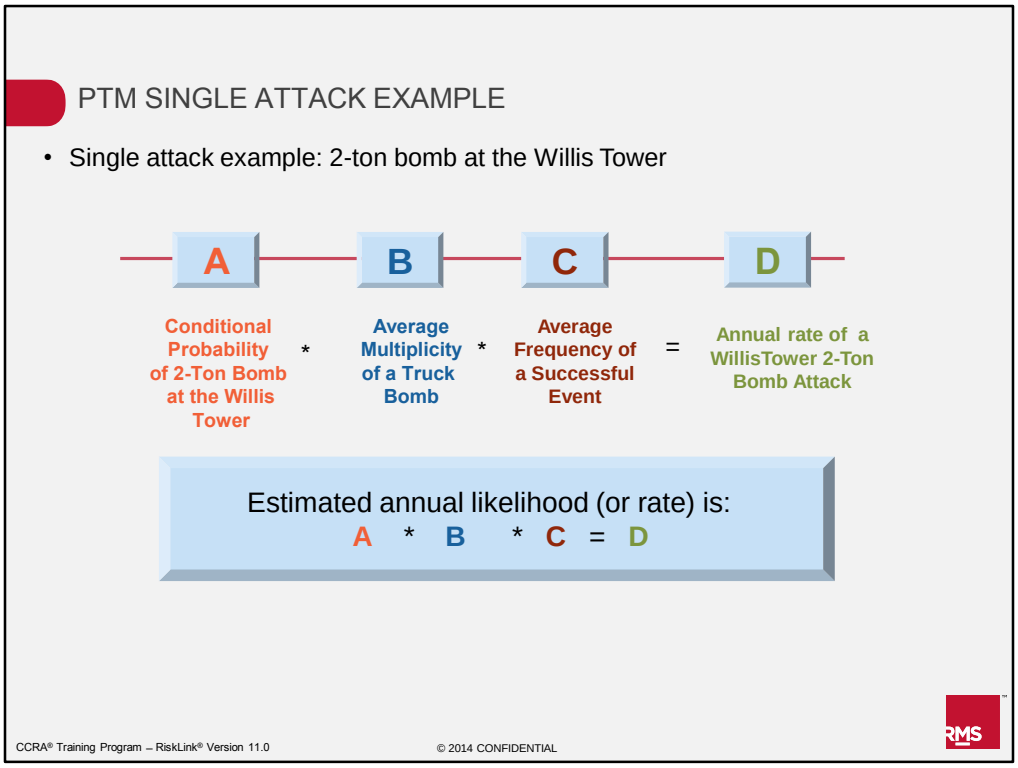
p(n) = probability of having n events in a year



A final probabilistic terrorism model event rate component is the event frequency.

The event frequency can be defined as the probability of having 0, 1, 2, 3, 4, or more events occurring in a year. As described earlier, the frequency distribution is derived using a control process based on a simulation of the probability of attempted event, the probability of success, as well as a suppression factor given an event is successful.

The average frequency can be defined as the sum product of the possible number of events in a year and the probability of having that number of events in a year.



This slide illustrates how to build a terrorism rate from each of the three probabilistic model rate components we just discussed.

AAL CALCULATION FOR TERRORISM

- AAL Calculation for Terrorism
  - Calculation must account for the three terrorism rate components
  - AAL is the sum product of loss, conditional probability, average multiplicity, and average frequency across all attacks in the attack set

$$AAL = f \sum_{i=1}^{N} L_i * cp(i) * m(i)$$

Where…

f = average event frequency

N = number of attacks

Li = amount of loss for attack i (based on the financial perspective under consideration)

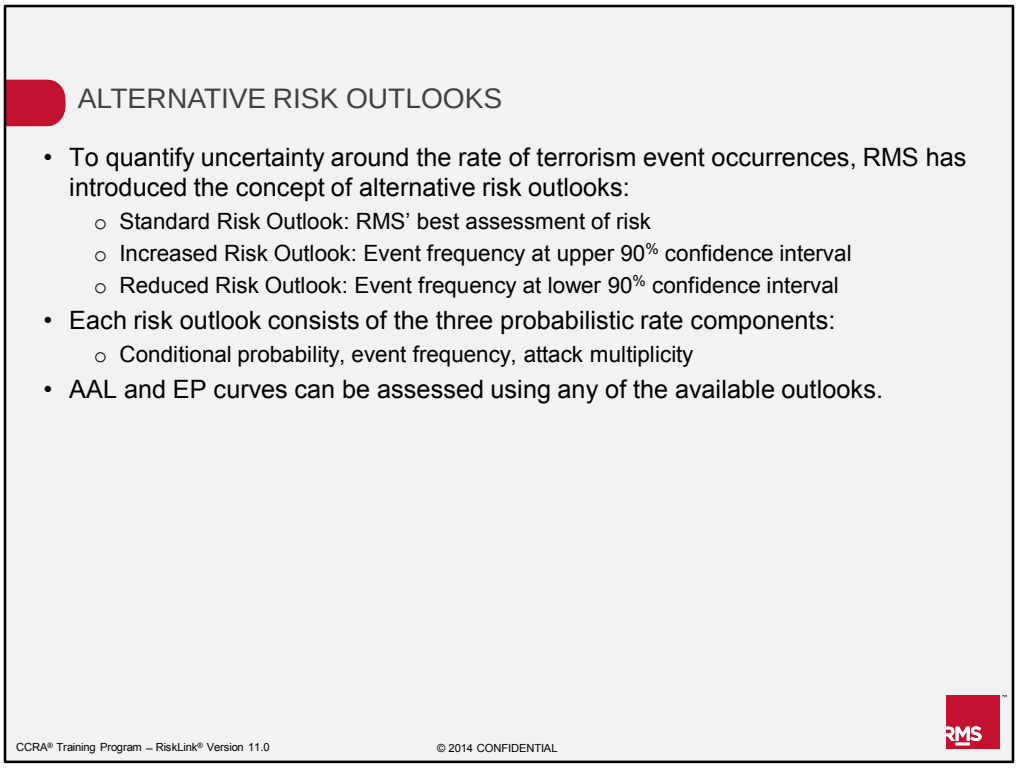
cp(i) = conditional probability for attack i

m(i) = average multiplicity for attack i

Now that we have described how to build a terrorism event rate from the three probabilistic terrorism model components, we can describe how to calculate a terrorism average annual loss (AAL).

As for natural perils, the modeled AAL for terrorism **is the expected loss based on the events represented in the stochastic attack set**. The main difference for the terrorism AAL calculation is that the rate for each attack in the stochastic set must account for all three probabilistic components: the attack conditional probability, the average multiplicity, and the average frequency.

The terrorism AAL can be calculated as the sum product of the loss, conditional probability, average multiplicity, and average frequency for all attacks in the attack set.



To quantify uncertainty around terrorism occurrence rates, RMS models alternative risk outlooks for a given stochastic attack set. For each model release, RMS models three outlooks. The standard outlook for the year is the recommended or expected risk outlook. In addition, we model an increased outlook and a reduced outlook. Alternative risk outlooks are provided in order to capture that terrorism is a dynamic risk and that terrorism risk could change in the year given optimistic and pessimistic changes to the threat environment.

Each risk outlook is comprised of its own set of attack conditional probabilities for each attack in the stochastic set as well as a frequency and multiplicity distribution. As described in an earlier slide on the probabilistic model, the 90% confidence limits from the simulation to determine event frequency are used to model the increased and reduced frequency distributions.

CALCULATING OTHER FINANCIAL PERSPECTIVES

- Other financial perspective ALTs are calculated from the ground up loss.
  - All calculations are in distributed mode using the beta distribution.
- AAL can be calculated from the ALT for each perspective code.
- Only a subset of financial perspectives are supported in PTM.
  - Considers policy structures, facultative and treaty reinsurance

Attack Loss Table – All Other Perspectives

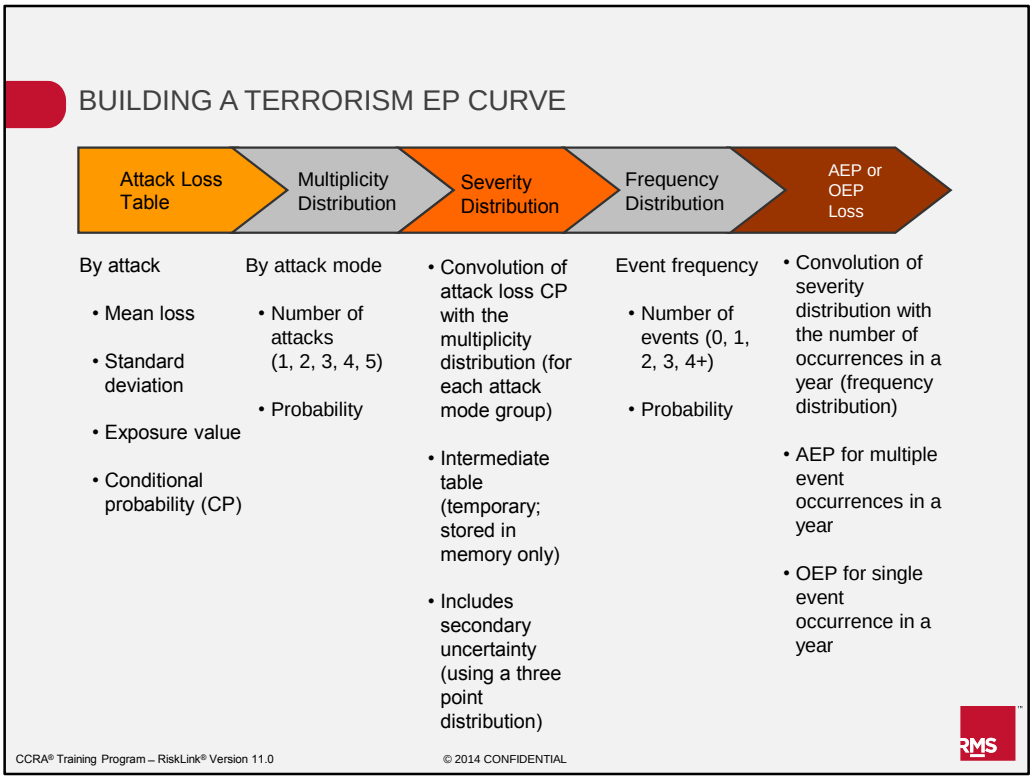
Event Id	Financial Perspective	Mean Loss	Std Dev - Correlated	Std Dev - Independent	Exposed Value	Conditional Probability
A	GU	1,000			100,000	0.025
A	GR	900				0.025
A	RL	750				0.025
A	RP	500				0.025
A	RC	500				0.025
A	FA	150				0.025
A	RG	250				0.025

Similar to the natural peril ELT, the attack loss table for terrorism is output for a variety of financial perspectives. As mentioned in the financial modeling unit of the terrorism course, RMS makes a simplifying assumption that the possibility for multiple attacks making up a single event is considered in the generation of the exceedance probability curve in order to maintain attack specificity at the attack loss table level. This means that most modeled insurance and reinsurance structures apply to single attacks from the stochastic set. The only exception to this is the RMS stop loss treaty that applies to the final exceedance probability curve directly.

The attack loss table is output for various gross and net loss financial perspectives. AAL for each of the financial perspectives can be calculated using the same calculation described in a prior slide in this unit. Note that the underlying assumption is that policy and reinsurance financial structures apply on an attack by attack basis and not to an event loss after considering it could be make up of multiple attacks.

In the RMS Probabilistic Terrorism Model, only a subset of the financial perspectives that are supported in RiskLink are available. Note that all financial calculations in the PTM are run in distributed mode. Financial perspectives, in addition to ground up loss, available for terrorism include:

- Gross loss (GR): net loss after policy deductibles and limits
- Net loss pre-cat (RL): net loss after all facultative and per-risk reinsurance
- Net loss post-cat (RP): net loss after all cat/corporate cat reinsurance
- Net loss post-corporate cat (RC): same as RP
- Facultative reinsurance loss (FA): aggregation of all facultative reinsurance
- Reinsurance gross loss (RG): aggregation of all per-risk, cat and corporate cat reinsurance
- Treaty loss (TY): individual treaty losses (stored in rdm_treaty table)



Once we are able to establish the concept of a stochastic attack set for terrorism, we can start thinking about how to generate an exceedance probability curve based on the attack loss table. We have already highlighted a few of the primary differences between the attack loss table and a natural peril event loss table… namely 1) that the event frequency is not random and should not follow a Poisson distribution; 2) that individual attacks in the attack loss table are not independent as they are for natural perils; and 3) that there is a possibility to have multiple attacks that make up a single event.

In order to address these terrorism-specific model requirements, RMS has implemented a new methodology to build a terrorism-specific exceedance probability curve. The basic concept of the EP curve generation for terrorism is to use a convolution between the loss distribution from the attack loss table with the multiplicity distribution, to generate a severity distribution that considers the possibility for having multiple attacks making up a single loss event. Another convolution is then used to combine the severity distribution with the terrorism-specific frequency distribution to calculate the exceedance probability loss.

TERRORISM SEVERITY DISTRIBUTION

- A severity distribution is built using a convolution process.
  - Loss thresholds and probabilities are calculated from the ALT and multiplicity distribution
  - This is done for nine groups of attacks separately
    - Bombs, aircraft impact, conflagration, dirty bombs, chemical attacks, biological attacks, nuclear bombs, industrial plant sabotage, nuclear plant sabotage
  - A three-point distribution is used instead of a beta distribution to quantify secondary uncertainty

ALT (by attack group)

Eventid	Loss	CP
1		0.0003
2		0.0002
3		0.0065
4		0.0050
5		0.0001

Multiplicity (by attack group)

Attack Mode	# Attacks	Prob
bomb	1	0.50
bomb	2	0.20
bomb	3	0.15
bomb	4	0.10
bomb	5	0.05

Severity Distribution

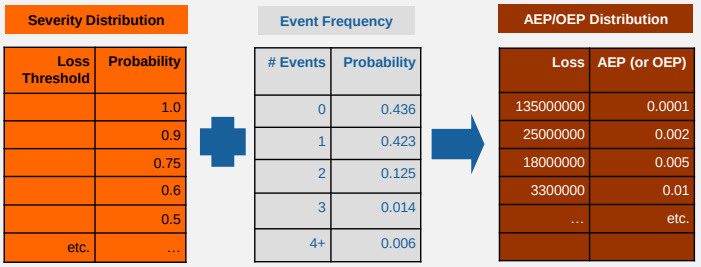
Loss Threshold	Probability
0	1.0
1000000	0.9
2500000	0.75
5000000	0.6
etc.	0.5

Similar to the natural perils, the severity distribution for terrorism is made up of a set of loss thresholds and their corresponding conditional probabilities based off of the stochastic event set. Unlike natural perils, the severity distribution for terrorism is generated using a convolution between the attack loss table and the multiplicity distribution for a set of attack groups.

The resulting severity distribution therefore includes loss thresholds and likelihoods that consider that multiple attacks could make up a single event. Secondary uncertainty is also captured in the terrorism severity distribution; however, when generating the severity distribution, the PTM currently uses a three-point distribution rather than a beta distribution to model secondary uncertainty.

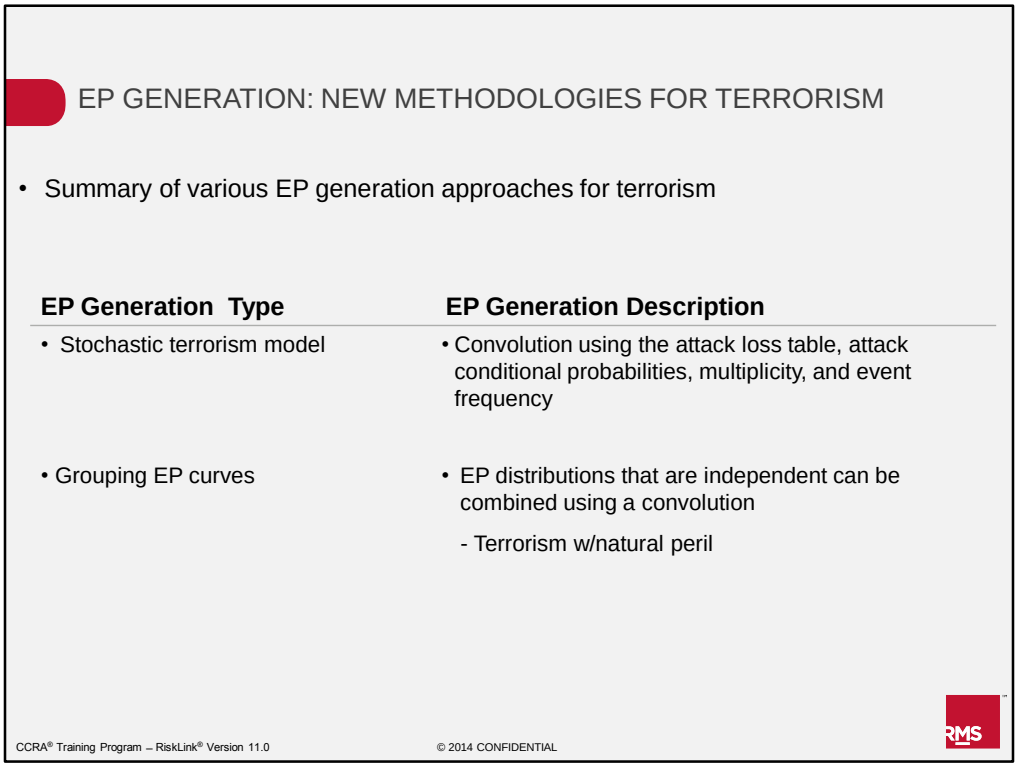
TERRORISM AEP/OEP LOSS DISTRIBUTION

- The AEP and OEP loss distribution is built from a convolution of the severity distribution with the terrorism event frequency distribution.
  - AEP loss distribution considers multiple event occurrences in a year.
  - OEP loss distribution considers a single (maximum loss) event occurrence in a year.



The aggregate exceedance probability (AEP) and occurrence exceedance probability (OEP) curves are generated from a convolution of the severity distribution described in the previous slide and the terrorism event frequency distribution from the probabilistic model. The AEP distribution considers that multiple event occurrences could happen in a year while the OEP distribution looks at only the maximum event loss in a year.

Note that the EP generation for terrorism not only requires an attack loss table, but also each of the three components of the probabilistic model – the attack conditional probabilities, the multiplicity distribution, and the frequency distribution – as inputs. In the RMS PTM, once the attack loss table is generated, you can use the grouping feature to switch the probabilistic model inputs to the EP generation process to quickly assess EP curves and AAL for the different alternative risk outlooks.



The different nature of terrorism risk has required RMS to modify its approaches to generating exceedance probability curves and AAL. This slide is a summary of new approaches to EP generation that RMS has introduced to provide a comprehensive view of terrorism risk that reaches beyond simply looking at deterministic scenario results to manage your terrorism risk.

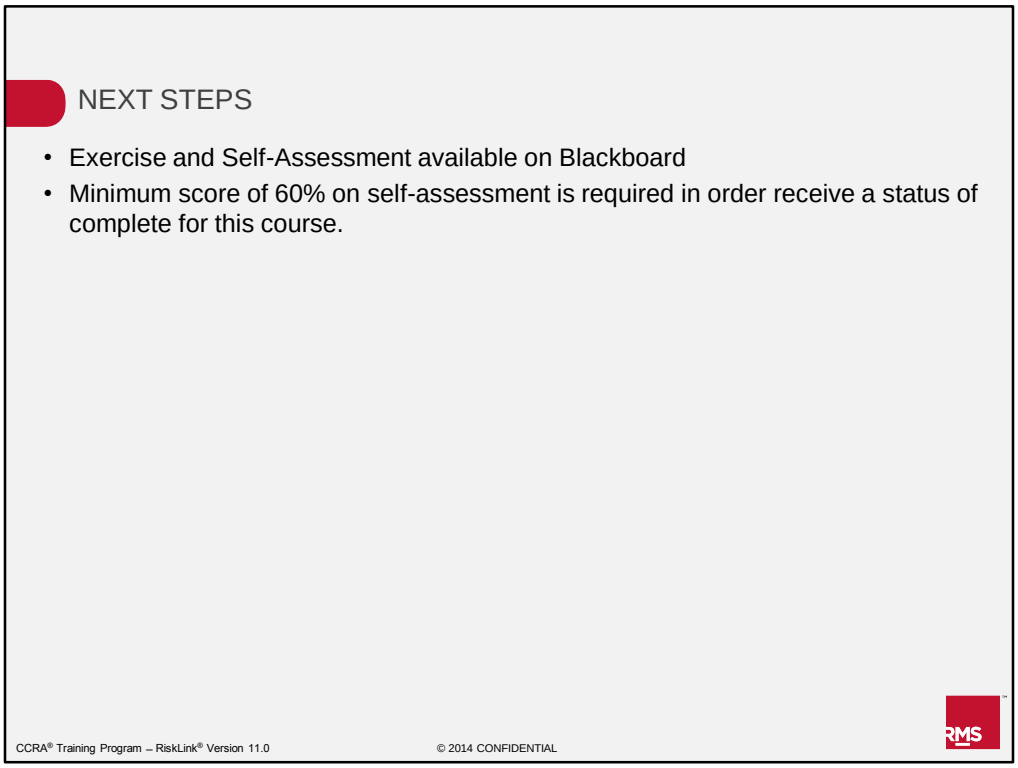
As mentioned in the previous few slides, RMS introduced a terrorism-specific EP generation that uses a convolution to combine various distributions based on inputs that include the attack loss table, the attack conditional probabilities, the attack multiplicity distribution, as well as the event frequency distribution. It should be noted that RMS uses a convolution for speed and accuracy, but the terrorism EP curve could also be generated using a simulation process using the same inputs.

RMS also introduced a way to combine independent EP distributions using a convolution process. For example, grouping is a feature that is available in the RMS PTM application. The grouping feature supports the ability to combine the terrorism model using the terrorism stochastic attack set with natural peril EP curves using a convolution that assumes the EP curves are independent.

U.S. PROBABILISTIC TERRORISM MODELING
KEY CONCEPTS

- RMS has developed a framework for modeling terrorism probabilistically.
  - A model parameterization process is used to develop key probabilistic inputs including
    - Stochastic attack set, conditional probabilities, event frequency, attack multiplicity
  - Designed to support annual updates to incorporate new intelligence made available through RMS terrorism experts
- The probabilistic model maintains key concepts used in natural peril models
  - A stochastic attack set is developed which allows us to model
    - Attack loss table
    - EP curves, AAL, and loss volatility
  - Though similar to natural perils, there are key differences from natural perils
    - Terrorism rates do not follow a Poisson process; RMS uses a control process to model terrorism event frequency
    - Terrorism attacks in the attack loss table are not independent
    - Multiple attacks can make up a single event
    - These differences require a different methodology to generate EP curves and to calculate AAL and volatility

This slide, and the one following, summarize the key points from Unit 6. If any of these points are unclear, please revisit the associated slides within the unit.



In order to fully complete the course work for this peril, complete the exercise and self-assessment available on the Blackboard. You must score a minimum of 60% on the self-assessment in order to receive credit for completing this course.

Completion of three peril model courses is mandatory in order to be eligible to sit for the CCRA® exam.