Journal of Strategic Security

Volume 4
Number 1 *Volume 4, No. 1: Spring 2011*

Article 5

Alternative Threat Methodology

Charles B. King III
Transportation Security Administration, chas.king@dhs.gov

pp. 57-68

Recommended Citation
King, Charles B. III. "Alternative Threat Methodology." *Journal of Strategic Security* 4, no. 1 (2011) : 57-68.
DOI: http://dx.doi.org/10.5038/1944-0472.4.1.4
Available at: https://digitalcommons.usf.edu/jss/vol4/iss1/5

Alternative Threat Methodology

Abstract

Of the many challenges facing risk analysis practitioners, perhaps the most difficult to overcome is in the field of terrorist threat analysis. When estimating the threat associated with naturally occurring events, historical data provides a great deal of insight into the frequency of those events. Threat associated with accidents applies many operations research tools to gauge future failure-rates (Failure Mode and Effects Analysis being perhaps the most widely known). However, estimating the probability of an individual's or group's attacking a specific (or even a generic) target is an element of risk analysis in which art and intuition are applied far more regularly than is science.

Journal of Strategic Security
Volume IV Issue 1 2011, pp. 57-68
DOI: 10.5038/1944-0472.4.1.4

JSS
Published Quarterly by Henley-Putnam University Press
with support from the University of South Florida Libraries

Alternative Threat Methodology

Charles King
Transportation Security Administration
chas.king@dhs.gov

Abstract

Of the many challenges facing risk analysis practitioners, perhaps the most difficult to overcome is in the field of terrorist threat analysis. When estimating the threat associated with naturally occurring events, historical data provides a great deal of insight into the frequency of those events. Threat associated with accidents applies many operations research tools to gauge future failure-rates (Failure Mode and Effects Analysis being perhaps the most widely known). However, estimating the probability of an individual's or group's attacking a specific (or even a generic) target is an element of risk analysis in which art and intuition are applied far more regularly than is science.

Introduction

To the extent one can use the term, the "traditional" method to estimate terrorist threat is to decompose threat into two components,[1] "intent" and "capability," estimate the two variables independently, and then combine them (usually, but far from always, multiplicatively) to generate a non-dimensional threat score.[2] This threat score may take the form of an ordinal ranking (some variant on high, medium, or low), or it may take on a cardinal value (where, for example, a value of six represents a threat which is twice as likely to occur as a threat represented by a three). Which form the score takes depends on the nature of the problem which the analyst is to address.

While the specific terminology varies from tool to tool, "capability" ranges on a scale which begins with a variant on the theme "the group does not possess the resources, training, or experience" to execute the attack. "Capability" ratings steadily increase until they end with "the group has executed a very similar attack before."

"Intent" ratings follow a similar course. They begin with a variant of the theme that the group in question posses "no known desire" to execute such an attack and end with the assessment that the group has developed and is implementing "a feasible plan" to conduct that attack.

For both "intent" and "capability" ratings, analysts reference a scoring matrix which provides several descriptions and corresponding scores. They match their understanding of the threat to the closest "intent" and "capability" description the matrix offers. They then pull out the scores linked to the descriptions which they previously choose. Finally, they combine those scores in a predetermined function to generate a single threat number.[3] That combination mechanism is either a look-up table or a simple function (additive or multiplicative) and does not require analytical interpretation to produce.

Issues with Current Approaches

There are five major issues associated with this "intent" and "capability" framework, and these issues are both interrelated in nature and compounding in effect. They all, directly or indirectly, impact the inherent uncertainty of threat estimates, uncertainty which arises from both a paucity of specific data regarding "intent" and the environmental reality that "intent" can change rapidly.

Implied Precision

When applying ordinal scales, precision is not an issue because the difference between a "low" rating and a "very low" rating is not a relevant concern. Unfortunately, quantitative assessments—the types which provide analysts the ability to combine factors—require a great degree of differentiability in scores, and that requirement demands cardinal scales. Additionally, the use of these scales creates a perception that the threat assessment is both defensible and reproducible, characteristics which are at odds with the subjective and uncertain data which serve as input.

In cases where analysts examine scenarios which are relatively similar (e.g., Vehicle-Borne Improvised Explosive Device (VBIED) attacks on air-

https://digitalcommons.usf.edu/jss/vol4/iss1/5
DOI: http://dx.doi.org/10.5038/1944-0472.4.1.4

ports versus IED attacks on aircraft), this differentiability requirement is not a significant burden. The challenge comes to the fore when comparing the threats associated with very different scenarios. When the nature of either the attack method or the target changes significantly from scenario to scenario (e.g., VBIED attacks on bridges versus biological attacks on bus stations), "intent" and "capability" scores may vary by several orders of magnitude—and it is then that the difference between a "low" and a "very low" score matters greatly.

Relative Nature of Estimates

The second issue, related to the first, is that terrorist threat assessments produce relative likelihood estimates, not absolute ones. When comparing similar scenarios, this is not materially important; analysts can generate reliable estimates using techniques such as benchmarking and reasoning-by-analogy. However, this characteristic becomes more and more important as scenarios become increasingly dissimilar.

Analysts can make judgments regarding the relative likelihood of two similar scenarios—they simply point to areas of divergence and make reasoned comparisons between the two. However, when there are very few points of similarity, it is no longer possible to make that comparison, and the technique—along with the analysis it supports—loses its value.

Human Factors

What makes the situation so frustrating is that it is exceptionally challenging to develop cardinal scales of "intent" and "capability," especially—but not exclusively—at the very low end of the scale. Because quantitative formulas combine several variables multiplicatively, the impact of a change of X basis points increases as the score decreases ($\Delta X/4$, for example, is twenty times greater than $\Delta X/80$). Compounding that challenge is the behavioral reality that people do not have the capacity to make material distinctions between frequency estimates when the difference between one estimate and another is small (e.g., a 4% probability and a 5% probability are both "low" even though one is 25 percent greater than the other). In that light, it is potentially problematic to believe quantitative analyses in cases where analysts have to decide whether a low probability event—an event which has never happened—has a 1 in 100, 1 in 1,000, or 1 in 10,000 chance of occurring.

Correlated Variables

The fourth issue is that it is difficult to develop an approach which combines "intent" and "capability" scores in a consistent, defensible fashion. Federal analysts have been using variants of the "intent" and "capability" framework for decades, and it was a particularly useful model when decomposing threat on a large-scale, multi-year, nation-state level (e.g., the Soviet Union's development of a manned bomber program). However, for terrorism threat assessment purposes, applying that same framework can present its own issues.

Because "intent" and "capability" are not independent variables (an organization which does not possess chemical weapons is not going to develop tactical plans to use them), a formula for combining the two variables has to be non-linear (the threat associated with an "intent" score of 0.5 and a "capability" score of 0.5 cannot automatically be equivalent to a threat with an "intent" score of 0.25 and a "capability" score of 1.0). While it is clear that there is a correlation between the two variables, the nature of the relationship between the two variables is not well understood. Indeed, it may change on a scenario-by-scenario basis.

Inter-Judge Consistency

The final issue is that multiple analysts, all sorting through complex, incomplete data, and converting that information into a single score, do not consistently agree about what that score should be. Part of the challenge is that neither "intent" nor "capability" data is sufficiently clear-cut as to allow for a mechanistic conversion from textual information to a point score. Part of that challenge is that analysts have individual biases upon which they rely to weigh the value of the information they use to make their judgments. And part of that challenge is analysts do not always feel compelled to follow the ranking guidance they receive.

These challenges combine to reduce the degree to which scores are repeatable across analysts. While there are techniques to improve cross-analyst consistency (such as beginning the process by ranking a representative set of scenarios as a group), these techniques only reduce the consistency problem; they do not eliminate it.

https://digitalcommons.usf.edu/jss/vol4/iss1/5
DOI: http://dx.doi.org/10.5038/1944-0472.4.1.4

A Different Approach

To partially compensate for these issues, analysts may consider using a threat-scoring system based on the resources necessary to carry out the attack. Such a system assumes that organizations do not pursue acquiring the capability to conduct attacks which they have no intent of executing.

To apply this system, the analyst first determines the level of resources terrorists need. There are six options from which to choose, ranging from those of a nation-state to those of a single, law-abiding resident.

Once the analyst decides which table to apply, he or she determines which description of activity/reporting is most similar to the threat being examined. The analyst then uses the three scores corresponding to that description either as the points of a triangular distribution (for a Monte Carlo simulation) or as the limits of a range in which they independently choose a point estimate of threat—using the value in bold font as a default.[4]

Example Using Proposed Approach

Consider the case where an analyst is examining the likelihood of al-Qaida using a nuclear weapon against the United States. The analyst would first decide, based on the North Korean experience, that executing such an attack would require both a decade and resources of a nation-state. That decision would drive the analyst to use Table II. After reviewing current intelligence, the analyst would decide that, within Table II, the word picture which comes closest to describing the current intelligence is, "There are no indications of any nation-state transferring technical knowledge, material, or devices to the enemy." Accordingly, the analyst would use the points .00–**.001**–.003 as the low, medium, and high points for a Monte Carlo simulation.

Example Using Current Approach

Consider the same case, but change the analytic framework to the "intent" times "capability" approach, where both "intent" and "capability" are measured on ten-point scales. That same analyst would agree with President Obama's statement on April 12, 2010, when he said, "We know that organizations like al-Qaida are in the process of trying to secure nuclear weapons or other weapons of mass destruction, and would have no compunction at using them." Accordingly, the analyst would assign an "intent" score no lower than a "1"—meaning that al-Qaida's level of intent is as least aspirational. The analyst's next step would be to examine "capa-

bility." For that category, the analyst would again review current intelligence and would decide that al-Qaida does not have, but is trying to acquire, components for a nuclear device. Accordingly, the analyst would assign a "capability" score no lower than a "1."

Multiplying the two terms generates a threat score of 1 (out of 100)—implying that the likelihood of al-Qaida using a nuclear weapon against the United States is at least 1% as great as that of al-Qaida attempting an attack via any other vector (such as Improvised Explosive Device [IED]). It is clear that this conclusion materially overstates the likelihood of al-Qaida attempting to attack the United States with a nuclear weapon, given:

- existing safeguards on fissile material;
- al-Qaida's limited resource base;
- their familiarity with other attack vectors; and
- the relative ease with which they could execute an IED attack.

Limitations

The scales used are relative. While these tables provide analysts with a tool which allows them to compare across materially different threat scenarios, the scores are not directly comparable with the frequency estimates associated with natural hazards. For example, it is reasonable to assign Umar Abdulmutallab's attempt to bomb Northwest Flight 253 to the ".60–**.75**–1.0" range in Table V, where "Delivery to the target site requires specialized knowledge or equipment **and** there are credible indications that the enemy possesses that knowledge or equipment." However, that range (0.60–1.0) is far too high to be an annual probability since the previous attempt, Richard Reid's plot to bomb American Airlines Flight 63 occurred eight years prior. The time lag between those two events indicates that the suggested probabilities may be six to ten times too high to be absolute values.

The validity of low-end scores remains questionable. While the range of the scale used (0.001–1.0) provides for finer low-end gradation than does a 1 to 10 scale, there is little to suggest that the scores for very low probability threats (e.g., improvised nuclear devices) are within even an order-of-magnitude of reality.

https://digitalcommons.usf.edu/jss/vol4/iss1/5
DOI: http://dx.doi.org/10.5038/1944-0472.4.1.4

This approach assumes that analysts will be aware of terrorists' efforts to develop innovative ways to combine existing skills and knowledge to create new attack vectors. Terrorists have repeatedly demonstrated their ability to innovate; and there is every reason to assume that they will continue to do so. They will creatively combine resources to circumvent existing security measures, and, when they do, it is quite likely that their adaptability will surprise analysts and security professionals alike.

Finally, this approach does not account for serendipity. While terrorists take a deliberate approach to planning attacks, random chance plays a part in target selection as well (e.g., a terrorist cell with a member who is a bridge engineer is more likely to attack a bridge than is a cell without one). Similarly, random chance is likely to play a role in capability development. If a terrorist cell happens to recruit both a chemical engineer and an HVAC repairman, that cell is far more likely to attempt to develop a chemical weapon than would otherwise be the case.

Conclusion

Terrorism risk analysis is a field in its infancy, and it faces many challenges, not least among them being the development of useful and accurate quantitative threat assessment methodologies. Practitioners have identified a need for a substitute for the "intent" and "capability" model of threat analysis, and this monograph serves to shine a light on one possible alternative.

About the Author

Mr. Charles B. King III is the Risk Analysis Branch Chief for the Transportation Security Administration. He earned a B.S. from the United States Military Academy, an M.B.A. from Duke University, and an M.S. in National Security Studies from the National War College. You may reach him at: *chas.king@dhs.gov*.

Table I: Ranking Estimated Capability

Score	**A**	**B**	**C**	**D**	**E**	**F**
Resources needed to execute attack	Requires a decade and resources of a nation-state to execute	Requires years of multiple people with graduate degrees in technical sciences, and resources of Fortune 1,000-like company to execute	Requires multiple people with graduate degrees in technical sciences, and luck, to execute	Requires specialized knowledge of technical or engineering processes to execute	Requires the acquisition of illegal/ controlled products to execute	Requires legally purchased products and readily available manufacturing instructions to execute

https://digitalcommons.usf.edu/jss/vol4/iss1/5
DOI: http://dx.doi.org/10.5038/1944-0472.4.1.4

Table II: Nation-State

Score	.00 – **.001** – .003	.01 - **.05** – .20	.05 – **.20** – .30	.40 – **.60** – .85
Requires a decade and the resources of a nation-state to execute	There are no indications of any nation-state transferring technical knowledge, material, or devices to the enemy	There is unconfirmed reporting that a nation-state has transferred knowledge to the enemy **or** there are indications that the enemy can acquire device due to inadequate security at a storage site	There is unconfirmed reporting that a nation-state has transferred material to the enemy	There is confirmed reporting that a nation-state has transferred material to the enemy **or** there are indications that a nation-state has lost control of a man-portable device

Table III: Fortune 1,000 Company

Score	.001 – **.005** – .01	.05 – **.15** – .50	.35 – **.40** – .85
Requires years of multiple people with graduate degrees in technical sciences, and the resources of Fortune 1,000-like company to execute	There are no indications of any organization transferring technical knowledge, material, or devices to the enemy	There is unconfirmed reporting that a company has transferred manufacturing knowledge to the enemy **or** there are indications that the enemy can acquire material due to inadequate security at a storage site	There is confirmed reporting that a company has transferred manufacturing knowledge to the enemy

Table IV: Multiple Technically-Trained People

Score	.001 – **.01** – .02	.01 – **.05** – .10	.30 – **.50** – .80	.70 – **.80** – 1.0
Requires years of multiple people with graduate degrees in technical sciences, and luck, to execute	There are no indications that the enemy has begun a research program	There are multiple reports that the enemy has begun a research program	There are multiple reports that the enemy has begun testing a delivery device	There are multiple reports that the enemy has completed an effective distribution system

Table V: Specialized Knowledge

Score	.05 – **.20** – .30	.40 – **.50** – .80	.60 – **.75** – 1.0
Requires specialized knowledge of technical or engineering processes to execute	Delivery to the target site requires specialized knowledge or equipment **and** there are no credible indications that the enemy possesses that knowledge or equipment	Delivery to the target site requires specialized knowledge or equipment **and** purchasing or renting that knowledge or equipment is a commercially viable option	Delivery to the target site requires specialized knowledge or equipment **and** there are credible indications that the enemy possesses that knowledge or equipment

https://digitalcommons.usf.edu/jss/vol4/iss1/5
DOI: http://dx.doi.org/10.5038/1944-0472.4.1.4

Table VI: Illegal Products

Score	.10 – **.15** – .40	.20 – **.40** – .50	.20 – **.40** – .60	.50 – **.60** – .70	.50 – **.60** – 1.0
Requires the acquisition of illegal/ controlled products to execute	The enemy would have to steal a product to acquire it in the U.S. **and** there are no indications this has happened	The enemy would have to steal a product to acquire it in U.S. **and** there are indications this has happened	The enemy could purchase the product in the U.S. **and** there are no indications this has happened	The enemy could purchase the product in the U.S. **and** there are indications this has happened	There are indications that the enemy has acquired the product outside of the U.S.

Table VII: Legal Products

Score	.70 – **.80** – .90	.80 – **1.0**
Requires legally purchased products and readily available manufacturing instructions to execute	The target is easily accessible and the purchase of a quantity of equipment necessary to develop a device may raise suspicion	The target is easily accessible and the purchase of a quantity of equipment necessary to develop a device would not raise suspicion

References

1 Threat is the likelihood of an attack being attempted by an adversary or the likelihood that a hazard will manifest itself within a given time-frame.

2 In this model, capability is the ability of an adversary to attack with a particular attack method, while intent is the desire or design to conduct a type of attack or to attack a type of target.

3 These scores are either cardinal or ordinal in nature.

4 The look-up tables are at the end of this monologue.

Journal of Strategic Security

https://digitalcommons.usf.edu/jss/vol4/iss1/5
DOI: http://dx.doi.org/10.5038/1944-0472.4.1.4