WORKING PAPER

Using Risk Analysis to Inform Intelligence Analysis

HENRY H. WILLIS

WR-464-ISE

February 2007

RAND INFRASTRUCTURE, SAFETY, AND ENVIRONMENT

ABSTRACT

The study and application of risk analysis provides a set of tools with a strong methodological foundation. This chapter describes how risk analysis can be integrated into the intelligence cycle for producing terrorism threat assessments and warnings. Intelligence professionals can use the risk analyst's toolbox to sharpen conclusions that are made in intelligence products by providing support for identification of scenarios of greatest concern. Risk analysis can also be used to focus future collection efforts on information that appears to be most relevant to refining existing estimates of terrorism risks. However, risk analyses must be conducted to meet challenges of information availability, matching resolution of results to the problem, reflecting risk as the social construct that it is, and not ignoring the possibility of surprise.

Key Words: intelligence analysis, risk analysis

The goal of intelligence is to produce guidance based on available information within a time frame that allows for purposeful action. In efforts to combat terrorism actionable guidance could come in many forms.

Sometimes guidance is needed to shape strategy. For example:

- the federal government must decide whether to maintain stockpiles to enhance emergency preparedness, or
- state and local governments must choose for which scenarios to develop response plans and train.

Sometimes guidance is needed to inform operational decisions. For example:

- if the federal government decides to use stockpiles, it must decide what to put in them and how to preposition them, or
- airports must decide how to deploy technologies and modify operations to enhance security.

Sometimes the required guidance is on a tactical level. For example:

- law enforcement must know when to deploy additional surveillance around a building or for an event,
- law enforcement is interested in which people may be planning an attack, or
- critical infrastructure owners and operators need to know when greater security is required.

All of these examples require different information, but have one thing in common. They all require that the information be appropriate for the intended use.

The concept of the intelligence cycle provides a structure to the process of producing this guidance. The intelligence cycle (see Figure 1) begins with the direction of intelligence collection (Step 1). This results in collection of new information (Step 2) that must be processed (Step 3), analyzed (Step 4), and disseminated and used (Step 5). Use of the intelligence products creates new information through either active (i.e., new directed intelligence collection) or passive (i.e., observance of resulting events) means. The intelligence cycle is closed by feeding this new information back into this process (Krizan 1999).

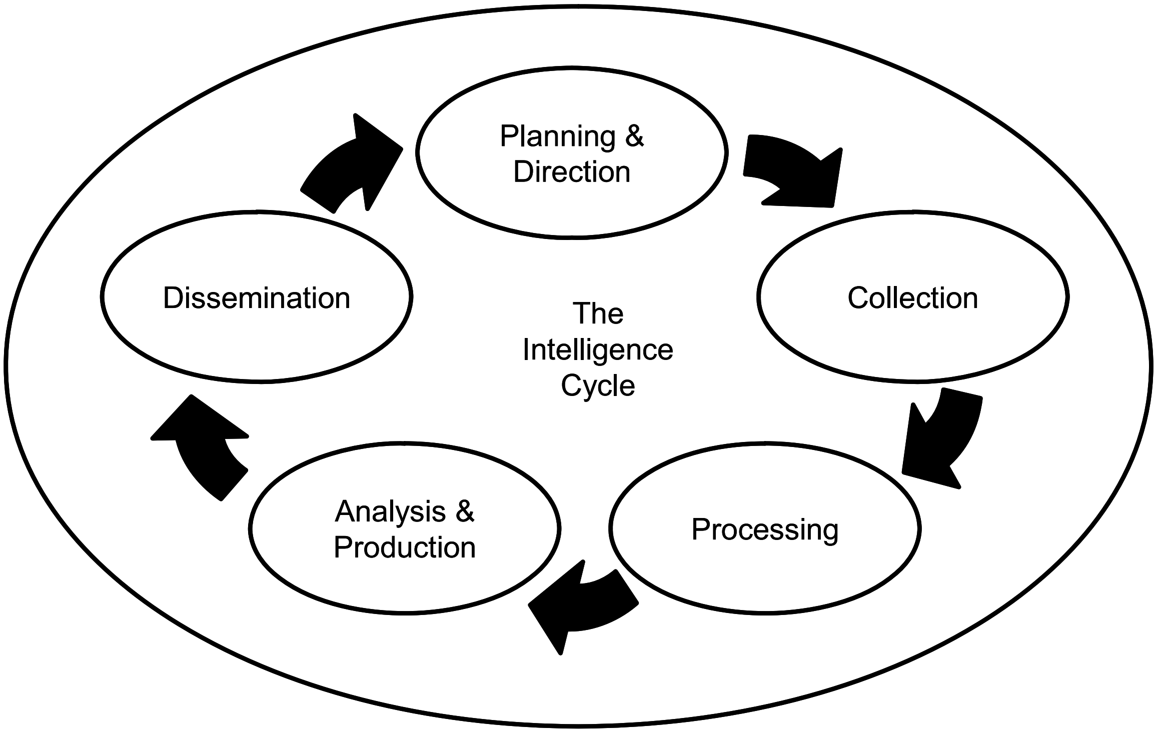


Figure 1 The Intelligence Cycle (adapted from Krizan 1999)

Time is critical to the success of this process because adversaries also carry out their own intelligence processes to identify promising opportunities for attack and target vulnerabilities. Intelligence is more valuable if the intelligence cycle operates faster than the opponent's. More rapid intelligence enables faster recognition of new threats and adaptation to shifts in opponents' strategies. Thus, methods to improve the accuracy and speed of the process provide a strategic advantage in efforts to combat terrorism.

This chapter discusses how risk analysis can help intelligence analysts assess threats of terrorism. The discussion leads to two conclusions. First, risk analysis can be used to sharpen intelligence products. Second, risk analysis can be used to prioritize resources for intelligence collection. However, it is important that practitioners applying risk analysis recognize its limitations to ensure that results are appropriate for the purpose and that its use does not blind the analyst to potential surprises.

The remainder of the chapter is organized as follows. The next section describes intelligence analysis as an input-output process and maps risk analysis to this process. Following this description is an introduction of challenges to the successful application of risk analysis to intelligence analysis. The chapter closes with a summary of how risk analysis can best serve the intelligence analysis community.

INTELLIGENCE ANALYSIS AS AN INPUT-OUTPUT PROCESS

The analysis function of the intelligence cycle in Figure 1 can be considered an input-output process where raw intelligence is the input and intelligence products are the outputs. Within this framing, Willis et al. (2006) described how risk analysis can be connected to the intelligence cycle (see Figure 2).

The process outlined in Figure 2 represents an interaction between the intelligence community and the intelligence customer. In the case of terrorism risk, this is the managers responsible for implementing homeland security policies and programs. In the same way that the intelligence cycle must be an iterative process, the intelligence community and the homeland security community must interact closely and at many stages throughout the process of collection, processing, and analysis.

Collection activities produce intelligence that can be used to assess the magnitude and nature of terrorism threats. Here relevant information is that which describes terrorist capabilities to carry out attacks of different complexity, fiscal and personnel resources to support such attacks, goals in pursuing terrorist activities, and objectives associated with any particular attack plan. This information alone has been used to assess the range of terrorist threats that exist and how they are adapting to evolving security postures. Analyzing all of these factors is important for threat does not exist unless a group or individual has both the intent and capability to conduct an attack (Cragin and Daly 2004; Chalk et al. 2005).

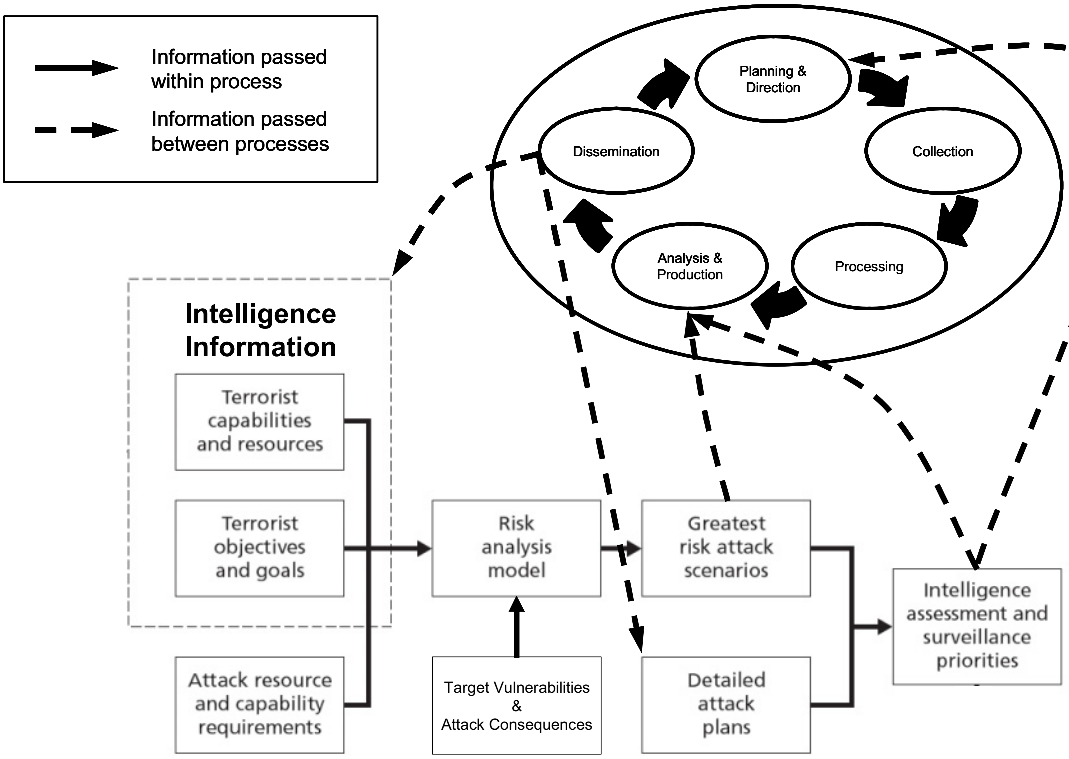

Information passed within process
Information passed between processes
Planning & Direction
Collection
Processing
Analysis & Production
Dissemination
Intelligence Information
Terrorist capabilities and resources
Terrorist objectives and goals
Attack resource and capability requirements
Risk analysis model
Target Vulnerabilities & Attack Consequences
Greatest risk attack scenarios
Detailed attack plans
Intelligence assessment and surveillance priorities

Figure 2 Connections between risk analysis and the intelligence cycle (adapted from Willis et al., 2006)

However, terrorism risk is not determined by threat assessment alone. Risk from terrorism only exists when there is a credible threat of attack that could cause harm to a target that is vulnerable (Willis et al 2005). Risk analysis provides a framework for considering threat, vulnerability, and consequences of potential terrorist attacks and developing strategies to manage these risks most effectively with limited resources.

As depicted in Figure 2, risk analysis combines intelligence about the objectives and capabilities of terrorist groups with assessments of the required capabilities and resources to complete successfully an attack, assessments of the vulnerabilities of targets to different attack modes, and assessments of consequences of different types of attacks on different targets. The product of this analysis is identification of terrorism scenarios that present the greatest risk.

This result itself can be used by the intelligence cycle. Thus, at its most basic form, risk analysis can be integrated into the intelligence cycle as part of the analysis and production step. However, assessments of the relative risks of different attack scenarios may only be adequate as intelligence products to support for strategic and operational analysis.

Often more specificity than relative risks of different attacks is required about where an attack will occur, when the attack will occur, or who will try to attempt the attack. In particular, law enforcement agencies attempting to prevent future terrorist attacks need to have guidance of where to conduct further surveillance and who to target with such efforts. This information requires an understanding of the detailed steps and timelines associated with planning and orchestrating an attack. Some aspects of this are specific to the target and attack mode being considered. Others aspects are specific to how the group that is planning the attack operates.

Detailed information about attack planning can be developed through surveillance of terrorist groups, investigations into foiled or successful plans for attacks, and red-teaming studies facilitated by tools of risk analysis. Rosoff and von Winterfeldt (2006) demonstrated how probabilistic risk analysis can be used in this way within the context of scenarios for detonating a radiological device at the ports of Los Angeles and Long Beach. In this study, probabilistic risk analysis was used to decompose the attack scenario into its component steps and explore how defensive countermeasures directed at each step could reduce the risks of attack.

By combining the results of risk analysis with detailed assessments of the planning stages of terrorist attacks, the intelligence process can provide directed intelligence products and refine future planning and direction of intelligence collection.

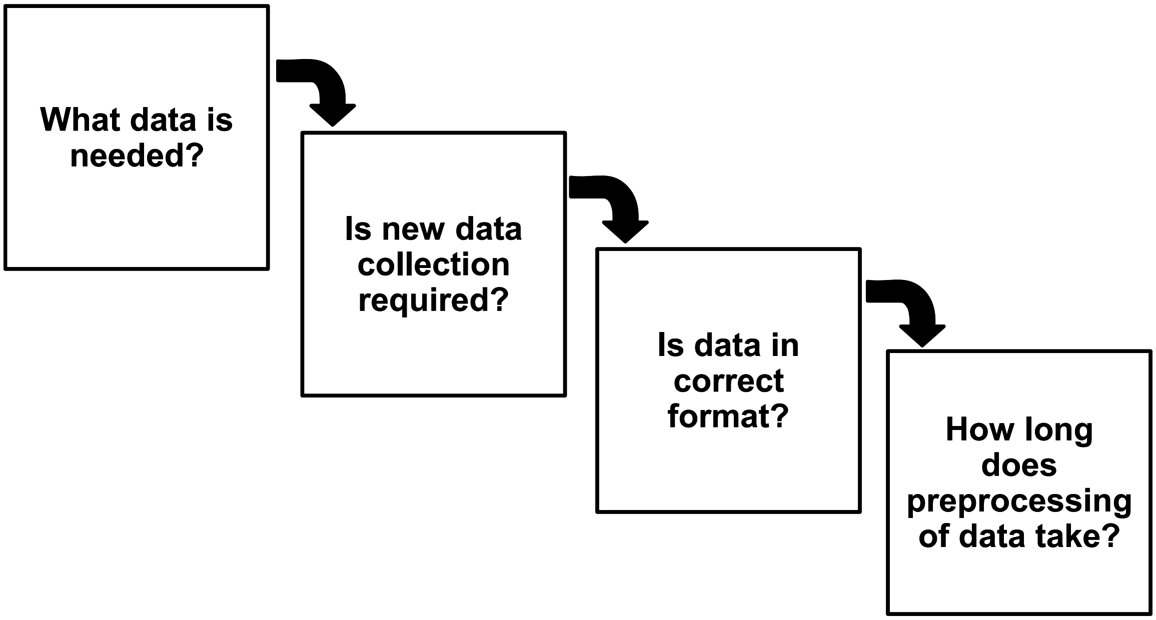
ANALYST’S CHALLENGES TO APPLYING RISK ANALYSIS PRODUCTIVELY

The productive application of risk analysis to support intelligence analysis must address four methodological challenges: (1) developing methods that can be supported with obtainable information; (2) matching resolution of results with the problem; (3) applying the best practices of risk analysis; and (4) avoiding the potential for blinding analysts to the possibility of surprise.

Basing analysis on obtainable information

While discussions of terrorism risk have received more attention recently, the methods of risk analysis are supported by decades of development and application which include the study of risks of terrorism to critical infrastructure (Garrick 2002, Haimes 2004). This creates a strong methodological foundation on which to build and pool of expertise on which to draw.

However, it also creates the potential that well intentioned risk analysts could develop tools for which required input data are not obtainable in an effort to bring their capabilities to bear on the issue de jour. This problem of pushing tools in a manner for which they cannot be used can be avoided by asking and answering four questions at early stages of a risk analysis (see Figure 3).



What data is needed?

Is new data collection required?

Is data in correct format?

How long does preprocessing of data take?

Figure 3 Considerations regarding availability of information to support risk analysis

First, simply consider what data are needed. Asking this question initiates the process of considering what information is required and what information is available.

Second, determine whether the risk assessment requires additional data collection. In some cases, if the data aren't already available financial or time considerations will preclude going further. In other words, if the data are not obtainable, the analytic approach is dead on arrival. In other cases, learning that new data are needed initiates a process of refining future planning and direction of intelligence collection or developing innovative approaches to obtaining proxies for required data elements.

Third, analysts must consider whether data are in the correct format and resolution for the analysis. Typically, the data that have been already collected will not have been assembled with risk analysis in mind. The data could be in an incorrect format, could be incomplete because of missing data elements, or could also be internally incoherent because of conflicting reports or assessments of particular data elements. In any of these cases, the data may require cleaning and processing before they can be used in risk analysis. This is important because of the fourth question: How long does any required preprocessing take to complete?

It may be the case that new data are required and that new or existing data must be preprocessed before the data can be used in a risk analysis. However, the time required to do this affects whether and how the information can be used to support intelligence analysis. Tactical decisionmaking is generally very time critical and allows little time for analysis. Strategic and operational decisionmaking is generally less urgent. Ideally, all required information is immediately available and the collection and processing of it does not lengthen the time of the intelligence cycle. To the extent more time is required, the information may become less useful for supporting tactical operations where the value of intelligence information is measured in its ability to inform decisions that are made in a matter of hours if not a few days.

These four questions are all basic and seemingly second nature to analysts familiar with informing real decisions. However, if not carefully considered when developing or proposing applications of risk analysis, the results can be a process of little or no value.

Matching resolution of analysis to the problem

There is no single risk assessment tool that fits the demands of all problems. Each problem has unique aspects that determine requirements for the spatial and temporal resolution of results (Willis 2005).

Risk assessments intended to support design or performance assessment for security need to be tuned to a specific threat or target, but not necessarily on a specific time. For example, consider an assessment used to buttress physical security at a nuclear power plant. Designs need to be focused on specific types of attacks on specific parts of the plant, but it is much less important whether the attacks would occur this year or next.

Risk assessments for strategic planning need to be specific about what types of attacks could occur, but do not require specificity of when or where the attacks will occur because strategic assessments need only reflect the range of threats of terrorism. For example, think of analysis to support the division of resources among control of nuclear proliferation and border security. Here the decisionmaking does not require distinctions between specific places or which attack will happen first. It is important instead that the planning consider the correct range of attacks.

Finally, risk assessments to support tactical decisions require both spatial and temporal specificity. They will be used to help commanders decide what actions to take and when to take them. For example, consider analysis that would help local law enforcement determine where and how many officers to deploy in security around a national political convention and when and where to supplement security in response to specific threats. Assessments of risks based on capabilities terrorists had last year are irrelevant if the way the group operates has changed dramatically.

Figure 4 presents the results of a comparative risk assessment that one user may see as having little value but another could see as insightful. This figure presents an estimate of the distribution of the relative risk of terrorism across Manhattan in terms of casualty costs associated with workers' compensation claims following a terrorist attack. In this figure, darker shaded areas reflect regions of higher risk. A first order conclusion drawn from this figure is that terrorism risk is greatest in mid-town Manhattan and the financial district of lower Manhattan.

To the New York Police Department, such information likely has little value. The local community enters the challenge of protecting New York with a strong understanding of where the greatest vulnerabilities exist, and which events or locations represent particular value targets. For them, risk analysis must have a much sharper resolution to be useful. In the effort to prevent future terrorist events, local law enforcement require help determining which intersections to patrol, what questions to ask detainees to crack terrorist networks, and when to step-up security because threats seem more imminent.

For state or federal officials, the analysis may have more value. These groups may not have the same entrenched knowledge of local vulnerabilities and targets. They also may be solving different problems. For example, federal officials are responsible for allocating resources to combat terrorism across the United States in proportion to terrorism risk (Willis et al 2005). Also, when faced with new threat information, federal officials may need to ascertain quickly for which communities the threat information is relevant (Willis et al. 2006). In each of these cases, there is value in having the capability to access quickly or conduct studies of relative risks of terrorism across multiple cities using a common approach with consistent assumptions and data. In such cases, results like those presented in Figure 4 could be useful if accompanied by similar analyses for other communities across the nation.

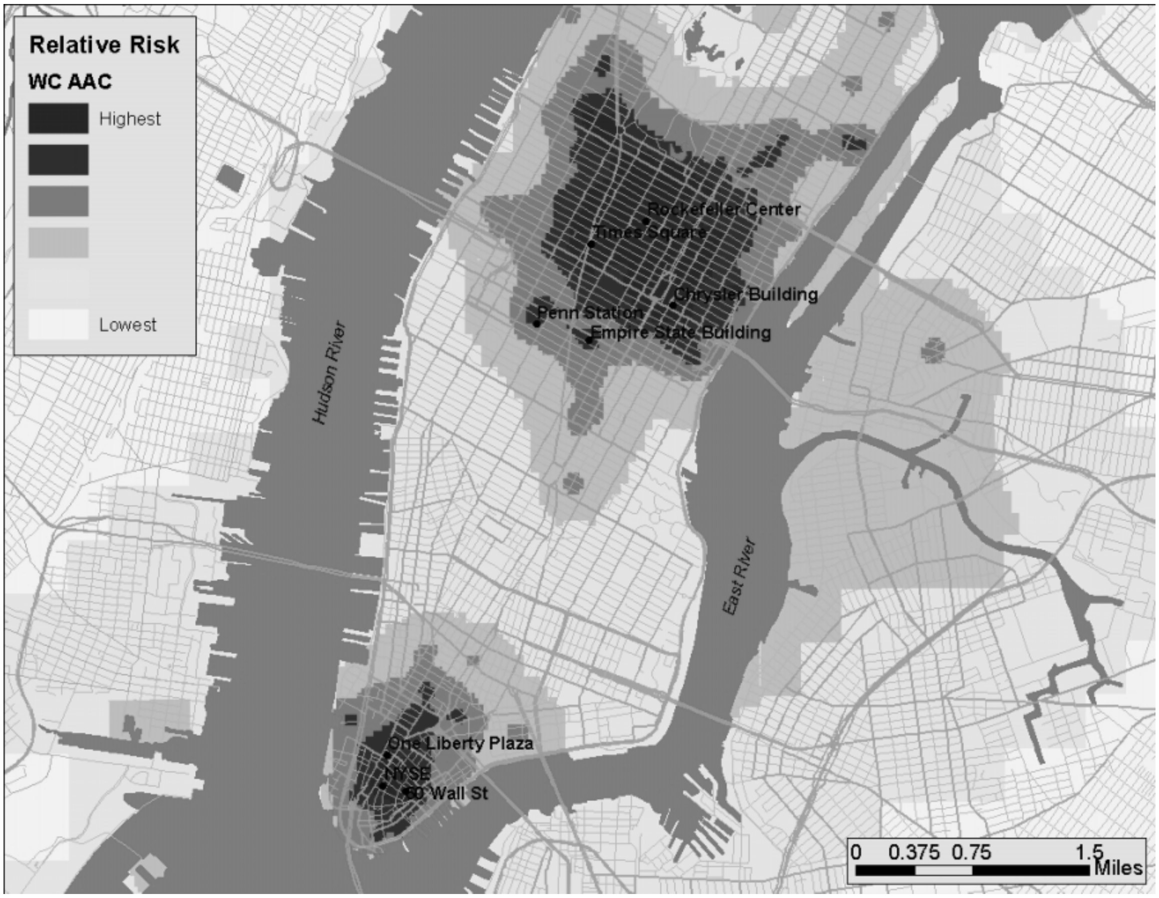


Figure 4 Graphical depiction of assessment of relative terrorism risk in Manhattan from the Risk Management Solutions Terrorism Risk Model expressed as Workers' Compensation (WC) Average Annual Consequences (AAC) Source: Willis et al (2006)

Applying the best practices of risk analysis

The best practices of risk analysis recognize that risk is a social construct and that risk analysis requires an analytic and deliberative process (International Risk Governance Council 2005). For terrorism risk, these characteristics can be refined to provide further definition to a good assessment.

Analytic

An analytic terrorism risk assessment must address all three of the factors that determine terrorism risk: 1) threat, 2) vulnerability, and 3) consequence (Willis et al 2006). When feasible, this should be done quantitatively, using qualitative methods to fill in data gaps were necessary and appropriate. To the extent qualitative methods are used, risk analysis will be more useful for sorting high risks from low ones than for optimizing or fine tuning risk management strategies.

Risk assessments must be repeatable so all parties can replicate, analyze, and understand them. Risk assessment will require standard definitions within an analysis or methodology to ensure that results are consistent among analysts. It may be impossible to develop consistent definitions across all risk analyses. However, that is not necessary so long as consistency is applied within an analysis and when results are compared from one analysis to another. It is most important that the analysis is transparent such that definitions are clearly documented and appropriate for the problem at hand.

Because of uncertainties associated with terrorism risk, standard expected value decisionmaking tools that focus on the average or best estimate of risks may not be appropriate (Haimes 2004). In particular, the most significant uncertainty surrounds assessment of terrorism threat. There is little consensus about when terrorists will attack next, how severe such an attack will be, and how quickly terrorist threats are evolving as terrorist groups attempt to obtain weapons of mass destruction and governments adopt tighter security. In light of this tremendous uncertainty, approaches that consider a very broad range of plausible threats may be necessary as well as adoption of decision support tools that help to identify strategies that perform well across a wide spectrum of these plausible scenarios (see Lempert et al 2003 for an example of such an approach).

Deliberative

A deliberative process is necessary because the notion of a cold, actuarial risk assessment is unrealistic. Although one might think risk analysis could be performed only on the basis of data about threat, vulnerability and consequences, it is not possible to assess risks without considering individual values and judgments about risks and risk exposures. As a result, risk analyses must include deliberative processes that make it possible to take these judgments into account. A transparent analytic process, as outlined above, in necessary to support the deliberative process. This is the only way to address credibly tradeoffs between risks to people from risks to property and risks from a conventional bomb, nuclear attack, biological attack, or even hurricane or other natural disaster. Applications of risk analysis to terrorism have to date focused more on the analytic components of risk than on the deliberative dimensions that require difficult discussion of priorities and judgments of which risks shall be tolerated.

Avoiding blinding analysts to surprise

The strength of applying risk analysis to intelligence analysis is that it provides a set of tools for translating available information about terrorist motivations, terrorist capabilities, infrastructure vulnerabilities, and attack consequences into a set of common metrics that can be used to develop strategies to protect communities from attack effectively. However this is also the root of one weakness of the approach.

The results of a risk analysis are bounded by the information and assumptions that go into it. Only those attacks that are envisioned will be assessed and only those targets that are considered relevant will be considered. As a result, the potential exists that risk analysis could lead the intelligence community to place too much attention on events that are presumed to be likely, thus only reinforcing prior beliefs about terrorist threats and risks and not revealing new insights or trends.

To counter this potential bias, it is necessary to state explicitly the principal assumptions built into terrorism risk assessments and homeland security plans, fully explore uncertainties around terrorism risk (Willis et al 2005), adopt methods that allow analysts to consider the extent to which information they are assessing could explain alternatives that they are not considering (McGill and Ayyub 2006), and consider institutional structures designed to prevent myopic policies with respect to the possibility of surprise (Posner 2005).

SUMMARY

This chapter describes how methods of risk analysis can be integrated into the intelligence cycle used to produce terrorism warnings and threat assessments. This connection reveals two ways that risk analysis can be of potential value to the intelligence community.

Risk analysis can be a tool that can help intelligence practitioners sharpen their conclusions by providing analytic support for identification of scenarios of greatest concern. Risk analysis can also be used to direct future collection efforts on information that appears to be most relevant to refining existing estimates of terrorism risks.

However, risk analyses must be conducted to meet challenges of information availability, matching resolution of results to the problem, reflecting risk as the social construct that it is, and not ignoring the possibility of surprise.

ACKNOWLEDGEMENTS

Preparation of this chapter was supported by the United States Department of Homeland Security through the Center for Risk and Economic Analysis of Terrorism Events (CREATE) under Contract N00014-05-0630 (Office of Naval Research). Any opinions, findings, conclusions or recommendations in this document are those of the authors and do not necessarily reflect views of the United States Department of Homeland Security. I would also like to thank my colleagues Brian Jackson, Terrence Kelly, Don Kleinmuntz, Tom LaTourrette, Jack Riley, Errol Southers, Greg Treverton, Detlof von Winterfeldt, and Mike Wermuth at RAND and USC for their informal comments on my work in this research area.

REFERENCES

1. Chalk Peter, Bruce Hoffman, Robert Reville, and Anna-Britt Kasupski (2005). *Trends in Terrorism: Threats to the United States and the future of the Terrorism Risk Insurance Act*, MG-393, RAND Corporation, Santa Monica, CA.

2. Kim Cragin and Sara Daly (2004). *The Dynamic Terrorist Threat: An assessment of group motivations and capabilities in a changing world*, MR-1782-AF, RAND Corporation, Santa Monica, CA.

3. John B. Garrick (2002). Perspectives on the Use of Risk Assessment to Address Terrorism, *Risk Analysis,* 22 (3), 421-423.

4. Yacov Y. Haimes (2004).*Risk Modeling, Assessment, and Management*. John Wiley and Sons, Hoboken, New Jersey, 2nd Edition.

5. International Risk Governance Council (2005). *White Paper on Risk Governance: Towards an Integrative Approach*. International Risk Governance Council, Geneva, Available online at http://www.irgc.org/irgc/projects/risk_characterisation/_b/contentFiles/IRGC_WP_No_1_Risk_Governance_(reprinted_version).pdf as of February 5, 2007.

6. Lisa Krizan (1999). *Intelligence Essentials for Everyone*. Occasional Paper Number Six, Joint Military Intelligence College, Washington, DC. Available online at http://www.scip.org/2_getinteless.php as of February 5, 2007.

7. Lempert R., Steven W. Popper, and Steven C. Bankes (2003). *Shaping the Next One Hundred Years: New Methods for Quantitative, Long-Term Policy Analysis*. MG-1626-RPC, RAND Corporation, Santa Monica, CA.

8. William McGill and Bilal Ayyub (2006). Quantitative methods for terrorism warnings analysis, *Presentation at the Annual Meeting of the Society for Risk Analysis*, December 6, 2006, Baltimore, Maryland.

9. Richard A. Posner (2005). *Preventing Surprise Attacks: Intelligence Reform in the Wake of 9/11*. Roman and Littlefield Publishers, Lanham, MD.

10.Rosoff, H., & von Winterfeldt, D. (2006). A Risk and Economic Analysis of Dirty Bomb Attacks on the Ports of Los Angeles and Long Beach, *Risk Analysis*, in Press.

11.Henry H. Willis (2005). *Analyzing Terrorism Risk*, Testimony presented before the House Homeland Security Committee, Subcommittee on Intelligence, Information Sharing, and Terrorism Risk Assessment on November 17, 2005.

12.Willis, Henry H., Andrew R. Morral, Terrence K. Kelly, Jamison J. Medby (2005). *Estimating Terrorism Risk*. MG-388-RC, RAND Corporation, Santa Monica, CA.

13. Willis, Henry H., Tom LaTourrette, Terrence K. Kelly, Scot C. Hickey, and Sam Neill (2006). Unpublished work on using risk analysis for intelligence analysis. RAND Corporation, Santa Monica, CA.