Threat and Risk Analysis (TRA): The Intelligence Analysts (IA) Contribution

H. Doucette
KBHS Canada
PO Box 53292 – 50 Rideau Street
Ottawa Ontario Canada
Email kbhs@rogers.com Website www.kbhs.ca
Tel: (613) 859-4404

ABSTRACT
In this post 9/11 environment, the focus on security and force protection issues has significantly increased the demand for suitably developed and accurate intelligence. A residual product that has often been touted as essential is the Threat and Risk Analysis (TRA) ¹ frequently produced by security/force protection advisors with intelligence branch input. Although the Intelligence Community continues to develop innovative and effective methods of analyzing and preparing a well developed product, the end users (ie Force Protection advisors) have often, subjectively relegated the intelligence analysis ineffective or at least reduced its significance in favour of a more mechanical matrix driven format. Although there are several TRA methods, forms and systems currently in use, they generally appear to be lacking in the proper employment of the intelligence cycle and the assimilation of analyzed threat intelligence. The resulting risk analysis therefore becomes questionable and the consequences hazardous. The aim of this tutorial is to review the purpose of the TRA, clarify existing government policy and terminology, illustrate and discuss the role and responsibilities of the intelligence analyst (IA), and demonstrate an “Intelligence Based” process and format that will provide the Commander/manager with a straightforward and accurate report.

KEYWORDS
Information Sharing, Fusion, visualization, usability, all sources, global multinational issues, information Sharing and Collaboration, All Source, terrorism.

TARGET AUDIENCE
This tutorial is intended for Intelligence analysts in general, however, those who are providing support to TRAs in the security, domestic and overseas operations as well as force protection environments will benefit. This tutorial will also be useful for those who are recipients of threat information who are expected to prepare risk analysis such as Commanders, senior management and security advisors. There is no prerequisite knowledge required, although a general understanding of the intelligence cycle and threat analysis process will add to the value of this course for participants.

INTRODUCTION
In the pre and post 9/11 era, several Western governments and subordinate departments have been promoting the need for, and wrestling with, the concept of TRAs. One common thread in government audits is the belief that the critical element of the TRA, is the threat analysis. Although the intelligence community continues to develop innovative and effective methods of analyzing and preparing a well developed product, end users have often, subjectively relegated the intelligence analysis in the TRA report to a mere “HIGH, MEDIUM or LOW” threat, removing, or at least reducing, the significance of the properly developed intelligence analysis. The ensuing risk assessment therefore becomes questionable without a proper intelligence contribution. The role of the IA in the entire TRA process is critical and therefore a proper understanding of the process, terminology and constant participation from the onset of the process as-well-as follow on review by the IA is necessary for an accurate and authoritative product. A product which the Commander can take comfort in when important, informed decisions must be made.

“... I have concluded that there were lapses with respect to force protection at Khobar Towers for which Brig Gen Schwalier must be held accountable. Accordingly, I have recommended to the President that his name be removed from the list of those to be appointed to the grade of Major General.”²

ROLE OF THE IA
In order to ensure the Commander makes informed decisions, it is necessary that the IA become proactive when it comes to the process and the format of the TRA so as to properly incorporate and merge the threat analysis into the report. The IA must be clear on the scope and the objective of the TRA so as to provide specific intelligence analysis rather than generic information on the threat. Allowing the Force Protection advisor to reinterpret, reduce the intelligence analysis to a simple matrix, or include unsubstantiated “what ifs” must be prevented or the goal of the TRA will be lost. The IA must become involved in the process from the very beginning to ensure that the basic intelli-

¹ It should be noted that a TRA has been referred to as a Threat and Risk Assessment and a Threat and Risk Analysis. I advocate the use of the analysis to better describe the product based on the subject of this tutorial.

² Secretary of Defence William S. Cohen, July 31, 1997 - Personal Accountability for Force Protection at Khobar Towers 1997
The intelligence cycle is understood by those preparing the risk assessment. That is to say, often there are additional issues or concerns by the Commander regarding the threat that must be reanalyzed and returned to the intelligence cycle. Additionally, it must be understood that a TRA is a living document and therefore there must be follow up dialogue so that changes to the threat are identified and updated.

**TERMINOLOGY**

There appears to be inconsistent use of terms and acronyms across Intelligence and Operations Groups. It is therefore necessary, to establish common terms. The use of the term “threat”, although clearly defined in the intelligence community and to the IA, is often unintentionally interchanged by those evaluating and preparing the “risk assessment.” It is important to confine the use of the term “threat” to the documented threat analysis and reserve the term “risk” for the subjective correlation of how, or if, the threat can affect the Commanders mission, facilities or personnel. Additionally the terms vulnerability/criticality assessment is applied to, and forms part of a risk assessment. The vulnerability assessment process is an evaluation/inspection of the existing force protection/security measures used as a reporting process to measure the potential and real vulnerable points of a facility or mission. The criticality assessment examines/rates how critical an item is to the Commanders mission, facilities or personnel.

**FORMATS**

Although there are several TRA methods, forms and systems currently in use, it is clear that there is little consensus on an agreed format. It appears that several of the formats reviewed, seem to be lacking in the proper employment of the intelligence cycle and the assimilation of analyzed threat intelligence. The most successful formats take direct and clear references from the intelligence analysis and link them to specific risks, avoiding the often over-subjective matrix style. Matrixes that attempt to reduce the intelligence analysis to categories such as High, Medium, Low without providing the details of why these levels are assessed, does not portray a proper evaluation. The tutorial provides several examples of “Intelligence Based” TRA formats that arguably support the concept of an integrated intelligence analysis TRA.

**AIM OF RISK MANAGEMENT**

The aim of security risk management is to acknowledge that it is impossible to protect everything, all the time, with “standard/recognized” security measures without interfering with normal daily functions or fiscal collapse. The risk management policy mandates specific levels of management to accept a certain amount of risk so that neither the mission nor the budget is compromised. Attempting to strike a balance between the need for force protection/security and accomplishing the mission is the goal of risk management, and the TRA provides the necessary detail. Commanders must often accept responsibility, but must do so fully informed.

**SUMMARY**

The TRA plays an important role in force protection planning and ultimately the safety of personnel. The threat analysis provides the backbone of the TRA and it is therefore necessary that the IA become involved throughout the TRA process including follow on support to ensure the validity of the intelligence input. It is necessary that the IA understand common terminology and is satisfied with the format of the end product as an easily read and accurate account of the threat and inherent risks will undoubtedly ensure that informed decisions are being made.

**TUTORIAL STRUCTURE**

The tutorial will presented in a lecture format and will follow this basic outline:

- Introduction to government policy
- Terminology
- IA responsibilities
- Proposed formats
- TRA follow on/maintenance

**LEARNING OBJECTIVES**

Participants who complete the tutorial will:

- Understand the purpose of the TRA and how governments appear to embrace the concept
- Understand the common terminology of the TRA
- Understand the responsibilities of the IA in the TRA process and reporting
- Recognize, compare and evaluate the different processes and formats of the TRA and the need for follow on action

**LENGTH:** Half day tutorial

**INSTRUCTOR**

Henry Doucette served over 27 years with the Canadian Regular Military, 14 of which with the Intelligence Branch and 10 with the Military Police and Security Branch and continues to serve as an Intelligence Analyst for the Department of Defence in Ottawa. He has been studying the use of TRAs and how they are applied for over 15 years, originally out of necessity when attempts at finding existing policy failed. In addition to studying criminology and political science, at a Bachelor level, he is currently working on a tailored Masters Program (Canadian Military College) focusing on war studies, specifically how intelligence is, and has been used throughout history, innovative regional intelligence analytical techniques and most recently the asymmetric threat analysis techniques. He has prepared TRAs for operations such as; Kabul, Kandahar, Istanbul, DRC, amongst other operations, as well as static sites in Kingston, Trenton and the military wing of the Canadian embassy here in Washington. He has worked as an instructor at both the Canadian schools of Military Intelligence and Military Police/Security. He has a long list of related training conducted in Canada, the US and the UK.