Chapter 8.19
Intelligence and Counterterrorism Tasks

Antonio Badia
University of Louisville, USA

INTRODUCTION

At the end of the Cold War, the intelligence situation (characterized in the past by a confrontation among equals and information scarcity) changed radically to the current situation of today, characterized as an asymmetric threat: On one side, there is still a nation, but on the other, there is a relatively small group of individuals brought together by a common ideology, usually with ethnic and religious elements. These individuals can only confront their opponent by using subterfuge, deception, and terrorist acts. They try to disguise their activities by infiltrating society at large and seeking refuge in anonymity. This kind of conflict has long been analyzed in the military literature under names like low-intensity conflict (LIC) or operation other than war (OOTW; for more on this perspective, the reader is referred to the classic work by Kitson, 1971). The task of the nations under terrorist threat is to detect the group's individuals and their intentions before they can carry out destructive actions. For this, their intelligence services count with large amounts of raw data obtained from many different sources: signal intelligence, open sources, tips from informants, friendly governments, and so forth. However, this data is not always reliable and almost never complete, and the truly interesting events are usually to be found hidden among large amounts of similar looking facts. To deal with this situation, intelligence officers use sophisticated information technology tools. Several authors have pointed out that this task is not at all dissimilar from the task that strategists in business intelligence (BI) and knowledge management (KM) face: As in KM, in intelligence the challenge is that "the right knowledge must get to the right people at the right time" (Pappas & Simon, 2002). Therefore, intelligence experts may learn something from studying BI and KM, and their history and milestones, while business strategists may also be

enlightened by the history and lessons of military intelligence (after all, military intelligence is an ancient discipline; in contrast, KM can be considered a newcomer). In this article, we describe the intelligence analysis cycle and compare it with the KM cycle (we assume the reader is familiar with KM, but not with intelligence tasks). We point out the similarities (and the differences) between the two, and highlight several ways in which military intelligence may benefit from the hindsights and techniques developed by KM practitioners. We also briefly describe tools and methods from military intelligence that KM practitioners may find illuminating. We close with a discussion of future trends and some conclusions.

BACKGROUND: INTELLIGENCE ANALYSIS

The ultimate goal of intelligence analysis is to provide a customer, military or civilian, with the best possible information to help in making policy, strategic, and tactical decisions that affect national security[1]. In this task, intelligence is used to refer to knowledge and information, the basic end product of the analysis. Such analysis is carried out by highly trained analysts who work in a continuous process involving the following steps[2].

- Need Analysis: Customers (policy makers and others) make requests that the analyst must translate to specific requirements and tasks in order to make sure that the final product answers the needs of the customer. Customer demands often need interpretation or analysis before they can be expressed as an intelligence requirement (Krizan, 1996). The customer may have additional constraints on the intelligence product; the request may have time constraints (short term vs. long term) or scope constraints (broad or strategic vs. narrow or tactical).
- Collection: This refers to the gathering of raw (uninterpreted) data. Nowadays, there is an abundance of data due to the variety and richness of sources:
  - Signal intelligence (SIGINT) includes information from radar, telemetry, and intercepted communications.
  - Imagery intelligence (IMINT) refers to images delivered by electronic means, mostly satellites.
  - Measurement and signature intelligence (MASINT) is data produced from sensors (chemical, acoustic, etc.) other than SIGINT and IMINT.
  - Human-source intelligence (HUMINT) refers to data provided by informants, either through clandestine means, official contacts with allied nations, or diplomatic missions.
  - Open-source intelligence (OSINT) refers to publicly available information (radio, television, newspapers, commercial databases, etc.); this is in contract with all previous sources, which are usually classified and not open.
- Processing and Exploitation: In this stage, the raw data is converted to a form suitable for further analysis. This includes the translation of documents in foreign languages, analysis of sensor data, decoding of messages, and so forth. These tasks consume a large amount of resources from intelligence agencies since many of them are labor intensive, and specialized personnel are needed to carry them out. Moreover, in this phase, the evaluation of the accuracy, reliability, and meaning of the raw data (which continues in the next step) gets started.
- Analysis and Production: In this stage, the processed data are integrated, interpreted, and evaluated. In this crucial phase, the analyst must assess how reliable and complete the data pieces are, how distinct pieces of