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 data can be interpreted, and how they fit in an overall picture. The first task is needed since many times the sources of information are not trustworthy, and an adversary may leave indications that actually mislead an intelligence agency in order to disguise real intentions. The second task is needed since raw data is rarely unambiguous; the same act (for instance, buying fertilizer) may signal completely different intentions depending on the context (to work on a farm or to prepare explosives). The last task is needed since data is rarely complete; after all collection is done, analysts usually have only fragmented and sometimes unrelated evidence. Finally, even after some conclusion is reached, there are two tasks left. First, analysts try to verify their work by correlating finished intelligence with data from other sources, looking for supporting evidence and/or inconsistencies. Because the process is far from exact, and is based on partial, tentative evidence, all conclusions reached are by necessity also tentative, best estimate interpretations. Note that in this step we go from facts to interpretation and judgment; hence, it is in this step that the danger is greater for presumptions, biases, and other problems to arise. Second, the created intelligence must be tailored to the customer, and an effort must be made to make sure that the product answers the customer's needs. In particular, the information produced must be relevant to the original answer, as accurate as possible (and, if uncertain, accompanied by some measure of its certainty), objective, usable (i.e., actionable), and timely.
- **Dissemination:** This is simply the process of delivering the finished product to the consumer. Sometimes, this is followed by the consumers providing feedback to the intelligence analyst so that the process can be improved.

While some intelligence is produced in response to a specific demand from a consumer, other intelligence is produced simply in order to keep track of ongoing events, to detect trends and patterns, or to be aware of events that may develop. As a result, finished intelligence can be of one of several categories, depending on its origin, subject, type of analysis, and/or intended use. With regard to origin, intelligence may be analyst driven, event driven, or scheduled (periodical). With regard to subject, intelligence may be economic, geographic, political, scientific, and so forth. With regard to the type of analysis, intelligence can be descriptive or inferential; in the latter case, it can be about the past, the present (warnings), or the future (forecasts; Waltz, 2003).

In the United States alone, there are several intelligence agencies that are collectors of data and/or producers of finished intelligence based on several departments. Collaborations among these agencies have been notably absent in the past.

KM IN INTELLIGENCE ANALYSIS

The idea that KM has a role to play in intelligence analysis is not new. In a seminar paper, Brooks (2000) already stated our main thesis, namely, because of similarities in goals, issues, and tasks, KM could lend significant insight when analyzing intelligence work and vice versa. The book by Waltz (2003) has this very same thesis at its core. Moreover, the 9/11 Commission has stated that some of the most serious failures in intelligence that had been observed (the lack of communication between the FBI and CIA, and the obsolete information technology deployed at the FBI) stem from not having an adequate knowledge management strategy in place: "In essence, the agency didn't know what it knew." Also, the book by Krizan (1996) starts with a prologue under the subtitle "National Intelligence meets Business Intelligence." But the most revealing proof of the influence of KM in intelligence work may be the creation, by the Central Intelligence Agency, of a nonprofit enterprise (In-Q-Tel) devoted to identifying promising technologies and funding