Two Comments on:

“Intelligence Operations Research: The 2010 Philip McCord Morse Lecture” By Edward H. Kaplan

Moshe Kress

Operations Research Dept. Naval Postgraduate School, Monterey CA

In this paper, Kaplan reviews intelligence operations, and then identifies some potential areas of operations research that could be applied for intelligence-related problems. He calls the former “***intelligence operations*** research”, while the latter is labeled “intelligence ***operations research***”*.* I have two comments: one regarding *intelligence operations* research and the other concerning the other topic -- OR applications.

The article mostly addresses peacetime intelligence and focuses, on the one hand, on homeland security (e.g., “how many terror plots are in progress?”) and, on the other hand, on the national-strategic level (e.g., NIPF and NIEs). Intelligence during combat operations has somewhat different characteristics that may require different treatment. First, the time scale of the intelligence cycle during combat is much shorter; it may be measured in hours, and perhaps even in minutes. If there is a Red Anti-Tank Missile company hiding behind the hill, waiting for a Blue tank battalion approaching that hill, the information about this threat to the battalion may become obsolete in a matter of minutes. While time-critical intelligence may also be present in anti-terror operations, in particular during targeted attacks, it is more prevalent in conventional military operations. Second, the intelligence “supply-chain” during combat is subject to significant degradation caused by the fog of war. Misinterpretations and overflow of data, broken communication lines and the stressful combat environment result in disinformation and misinformation. These predicaments are much more notable during wartime than peacetime. Third, while terrorists will try to hide their plots and states may conceal their intentions and plans, they seldom engage in persistent, well orchestrated, information operations. This type of intelligence warfare, manifested in deception and disinformation, is embedded in combat operations.

The second comment is about intelligence *operations research*. With the advent of sensing, communication and cyber technologies, the *collection* stage in the intelligence cycle becomes relatively easy to implement. However, this stage produces a glut of information and data that is very difficult to digest. Thus, the *processing* stage, which follows collection, becomes crucial because at this stage the raw information and data are filtered and transformed into a form that can be effectively analyzed at the following analysis stage. One of the critical processing tasks is screening the collected intelligence items and determine those items that are relevant for analysis. More specifically, given an intelligence query--a concrete question posed to the collector by an intelligence analyst or a decision maker--each item is either relevant to the query or irrelevant (in general, there may be multiple levels of relevance). The collector's task is to pass on to analysts as many relevant items as possible during a limited time period, which is insufficient for screening all the items collected. The objective is to determine the screening sequence of a given length that maximizes the expected number of identified relevant items. This problem can be looked at as a multi-armed bandit problem with two significant distinctions from the classical model: First, the “arms” (items) are not independent, and second, the time horizon is finite. Bayesian updating techniques and machine-learning algorithms may help in this formidable task. An example that manifests the criticality of this problem is the case of the Christmas Day Bomber - Umar Farouk Abdulmutallab - who almost succeeded to blow up Northwest airline flight 253 on December 25, 2009. Reports indicated that intelligence regarding a Yemen-based Nigerian terrorist planning such an attack had been collected, but not processed or analyzed properly.