Chapter 22 Quantitative Approaches to Representing the Value of Information Within the Intelligence Cycle

Christopher M. Smith TRADOC Analysis Center, USA

William T. Scherer University of Virginia USA

Andrew Todd University of Virginia, USA

> Daniel T. Maxwell KaDSci, LLC, USA

ABSTRACT

The authors propose that valuation of information metrics developed near the end of the intelligence cycle are appropriate supplemental metrics for national security intelligence. Existing information and decision theoretic frameworks are often either inapplicable in the context of national security intelligence or they capture affects from inputs aside from just the information or intelligence. Applied information theory looks at the syntactic transmission of information rather than assigning it a quantitative value. Information economics determines the market value of information, which is also inapplicable in a national security intelligence context. Decision analysis can use the value of information (EVII) and although this method can be used with utility theory and not just monetary objectives, it has been shown that decision makers within the intelligence community (IC) have difficulty agreeing upon how to value objectives within analysis. Additionally, it is difficult to determine how decision makers use intelligence in the decision-making process, which makes existing decision theoretic methods problematic, and might include inputs from variables besides just the intelligence.

DOI: 10.4018/978-1-5225-7912-0.ch022

1. INTRODUCTION

The U.S. Intelligence Community (IC) harvests over a billion pieces of data a day, but often lacks the ability to analyze that data and produce valuable intelligence (McConnell, 2007). Efforts to improve intelligence often focus on collection rather than analysis. According to the 9-11 Commission's report, the intelligence community had information that may have either helped decision makers mitigate or even stop the 9-11 attack. Even though the IC had enough information to determine that "the system was blinking red," according to a Central Intelligence Agency (CIA) supervisor, "no one looked at the bigger picture; no analytic work foresaw the lightning that could connect the thundercloud to the ground" (9/11 Commission Report, 2004).

Collection management within the IC is a practice that focuses on knowing the needs of the intelligence users and determining how best to allocate limited collection resources (Clark, 2011). Collection managers also review existing allocation strategies by determining if intelligence collected is valuable and relevant. Existing methods for evaluating intelligence, however, have focused on their value to the decision maker.

Since decisions, especially at the national level, are subject to conflicting priorities and politics, it is difficult to determine what role intelligence plays in decisions. The current value of information methods, however, rely crucially on whether or not information is used in a decision and since collection managers can never truly determine how intelligence is used, existing methods are often inapplicable (see Figure 1).

Collection managers in the IC will benefit from an assessment methodology that allows a quantitative measure of the impact certain intelligence has on an analysis. A robust method of this type will allow managers to objectively measure "good" or effective intelligence vs. "bad" or ineffective intelligence. A quantitative measure applied across the different classes of analyses would provide a relative scoring of the intelligence that different sources produce thereby allowing collection managers to more effectively manage expensive collection resources.



Figure 1. Intelligence collection management within the intelligence cycle

18 more pages are available in the full version of this document, which may be purchased using the "Add to Cart" button on the publisher's webpage: <u>www.igi-global.com/chapter/quantitative-approaches-to-representing-the-</u> value-of-information-within-the-intelligence-cycle/220895

Related Content

Clustering Based on Two Layers for Abnormal Event Detection in Video Surveillance

Emna Fendri, Najla Bouarada Ghraband Mohamed Hammami (2019). *Censorship, Surveillance, and Privacy: Concepts, Methodologies, Tools, and Applications (pp. 433-453).* www.irma-international.org/chapter/clustering-based-on-two-layers-for-abnormal-event-detection-in-videosurveillance/213815

Importance of a Versatile Logging Tool for Behavioural Biometrics and Continuous Authentication Research

Soumik Mondal, Patrick Bours, Lasse Johansen, Robin Stenviand Magnus Øverbø (2017). *Developing Next-Generation Countermeasures for Homeland Security Threat Prevention (pp. 282-305).* www.irma-international.org/chapter/importance-of-a-versatile-logging-tool-for-behavioural-biometrics-and-continuousauthentication-research/164726

Understanding Digital Intelligence: A British View

David Omand (2019). *National Security: Breakthroughs in Research and Practice (pp. 590-613).* www.irma-international.org/chapter/understanding-digital-intelligence/220902

CVSS: A Cloud-Based Visual Surveillance System

Lei Zhou, Wei Qi Yan, Yun Shuand Jian Yu (2019). *Censorship, Surveillance, and Privacy: Concepts, Methodologies, Tools, and Applications (pp. 19-32).* www.irma-international.org/chapter/cvss/213792

The USA Electrical Grid: Public Perception, Cyber Attacks, and Inclement Weather

Eugene de Silvaand Eugenie de Silva (2019). National Security: Breakthroughs in Research and Practice (pp. 659-672).

www.irma-international.org/chapter/the-usa-electrical-grid/220907