

Integrating Methods and Tools to Counter Denial and Deception

Ed Waltz

BAE SYSTEMS Advanced Information Technologies

3811 North Fairfax Drive, Suite 500

Arlington, VA 22203 USA

ed.waltz@baesystems.com

Tel: (703) 622-4385 Fax: (703)524-6280

<http://baesystems.com>

ABSTRACT

Analysts face severe analytic challenges when seeking to counter a wide range of targets (e.g. enigmas, concealed facilities, covert programs, secured leadership, deep-hide weapons) that employ denial and deception (D&D) to avoid discovery, evade surveillance and deny description. This tutorial introduces the principles of D&D employed to counter intelligence collection and analysis, before describing the methodologies and associated analytic tools that may be employed in an effort to counter a variety of these activities. Participants will gain an understanding of the principles of D&D, the challenges to collection and analysis, and the prominent analytic methods and tools that may be integrated to focus on the most difficult targets to counter D&D.

Keywords

Denial, Concealment Deception, Misdirection, Counterdeception, Incongruity testing, Alternatives analysis, Inferential analysis, Exploratory analysis, Reconstructive inference, Structured argumentation.

Target Audience

This tutorial is suitable for both analysts and developers of analytic tools that marshal evidence and explore alternative explanations of hard targets (e.g. enigmas, concealed facilities, covert programs, secured leadership) that employ denial and deception to evade surveillance and deny analysis. Prerequisite knowledge is a basic understanding of analytic reasoning, and all-source analysis processes.

DENIAL AND DECEPTION

The *Commission on the Intelligence Capabilities of the United States Regarding Weapons of Mass Destruction* concluded that: "Iraq's denial and deception efforts successfully hampered U.S. intelligence collection" (Chapter 1, Conclusion 4, page 161). This and earlier commissions on intelligence have all noted the significant challenge that sophisticated D&D methods pose to intelligence collection and analysis. D&D includes the integration of three processes to mislead analysis: *dissimulation*, the concealing of evidence of the truth, *simulation*, the presentation of evidence which is false, and *misdirection* to degrade or distract the attention of the analyst from evidence of the truth. This

tutorial begins with a brief survey of the classic D&D process models that describe the relationships between simulation, dissimulation and misdirection – and the methods and channels by which they are delivered to the analyst. The 2x2 deception matrix, formed by the set of operations to reveal and conceal the truth, and to real and conceal the false, is used to illustrate Libyan and Iraqi strategic deception activities and the basic principles of D&D. The deception matrix is used to illustrate deception examples in three general channels to the intelligence analyst: Physical phenomena and sensing, Signal phenomena and information processing, and HUMINT channels.

COUNTERDECEPTION

The underlying principles of denial and deception are compared to corresponding principles and elements of counter D&D (CDD); the basic elements of CDD include:

- Collection – activities to enhance the access, revisit, spectrum, and fidelity of collectors against D&D targets.
- Processing – processes that filter, align, correlate and combine technical data to identify potential D&D relevant data to provide cueing to missing, spurious and ambiguous information for subsequent analysis
- Analysis – methods to increase analytic awareness, enhance the structure of objective argumentation from evidence to inference, while enhancing imaginative exploration of both the potentially concealed and the actually revealed.

ANALYTIC METHODS AND TOOLS

The focus of the tutorial is on the fundamental approaches to CDD processing and analytic methods. The approaches described are built upon principles described in classic works by Whaley, Harris, and others – translated to a formal methodology that embraces a structured approach to analytic argumentation and an exploratory approach to synthetic consideration of and associated tool; the classic CDD models are introduced (e.g. Whaley, Harris) before describing approaches to implement and integrate the basic analytic methods, including:

- Reconstructive inference – The deductive process that seeks to detect the presence of spurious signals (Harris)

uses the term *sprignals*) that are indicators of D&D – faint evidence predicted by conjectured D&D hypotheses that can be strong evidence confirming hypothesis A (the simulation), weak contradictory evidence of hypothesis C (leakage from the adversary’s dissimulation effort), or missing evidence that should be present if hypothesis A were true.

- Incongruity testing – The process that searches for inconsistencies in the data and inductively generating alternative explanations that attribute the incongruities to D&D (i.e. D&D explains the incongruity of evidence for more than one reality in simultaneous existence).
- Alternatives analysis – High-level evaluation of alternative competing hypotheses (including D&D hypotheses) based on supporting, refuting and missing evidence.
- Dynamic Exploratory analysis – Detailed exploration of the dynamics of alternative D&D hypotheses, with a focus on the dynamics of hidden processes. This process requires explicit target modeling of the critical hypotheses to predict behavior and resulting evidence for the D&D channels and methods hypothesized.

The tutorial concludes with taxonomy of supporting analytic tools to implement these methods in a CDD analytic workflow that includes the use of knowledge bases to support cueing collection and long-term analysis. A representative analytic workflow, integrating the tools is illustrated.

SUMMARY

Sophisticated strategic D&D has demonstrated the severe challenge it poses to the delivery of accurate and timely intelligence. The means to counter such D&D requires an equally sophisticated and careful integration of collection, processing and analysis, tailored to the D&D target, to reveal the structure and dynamics of an adversary’s true activities and intentions.

TUTORIAL STRUCTURE

The tutorial is structured according the following outline:

- Survey of the Classic D&D process models with examples to illustrate the models; Underlying Principles of Denial and Deception
- Elements of Counter D&D (CDD): Collection, Processing and Analysis Strategies
- Counter D&D Processing and Analysis Methods: classic CDD process models, implementing the processes, applying inferential and exploratory tools
- Integrating the Methods and Tools

LEARNING OBJECTIVES

Participants at this tutorial will receive:

- a background in the principles of deception – and the principles associated with countering (detecting, understanding, and penetrating) deception mechanisms,

- a survey of the analytic counterdeception methods and their application,
- a description of supporting analytic tools to conduct inferential and exploratory analysis, and,
- an understanding of how to integrate tools and methods to counter deception targeted at intelligence..

LENGTH: Half day tutorial

INSTRUCTOR

Ed Waltz is the Chief Scientist, Intelligence Innovation Division of BAE Systems Advanced Information Technology, where he leads hard intelligence target research. He has led several counter D&D studies and tool developments over the past decade for different agencies of the IC. He holds a BSEE from the Case Institute of Technology and an MS in Computer, Information and Control Engineering from the University of Michigan, and over 35 years of experience in developing and deploying signal processing, data fusion and analytic technologies for C2 and intelligence. He is the author of *Knowledge Management in the Intelligence Enterprise* (Artech 2003), *Information and Warfare Principles and Operations* (Artech 1998), coauthor of *Multisensor Data Fusion* (Artech 1990), and coeditor of *Multisensor Data Fusion* (Kluwer 2001). He is a recipient of the DoD Joseph Mignona Data Fusion Award (2004), and became a Veridian Technology Fellow in 2002. Mr. Waltz is coauthor of the technical text *Counterdeception Principles and Applications for National Security*, forthcoming from Artech House in the fall of 2005.

REFERENCES

1. Bennett, Michael and Waltz, Edward (2005), *Counterdeception Principles and Applications for National Security*, Boston:Artech, forthcoming.
2. *Report of the Commission on the Intelligence Capabilities of the United States Regarding Weapons of Mass Destruction*(2005), Washington DC, March 31, 2005.
3. Whaley, Barton, (1969), *Strategem: Deception and Surprise in War*, Cambridge: MIT Center for International Studies, MIT
4. Godson, Roy and Wirtz, James eds. (2002), *Strategic Denial and Deception: The Twenty First Century Challenge*, New Brunswick, Transaction Publishers
5. Harris, William R., *On Countering Strategic Deception* (1973), Advanced Research Projects Agency, R-1230-ARPA, November 1973.
6. Heuer, Richards J. (1999), *Psychology of Intelligence Analysis*, GPO; this document includes valuable discussions on the analyst’s cognitive vulnerabilities to deception based on the author’s earlier work, “Strategic Deception and Counterdeception: A Cognitive Process Approach”, published in *International Studies Quarterly*, Vol. 25, No. 2, June 1981.