

Working Group 3 – Issues of Information Assurance (IA) in Information Sharing

The lack of secure infrastructure significantly limits information sharing. Challenges range from implementing secure and readily accessible repositories of data in support of analyses, to real time access across Command and Control for immediate decision support. This Working Group will explore the technical and relational issues that need to be addressed to improve this information sharing in an assured manner. The state of the art and practice, as well as recommendations on where the analysis community might contribute to or benefit from emerging technologies, will be reported to the sponsors.

Working Group 4 – Information Assurance (IA) Related Advances and Opportunities in Modeling, Simulation, and Analysis

This Working Group will explore the current state-of-the-art, and practice for IA related modeling and simulation along two dimensions. First, how are IA issues and effects represented in the DoD's current suite of models and simulations? Second, what models and simulations exist that support IA analyses directly? This foundation then sets the stage for exploring and making recommendations about how IA should be represented in future DoD model, simulations, and analyses.

3. Overarching Issues

There are several overarching issues each Working Group will consider. Some of these issues are:

- How are IA issues considered in current DoD analyses? How should they be considered in the future?
- What should the role of DoD analysis agencies seek to fill in meeting the information related analysis needs of the Department and the nation?
- How should the DoD and other U.S. Agencies collaborate to conduct IA analyses?

4. Administrative Details

Location: Johns Hopkins APL, Laurel, MD

Classification Level: SECRET- US Only

Fees:

Entire Workshop

Non-Government/Non-Member: \$750

Non-Government/Member: \$675

Government/Non-Member: \$640

Government/Member: \$575

Mini-Symposium (1-day) Only

All/Non-Members: \$375

All/Members: \$325

Program Chair: Dr. Daniel Maxwell

dmaxwell@innovatedecisions.com

Co-Chairs: Mr. Donald Timian, ATEC
Ms. Donna Gregg, JHU/APL

MORS

1703 N. Beauregard St., #450

Alexandria, VA 22311

703-933-9070

FAX 703-933-9066

morsoffice@mors.org

www.mors.org



MORS Workshop

*Transforming Information
Assurance for Netcentric
Operations:
Providing Assured
Information for National
Security*

6-8 March 2007

**Johns Hopkins University
Applied Physics Lab
Laurel, Maryland**

1. Goals and Objectives

The twenty first century is accompanied by many changes that are influencing the national security landscape. One key change to the landscape is the arrival of a multi-polar world, with non-state actors that present unprecedented and often unpredictable asymmetric threats. The second is the arrival of the information age. The availability of advanced information technologies, accompanied by a creative vision on how to apply that technology, are fueling efforts to “Transform” the military into a “Network Centric” force. These two features of our modern world present opportunities to meet threats to peace and stability in ways that were previously unimaginable. The continually increasing reliance on information technology in military operations, and in fact across society, also presents risks that were previously unimaginable. Assured information is absolutely essential if these risks are to be effectively mitigated or managed.

This entire subject area is one which pushes the limits of both science and practice. Effective improvements in Information Assurance (IA) will require creative and open discourse among traditional operators, operations analysts, technologists, and scientists and engineers from many disciplines. If information is to be the cornerstone of our military’s future success, it is essential that meaningful efforts be initiated to adapt to the dynamic and

uncertain operational environment we are already facing, and are certain to face into the foreseeable future. The focus of this workshop will be to examine how the Military Operations Research community can contribute to these efforts.

2. Meeting Approach

The meeting will commence with a mini-symposium format on the first day that will include operational based discussions as well as some focusing presentations. There will be a rich collection of keynote and plenary presentations that will relate IA to information sharing and use to the need for efficient and effective approaches to risk analysis and management throughout information enterprises.

The Mini-Symposium will be followed by a two-day workshop where participants will meet in Working Groups to further examine specific topics, including discussing the overarching issues of the Workshop. To focus the discussion in each of the Working Groups, a select group of people will be requested to prepare and present papers.

Workshop attendees are expected to be organized as follows:

Working Group 1 – Lifecycle Information Assurance (IA) – There are three relevant “lifecycles” for analyzing our nation’s information systems and their relationship to military effectiveness. The first lifecycle is the physical infrastructure that performs core

computational and communicative operations; the second is the lifecycle of software that resides on the system; and the third is the information itself. Each of these lifecycles occurs over different time horizons and has different factors that must be considered in IA related analyses.

The challenge for this Working Group is to identify the most salient features for force level analyses. Toward this end, this Working Group will share ongoing work across these areas and attempt to develop a framework for considering systematic analysis issues throughout the lifecycles.

Working Group 2 – Evaluation and Analysis of “Net Ready” Key Performance Parameter (NR-KPP) in DoD Information Systems – NR-KPP was developed to assist in development, and to assess the information needs, information timeliness, information assurance, and net-ready attributes required for both the technical exchange of information and the end-to-end operational effectiveness of Information Technology and National Security systems.

This Working Group will focus on refining how the IA portions of the NR-KPP can and should be evaluated for the systems under development. Particular attention will be given to issues of measurability and operability in testing, and the role of modeling, simulation, and analysis in support of system testing and evaluation.