

Military Operations Research Society (MORS) Workshop

Mission Assurance: Analysis for Cyber Operations Terms of Reference (TOR)

As of 16 July, 2010

28 February – 3 March 2011, San Antonio, Texas

Workshop Vision

Cyberspace has joined land, sea, air and space as a domain of warfare. The President has declared our countries cyber infrastructure to be a “strategic national asset”. USCYBERCOM has stood up under the command of General Keith B. Alexander, USA, and each of the services is wrestling with its Organize, Train and Equip and its warfighting responsibilities for the cyber mission. MORS has held the Cyber Analysis Workshop on 28-30 October 2008 in Reston, Virginia, focusing on improving cyber M&S, developing a common understanding of the threat. The results of that workshop were very well received, and provided OSD and service level insights for M&S and policy development.

Since that workshop, service and major command roles regarding cyber have been clarified, and analysts at the service and subordinate levels are being challenged to apply their craft to the cyberspace domain. DHS has received the cyber defense mission for our civil cyber infrastructure. But in contrast to the other domains of warfare, there are very few analysts who have experience in cyber operations upon which to draw as they attempt to apply analytical techniques. This MORS workshop will focus on maturing the relationship between the cyber operations and the analytic community. The intent is to provide a forum and structure for analysts and cyber operators to generate a shared understanding of cyber operations activities and how analysts can support those activities.

Mission Assurance (MA) has been said to be an enveloping, overarching goal of our cyber forces. MA derives from these primary components of cyber capability:

- Situational Awareness (both friendly and other)
- Establish and Extend the Network
- Operate and Defend the Network
- Cyber Force Application

These components of cyber capability provide the framework for our working group structure below. Different services and agencies will have different taxonomies, and it will be the role of

the workshop planning staff to engage those services and agencies to translate their taxonomies to this one and demonstrate the applicability and value of their participation in the workshop.

Objectives

- Ensure attendees understand the nature of the current cyber threat
- Improve analytical approaches and techniques that support cyberspace operations.
- Facilitate discussions between cyber operators, consumers of cyber capabilities, and analysts to create an understanding analysis opportunities to improve mission assurance
- Write an unclassified report with classified appendices summarizing the workshop.
 - o The workshop report should articulate specific applications of analytical techniques to improve cyber operations and mission assurance
 - o The report will also provide recommendations for developing new or improving existing analysis techniques to for cyber applications

Workshop Goals

- Attendance of at least 100 participants.
- The meeting achieve an average attendee overall rating of 4 on 1 to 5 scale.
- Determine the efficacy of a Community of Practice (COP) for cyber analysis.

Workshop Organization

The workshop has both staff and line functions. The workshop will have several tracks addressing different aspects of cyber operations. Workshop participants will have matrix-style alternating attendance between tracks and discipline groups. These groups based on academic disciplines examine how the skills of their specialties may be applied to address the analytical issues across the tracks. The following shows the staff, track, and discipline group structure for the workshop.

- Co-Chairs (Maj Michael Artelli and Lee Lehmkuhl)
- Staff Leads
 - o Facilities (MORS Staff)
 - o Site Lead
 - o Security
 - o Senior Leader Coordinator
 - o Terminology (Clayton Bowen)
 - o Bulldog (Don Timian)
- Working Group Leads
 - o Establish and Extend the Network
 - o Situational Awareness and ISR
 - o Operate and Defend
 - o Cyber Force Application
- Synthesis Group (Greg Keethler)

Workshop Operation

This workshop will employ the traditional model of multiple working groups focused on different aspects of the cyber domain and a synthesis group looking across all working groups. The synthesis group will look for common themes, and recommend real-time modifications and improvements to the workshop. Each working group will be co-chaired. One chair will have a background in the cyber focus of the working group, and the other will be an analyst with broad professional and MORS workshop experience. The co-chairs will develop an abstract, agenda, and expected outcomes to shape the activities of the working group and maintain a balance between presentations and working group product creation.

The workshop will begin with a Keynote Speaker, an orientation to cyber operations, and a threat briefing.

Working Groups (WGs)

WG 1: Situational Awareness (SA) and Intelligence, Surveillance and Reconnaissance (ISR). This WG will explore analysis techniques to improve the understanding of the network, the friendly cyber forces and missions operating on the network, and non-friendly networks, forces and missions. Examples include sensor tasking algorithms, data fusion, and exploring the implications of network topology.

WG2: Establish and Extend the Network. While the analyst community has long supported the acquisition and fielding of networks, considering the network within the broader context of cyber indicates the potential for fresh analytical challenges. Some network modifications occur on a very rapid timeline, perhaps hours or days. An adapting cyber threat may add an additional dimension to analysis as it assists in the structuring, evaluation and prioritization of acquisition activities. The need to rapidly extension the network to support the warfighter, and ongoing development of air and terrestrial complements to satellite communications, present a rich set of alternative courses of action, with associated risks, that are amenable to analytic investigation.

WG 3: Operate and Defend the Network. This WG will focus on how analysis may assist the achievement of Mission Assurance as it relates to operating the network and defending it in depth. Specific areas of interest include the development of courses of action (COAs), prioritization of missions or activities to defend the network, and adaptation to dynamic warfighter priorities. This WG may require sub-groups to explore the different analysis needs of DoD, the Services, and DHS.

WG 4: Cyber Force Applications. This may include the application of analysis to enhance targeting and intelligence gain/loss determination.

Potential Government Senior Leader Involvement

Workshop Leadership

The following individuals are leading this workshop.

Keynote Speaker: MG Webber, 24AF/CC

Co-Sponsors: Air Force A9 Studies & Analysis, Assessments and Lessons Learned

Host Organizations: 24th Air Force
Air Force Space Command Analysis, Assessments and Lessons Learned

Workshop Co-Chairs: Maj Michael Artelli and Dr. Lee Lehmkuhl

Working Group Co-Chairs:
Synthesis Group Chair: Mr. Greg Keethler

MORS leadership attending include
Dr. Jacqueline R. Henningsen, SES, A9, Sponsor

Security Procedures

The workshop will be conducted at the SECRET level, US personnel only.

Facilities

If you need more information, please contact the workshop co-Chair, Dr. Lee Lehmkuhl at 719-572-8307 or leel@mitre.org or contact the MORS office at 703-933-9070 or www.MORS.org.