# Synthesis Group

## Final Report

**24 March 2011**

# Report Documentation Page

*Form Approved*
*OMB No. 0704-0188*



| 1. REPORT DATE | 2. REPORT TYPE | 3. DATES COVERED |
|---|---|---|
| **24 MAR 2011** | | **00-00-2011 to 00-00-2011** |

| 4. TITLE AND SUBTITLE | 5a. CONTRACT NUMBER |
|---|---|
| **Synthesis Group - Final Report** | 5b. GRANT NUMBER |
| | 5c. PROGRAM ELEMENT NUMBER |
| 6. AUTHOR(S) | 5d. PROJECT NUMBER |
| | 5e. TASK NUMBER |
| | 5f. WORK UNIT NUMBER |
| 7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) **Military Operations Research Society (MORS),1703 N. Beauregard St. Suite 450 ,Alexandria,VA,22311** | 8. PERFORMING ORGANIZATION REPORT NUMBER |
| 9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES) | 10. SPONSOR/MONITOR'S ACRONYM(S) |
| | 11. SPONSOR/MONITOR'S REPORT NUMBER(S) |

12. DISTRIBUTION/AVAILABILITY STATEMENT
**Approved for public release; distribution unlimited**

13. SUPPLEMENTARY NOTES
**MORS Mission Assurance: Analysis for Cyber Operations Special Meeting held in San Antonio, TX Mar 21-24, 2011.**

14. ABSTRACT

15. SUBJECT TERMS

| 16. SECURITY CLASSIFICATION OF: | | | 17. LIMITATION OF ABSTRACT | 18. NUMBER OF PAGES | 19a. NAME OF RESPONSIBLE PERSON |
|---|---|---|---|---|---|
| a. REPORT **unclassified** | b. ABSTRACT **unclassified** | c. THIS PAGE **unclassified** | **Same as Report (SAR)** | **30** | |

# Synthesis Group Members

Greg Keethler (Chair and Working Group 2 Synthesis member)

Gene Visco (Co-chair, Working Group 1 Synthesis member, MORS Fellow)

Dr. Stuart Starr (Working Group 4 Synthesis member, MORS Fellow)

Terry McKearney (Working Group 3 Synthesis member, MORS President)

Dr. Steve Baker (Synthesis Roamer)

Dr. Mike McGinnis (Synthesis Roamer, MORS Fellow)

# Agenda

- Context
- Insights from
  - Tutorials, Plenaries
  - Themes from the Working Groups
  - Synthesis Group Perspectives
- Summary

# Context

- What?
  - Mission Assurance: Analysis for Cyber Operations
  - Four working groups
    - Situational Awareness
    - Establish and Extend the Network
    - Operate and Defend the Network
    - Cyber Force Application
- Where?
  - Southwest Research Institute, San Antonio, TX
- When?
  - 21 – 24 March 2011

**Purpose –** identify
- Themes
- Common issues
- Dependencies
- Overarching issues

**Activities** of the Synthesis Working Group
- Participated in the four Working Groups
- Met during breaks
- Created workshop themes, synthesis perspectives

# Objectives

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

# Workshop Goals

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

# "Take-aways" from Tutorials (1 of 2)

- Schematic Protection Model (SPM) (Rusty Baldwin)
  - "The safety problem is undecidable in general; but limiting the scope of systems can make the problem decidable"
- Assessing Mission Assurance and System Reliance (Dave Alderson)
  - "Infrastructures are *systems"*
  - "Descriptive versus *prescriptive* models"
  - "Employ a 3 stage Stackleberger game: defender – attacker – defender (DAD)"
  - "Did not address hijacking"

# "Take-aways" from Tutorials (2 of 2)

- Live-Virtual-Constructive Analysis (Rajive Bagrodia, Kent Pickett)
  - Characterized cyber attacks, defense
  - For PEOSTRI, developed phase I: StealthNet
- Social Network Analysis (Jim Morris)
  - Fighting "Dark Networks"
  - "Math to the rescue!" … but
    - Most of the techniques assume perfect data
    - Devil is in the details

# "Take-aways" from Plenaries (1 of 2)

- MG Dick Webber
  - "The Network is a weapon system"
  - The "wiring diagram" and the authorities are very complicated!
  - 24th AF Challenges
    - Number 1: Situational Awareness and C2
    - Rapid/real time acquisition
    - We need to grow the cyber capacity
  - Bottom line: Amazing progress in two years!

# "Take-aways" from Plenaries (2 of 2)

- Mark Maybury, Chief Scientist of the AF
  - "Things are changing *rapidly*" (e.g., technology change, connectivity, foreign supply, threat, … and cost over runs)
  - "The cyber problem is a wicked problem"
  - "We need a science of cyber security" (e.g., JASON report)
- Fisher Little, 24th AF/A2
  - Focus on cyber threats and vulnerabilities (re: China, Russia)
  - Emerging threat: Stuxnet

# Agenda

- Context
- Insights from
  - Tutorials, Plenaries
  - Themes from the Working Groups
  - Synthesis Group Perspectives
- Summary

# Themes Across Working Groups (1 of 7)

- Mission Assurance requires an understanding of how network capabilities map into the mission
  - Must understand how actions to construct, extend, operate, and defend the network will impact the mission
  - Such maps are seldom, if ever, generated
- Recommendation:
  - Operational planning must anticipate and delineate the impacts of the network itself, cyber attacks on the network, and potential defensive actions on the mission
  - This should be a formal element of the operational planning and execution process as well as the building, implementation and operation of “the network”

# Themes Across Working Groups (2 of 7)

- For the US and allies, there appears to be an extreme shortage of personnel trained and capable of engaging in cyber warfare
  - Needed skills and associated training and certification requirements are not well understood
  - Manpower analyses seem to consistently underestimate the resources required
- Recommendation:
  - Department/Interagency-level emphasis and initiatives to correct
  - Review/apply available manpower analysis tools

# Themes Across Working Groups (3 of 7)

- There is little mutual understanding and engagement between the cyber and analysis communities
  - Cyber personnel generally do not know about operations analysis and how it can help them
  - Few Operations Analysts/Researchers focus on matters of cyber warfare
- Recommendation:
  - Establish a MORS Cyber Analysis Community of Practice
  - Cognizant organizations should obtain and assign more analysts to the area of cyber warfare
  - Establish an outreach program to avail the Cyber community of Operations Research and how it can help

# Themes Across Working Groups (4 of 7)

- Inadequate understanding of the threat is associated with:
  - Cyber situational awareness difficulties
  - Virtual inability to detect “low, slow” attacks
  - Lack of data, data reporting, and data sharing
- Recommendation: more rigorous analysis and dissemination of threat capabilities, techniques, targets, goals, MO’s, motivations, strengths and weaknesses

# Themes Across Working Groups (5 of 7)

- There is a lack of specificity and clarity in communication (i.e., dialog, discussion, written communications) associated with cyber warfare
  - Communication from users (i.e., the “theater”) tends to be qualitative rather than quantitative
  - Direct, meaningful and agreed-upon metrics are lacking
  - Lexicon is not common across Services, user communities, and operational communities
- Recommendation:
  - TTP’s and doctrine should be developed and practiced to eliminate this unnecessary aggravation of the problem
  - Complete and formalize use of the Joint Staff Cyber Lexicon.

# Themes Across Working Groups (6 of 7)

- For the US, Cyber Warfare is in a prolonged, nascent state of development
  - There is not an “organized body of knowledge”
  - Practices and procedures are frequently ad hoc and/or outmoded
  - Pace of network technology creates a constantly changing environment which exacerbates the “wicked” problem
  - Organizational constructs and relationships are arcane
  - Acquisition policies and practices do not fit the area well
  - We are playing “catch up”
- Recommendation:
  - A matter of emphasis, funding, training, awakening—and, leadership
  - Build a bibliography (see detailed backup slide)

# Themes Across Working Groups (7 of 7)

- There are ample opportunities for applying OR capabilities (existing or within reach)—for example,
  - Force-on-force analysis that accurately accounts for Cyber effects and actions
  - Statistical Process Control techniques to enhance Situation Awareness and threat awareness
  - Design of experiments methodologies to help assess rapidly fielded equipment and systems
  - Application of Neural Networks to help detect anomalies and hostile activity
  - Decision Analysis tools and techniques to facilitate response to attacks
  - Optimization/matching techniques to address requirements prioritization
  - Manpower Analysis tools and methodologies to assist with those issues
- Recommendation:
  - Analysis communities across the Services need to make doing this a priority
  - Need an associated “pull” from the Cyber community
  - Leaders’ roles are key

# Agenda

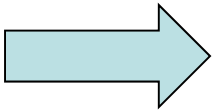
- Context
- Insights from
  - Tutorials, Plenaries
  - Themes from the Working Groups
  - Synthesis Group Perspectives
- Summary

# Synthesis Perspectives (1 of 2)

- Canonical Findings
  - We need a
    - Lexicon!
    - Bibliography!
  - "In God we trust; all others need to bring **DATA**!"
  - Given the speed that the cyber problem is changing, we need to hold meetings more frequently (e.g., every other year)

# Synthesis Perspectives (1 of 2)

- Canonical Findings
  - We need a
    - Lexicon (see attached SEI Taxonomy*)
    - Bibliography (see attached CSIS Bibliography*)
  - "In God we trust; all others need to bring **DATA**!"



Given the speed that the cyber problem is changing, we need to hold meetings more frequently (e.g., every other year)

*Documents provided as examples. This is not an endorsement by MORS or its Sponsors.

# Synthesis Perspectives (2 of 2)

- High Payoff Cyber Areas for Operations Research
  - Better understanding of the “situational awareness” problem
  - Formulating more meaningful Measures of Merit (MoMs)
  - Integrating network effects into Force-on-Force modeling/analysis
  - Decision Analysis Methods to aid Mission-Network Mapping
  - Cyber education and training
  - Manpower analysis applied immediately to the Cyber workforce
  - Use combat analyst “reach-back” model to help develop a similar capability in the Cyber Arena
  - Use established Operations Research VV&A methodologies to help the Cyber community similarly assess their tools and data
  - Identify the in-depth research issues that must be addressed by the operations research community

# Synthesis Perspectives (2 of 2)

- High Payoff Cyber Areas for Operations Research
  - Better understanding of the "situational awareness" problem
  - Formulating more meaningful Measures of Merit (MoMs)
  - Integrating network effects into Force-on-Force modeling/analysis
  - Decision Analysis Methods to aid Mission-Network Mapping
  - Cyber education and training
  - Manpower analysis applied immediately to the Cyber workforce
  - Use combat analyst "reach-back" model to help develop a similar capability in the Cyber Arena
  - Use established Operations Research VV&A methodologies to help the Cyber community similarly assess their tools and data
  - Identify the in-depth research issues that must be addressed by the operations research community

# Synthesis Perspectives (2 of 2)

- High Payoff Cyber Areas for Operations Research
  - Better understanding of the “situational awareness” problem
  - Formulating more meaningful Measures of Merit (MoMs)
  - Integrating network effects into Force-on-Force modeling/analysis
  - Decision Analysis Methods to aid Mission-Network Mapping
  - Cyber education and training
  - Manpower analysis applied immediately to the Cyber workforce
  - Use combat analyst “reach-back” model to help develop a similar capability in the Cyber Arena
  - Use established Operations Research VV&A methodologies to help the Cyber community similarly assess their tools and data
  - Identify the in-depth research issues that must be addressed by the operations research community

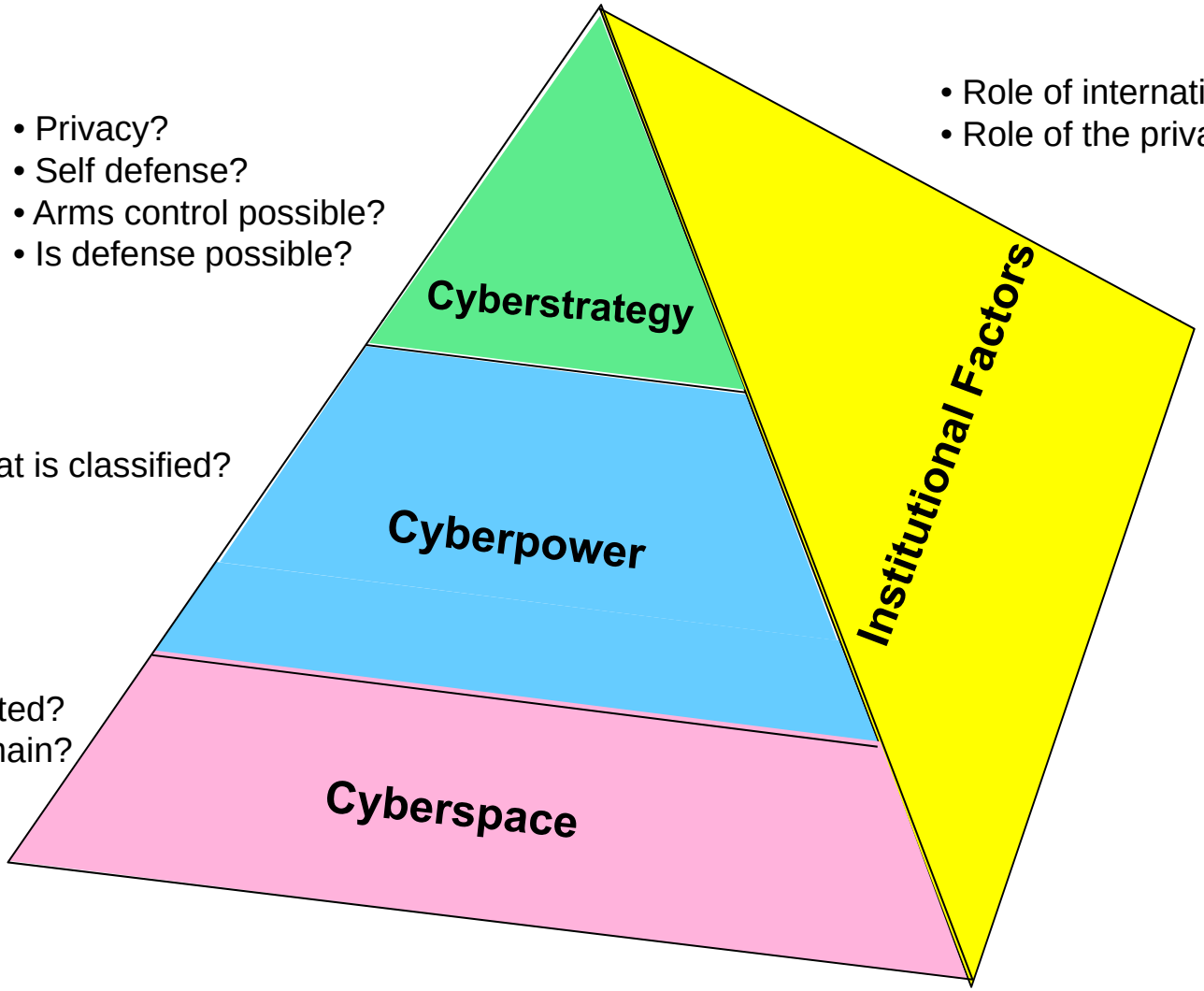
# Working Group Insights

- Working Group 1
  - Situational awareness is very important
  - For counter-stealth, how do you get the insight into what they are doing, how do you know their TTPs, how do you get to know their low observable tactics
- Working Group 2
  - The most vulnerable cyber component is still the people
  - Get social scientists and psychologists involved in the planning
- Working Group 3
  - We need evidence based on cyber analytics
  - Incident handling process is ripe for analysis
  - We need the doctrine to better define / accept
- Working Group 4
  - Must leverage existing doctrine
  - Cyber and hypersonic weapons change the battlefield
  - Exercise and experimentation are very important

# Summary

- We have shared!
  - Operations analysts
  - Cyber operators
  - Consumers of cyber capabilities
- A Community of Practice on Cyber is needed – MORS has a role to play!
- Areas of high payoff have been identified—let's get busy!

- Back-up Material


• Privacy?
• Self defense?
• Arms control possible?
• Is defense possible?
• Role of international law?
• Role of the private sector?
Cyberstrategy
Institutional Factors
• What is classified?
Cyberpower
• Unprecedented?
• Cyber a domain?
• Threat?
Cyberspace

# GEN Hayden: The Future of Things "Cyber"

- How do we deal with the unprecedented?
- Is cyber really a domain?
- How do we deal with privacy?
- Do we really know the threat?
- What should we expect from the private sector?
- What is classified?
- What constitutes the right of self defense?
- Is there a role for international law?
- Is cyber arms control possible?
- Is defense possible?