INSTITUTE FOR DEFENSE ANALYSES

Assessing Information Effects Workshop Proceedings

Stephen M. Olechnowicz, *Project Leader*

John T. Hanley, Jr.
John A. Cordero
G. Lee Kennedy

November 2017

IDA Non-Standard
NS D-8858

INSTITUTE FOR DEFENSE ANALYSES
4850 Mark Center Drive
Alexandria, Virginia 22311-1882

About This Publication

This work was conducted by the Institute for Defense Analyses (IDA) under Task C5107, "Cyberspace Operations Working Group." The views, opinions, and findings should not be construed as representing the official position of either the Department of Defense or the sponsoring organization.

For more information:

Stephen M. Olechnowicz, Project Leader
solechno@ida.org, 703-845-6633

Margaret E. Myers, Director, Information Technology and Systems Division
mmyers@ida.org, 703-578-2782

Copyright Notice

INSTITUTE FOR DEFENSE ANALYSES

IDA Non-Standard NS D-8858

Assessing Information Effects Workshop Proceedings

Stephen M. Olechnowicz, *Project Leader*

John T. Hanley, Jr.
John A. Cordero
G. Lee Kennedy

Preface

On October 16, 2017, representatives from the Institute for Defense Analyses (IDA), the Office of the Secretary of Defense for Cost Analysis and Program Evaluation (OSD CAPE), the U.S. Naval War College, the Chief of Naval Operations Assessments Division (OPNAV N81), academia, and industry met at IDA in Alexandria, Virginia, for a half-day workshop to foster dialog on assessing information. The topics addressed in this workshop offer ideas on how to model the effects of information through a variety of analytical efforts to gain insight on a potential adversary's behavior in cyber and information warfare. This document contains the proceedings of the workshop.

Contents

1. Introduction

> *Great part of the information obtained in war is contradictory, a still greater part is false, and by far the greatest part is of a doubtful character. What is required of an officer is a certain power of discrimination, which only knowledge of men and things and good judgment can give. The law of probability must be his guide.*
>
> On War, Book I Chapter 6 "Information in War," Carl von Clausewitz

A. Background

Information in warfare that is accurate and trusted can be a critical factor in the successful outcome of a mission or campaign. Advanced information technologies that are available to both friendly and adversarial forces enable the use of information in ways that provide opportunities and risks to a commander in the preparation for and the conduct of warfare. Modeling, simulation, and war gaming can provide useful insights for better use of information to gain advantages in physical and cyber conflict, and to shape or compel an adversary's behavior across the spectrum of warfare.

Dr. John T. Hanley engaged with Dr. Margaret Myers at the Institute of Defense Analyses (IDA) to host a workshop to explore a variety of topics such as assessing the effects of corrupt information, the use of artificial intelligence in combat, and evaluating cyber effects. This half-day Assessing Information Effects workshop was held October 16, 2017, at IDA to coincide with the Military Operations Research (MORS) Wargaming Special Workshop held October 17 to 19, 2017. Several of the participants in the IDA workshop also participated in the MORS workshop.

B. Workshop Panels

Three panels presented ongoing or proposed research efforts related to assessing or using information in warfare, including cyber warfare. Each panel was 45 minutes long with three panelists, each limited to 15 minutes for his or her presentation and a short question and answer period. A short summary of the discussions for each briefing is presented in the following sections followed by the presentations.

The Assessing Information Effects workshop agenda is below, and biographies of the panelists' and key participants' can be found in Appendix A. Please note that the views presented are those of the individuals and do not represent official organizational positions.

Agenda

Panel 1: Quantitative Analytic Approaches

John J. Borsi
OSD CAPE
Information Effects Analyses I Have Done

Phil Pournelle
Long Term Strategy Group
Modeling and Simulation of the value of C4ISR

LCDR Connor McLemore, USN
OPNAV N810
A Model for Geographically Distributed Combat Interactions of Swarming Naval and Air Forces

Panel 2: Information in Gaming

Stephanie Helm
Naval War College
Cyber Considerations for War Gaming

Elizabeth Bartels
Pardee RAND Graduate School
Resolving Hidden Information in Open Adjudication

Phil Pournelle
Long Term Strategy Group
Marinus

Panel 3: Applications

Kathleen Conley
IDA
C2 by Design

Diane Schroer
NAVSEA
Risk Assessment

Stephen Downes-Martin
Independent
Information Operations in COIN, and more

2. Opening Remarks

Summary

Dr. Margaret Myers, Director of the Information Technology and Systems Division (ITSD), and Mr. Stephen Olechnowicz, an ITSD cyber Research Staff Member, welcomed the conference participants to IDA and to the workshop. Dr. John Hanley noted that the idea for the conference began when Mr. Andrew Marshall, the legendary Director of Net Assessment in the Office of the Secretary of Defense (OSD), told him that the analytic community needed to place more attention on information in war games. Dr. Hanley referred to a Soviet saying that time was the only independent variable in warfare, and that the timing of “when who knows what” drives decision and action. Military Strategist Colonel John Boyd, United States Air Force (USAF), included this concept in his Observe, Orient, Decide, and Act (OODA) loop decision cycle shown in Figure 1, but capturing the effects of information in analysis and war gaming is difficult and illusive.

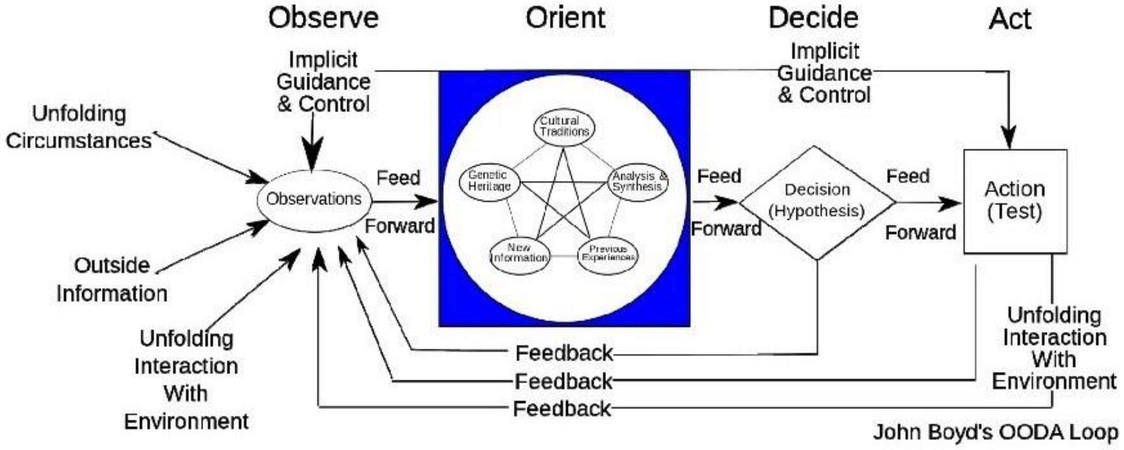


Figure 1. Col John Boyd's OODA Loop

Dr. Hanley provided examples of his experience in modeling combat, using game theory and gaming, the evolution of electronic warfare and information operations, and using artificial intelligence in cyber countermeasures as the motivation for panels on analysis, games, and applications. He noted that the panelists’ presentations were eclectic, would be intense, and were intended to start the initial set of many conversations on the many dimensions of this subject.

3. Panel 1: Quantitative Analytic Approaches

Discussion Summary

Dr. John Borsi discussed how he approached analyzing information and cyber effects. He emphasized the difference between systems and operations analysis and disparaged attempts to quantify the unknown and unknowable. He discussed how his approach to categorizing effects into well-defined discrete levels instead of attempting quantification through survey methods led to logically defensible insights.

Phil Pournelle discussed how N81 had employed a suite of models, taking advantage of the strengths of each to address a vignette involving a long sensor-to-shooter chain, how these models incorporated data from fleet exercises, and the challenges of scaling such approaches to deal with large numbers of networked entities.

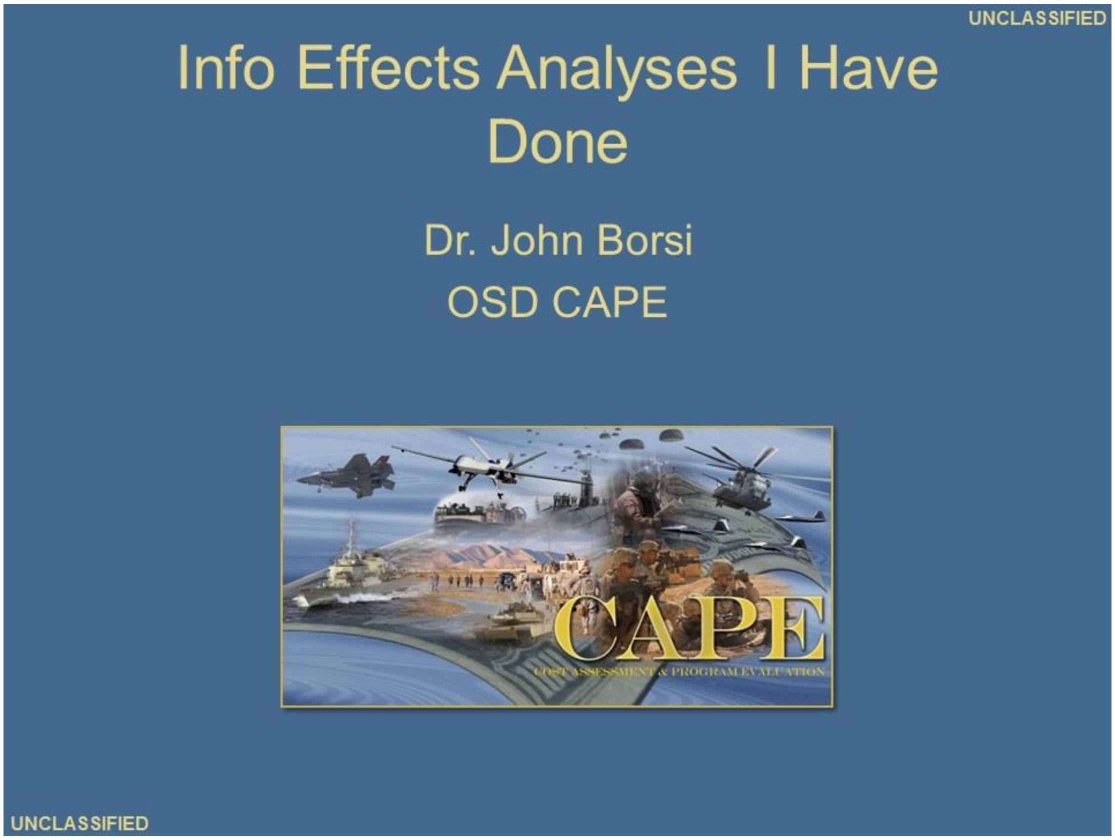
Commander Connor McLemore, United States Navy, described the use of Salvo Equations to explore distributed, swarm operations in future warfare. A small model with quick computations supported sensitivity analysis to determine which features of the model had the most effect and provided non-intuitive results that could be studied and explained. The model has applications as an operational decision aid beyond its use in analysis.

A. Dr. John Borsi: Information Effects Analyses I Have Done

Presentation Summary

Dr. Borsi began his discussion by providing recommendations for information technology (IT) operators' role in in gaming. He outlined step-by-step guidance for strategic command and control (C2) that can be applied to multiple scenarios using a process gleaned from years of experience. The main thrust of his presentation focused on asserting that "people don't know why they do things," which speaks to game theory, biases, and cognitive dissonance.

Next, he provided insight on desired outcomes of games and exercises with emphasis on effects of cyber. Essentially, outcomes should affect strategy, not tactics. One key insight from his experience in this domain is that quantification is often the goal but is of no use for its own sake. Additionally, he pointed out that operational assessments should be executed by mission operators, not solely by cyber troops. The relationship of mission readiness and the availability of IT-enabled capabilities needs to be explored further. A persistent theme of these discussions was the "limits of mathematics" as applied to gaming.



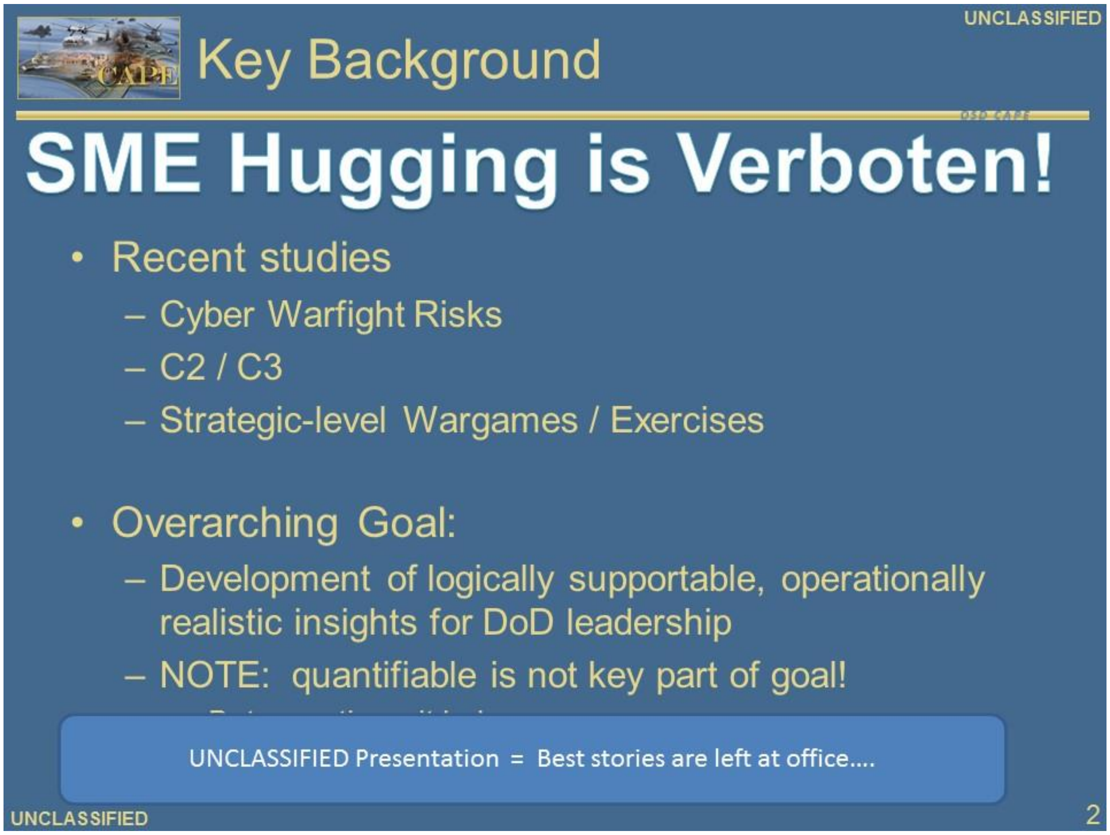
UNCLASSIFIED

Info Effects Analyses I Have Done

Dr. John Borsi

OSD CAPE

UNCLASSIFIED



UNCLASSIFIED

Key Background

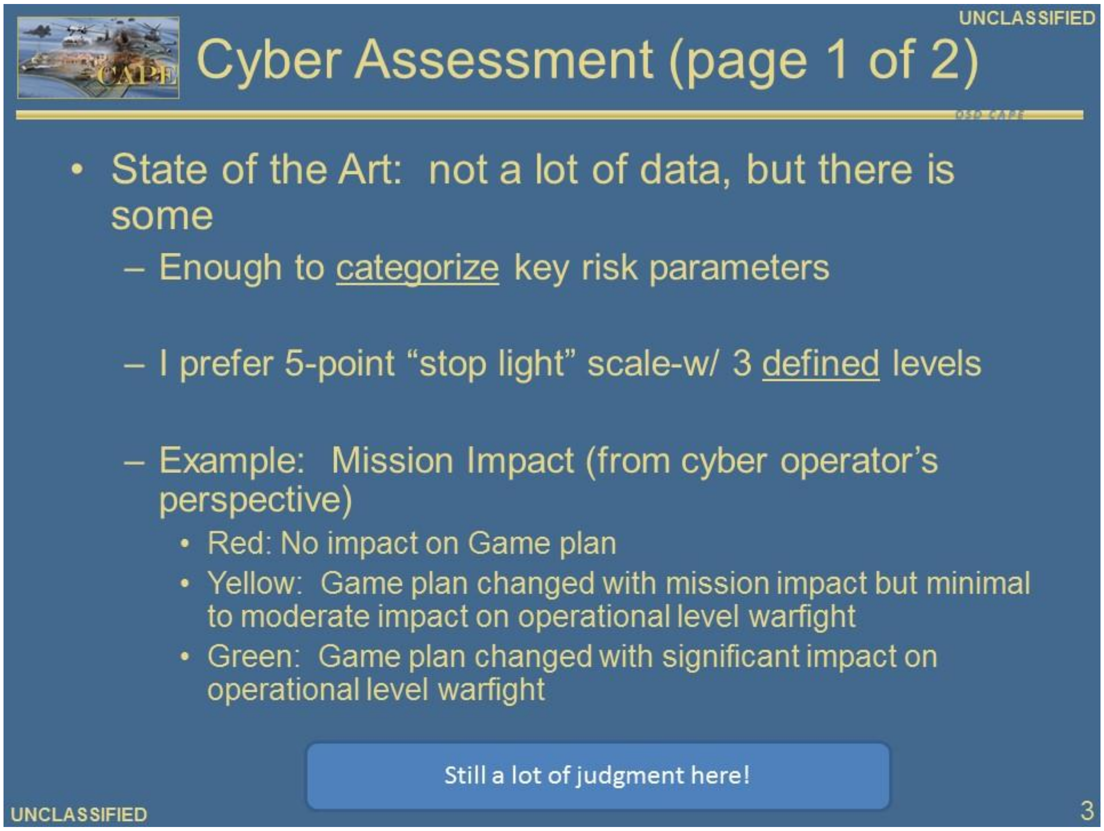
OSD CAPE

SME Hugging is Verboten!

- Recent studies
  - Cyber Warfight Risks
  - C2 / C3
  - Strategic-level Wargames / Exercises
- Overarching Goal:
  - Development of logically supportable, operationally realistic insights for DoD leadership
  - NOTE: quantifiable is not key part of goal!

UNCLASSIFIED Presentation = Best stories are left at office....

UNCLASSIFIED



UNCLASSIFIED

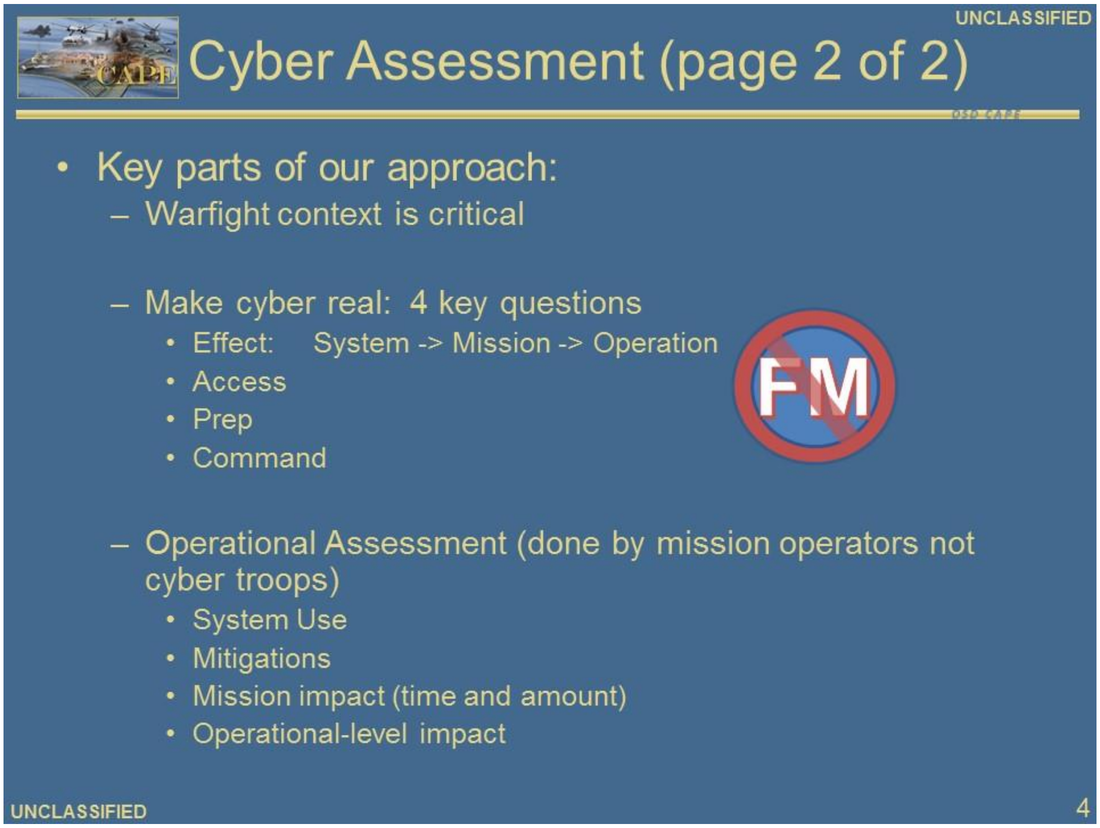
Cyber Assessment (page 1 of 2)

- State of the Art: not a lot of data, but there is some
  - Enough to categorize key risk parameters
  - I prefer 5-point “stop light” scale-w/ 3 defined levels
  - Example: Mission Impact (from cyber operator’s perspective)
    - Red: No impact on Game plan
    - Yellow: Game plan changed with mission impact but minimal to moderate impact on operational level warfight
    - Green: Game plan changed with significant impact on operational level warfight

Still a lot of judgment here!

UNCLASSIFIED

3



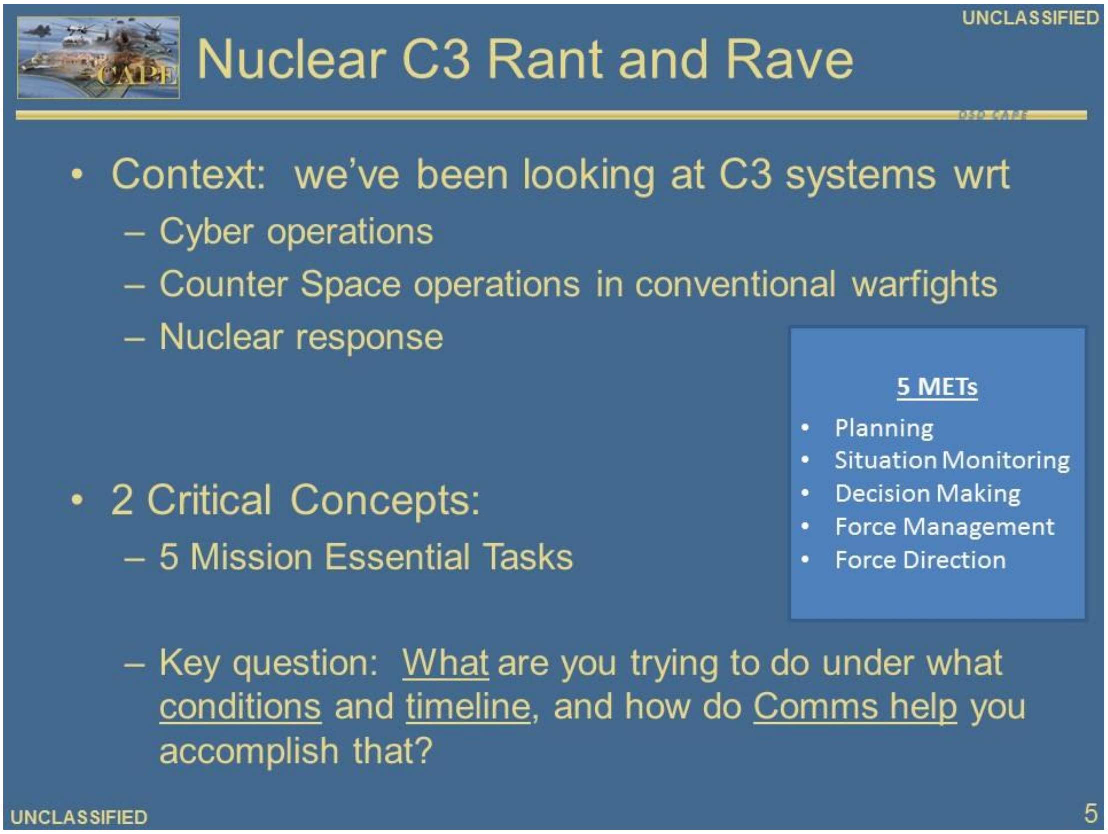
UNCLASSIFIED

Cyber Assessment (page 2 of 2)

- Key parts of our approach:
  - Warfight context is critical
  - Make cyber real: 4 key questions
    - Effect: System -> Mission -> Operation
    - Access
    - Prep
    - Command
  - Operational Assessment (done by mission operators not cyber troops)
    - System Use
    - Mitigations
    - Mission impact (time and amount)
    - Operational-level impact

UNCLASSIFIED

4



UNCLASSIFIED

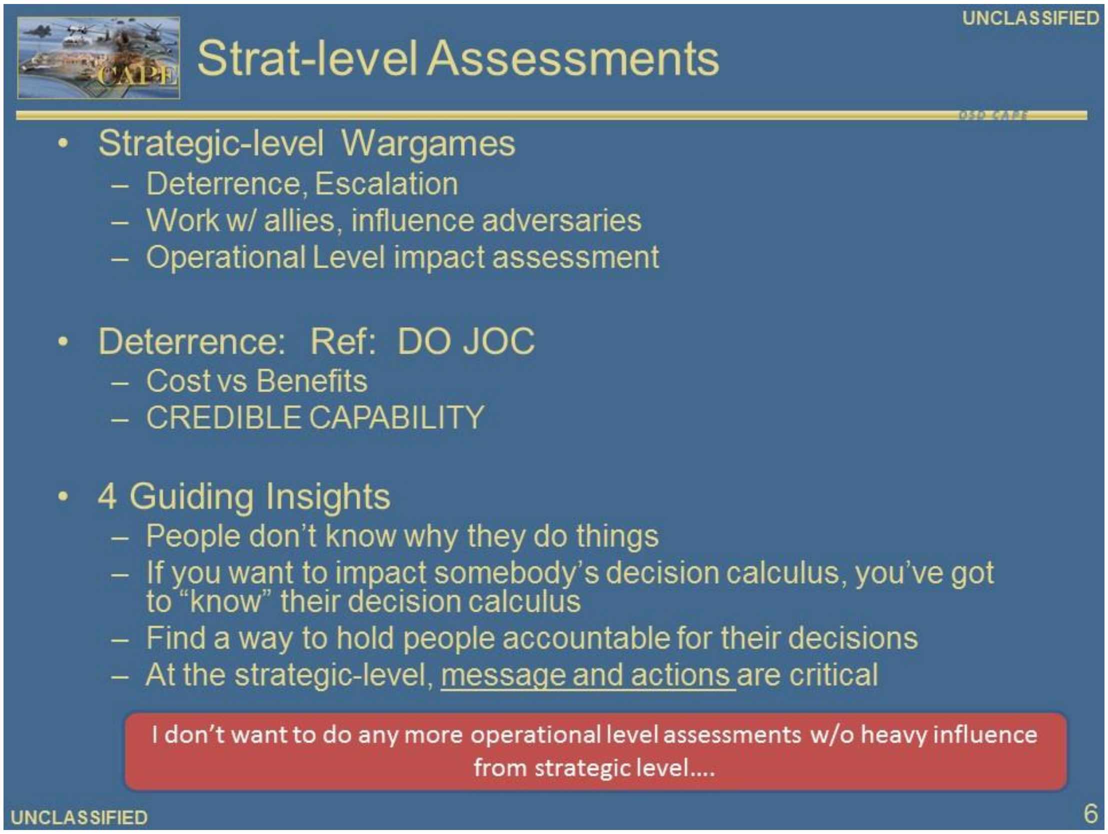
Nuclear C3 Rant and Rave

- Context: we've been looking at C3 systems wrt
  - Cyber operations
  - Counter Space operations in conventional warfights
  - Nuclear response
- 2 Critical Concepts:
  - 5 Mission Essential Tasks
  - Key question: <u>What</u> are you trying to do under what <u>conditions</u> and <u>timeline</u>, and how do <u>Comms help</u> you accomplish that?

<u>5 METs</u>

- Planning
- Situation Monitoring
- Decision Making
- Force Management
- Force Direction

UNCLASSIFIED 5



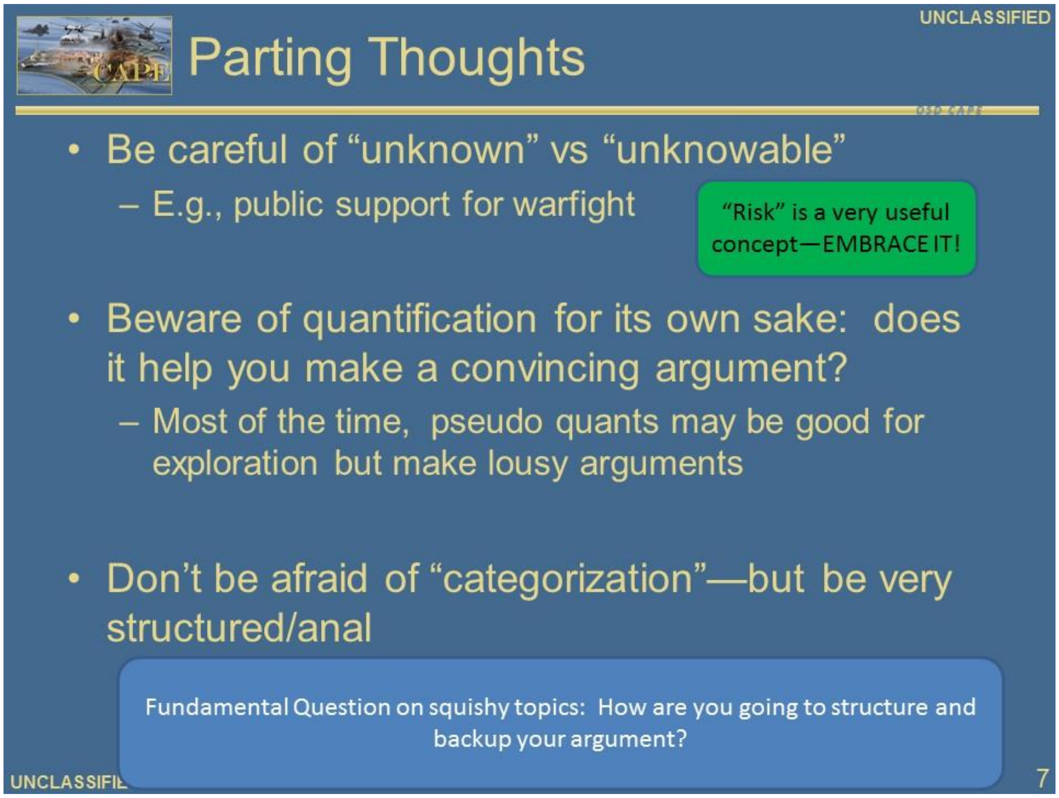
UNCLASSIFIED

Strat-level Assessments

- Strategic-level Wargames
  - Deterrence, Escalation
  - Work w/ allies, influence adversaries
  - Operational Level impact assessment
- Deterrence: Ref: DO JOC
  - Cost vs Benefits
  - CREDIBLE CAPABILITY
- 4 Guiding Insights
  - People don't know why they do things
  - If you want to impact somebody's decision calculus, you've got to "know" their decision calculus
  - Find a way to hold people accountable for their decisions
  - At the strategic-level, <u>message and actions</u> are critical

I don't want to do any more operational level assessments w/o heavy influence from strategic level....

UNCLASSIFIED 6



UNCLASSIFIED

Parting Thoughts

- Be careful of "unknown" vs "unknowable"
  - E.g., public support for warfight

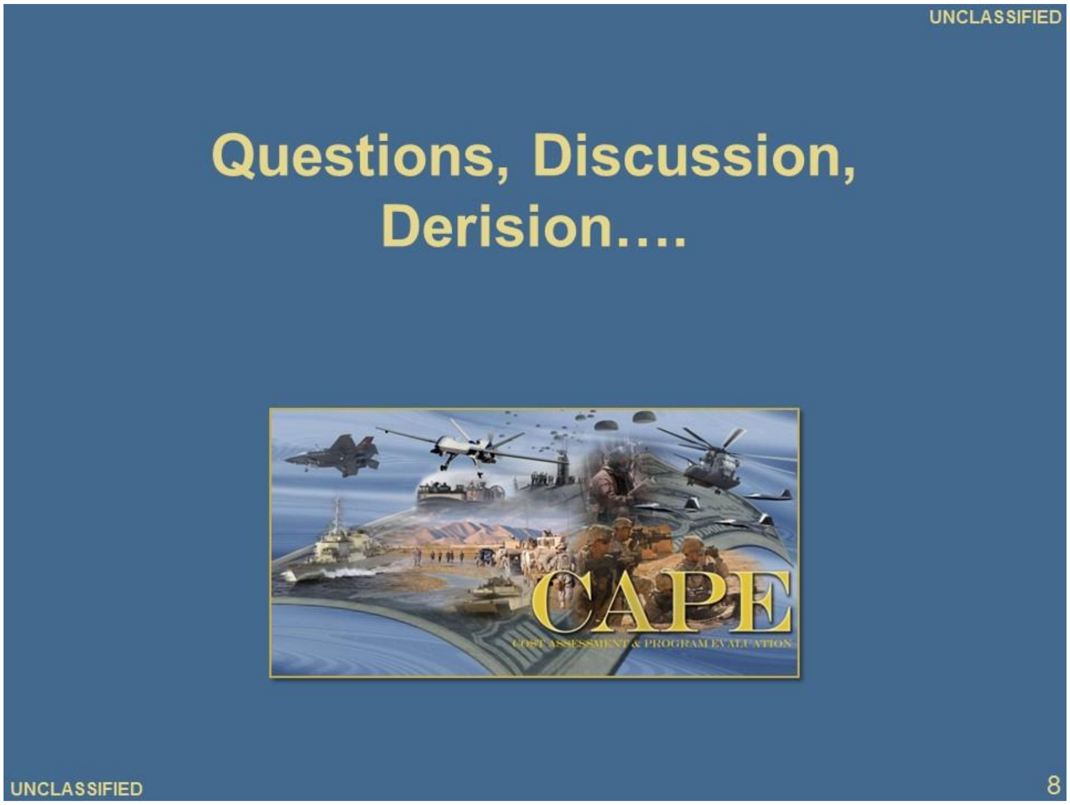
"Risk" is a very useful concept—EMBRACE IT!

- Beware of quantification for its own sake: does it help you make a convincing argument?
  - Most of the time, pseudo quants may be good for exploration but make lousy arguments
- Don't be afraid of "categorization"—but be very structured/anal

Fundamental Question on squishy topics: How are you going to structure and backup your argument?

UNCLASSIFI

7



UNCLASSIFIED

Questions, Discussion, Derision….

CAPE
COST ASSESSMENT & PROGRAM EVALUATION

UNCLASSIFIED

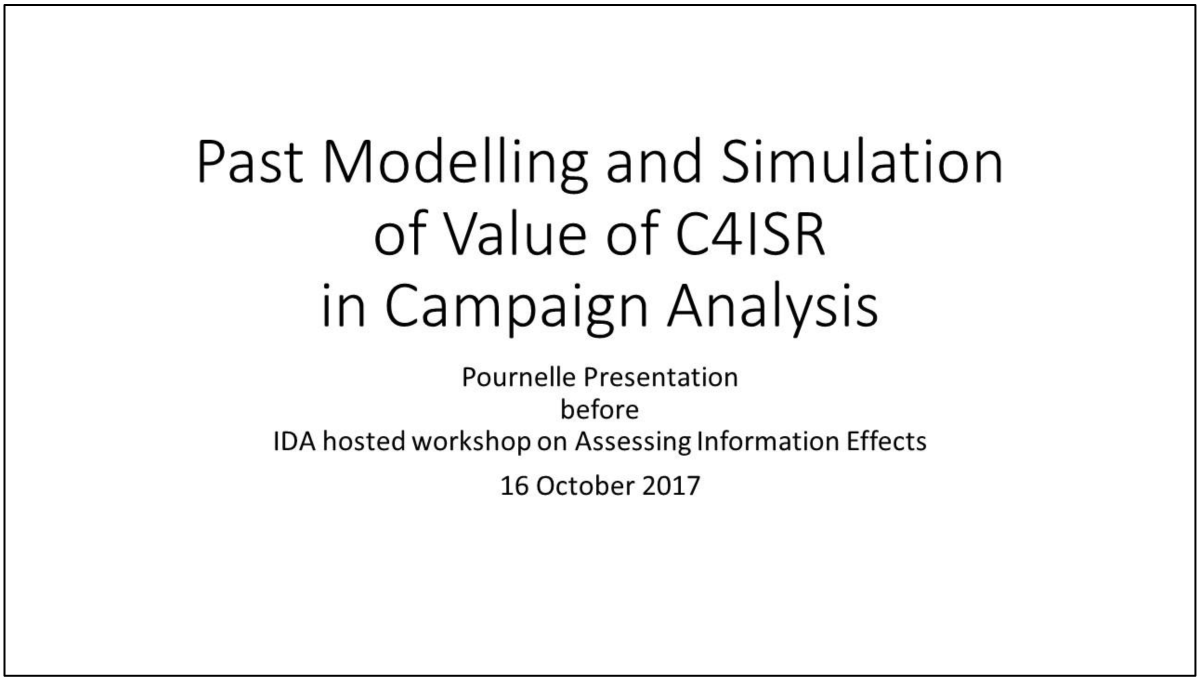
8

B. Phil Pournelle: Past Modelling and Simulation of value of C4ISR in Campaign Analysis

Presentation Summary

Mr. Pournelle started with an example of a reconnaissance and attack loop with a conventional surface target. He explained that at each stage of the process, data must be collected and verified before proceeding to the next stage. As the strike platform stage draws closer, risk increases. To reduce risk, he proposed grouping the decision stages into three distinct campaign model sectors: Command, Control, Communications, Computers, Intelligence, Surveillance and Reconnaissance (C4ISR) Space and Missile Operations Simulator (COSMOS) (overhead reconnaissance); Network Warfare Simulation (NETWARS) (communications data flow through multiple devices and decision makers); and Naval Simulation System (NSS) (Naval forces and kinetic action). All three should flow seamlessly (in an ideal world).

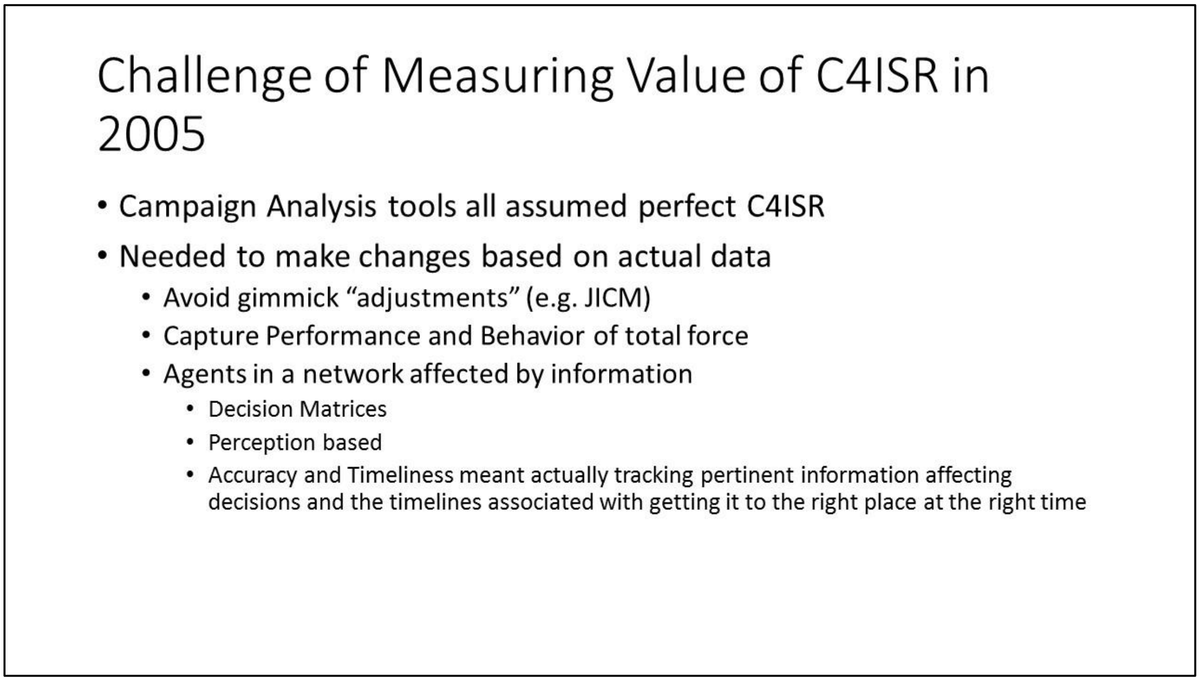
He documented his argument with specific examples to support his emphasis on decision loops and their impact on delivering effects in time. One key point of this model is that it reduces cyber to sensors, analysis, and communications, which is valuable for process modeling and improvement of C2. The model did not account for the potential of denial and disruption to processes driven by cyber effects, which is understandable given that the brief focused on improving the data-to-decision loop.



Past Modelling and Simulation of Value of C4ISR in Campaign Analysis

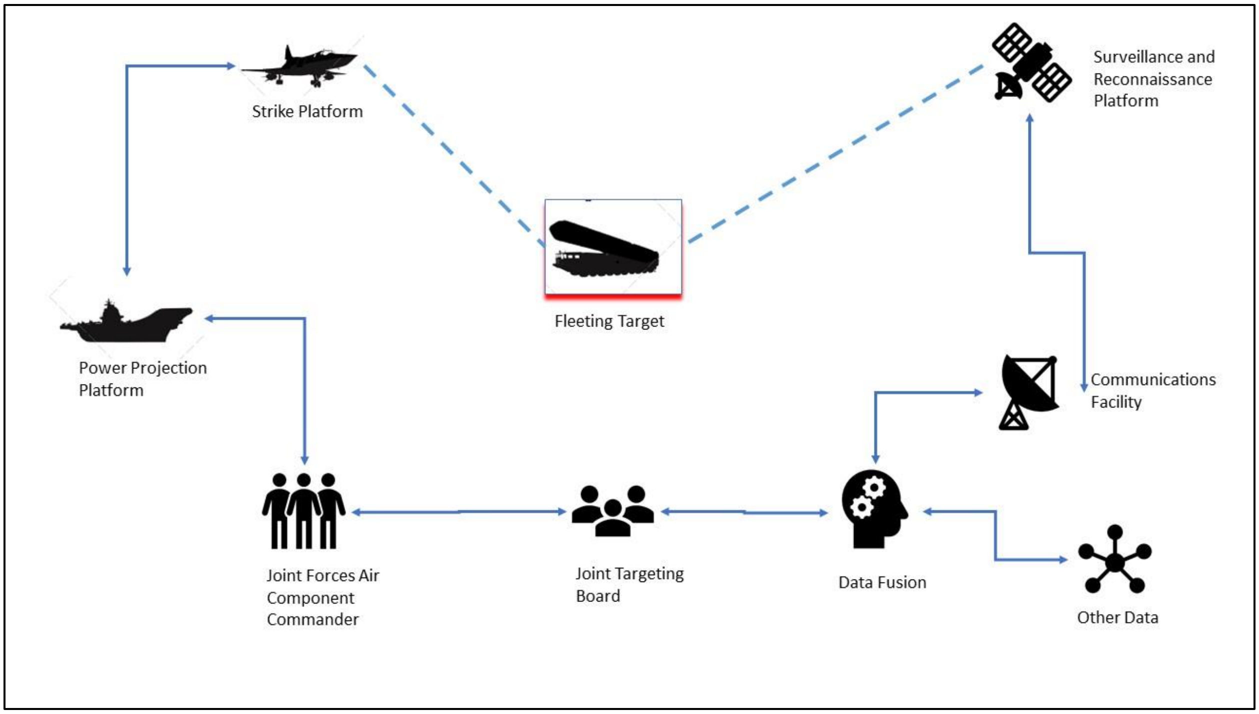
Pournelle Presentation
before
IDA hosted workshop on Assessing Information Effects

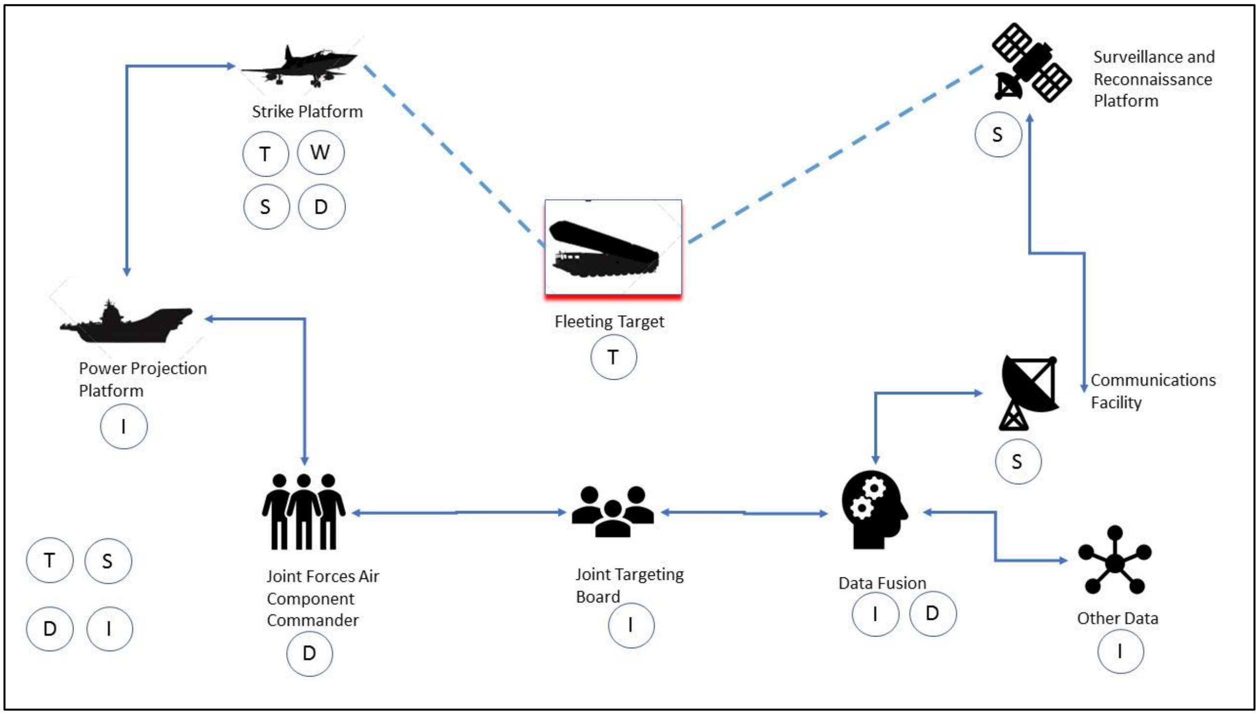
16 October 2017

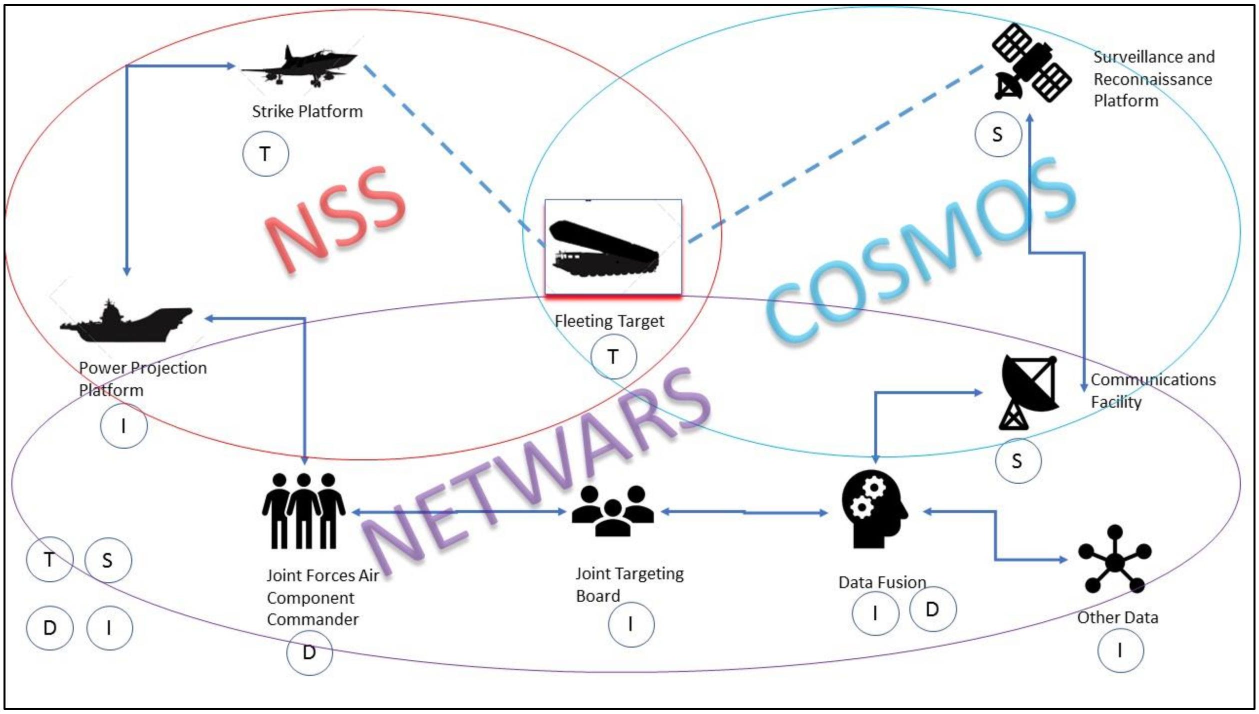


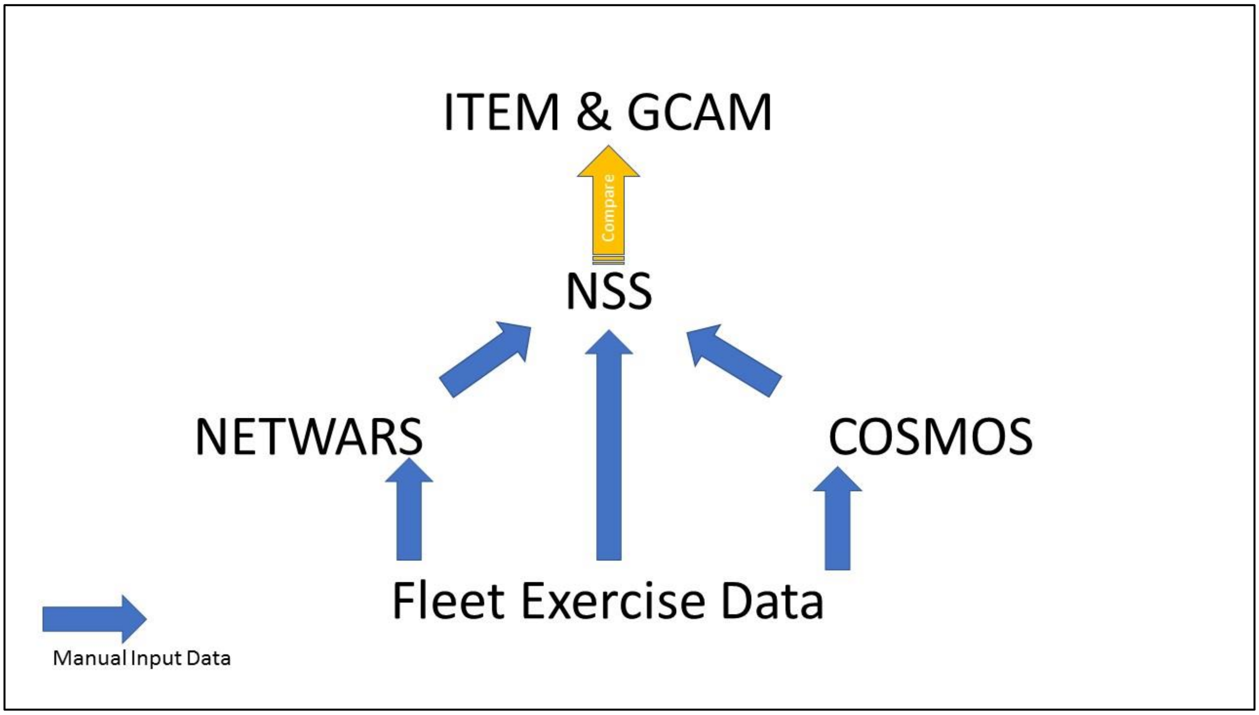
Challenge of Measuring Value of C4ISR in 2005

- Campaign Analysis tools all assumed perfect C4ISR
- Needed to make changes based on actual data
  - Avoid gimmick “adjustments” (e.g. JICM)
  - Capture Performance and Behavior of total force
  - Agents in a network affected by information
    - Decision Matrices
    - Perception based
    - Accuracy and Timeliness meant actually tracking pertinent information affecting decisions and the timelines associated with getting it to the right place at the right time


Strike Platform
Surveillance and Reconnaissance Platform
Fleeting Target
Power Projection Platform
Communications Facility
Joint Forces Air Component Commander
Joint Targeting Board
Data Fusion
Other Data

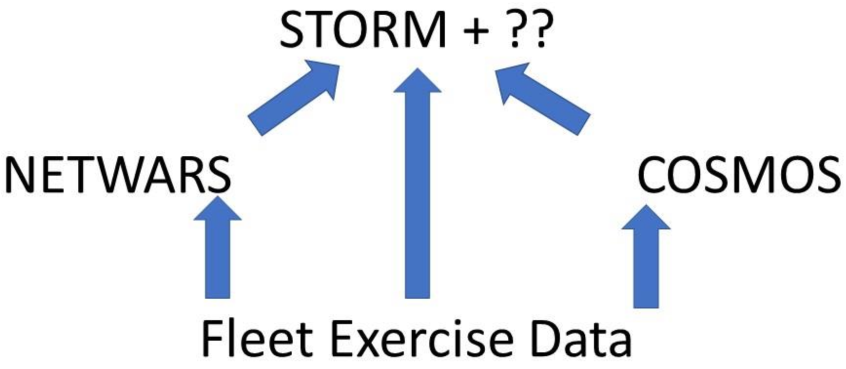

Strike Platform
T
W
S
D
Surveillance and Reconnaissance Platform
S
Fleeting Target
T
Power Projection Platform
I
Communications Facility
S
T
S
D
I
Joint Forces Air Component Commander
D
Joint Targeting Board
I
Data Fusion
I
D
Other Data
I


Strike Platform
T
NSS
Surveillance and Reconnaissance Platform
S
COSMOS
Fleeting Target
T
Power Projection Platform
I
NETWARS
Communications Facility
S
T
S
D
I
Joint Forces Air Component Commander
D
Joint Targeting Board
I
Data Fusion
I
D
Other Data
I


ITEM & GCAM
Compare
NSS
NETWARS
COSMOS
Fleet Exercise Data
Manual Input Data

Future

- Network vs. Network
  - Requires Red as well as Blue networks, decision matrices, data, etc.



STORM + ??

NETWARS

COSMOS

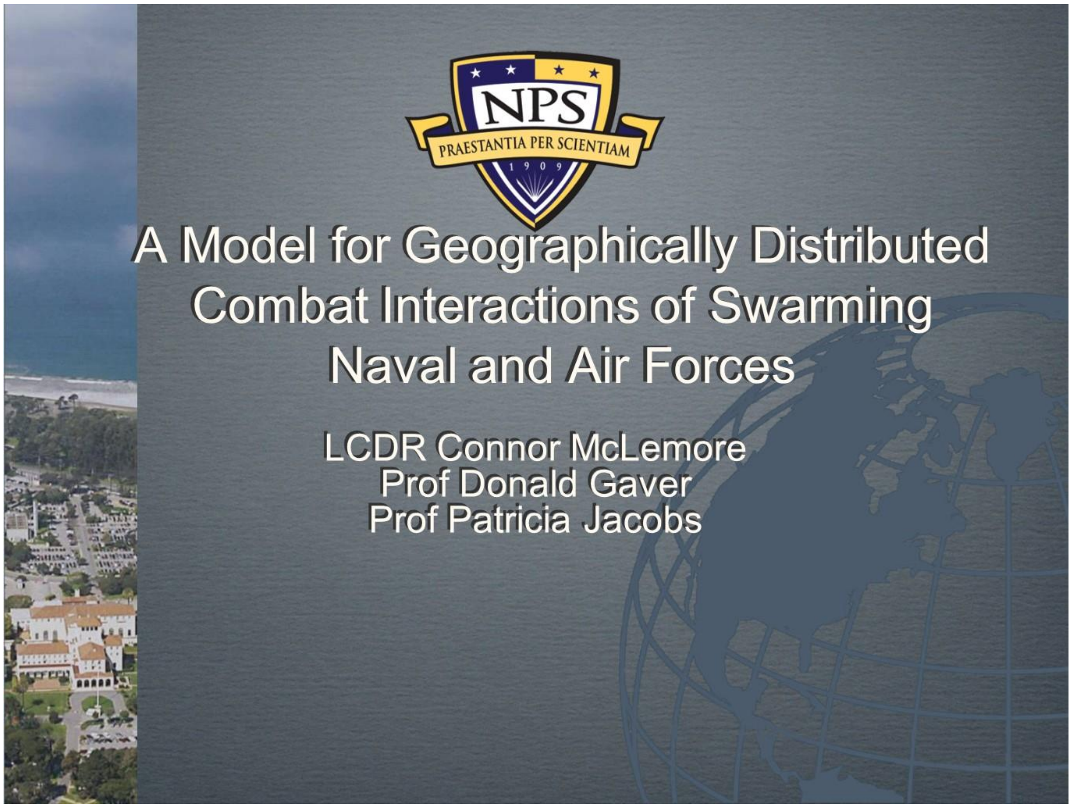
Fleet Exercise Data

C. LCDR Connor McLemore: A Model for Geographically Distributed Combat Interactions of Swarming Naval and Air Forces

Presentation Summary

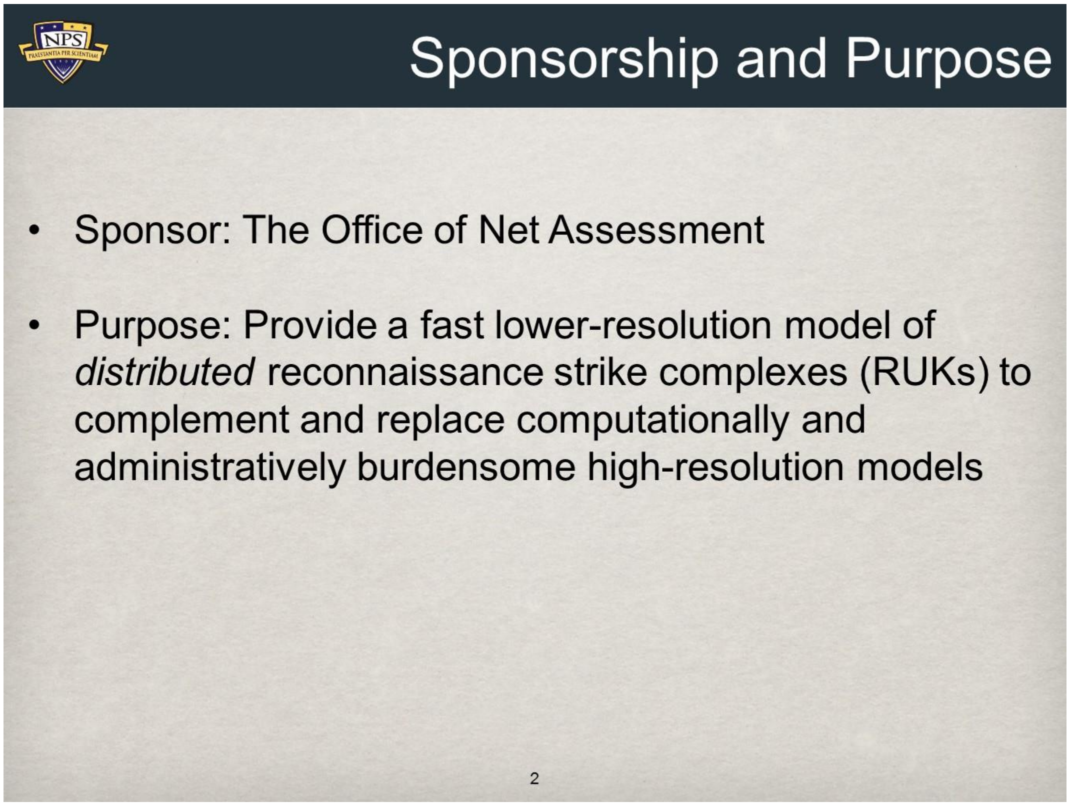
LCDR McLemore linked the efficacy of his models to actual experience, which made for a convincing presentation. Using a very specific model – a problem set of swarming of air platforms in an area of responsibility (AOR) – he demonstrated how his processes led to non-obvious connections. Due to time constraints, the presentation only briefly touched on some of the underlying equations supporting the model. Additional time would have been needed for detailed explanations.

A variety of models were presented, but he focused on the value of the Distributed Interaction Model: Strike platforms can be in states of unready, ready, active, degraded, or killed, and commanders must account for them when formulating strategy and tactics. The interactions can then be divided into grids with considerations for demand and conditions incorporated into decision-making. The decoy example toward the end of the presentation presented a real-world gaming scenario with a clear successful result, thereby supporting the model.



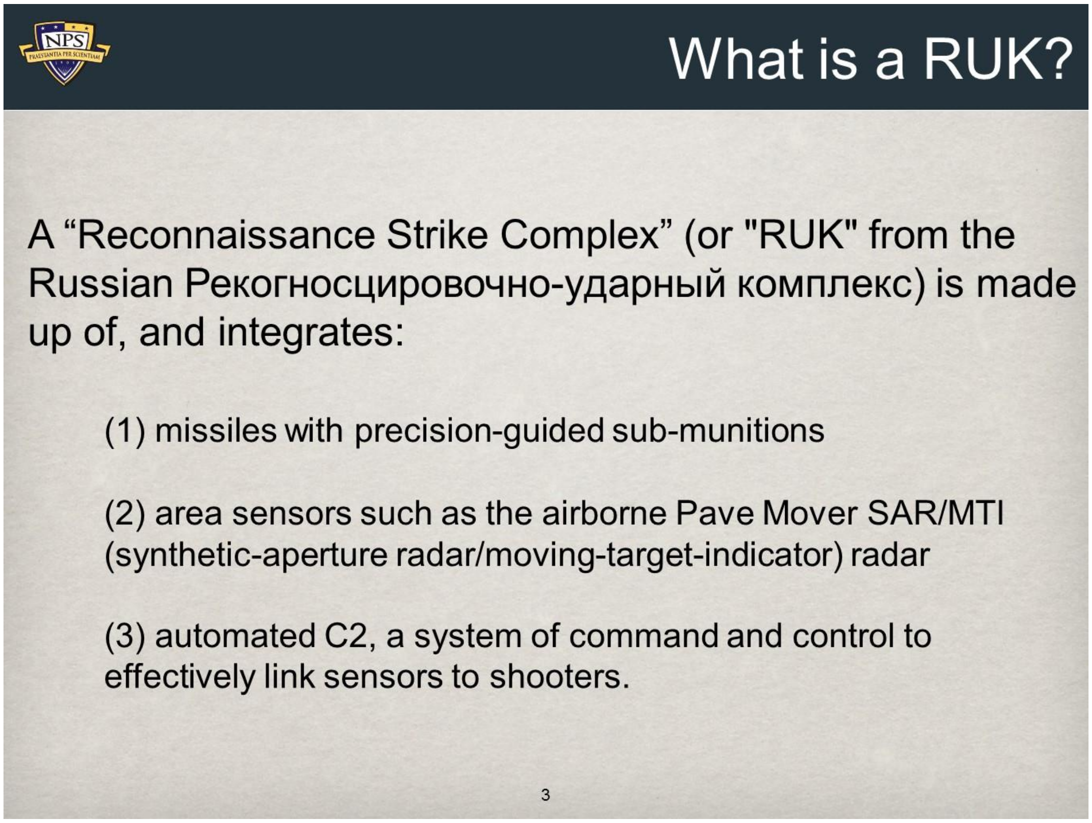
A Model for Geographically Distributed Combat Interactions of Swarming Naval and Air Forces

LCDR Connor McLemore
Prof Donald Gaver
Prof Patricia Jacobs



Sponsorship and Purpose

- Sponsor: The Office of Net Assessment
- Purpose: Provide a fast lower-resolution model of *distributed* reconnaissance strike complexes (RUKs) to complement and replace computationally and administratively burdensome high-resolution models



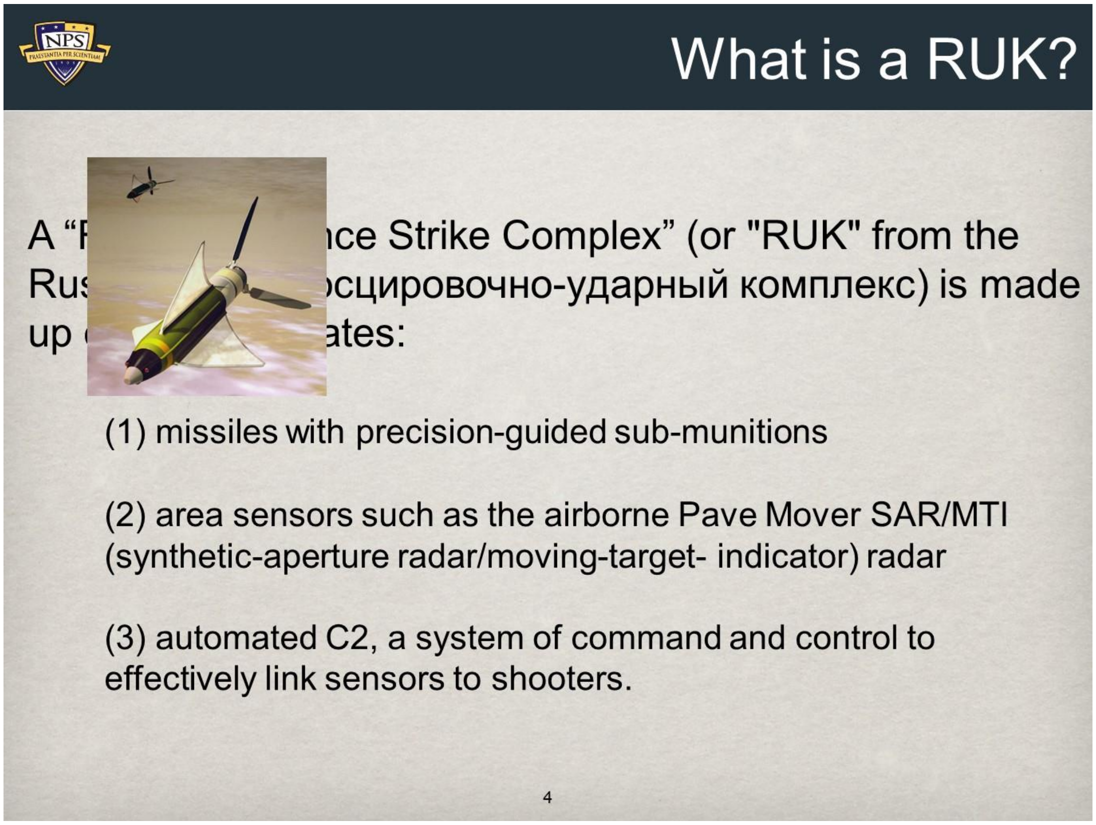
What is a RUK?

A “Reconnaissance Strike Complex” (or "RUK" from the Russian Рекогносцировочно-ударный комплекс) is made up of, and integrates:

(1) missiles with precision-guided sub-munitions

(2) area sensors such as the airborne Pave Mover SAR/MTI (synthetic-aperture radar/moving-target-indicator) radar

(3) automated C2, a system of command and control to effectively link sensors to shooters.



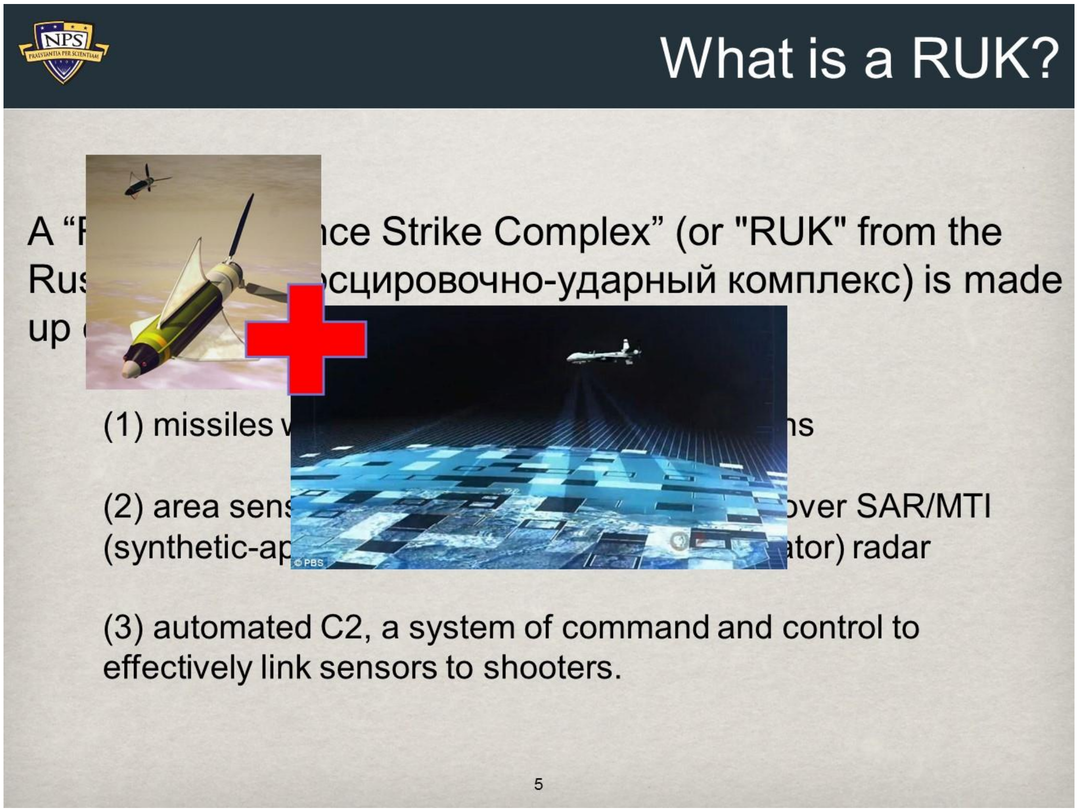
What is a RUK?

A “F ıce Strike Complex” (or "RUK" from the
Rus ɔсцировочно-ударный комплекс) is made
up ates:

(1) missiles with precision-guided sub-munitions

(2) area sensors such as the airborne Pave Mover SAR/MTI (synthetic-aperture radar/moving-target- indicator) radar

(3) automated C2, a system of command and control to effectively link sensors to shooters.



What is a RUK?

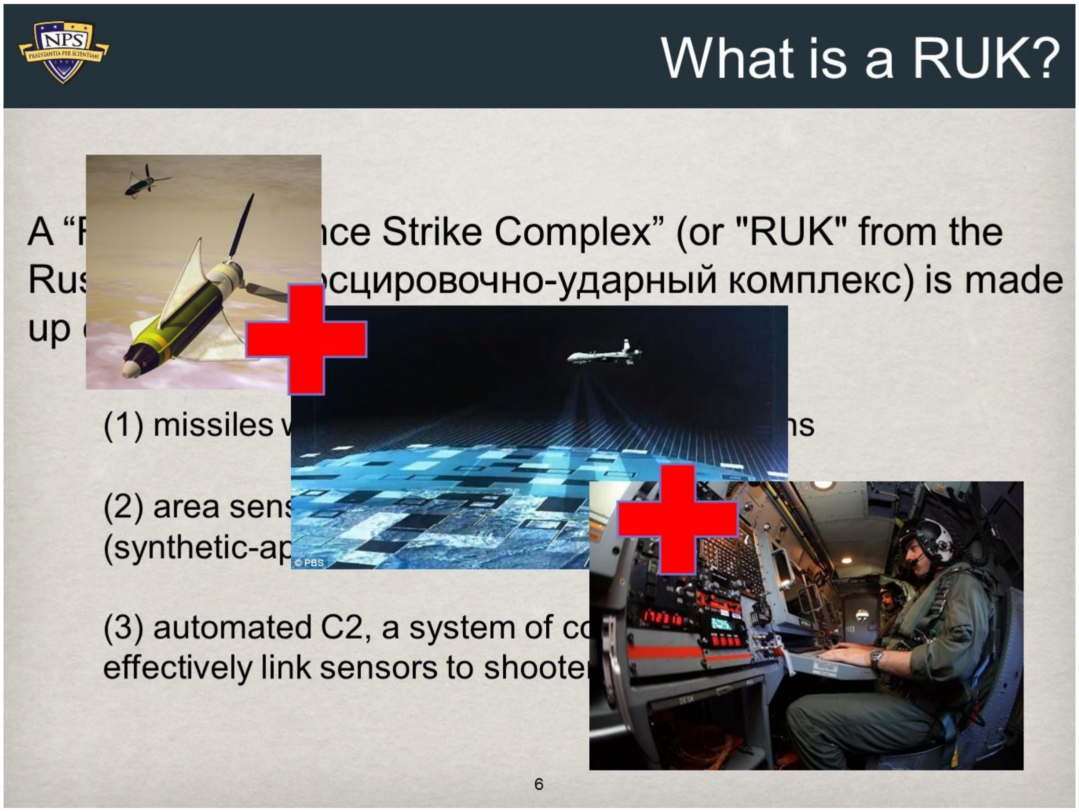
A “F nce Strike Complex” (or "RUK" from the Rus осцировочно-ударный комплекс) is made up

(1) missiles v ns

(2) area sens over SAR/MTI (synthetic-ap ator) radar

(3) automated C2, a system of command and control to effectively link sensors to shooters.

© PBS



What is a RUK?

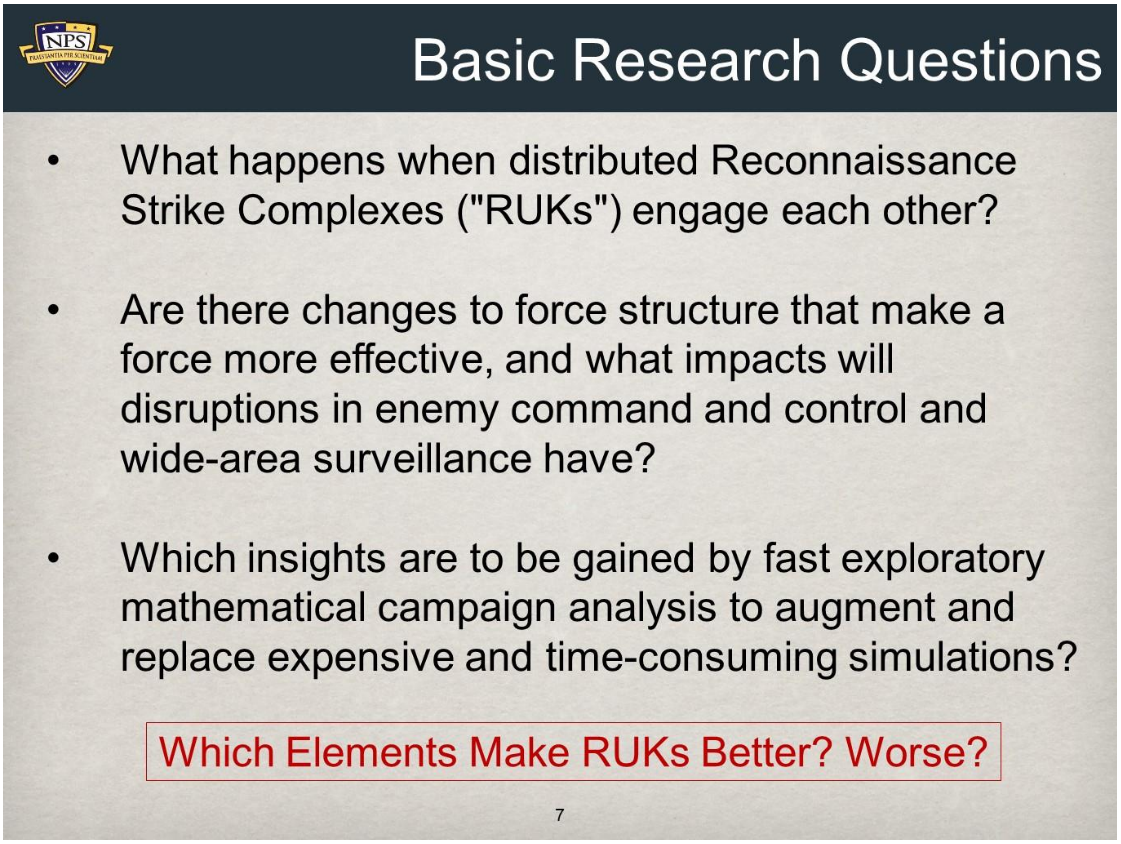
A “F nce Strike Complex” (or "RUK" from the Rus осцировочно-ударный комплекс) is made up

(1) missiles v ns

(2) area sens (synthetic-ap

(3) automated C2, a system of cc effectively link sensors to shoote

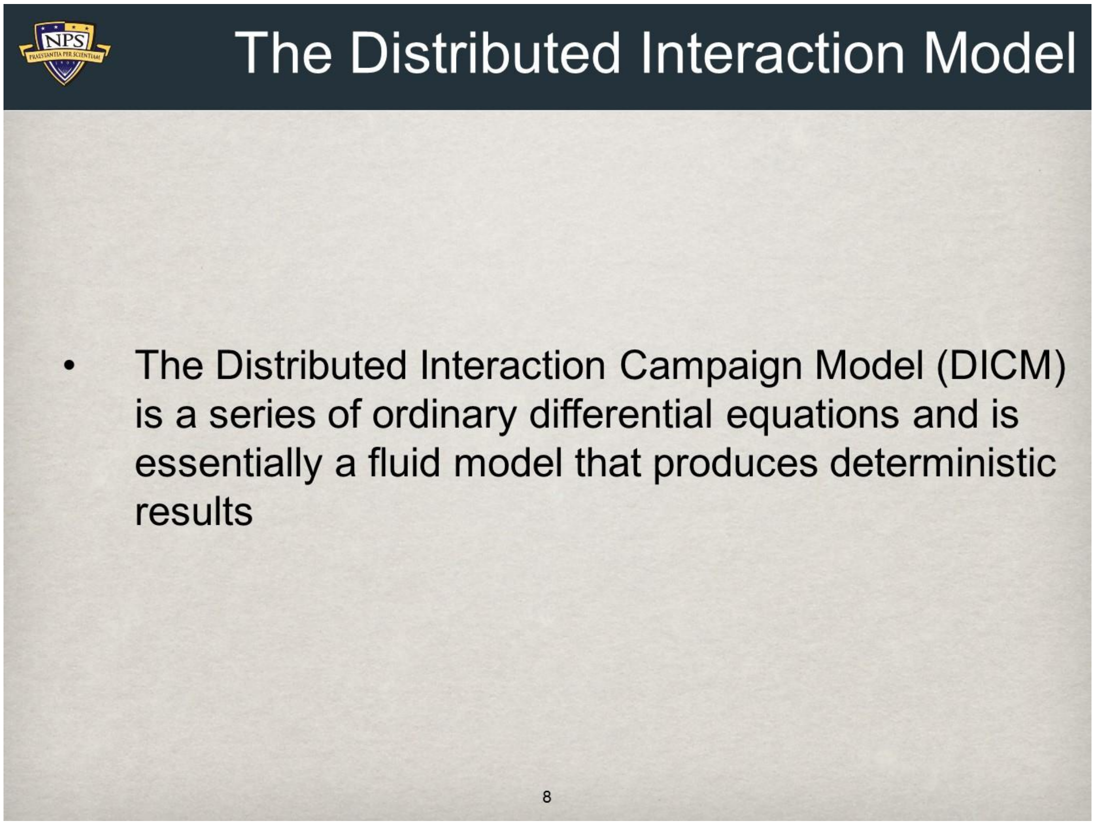
© PBS



Basic Research Questions

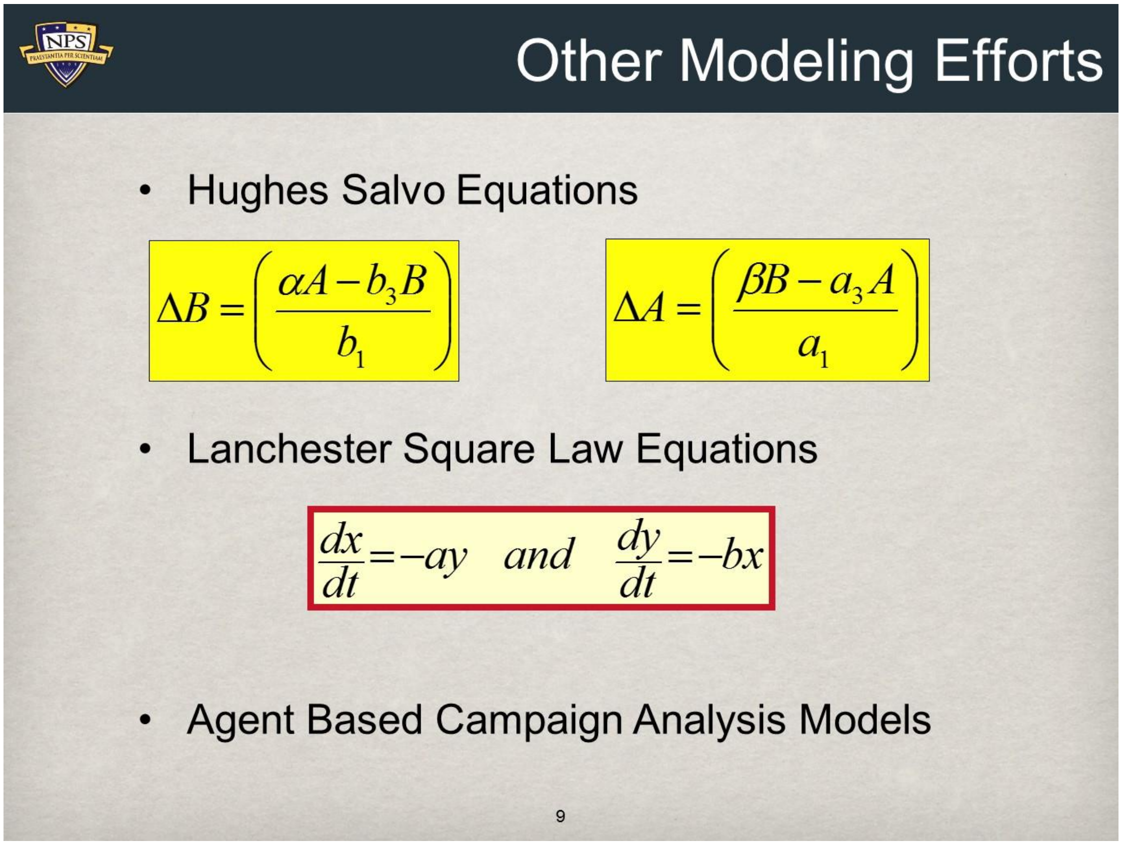
- What happens when distributed Reconnaissance Strike Complexes ("RUKs") engage each other?
- Are there changes to force structure that make a force more effective, and what impacts will disruptions in enemy command and control and wide-area surveillance have?
- Which insights are to be gained by fast exploratory mathematical campaign analysis to augment and replace expensive and time-consuming simulations?

Which Elements Make RUKs Better? Worse?



The Distributed Interaction Model

- The Distributed Interaction Campaign Model (DICM) is a series of ordinary differential equations and is essentially a fluid model that produces deterministic results



Other Modeling Efforts

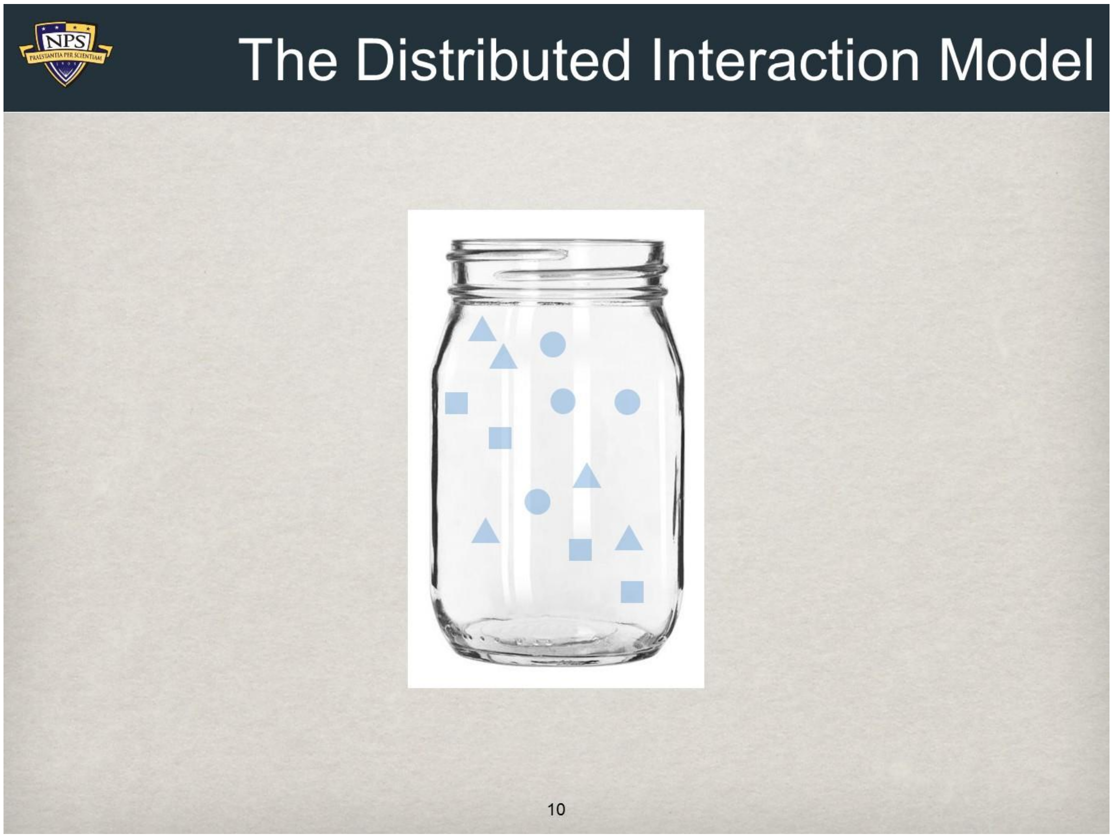
- Hughes Salvo Equations

$$\Delta B = \left(\frac{\alpha A - b_3 B}{b_1} \right) \qquad \Delta A = \left(\frac{\beta B - a_3 A}{a_1} \right)$$

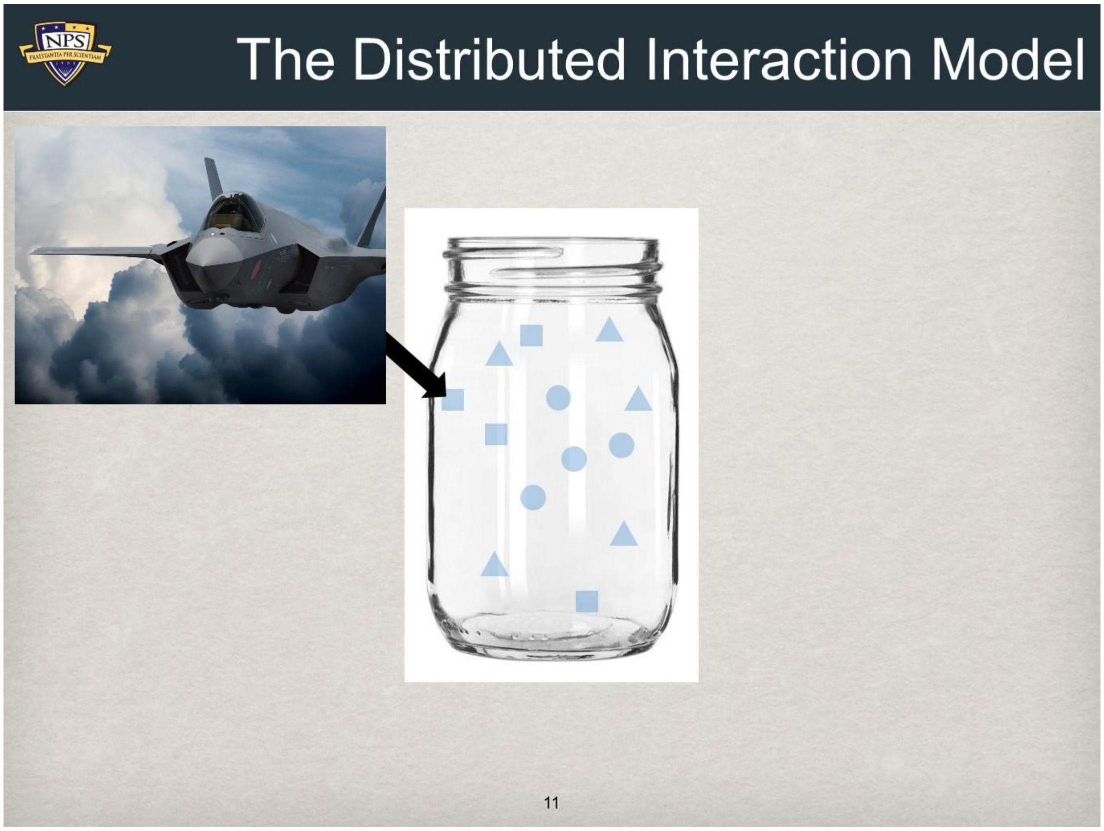
- Lanchester Square Law Equations

$$\frac{dx}{dt} = -ay \quad and \quad \frac{dy}{dt} = -bx$$

- Agent Based Campaign Analysis Models

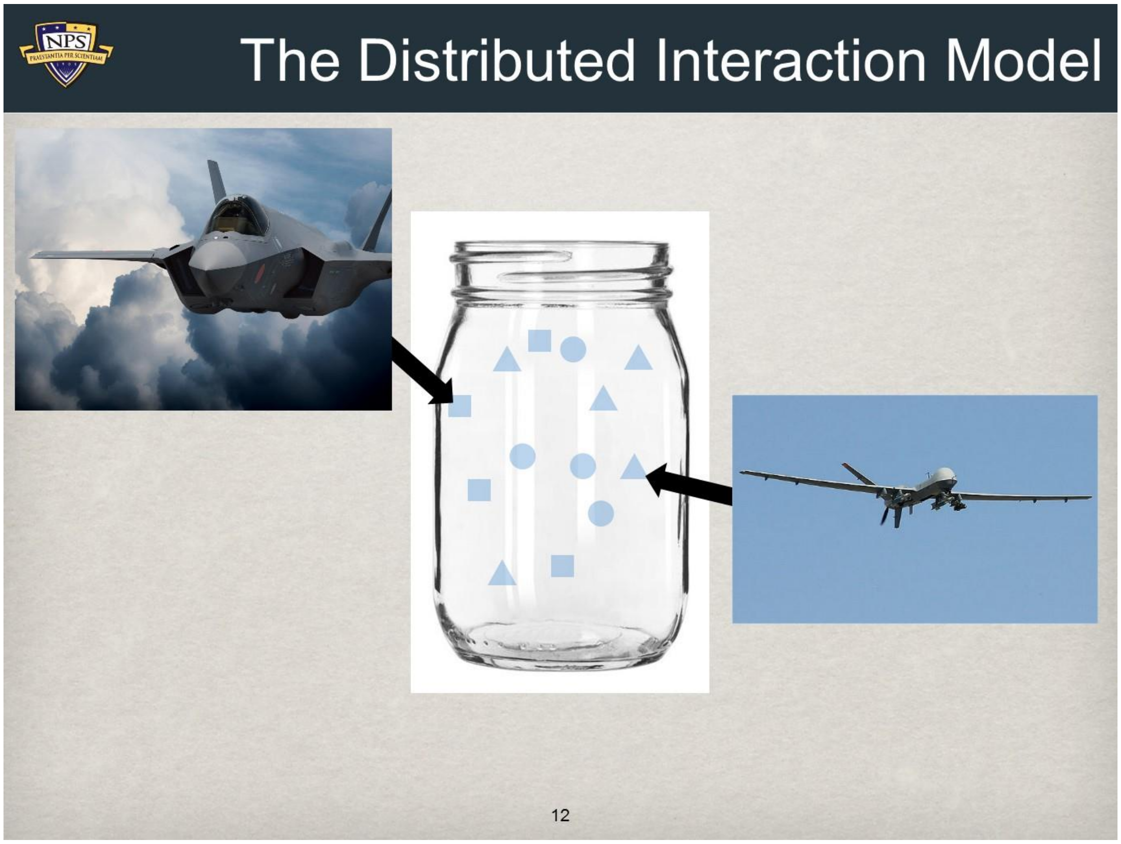


The Distributed Interaction Model



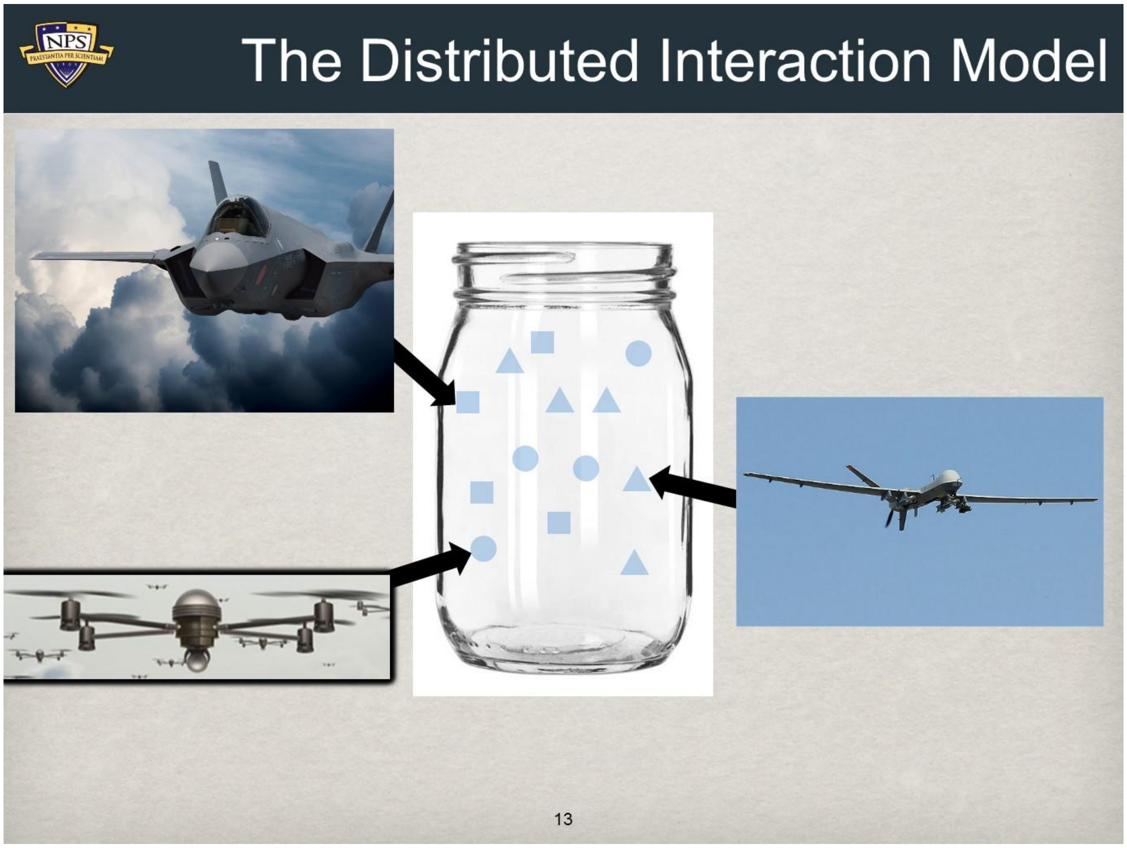
The Distributed Interaction Model

11



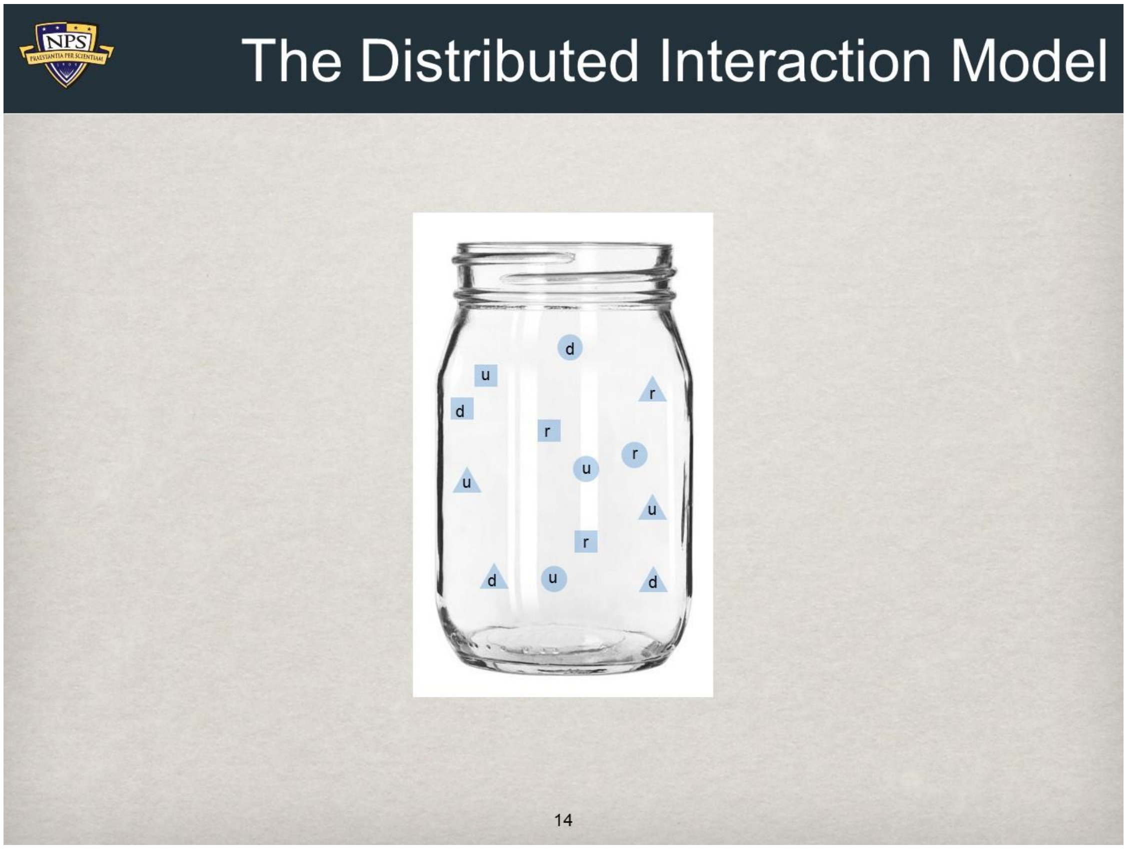
The Distributed Interaction Model

12



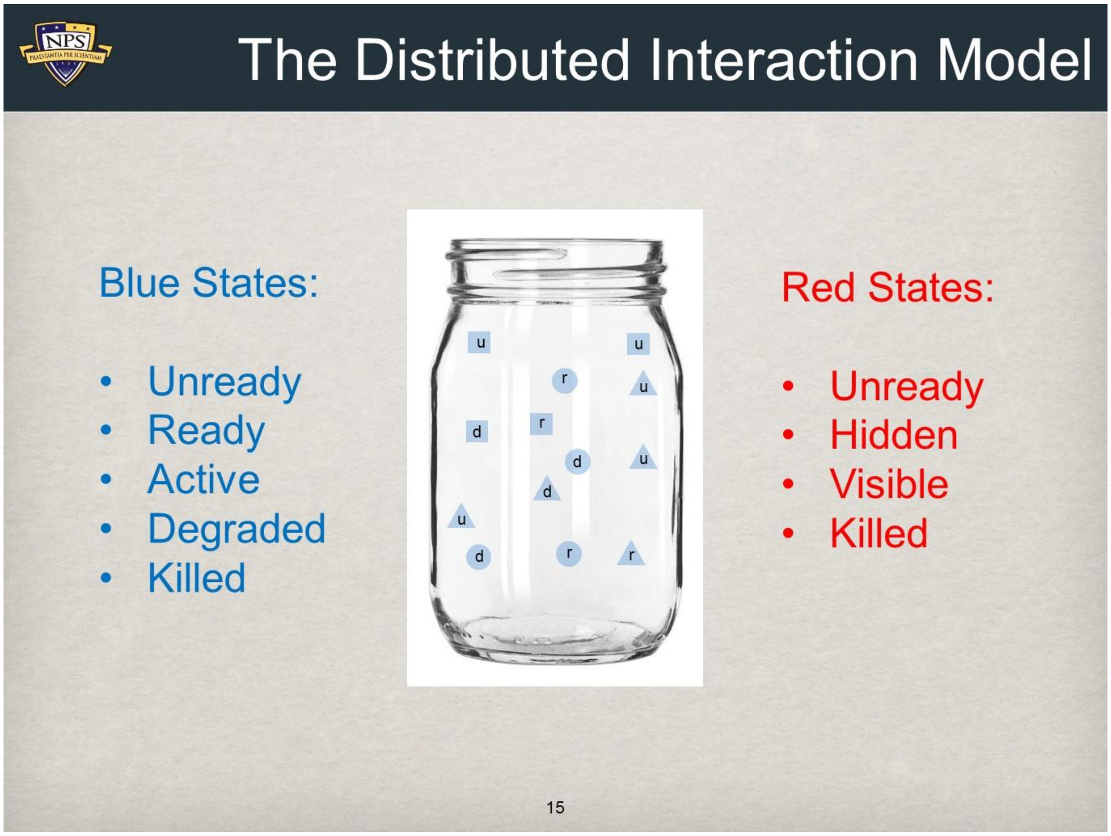
The Distributed Interaction Model

13



The Distributed Interaction Model

14



The Distributed Interaction Model

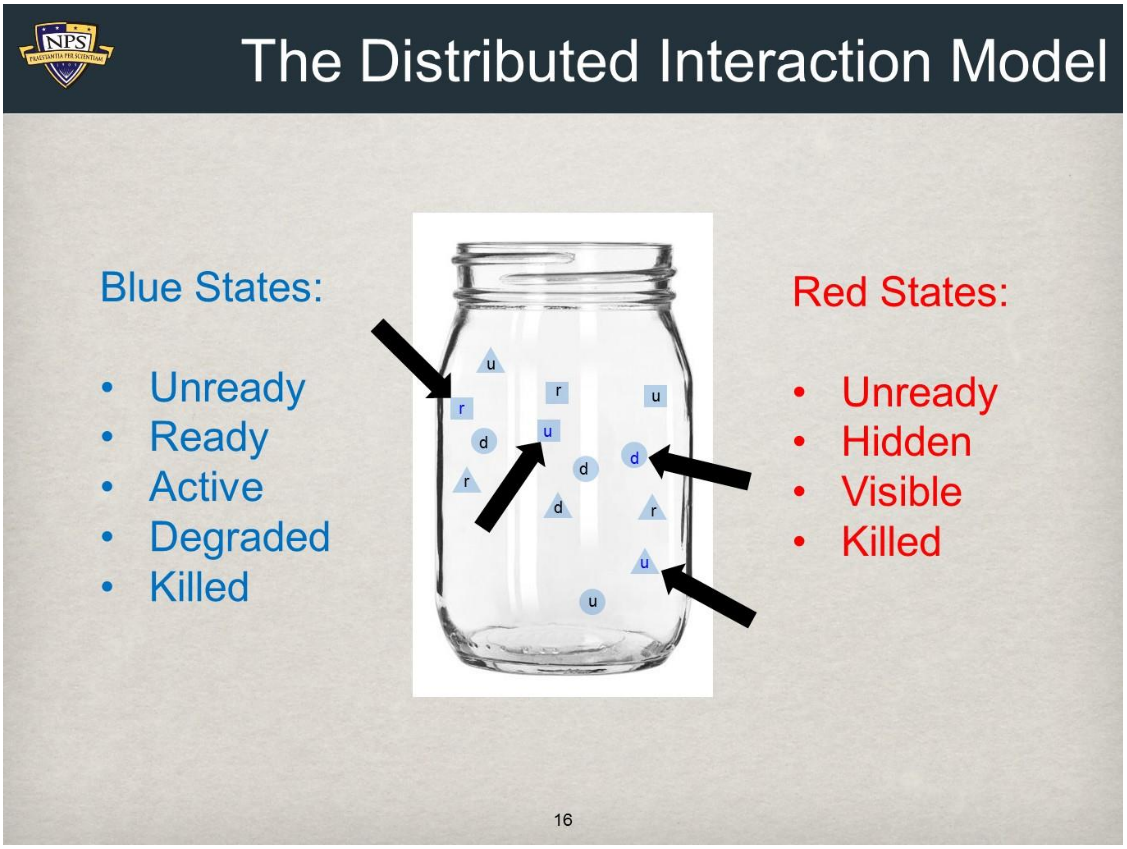
Blue States:

- Unready
- Ready
- Active
- Degraded
- Killed

Red States:

- Unready
- Hidden
- Visible
- Killed

15



The Distributed Interaction Model

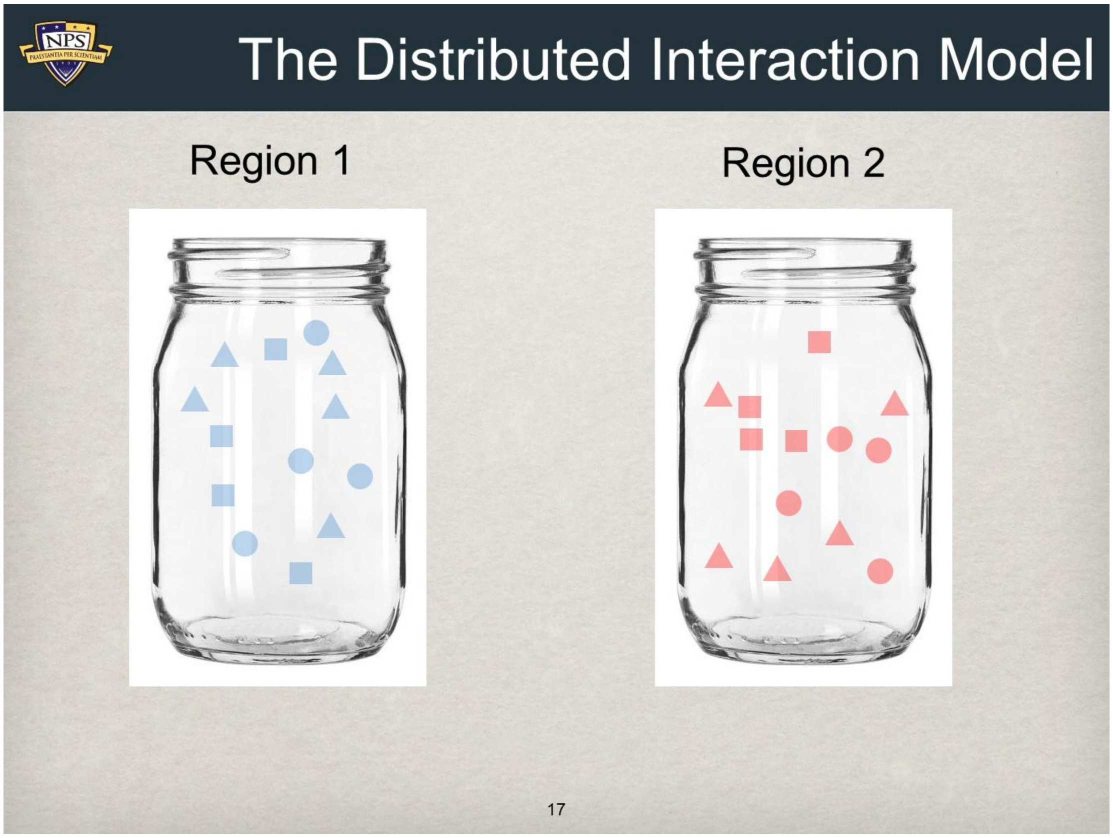
Blue States:

- Unready
- Ready
- Active
- Degraded
- Killed

Red States:

- Unready
- Hidden
- Visible
- Killed

16

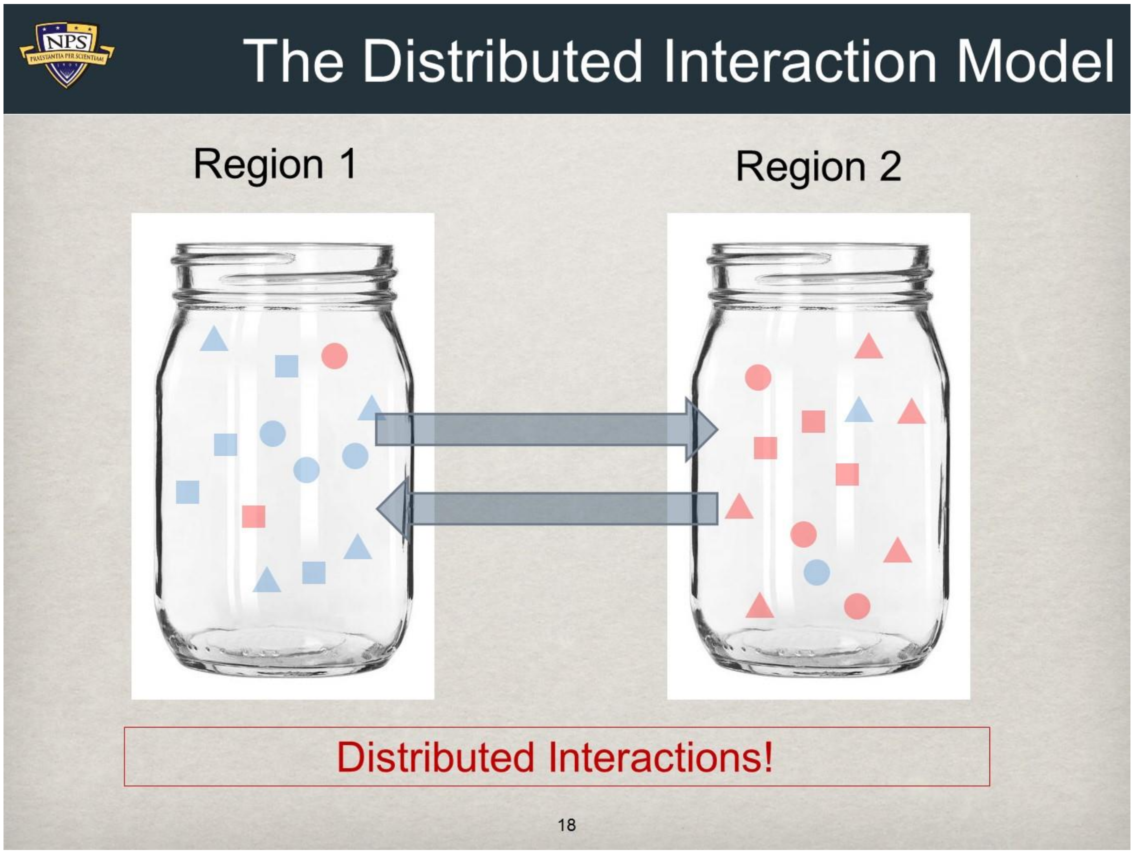


The Distributed Interaction Model

Region 1

Region 2

17



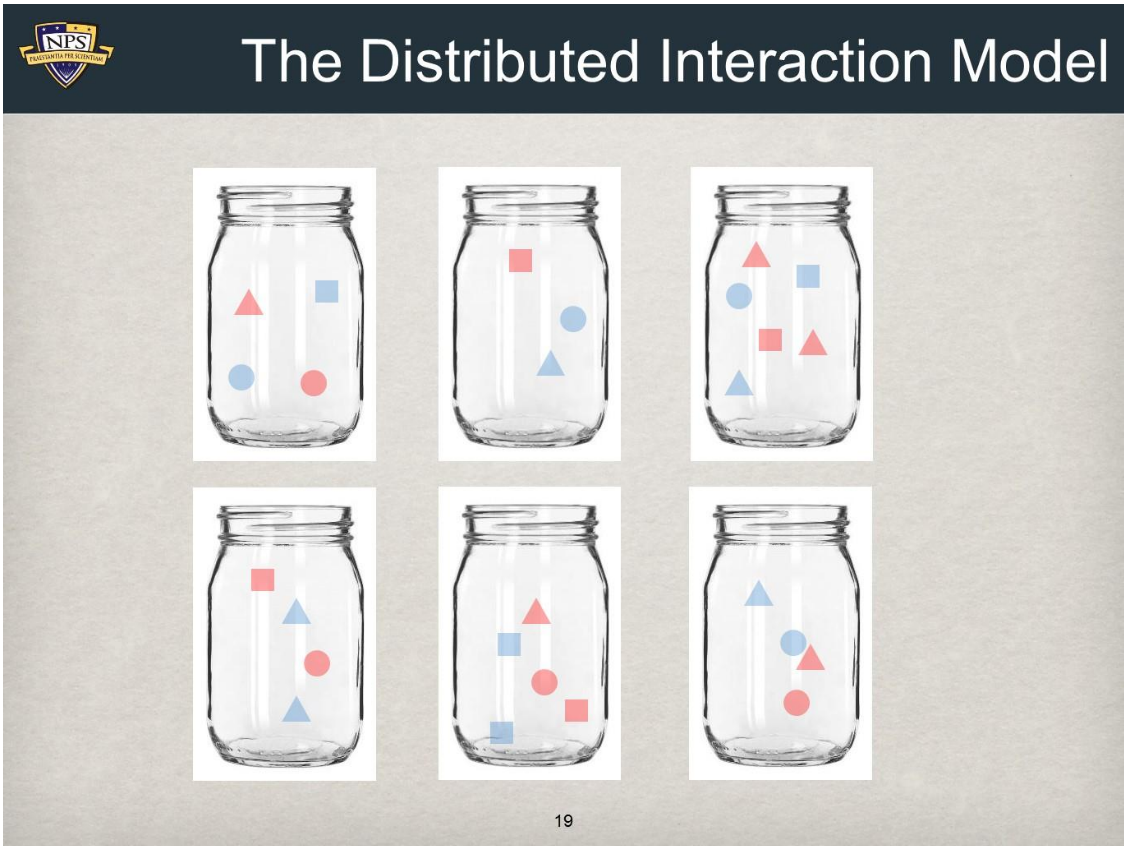
The Distributed Interaction Model

Region 1

Region 2

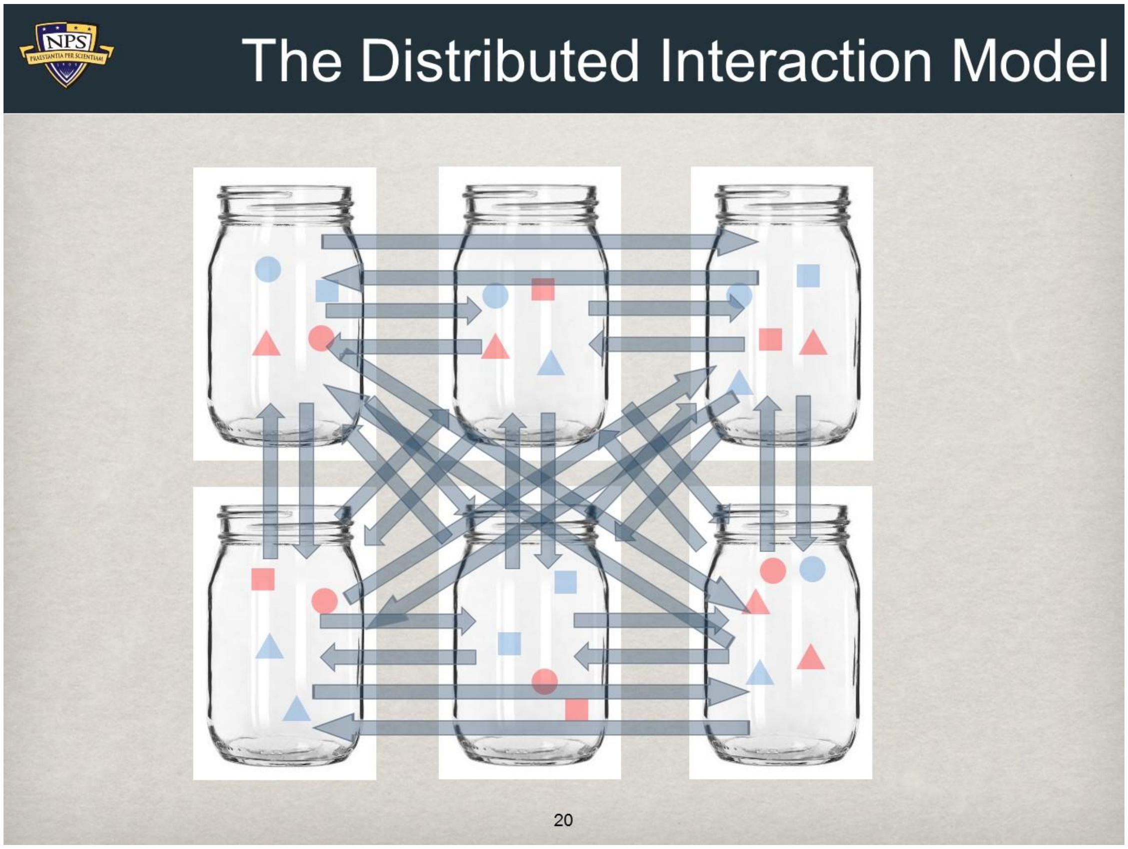
Distributed Interactions!

18



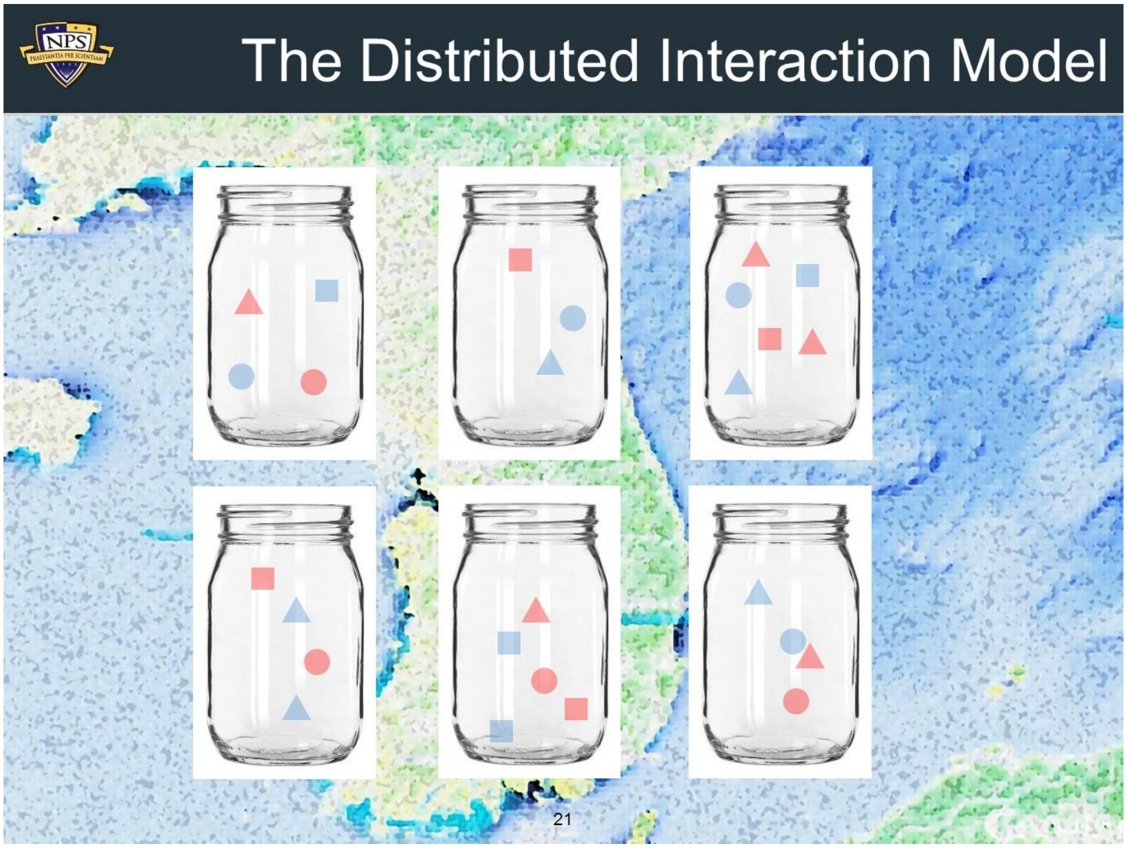
The Distributed Interaction Model

19



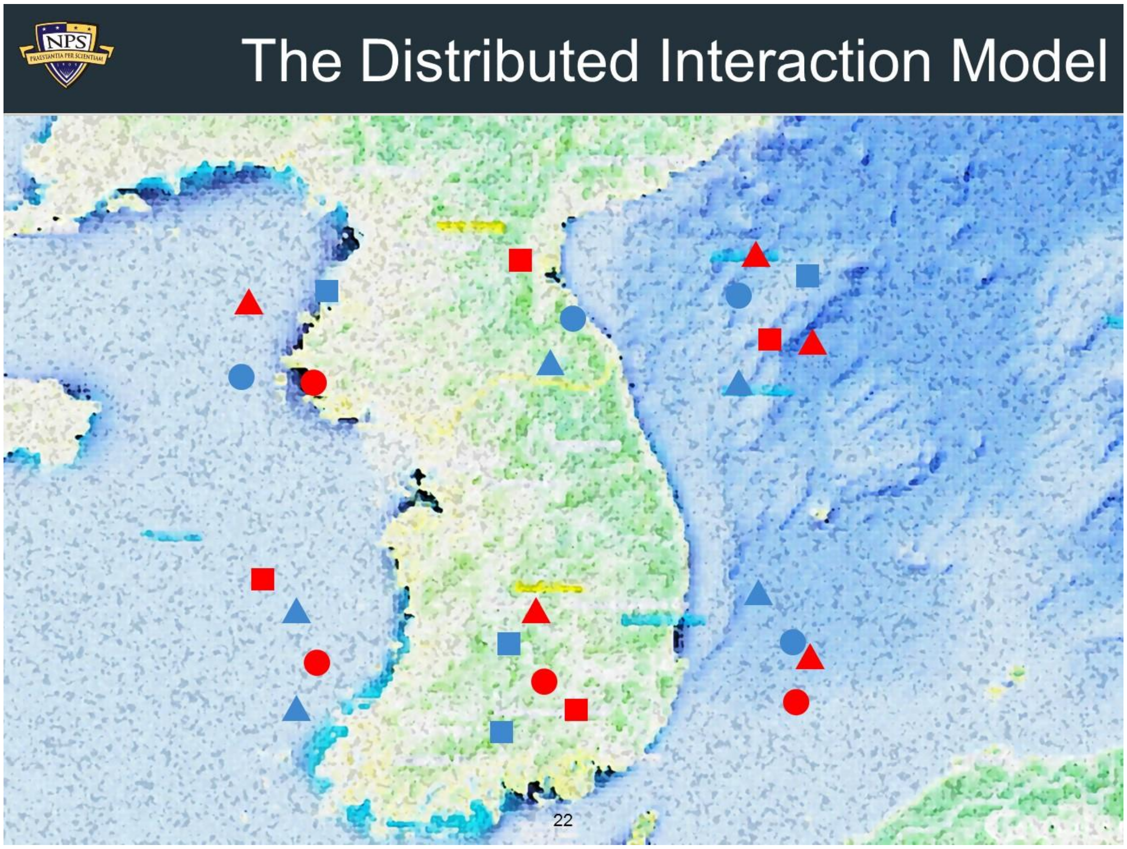
The Distributed Interaction Model

20



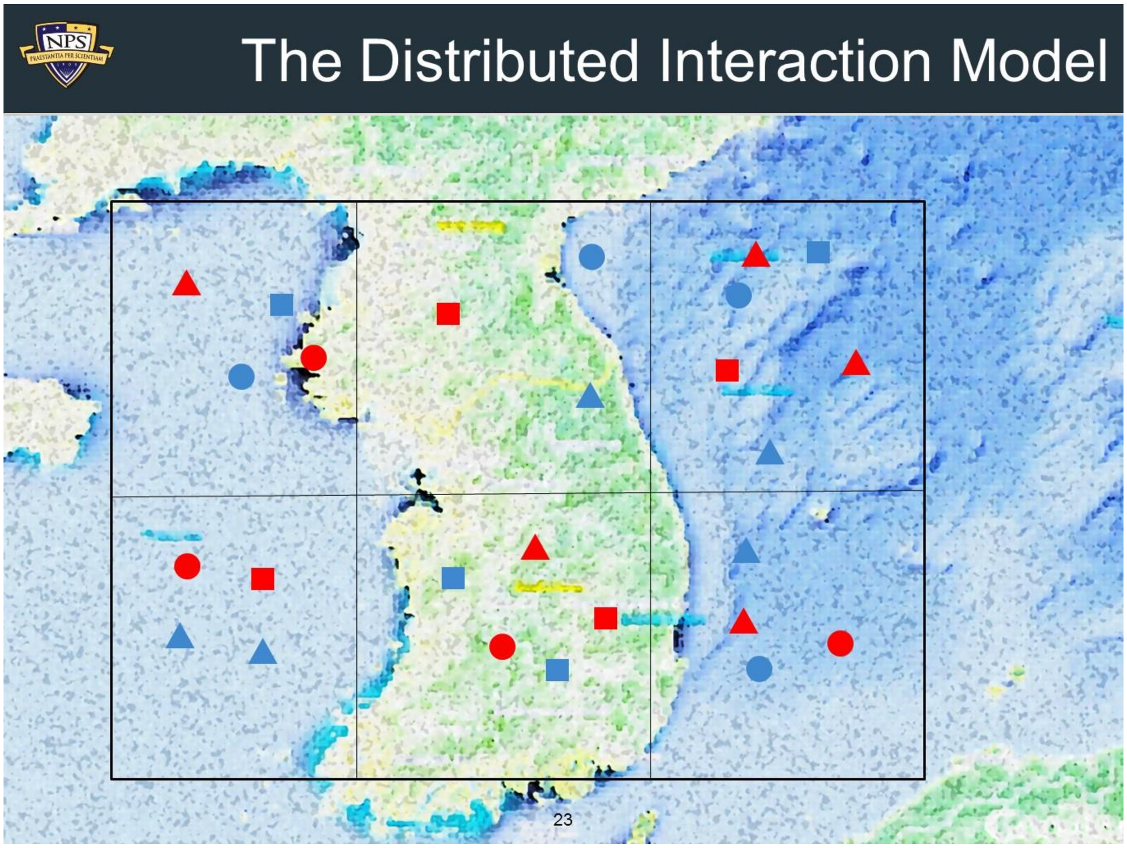
The Distributed Interaction Model

21



The Distributed Interaction Model

22



The Distributed Interaction Model

Some Rate Parameters

- Rate degraded Bs travel between regions
- Rate unready Bs transition to the ready state
- Rate ready Bs transition to the active state
- Rate ready Bs reinforce other regions
- Rate active Bs killed by R aimed fire
- Rate degraded Bs killed by R aimed fire
- Rate B broad area surveillance detects hidden Rs
- Rate unready Rs becomes ready
- Rate hidden Rs become visible
- Rate visible Rs become killed by B aimed fire

… the Model Uses Several Additional Rate Parameters Not Listed!

Other Considerations

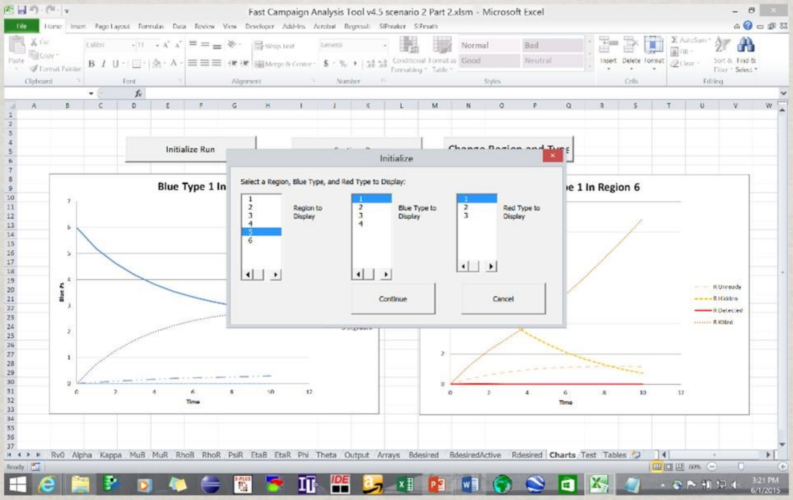
- Commander can set asset demand by region
- Broad area surveillance availability is binary by region
- C2 availability is binary by region
- User selects asset refuel/refit/rearm regions

25

Customized Decision Support Tool

VBA-based tool

- No commercial software = Zero cost per seat



Fast Campaign Analysis Tool v4.5 scenario 2 Part 2.xlsm - Microsoft Excel

Initialize

Select a Region, Blue Type, and Red Type to Display:

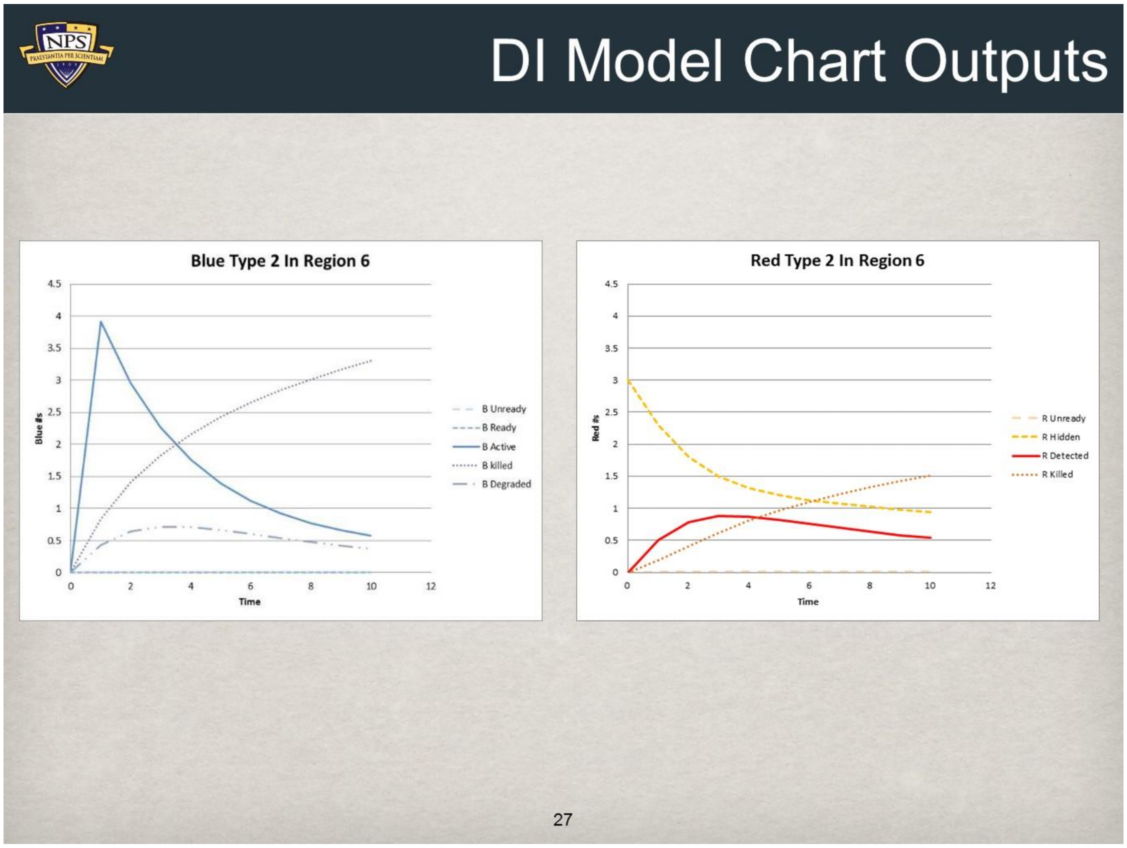
Region to Display: 1, 2, 3, 4, 5, 6

Blue Type to Display: 1, 2, 3, 4

Red Type to Display: 1, 2, 3

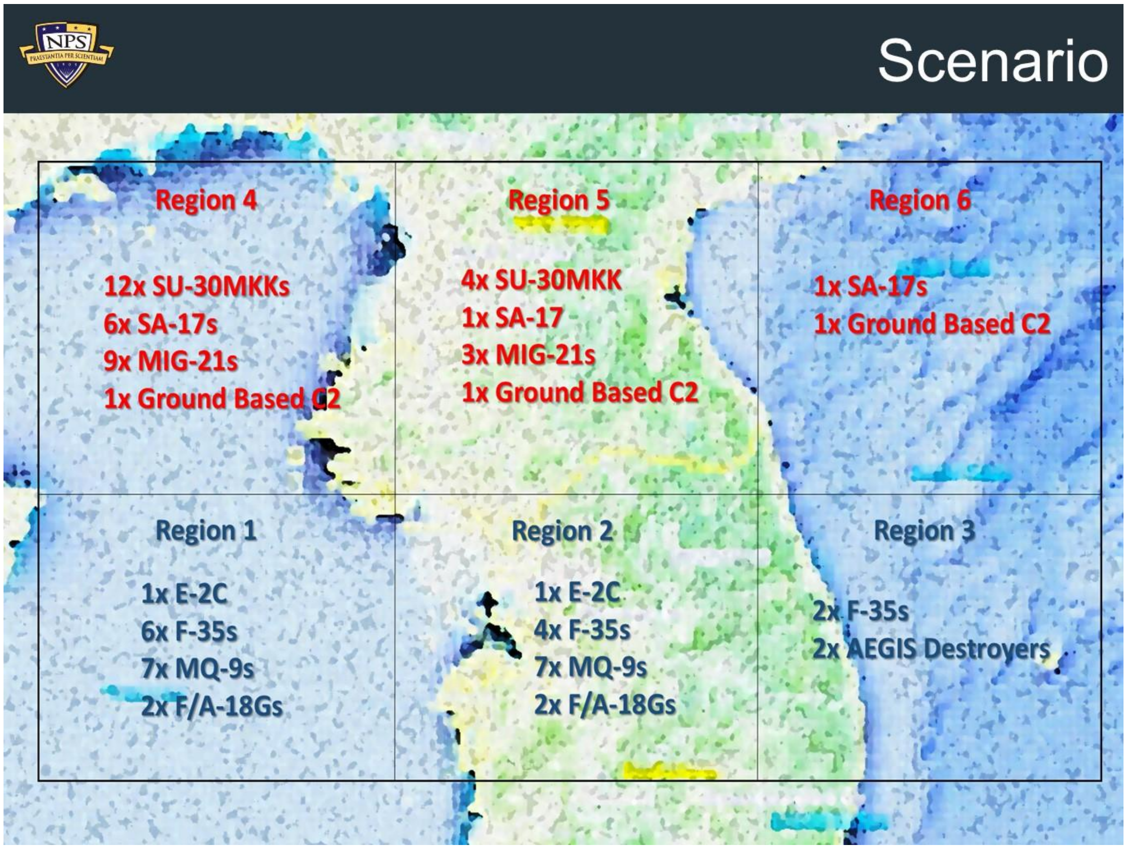
(Carlyle, 2011)

26



DI Model Chart Outputs

27



Scenario

Region 4

12x SU-30MKKs
6x SA-17s
9x MIG-21s
1x Ground Based C2

Region 5

4x SU-30MKK
1x SA-17
3x MIG-21s
1x Ground Based C2

Region 6

1x SA-17s
1x Ground Based C2

Region 1

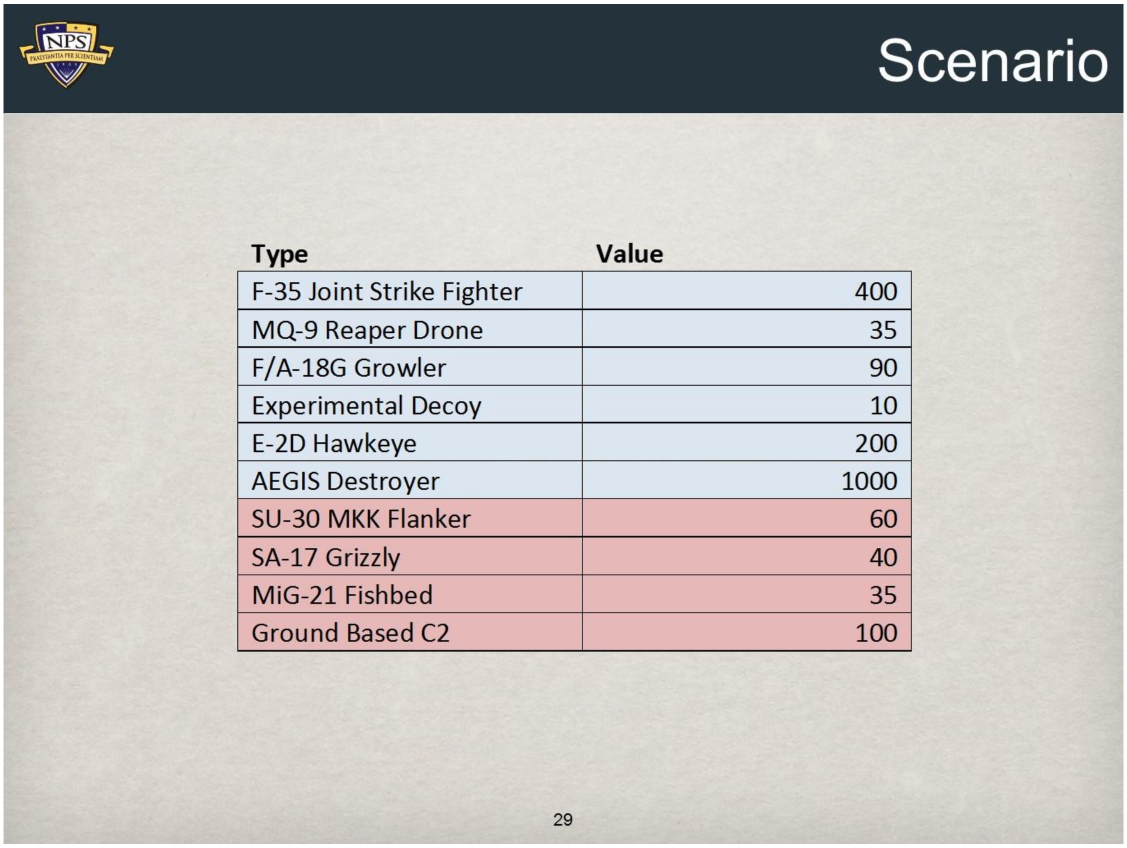
1x E-2C
6x F-35s
7x MQ-9s
2x F/A-18Gs

Region 2

1x E-2C
4x F-35s
7x MQ-9s
2x F/A-18Gs

Region 3

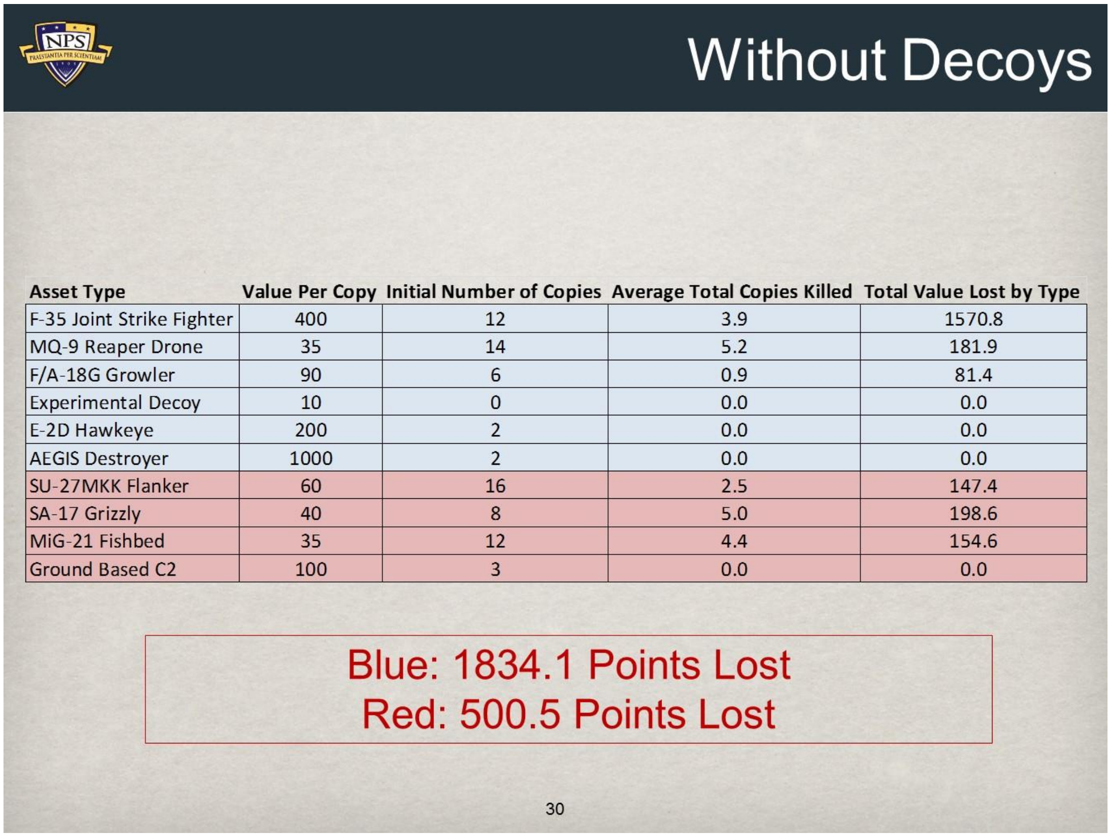
2x F-35s
2x AEGIS Destroyers



Scenario

Type	Value
F-35 Joint Strike Fighter	400
MQ-9 Reaper Drone	35
F/A-18G Growler	90
Experimental Decoy	10
E-2D Hawkeye	200
AEGIS Destroyer	1000
SU-30 MKK Flanker	60
SA-17 Grizzly	40
MiG-21 Fishbed	35
Ground Based C2	100

29

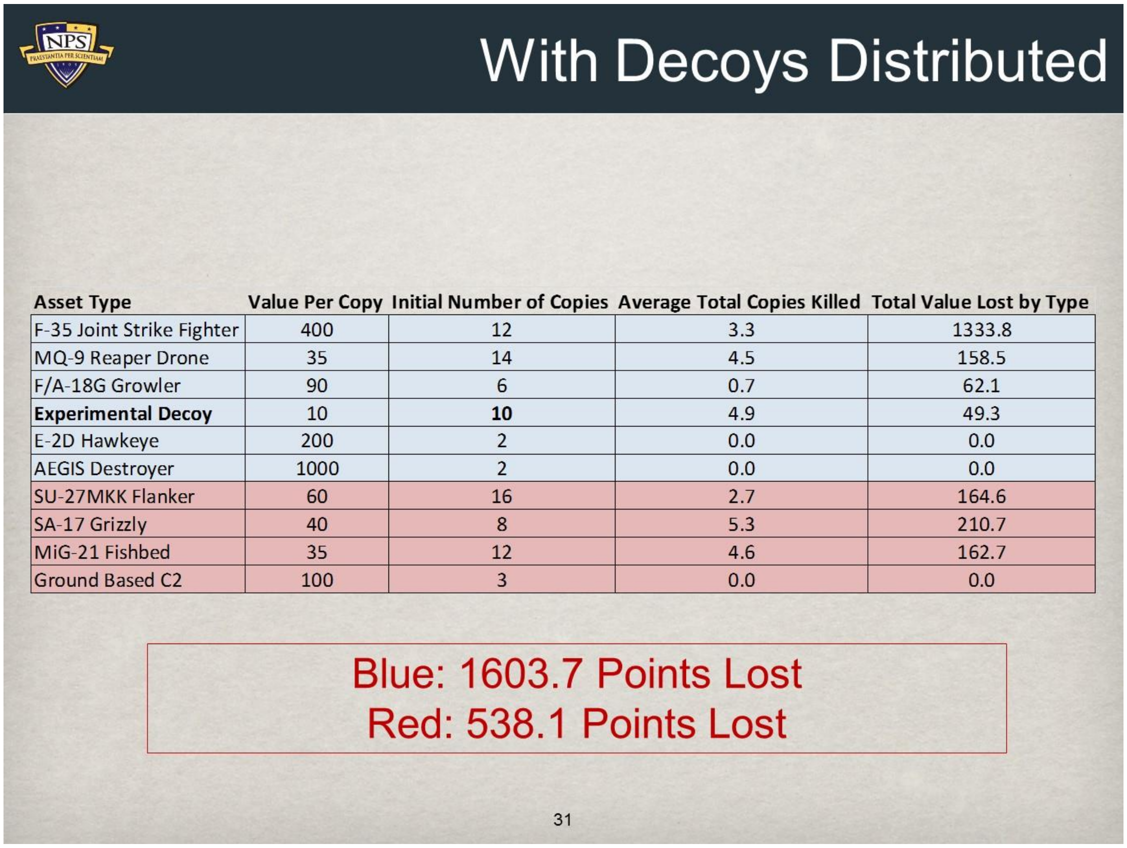


Without Decoys

Asset Type	Value Per Copy	Initial Number of Copies	Average Total Copies Killed	Total Value Lost by Type
F-35 Joint Strike Fighter	400	12	3.9	1570.8
MQ-9 Reaper Drone	35	14	5.2	181.9
F/A-18G Growler	90	6	0.9	81.4
Experimental Decoy	10	0	0.0	0.0
E-2D Hawkeye	200	2	0.0	0.0
AEGIS Destroyer	1000	2	0.0	0.0
SU-27MKK Flanker	60	16	2.5	147.4
SA-17 Grizzly	40	8	5.0	198.6
MiG-21 Fishbed	35	12	4.4	154.6
Ground Based C2	100	3	0.0	0.0

Blue: 1834.1 Points Lost
Red: 500.5 Points Lost

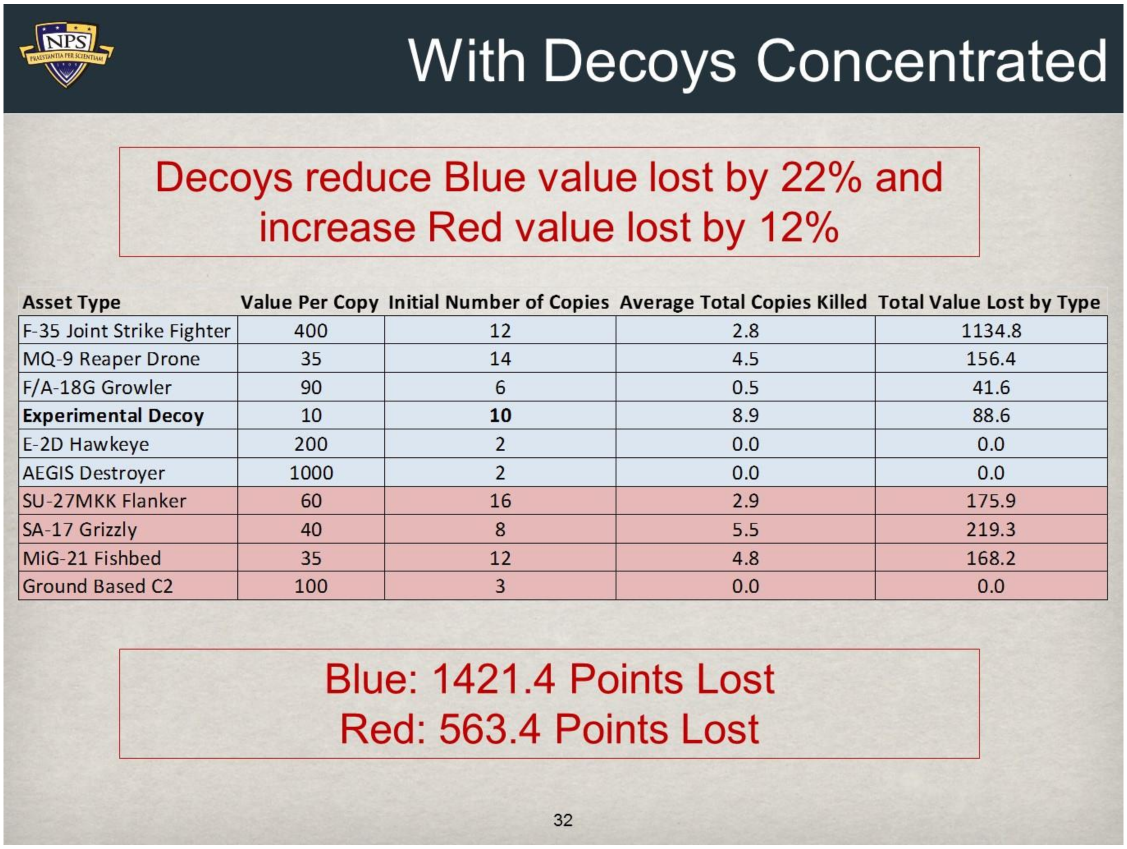
30



With Decoys Distributed

Asset Type	Value Per Copy	Initial Number of Copies	Average Total Copies Killed	Total Value Lost by Type
F-35 Joint Strike Fighter	400	12	3.3	1333.8
MQ-9 Reaper Drone	35	14	4.5	158.5
F/A-18G Growler	90	6	0.7	62.1
Experimental Decoy	10	**10**	4.9	49.3
E-2D Hawkeye	200	2	0.0	0.0
AEGIS Destroyer	1000	2	0.0	0.0
SU-27MKK Flanker	60	16	2.7	164.6
SA-17 Grizzly	40	8	5.3	210.7
MiG-21 Fishbed	35	12	4.6	162.7
Ground Based C2	100	3	0.0	0.0

Blue: 1603.7 Points Lost
Red: 538.1 Points Lost



With Decoys Concentrated

Decoys reduce Blue value lost by 22% and increase Red value lost by 12%

Asset Type	Value Per Copy	Initial Number of Copies	Average Total Copies Killed	Total Value Lost by Type
F-35 Joint Strike Fighter	400	12	2.8	1134.8
MQ-9 Reaper Drone	35	14	4.5	156.4
F/A-18G Growler	90	6	0.5	41.6
Experimental Decoy	10	**10**	8.9	88.6
E-2D Hawkeye	200	2	0.0	0.0
AEGIS Destroyer	1000	2	0.0	0.0
SU-27MKK Flanker	60	16	2.9	175.9
SA-17 Grizzly	40	8	5.5	219.3
MiG-21 Fishbed	35	12	4.8	168.2
Ground Based C2	100	3	0.0	0.0

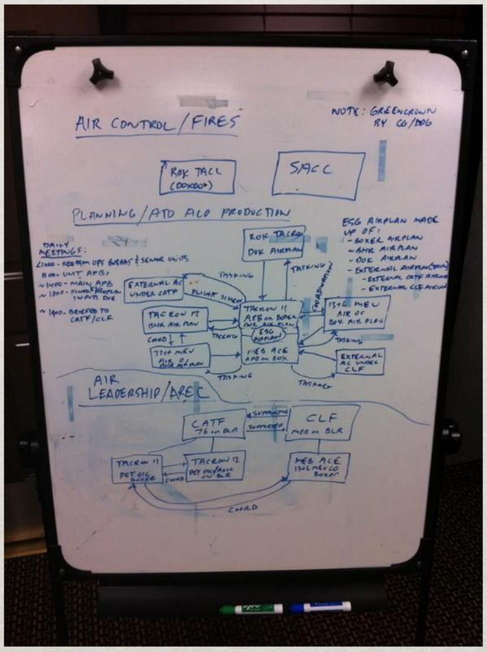
Blue: 1421.4 Points Lost
Red: 563.4 Points Lost

Insights From Other Scenarios

- It is essential to defend friendly C2 nodes
- Stealth platforms appear to be of little value
- Decoys appear to be consistently useful.
- Assets able to operate in “a seam” are valuable.
- Wide area surveillance assets are very valuable, especially in high clutter environments.
- Passive sensors and communications increase system survivability
- Fixed weapon systems are vulnerable
- Unexceptional platforms employing exceptional long range weapons are effective

33

Questions?



34

4. Panel 2: Information in Gaming

Discussion Summary

Stephanie Helm described approaches used in Naval War College gaming to address cyber operations. She addressed the value of gaming in understanding organizations and organizational relationships. The games also exposed how commanders approach and appreciate cyber threats, and demonstrated the challenges and the dimensions of what must be considered in dealing with cyber threats at the operational level.

Phil Pournelle briefed a game used for emulating Red, Green, and Blue perspectives and interests by capturing the communications and information transfer between teams. He demonstrated how Green (Blue's ally) perceptions and interests can affect a campaign in ways that Blue did not anticipate or desire. The design of the game captures each move in ways that admit detailed analyses.

Elizabeth Bartels discussed the challenges of exploiting player knowledge and expertise while hiding information that various players would not know in making their decisions. She provided approaches for addressing these challenges. She emphasized research showing that players do not know why they make the decisions that they do. Instead, they reconstruct plausible reasons.

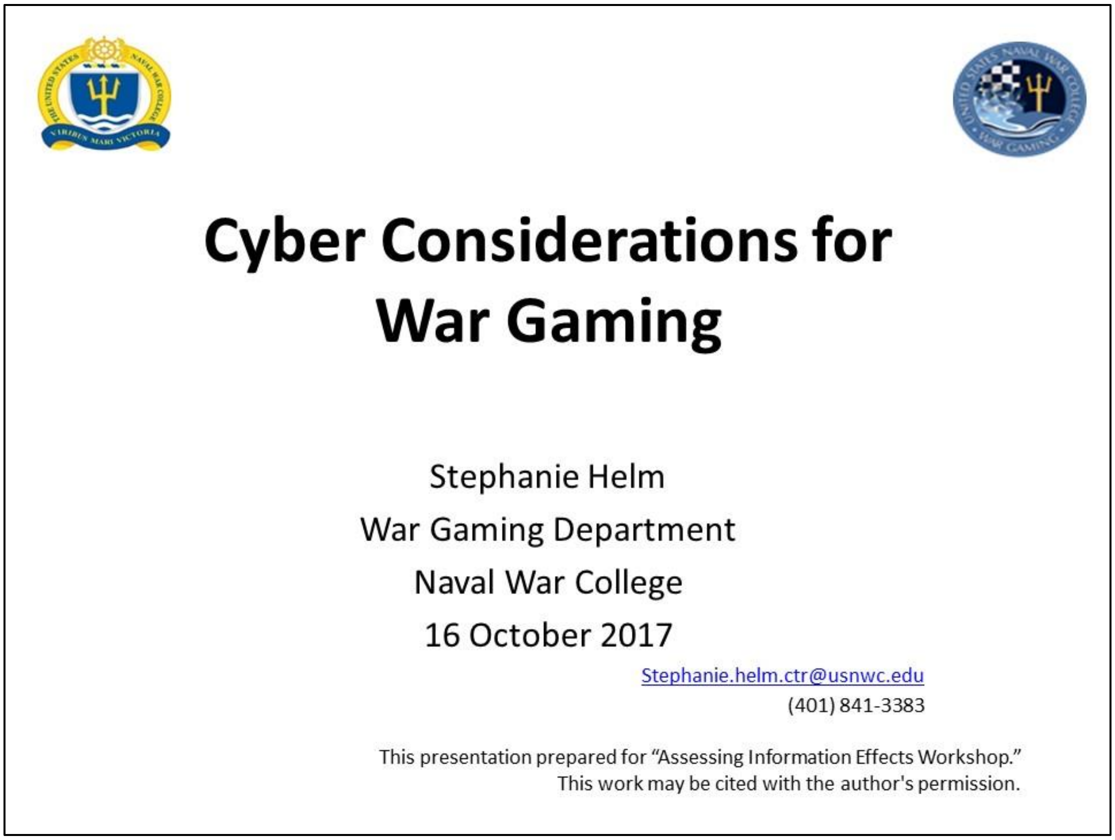
A. Stephanie Helm: Cyber Considerations for War Gaming

Presentation Summary

This presentation spotlighted a widespread limitation in readiness and response exercises. Cyber has consistently been used as an insert rather than an actual domain of play, because the leaders of the exercise didn't really understand the bounds of cyber and how to realistically bring it into exercise play. Because the cyber domain is logical as opposed to physical in terms of effects, visualization and definition of readiness and capabilities are difficult. Defining Cyber Key Terrain is a problematic concept for strategists who approach the problem with a physical world mindset. Conversely, cyber professionals sometimes overlook the physical infrastructure that bounds the domain.

This inability to address cyber as part of a unified C2 exercise is unrealistic and leaves participants totally unprepared for countering real-world effects. These problems were echoed in the adjudication issues discussed in the next presentation by Ms. Bartels. If only a single cyber subject matter expert (SME) contributes to game design and adjudication, this limits the ability to integrate cyber into play, and even the potential awareness of what is being excluded.

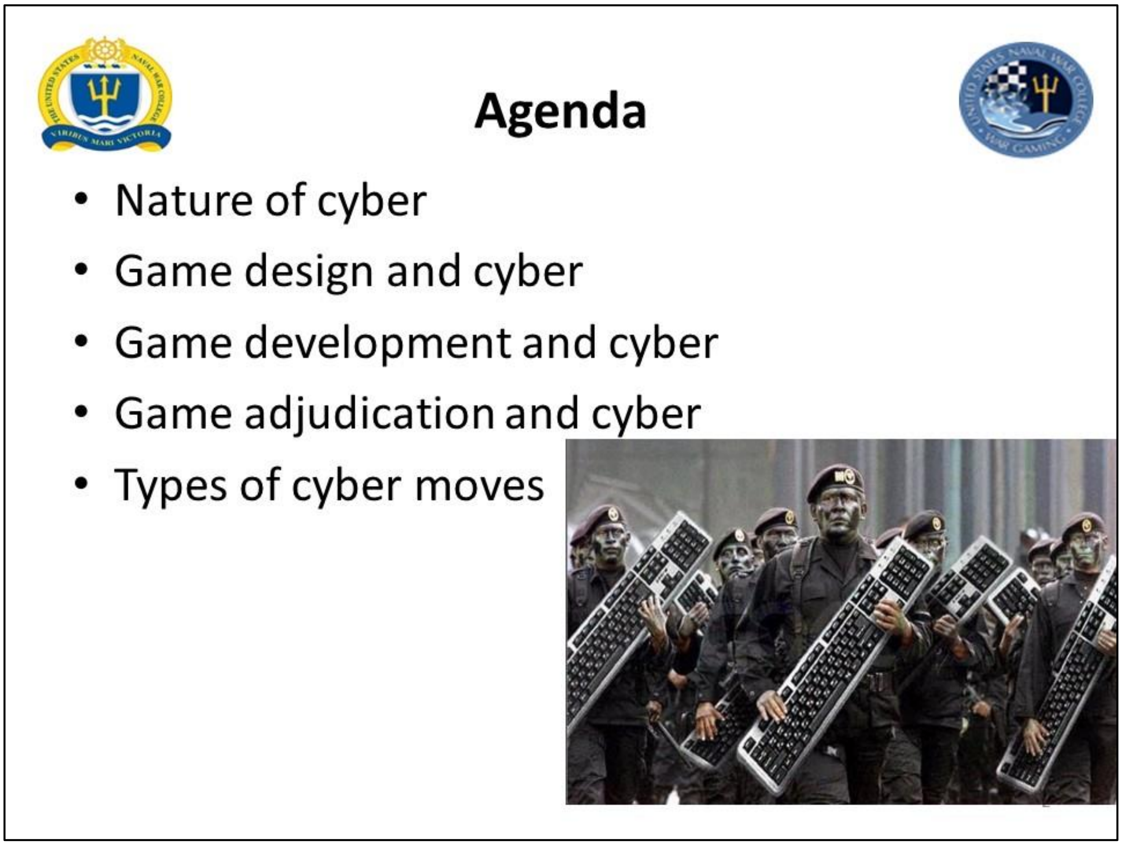
The quote "cyber is put into another room" summed up her argument. Until there is a paradigm shift, cyber will continue to be difficult to effectively integrate into game play other than as an afterthought. Despite the growing emphasis on the cyber domain and its importance, the reality is that it seems to be too abstract for commanders. The presentation also underlined the need for cyber SMEs to participate in game development and adjudication. These SMEs need to have a solid technical background, avoid mirror imaging and assumptions about adversaries, and elicit support from their command structure.



Cyber Considerations for War Gaming

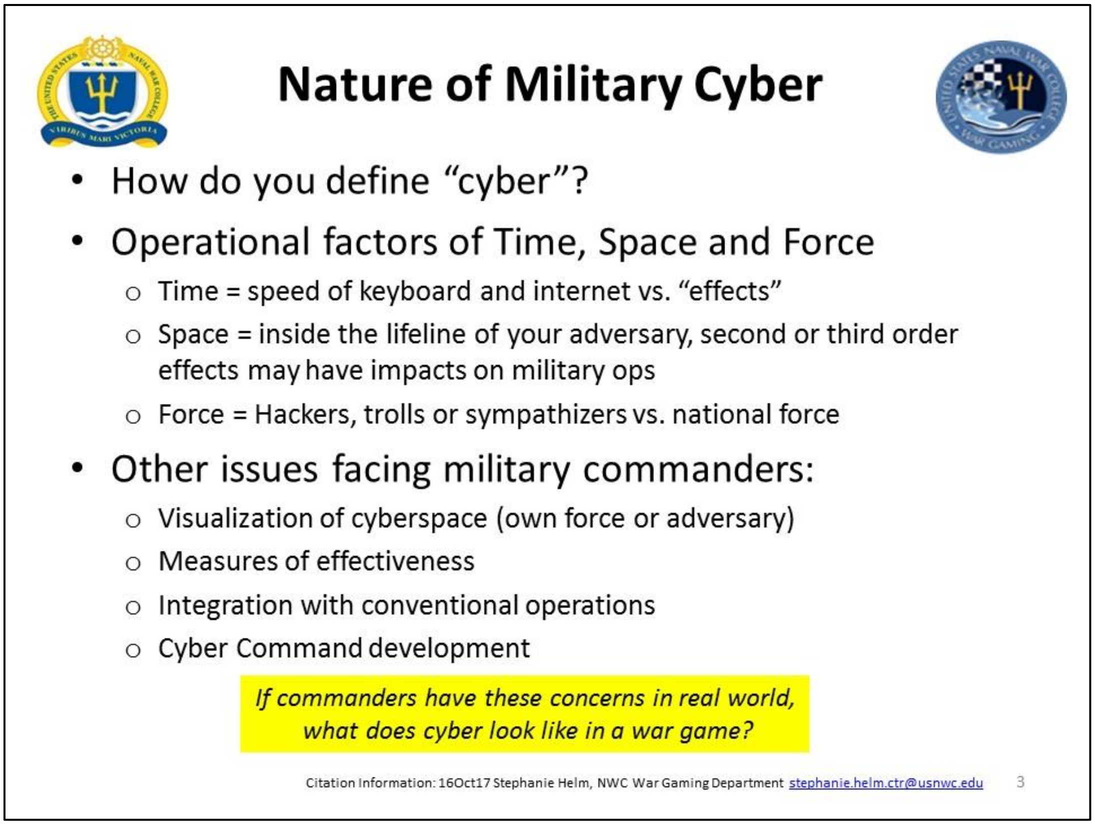
Stephanie Helm
War Gaming Department
Naval War College
16 October 2017
Stephanie.helm.ctr@usnwc.edu
(401) 841-3383

This presentation prepared for "Assessing Information Effects Workshop."
This work may be cited with the author's permission.



Agenda

- Nature of cyber
- Game design and cyber
- Game development and cyber
- Game adjudication and cyber
- Types of cyber moves

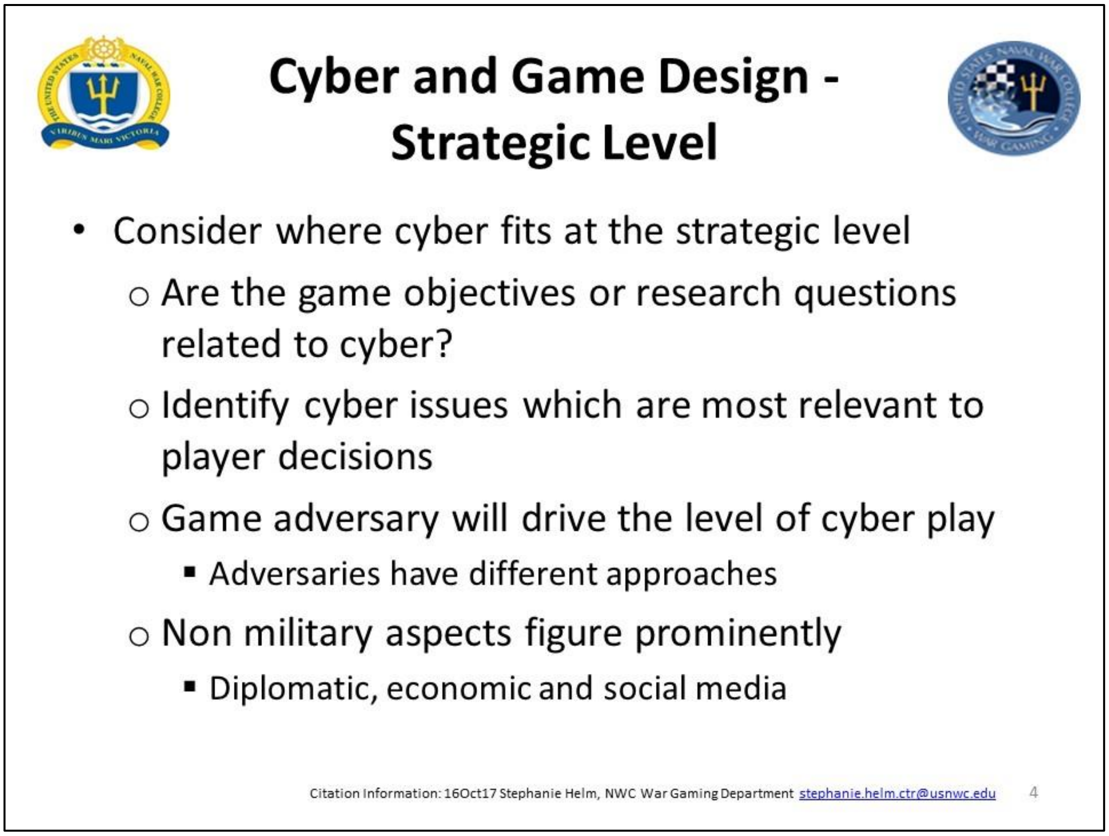


Nature of Military Cyber

- How do you define “cyber”?
- Operational factors of Time, Space and Force
  - Time = speed of keyboard and internet vs. “effects”
  - Space = inside the lifeline of your adversary, second or third order effects may have impacts on military ops
  - Force = Hackers, trolls or sympathizers vs. national force
- Other issues facing military commanders:
  - Visualization of cyberspace (own force or adversary)
  - Measures of effectiveness
  - Integration with conventional operations
  - Cyber Command development

If commanders have these concerns in real world, what does cyber look like in a war game?

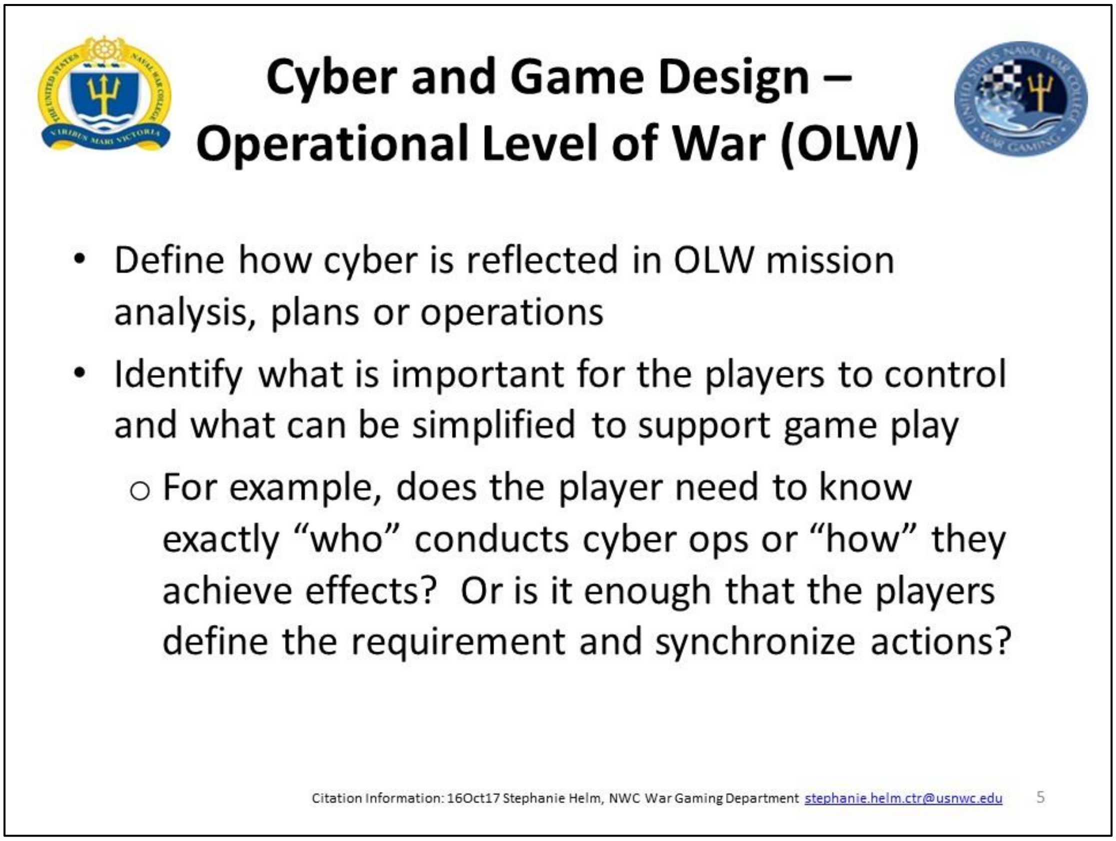
Citation Information: 16Oct17 Stephanie Helm, NWC War Gaming Department stephanie.helm.ctr@usnwc.edu



Cyber and Game Design - Strategic Level

- Consider where cyber fits at the strategic level
  - Are the game objectives or research questions related to cyber?
  - Identify cyber issues which are most relevant to player decisions
  - Game adversary will drive the level of cyber play
    - Adversaries have different approaches
  - Non military aspects figure prominently
    - Diplomatic, economic and social media

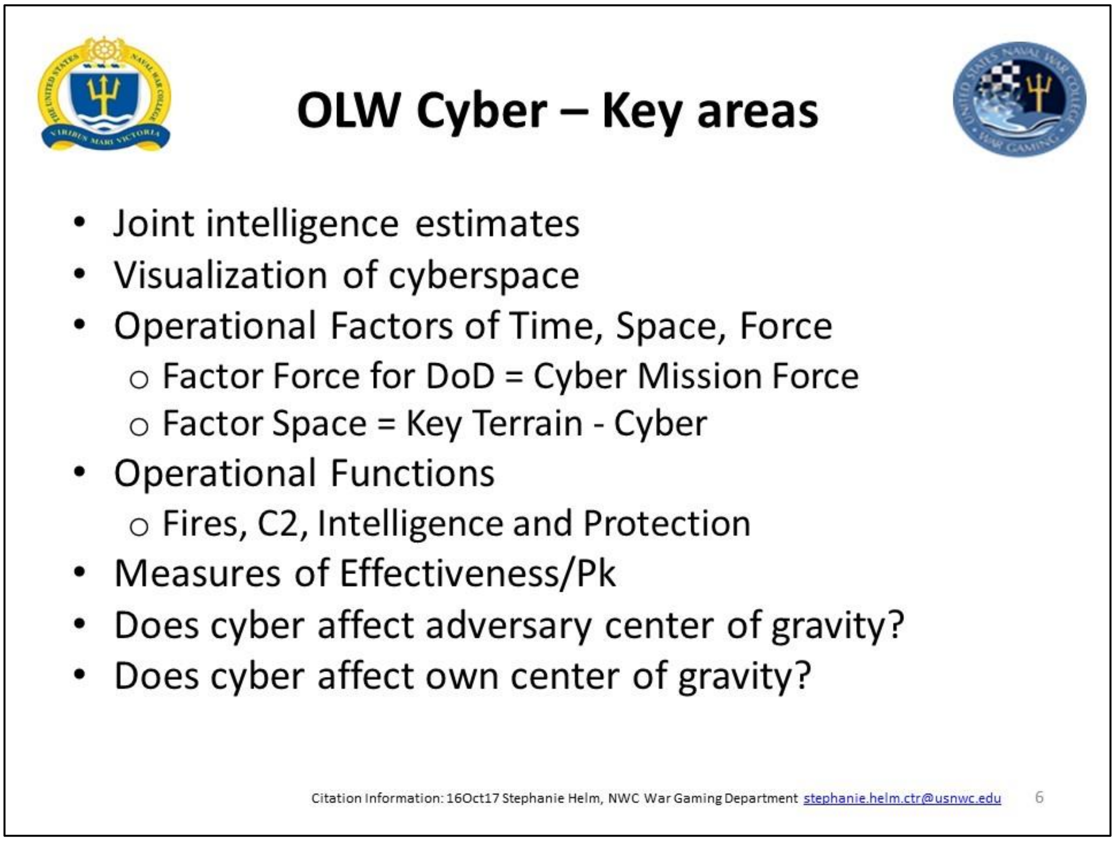
Citation Information: 16Oct17 Stephanie Helm, NWC War Gaming Department stephanie.helm.ctr@usnwc.edu



Cyber and Game Design – Operational Level of War (OLW)

- Define how cyber is reflected in OLW mission analysis, plans or operations
- Identify what is important for the players to control and what can be simplified to support game play
  - For example, does the player need to know exactly "who" conducts cyber ops or "how" they achieve effects? Or is it enough that the players define the requirement and synchronize actions?

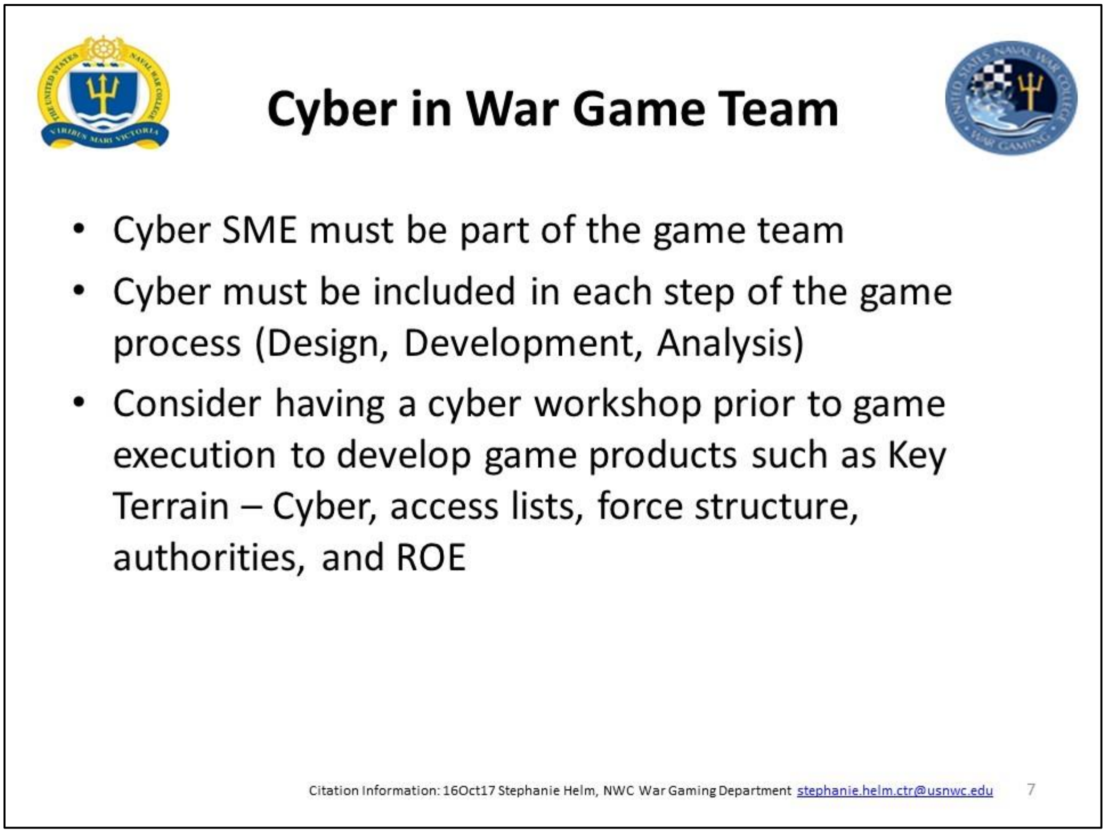
Citation Information: 16Oct17 Stephanie Helm, NWC War Gaming Department stephanie.helm.ctr@usnwc.edu 5



OLW Cyber – Key areas

- Joint intelligence estimates
- Visualization of cyberspace
- Operational Factors of Time, Space, Force
  - Factor Force for DoD = Cyber Mission Force
  - Factor Space = Key Terrain - Cyber
- Operational Functions
  - Fires, C2, Intelligence and Protection
- Measures of Effectiveness/Pk
- Does cyber affect adversary center of gravity?
- Does cyber affect own center of gravity?

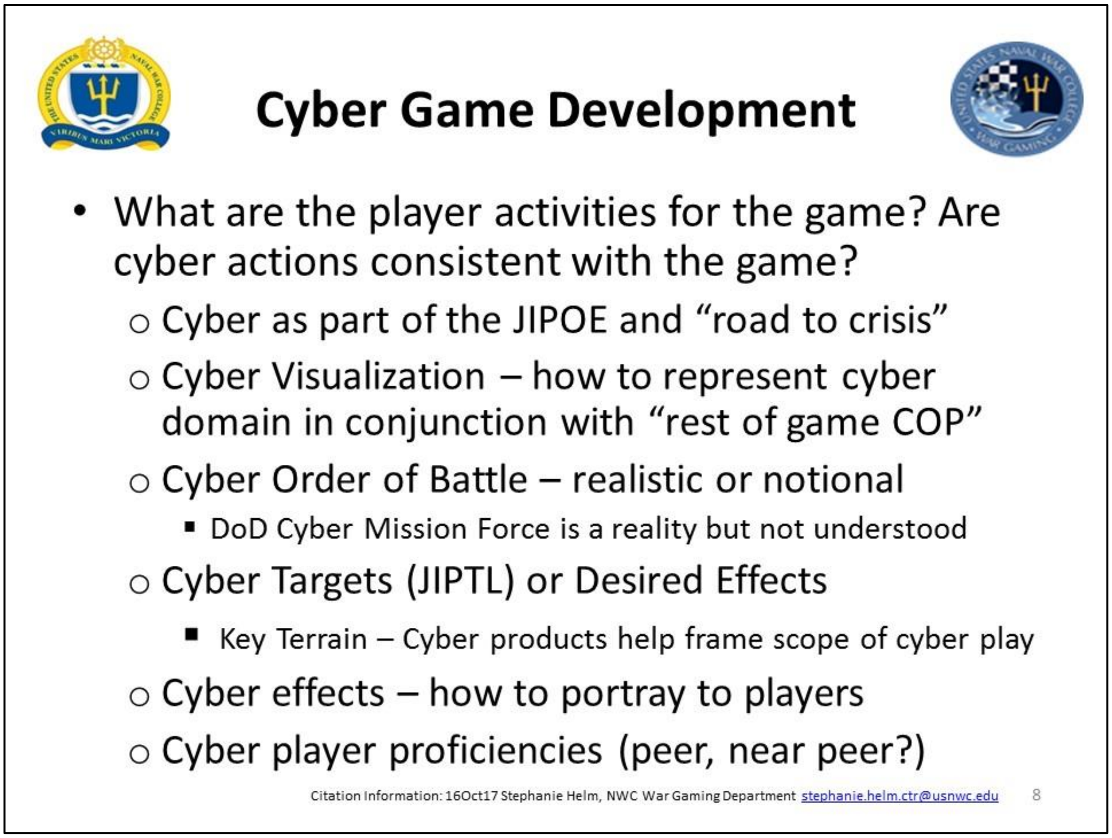
Citation Information: 16Oct17 Stephanie Helm, NWC War Gaming Department stephanie.helm.ctr@usnwc.edu 6



Cyber in War Game Team

- Cyber SME must be part of the game team
- Cyber must be included in each step of the game process (Design, Development, Analysis)
- Consider having a cyber workshop prior to game execution to develop game products such as Key Terrain – Cyber, access lists, force structure, authorities, and ROE

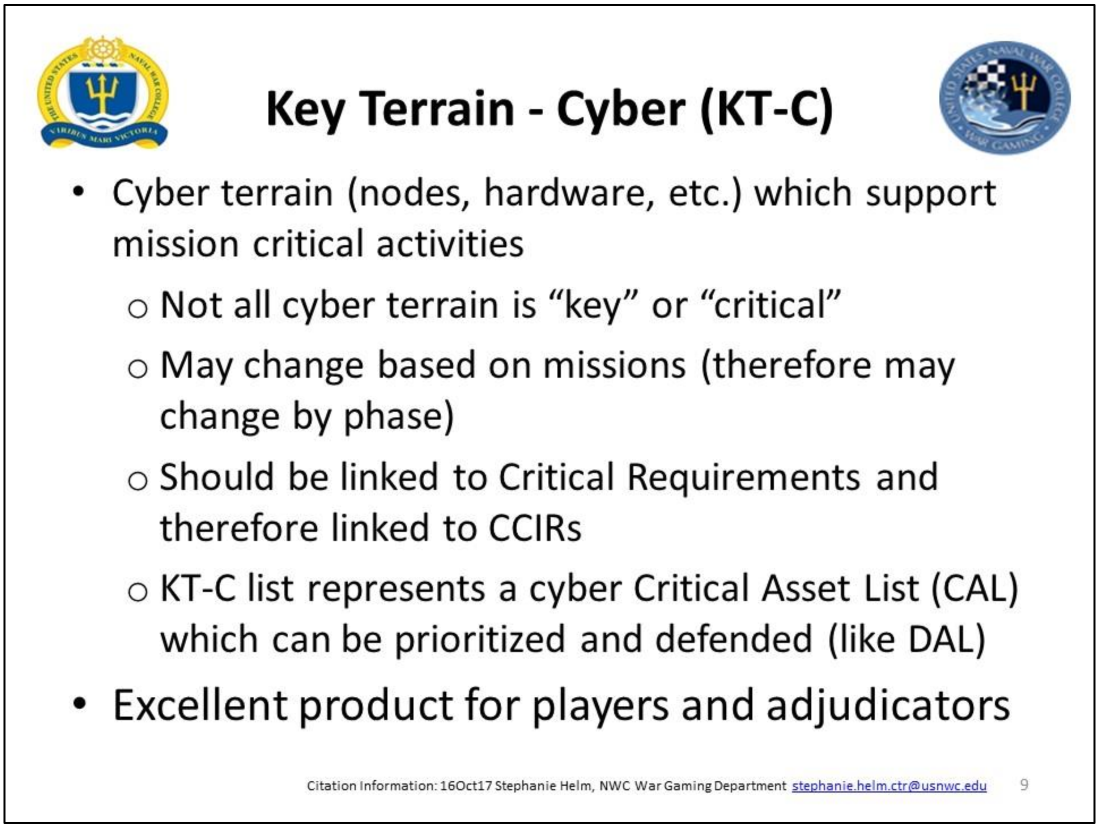
Citation Information: 16Oct17 Stephanie Helm, NWC War Gaming Department stephanie.helm.ctr@usnwc.edu 7



Cyber Game Development

- What are the player activities for the game? Are cyber actions consistent with the game?
  - Cyber as part of the JIPOE and "road to crisis"
  - Cyber Visualization – how to represent cyber domain in conjunction with "rest of game COP"
  - Cyber Order of Battle – realistic or notional
    - DoD Cyber Mission Force is a reality but not understood
  - Cyber Targets (JIPTL) or Desired Effects
    - Key Terrain – Cyber products help frame scope of cyber play
  - Cyber effects – how to portray to players
  - Cyber player proficiencies (peer, near peer?)

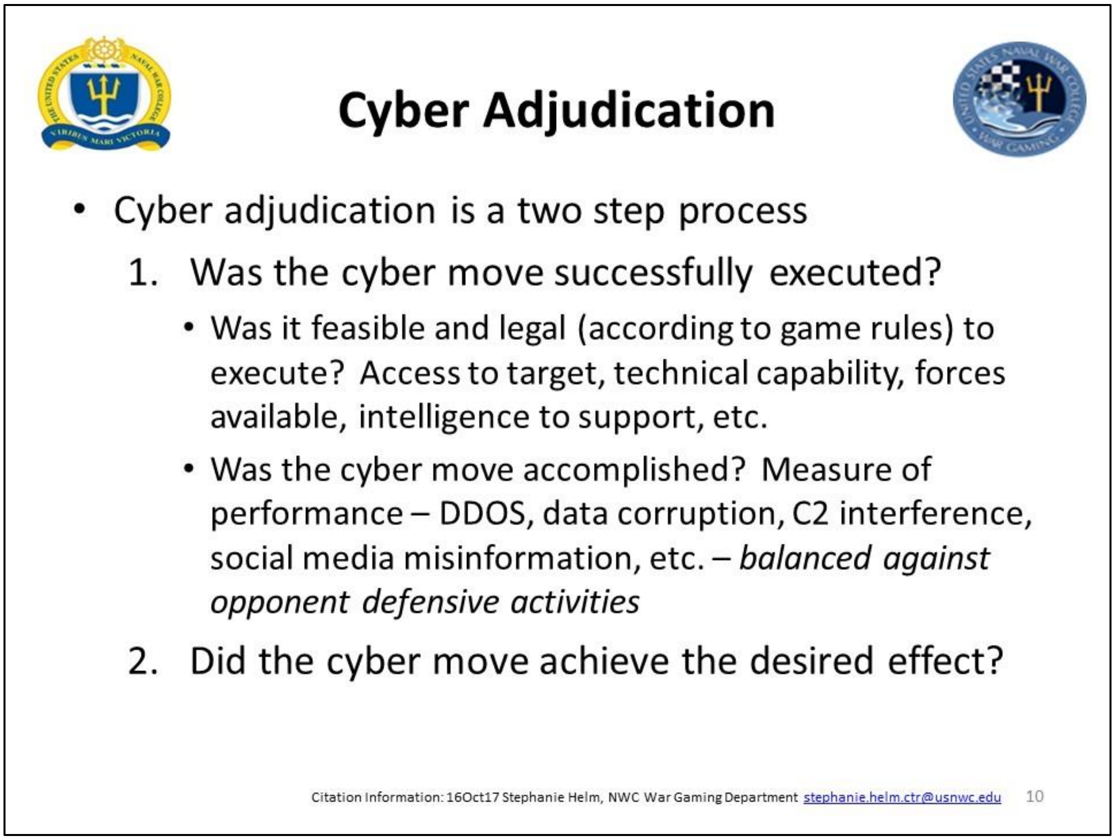
Citation Information: 16Oct17 Stephanie Helm, NWC War Gaming Department stephanie.helm.ctr@usnwc.edu 8



Key Terrain - Cyber (KT-C)

- Cyber terrain (nodes, hardware, etc.) which support mission critical activities
  - ○ Not all cyber terrain is "key" or "critical"
  - ○ May change based on missions (therefore may change by phase)
  - ○ Should be linked to Critical Requirements and therefore linked to CCIRs
  - ○ KT-C list represents a cyber Critical Asset List (CAL) which can be prioritized and defended (like DAL)
- Excellent product for players and adjudicators

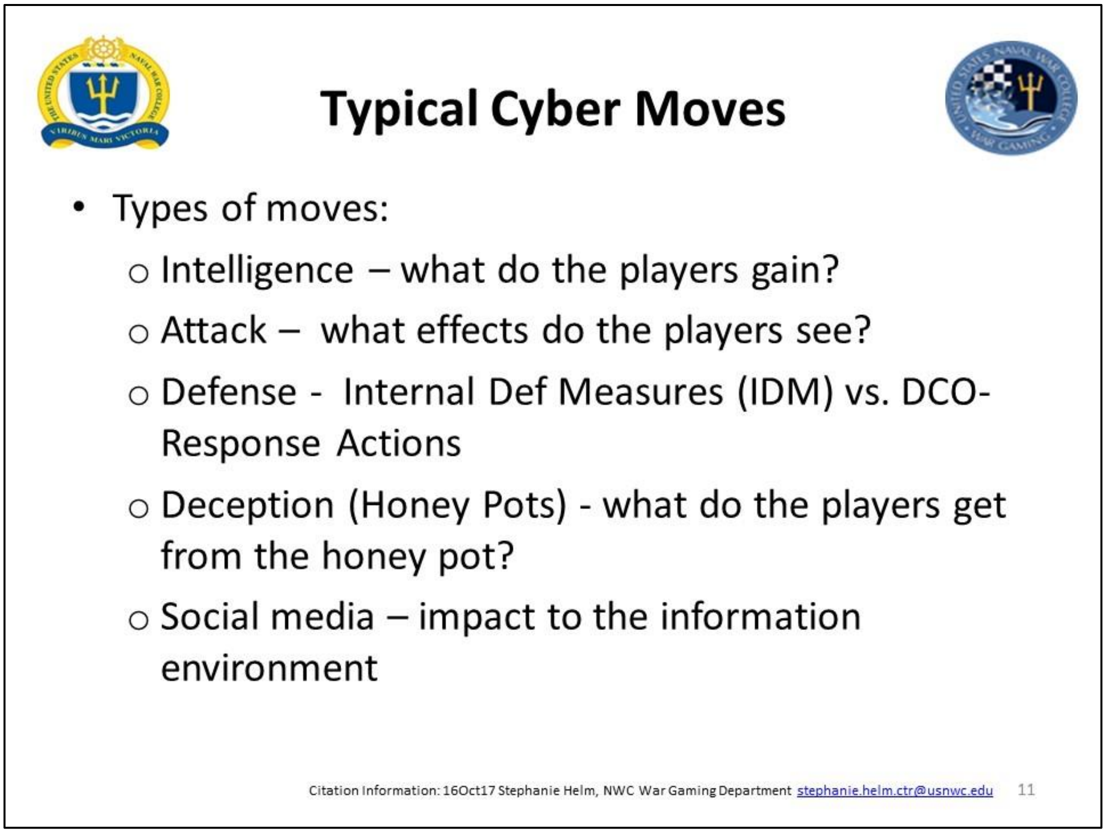
Citation Information: 16Oct17 Stephanie Helm, NWC War Gaming Department stephanie.helm.ctr@usnwc.edu 9



Cyber Adjudication

- Cyber adjudication is a two step process
  1. Was the cyber move successfully executed?
     - Was it feasible and legal (according to game rules) to execute? Access to target, technical capability, forces available, intelligence to support, etc.
     - Was the cyber move accomplished? Measure of performance – DDOS, data corruption, C2 interference, social media misinformation, etc. – *balanced against opponent defensive activities*
  2. Did the cyber move achieve the desired effect?

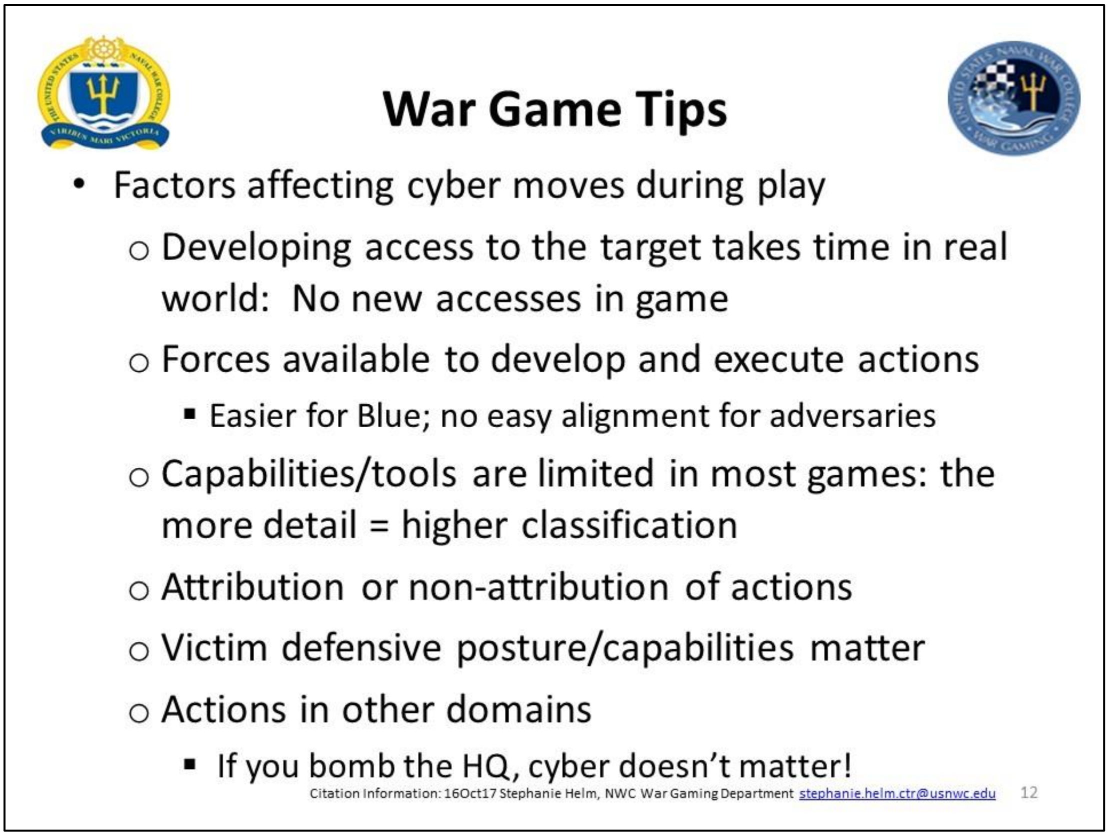
Citation Information: 16Oct17 Stephanie Helm, NWC War Gaming Department stephanie.helm.ctr@usnwc.edu 10



Typical Cyber Moves

- Types of moves:
  - ○ Intelligence – what do the players gain?
  - ○ Attack – what effects do the players see?
  - ○ Defense - Internal Def Measures (IDM) vs. DCO-Response Actions
  - ○ Deception (Honey Pots) - what do the players get from the honey pot?
  - ○ Social media – impact to the information environment

Citation Information: 16Oct17 Stephanie Helm, NWC War Gaming Department stephanie.helm.ctr@usnwc.edu 11



War Game Tips

- Factors affecting cyber moves during play
  - ○ Developing access to the target takes time in real world: No new accesses in game
  - ○ Forces available to develop and execute actions
    - ▪ Easier for Blue; no easy alignment for adversaries
  - ○ Capabilities/tools are limited in most games: the more detail = higher classification
  - ○ Attribution or non-attribution of actions
  - ○ Victim defensive posture/capabilities matter
  - ○ Actions in other domains
    - ▪ If you bomb the HQ, cyber doesn't matter!

Citation Information: 16Oct17 Stephanie Helm, NWC War Gaming Department stephanie.helm.ctr@usnwc.edu 12

Questions?

THE MOMENT YOU REALIZE YOU FORGOT TO PUSH THE MUTE BUTTON
Bacon ©2013 BROADSIDE.NET

Naval War College

War Gaming Department

Stephanie Helm

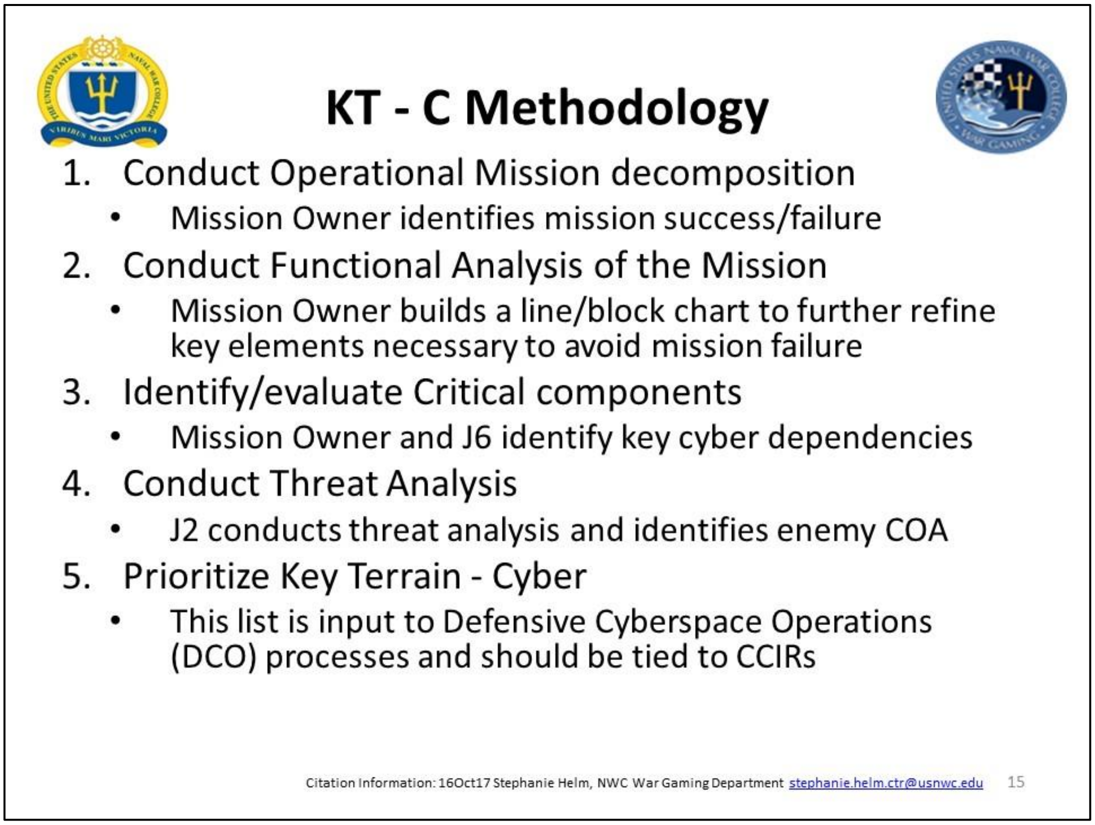
Stephanie.helm.ctr@usnwc.edu

(401) 841-3383

Who establishes KT-C?

- Jointly owned by mission commander and J6/N6
  - Mission owner understands what elements of the mission are most critical and cannot fail
  - Mission owner can divide the mission into functional areas and elements in order to refine cyber dependencies
  - J6/N6 can help further define the key nodes of the cyber dependencies to define the cyber terrain

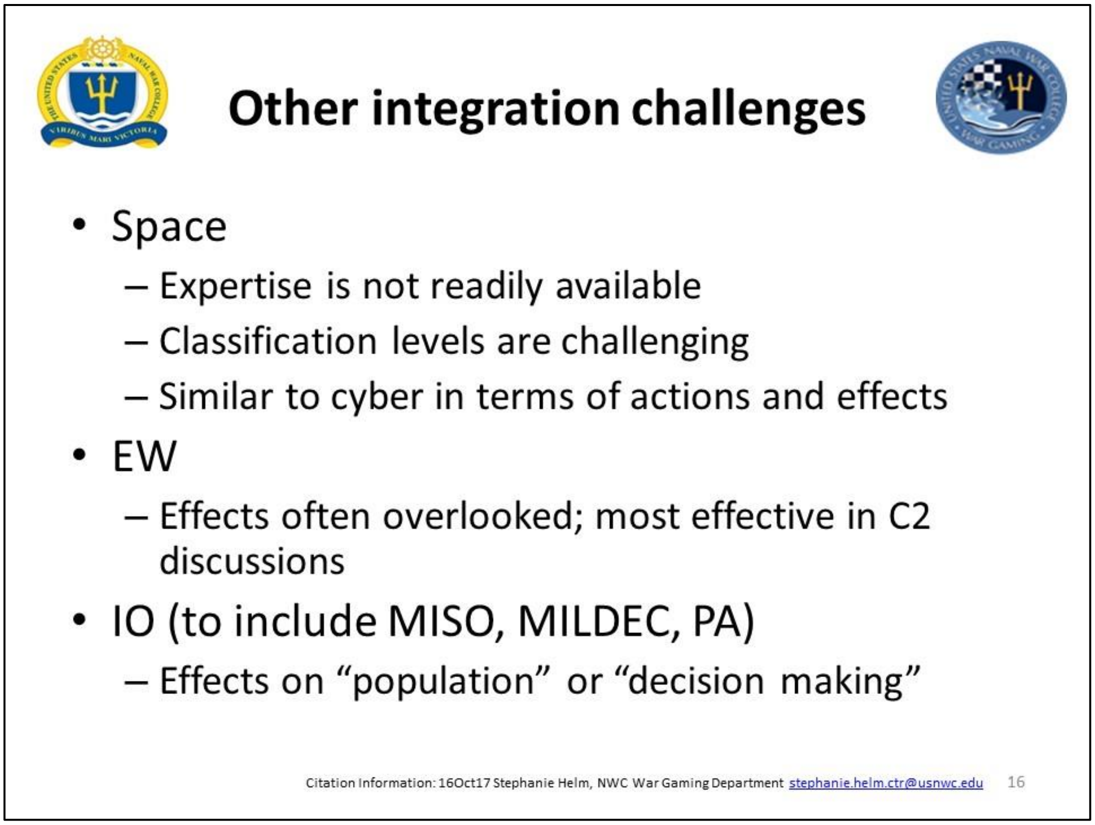
Citation Information: 16Oct17 Stephanie Helm, NWC War Gaming Department stephanie.helm.ctr@usnwc.edu



KT - C Methodology

1. Conduct Operational Mission decomposition
   - Mission Owner identifies mission success/failure
2. Conduct Functional Analysis of the Mission
   - Mission Owner builds a line/block chart to further refine key elements necessary to avoid mission failure
3. Identify/evaluate Critical components
   - Mission Owner and J6 identify key cyber dependencies
4. Conduct Threat Analysis
   - J2 conducts threat analysis and identifies enemy COA
5. Prioritize Key Terrain - Cyber
   - This list is input to Defensive Cyberspace Operations (DCO) processes and should be tied to CCIRs

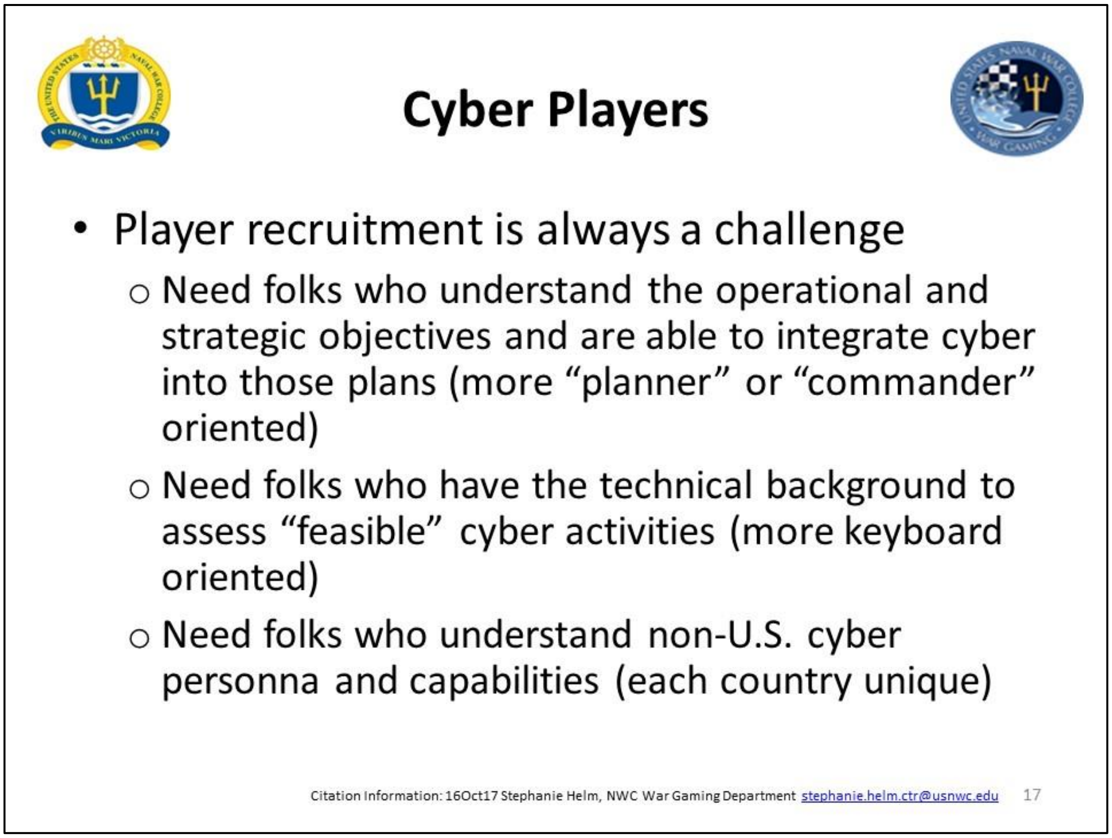
Citation Information: 16Oct17 Stephanie Helm, NWC War Gaming Department stephanie.helm.ctr@usnwc.edu 15



Other integration challenges

- Space
  - – Expertise is not readily available
  - – Classification levels are challenging
  - – Similar to cyber in terms of actions and effects
- EW
  - – Effects often overlooked; most effective in C2 discussions
- IO (to include MISO, MILDEC, PA)
  - – Effects on “population” or “decision making”

Citation Information: 16Oct17 Stephanie Helm, NWC War Gaming Department stephanie.helm.ctr@usnwc.edu 16



Cyber Players

- Player recruitment is always a challenge
  - Need folks who understand the operational and strategic objectives and are able to integrate cyber into those plans (more “planner” or “commander” oriented)
  - Need folks who have the technical background to assess “feasible” cyber activities (more keyboard oriented)
  - Need folks who understand non-U.S. cyber personna and capabilities (each country unique)

Citation Information: 16Oct17 Stephanie Helm, NWC War Gaming Department stephanie.helm.ctr@usnwc.edu 17

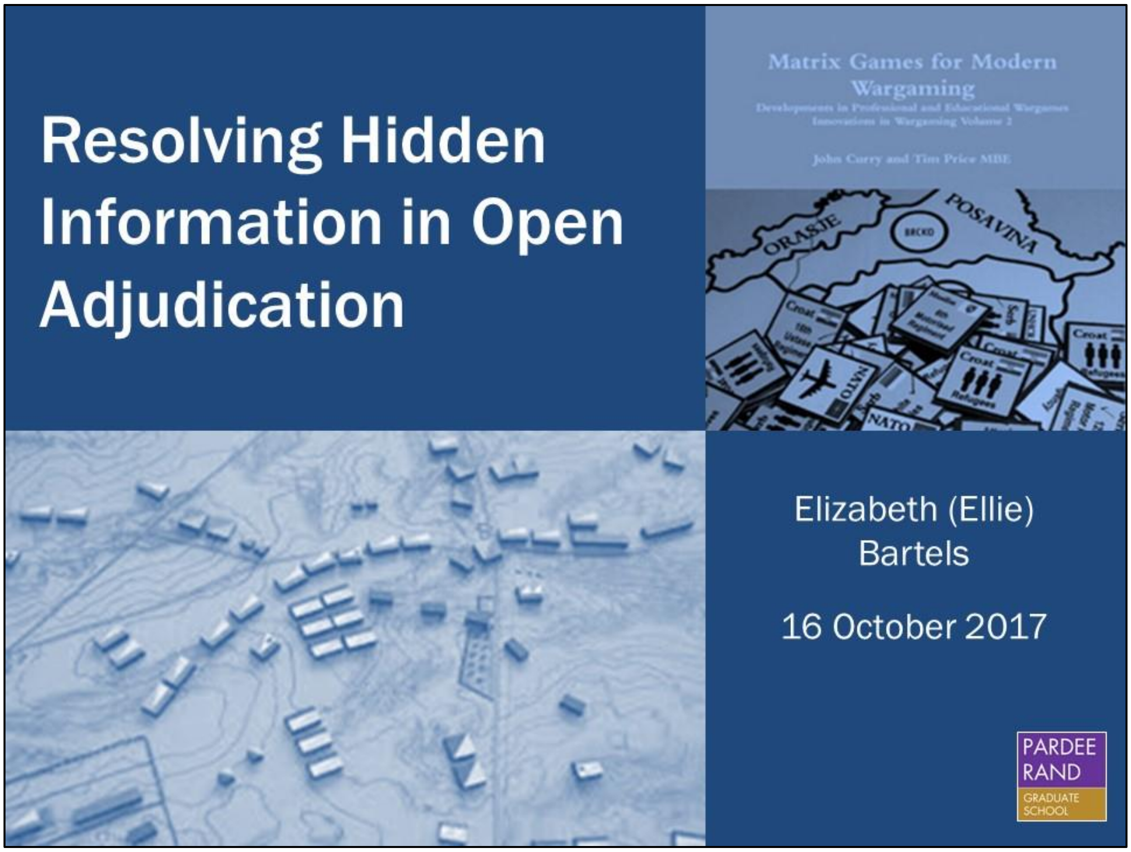
B. Elizabeth Bartels: Resolving Hidden Information in Open Adjudication

Presentation Summary

This presentation focused on a fundamental problem of gaming/exercise: the dichotomy between using open adjudication, in the interest of efficiency and maintaining a common understanding of the state of play, and keeping hidden information hidden, when its exposure could affect the validity of game play and outcomes. Ms. Bartels effectively captured the issues in dealing with cyber effects in gaming, where clear stealth and misdirection must be obscured to get "accurate" play in terms of response by an opposing force.

She exposed the limits of the traditional open adjudication model for exercise actions when dealing with knowledge that could influence play by a team that would not have that knowledge in "reality." The argument also reinforced the general problems with integrating cyber into gaming, where lack of subject matter expertise and models that integrate cyber hinder accurate assessment of cyber effects in scenarios.

Two arguments were presented: open adjudication, in which players and control are on the same level, resulting in transparency, and hidden information, where multiple factors may be obfuscated, thus limiting data to the players (this is closer to the real world). Ms. Bartels proposes combining the two and presented a number of options with varying degrees of discussion between teams and control. Her thesis is that there is no one way to combine both, so rather, an acceptable middle ground should be sought.



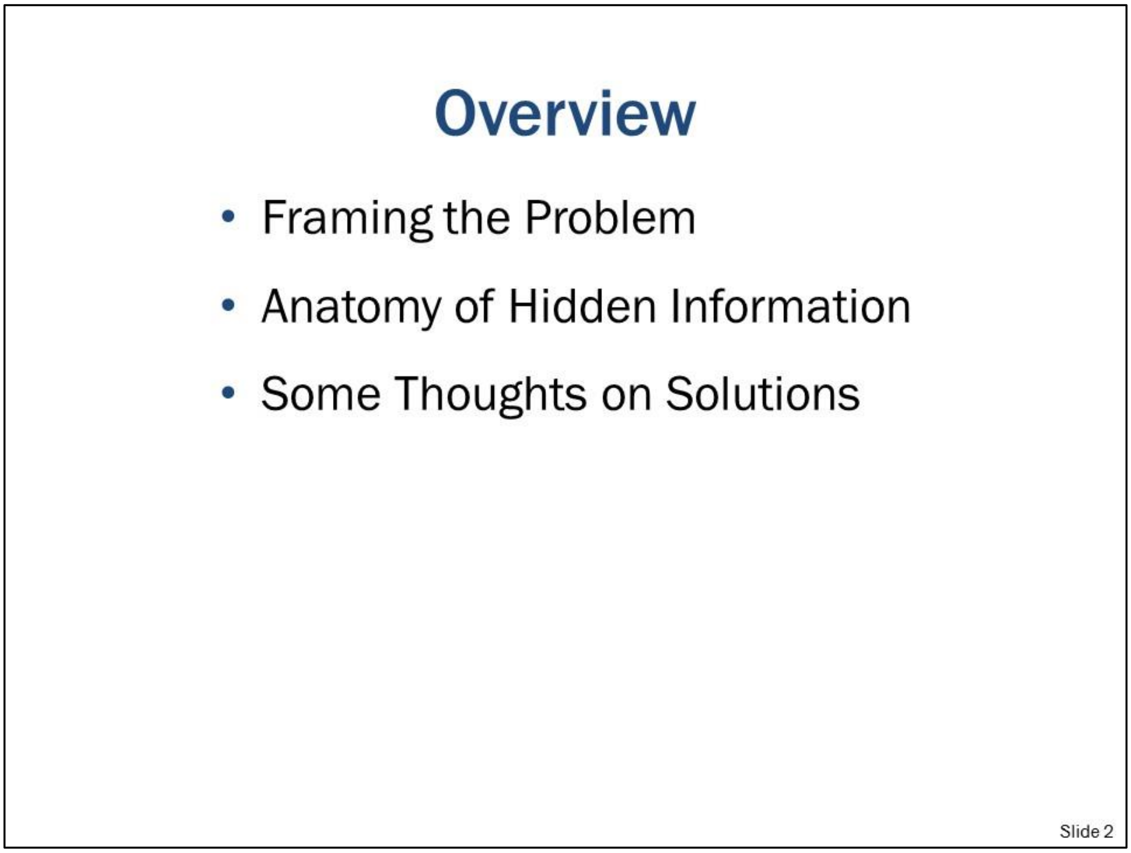
Resolving Hidden Information in Open Adjudication

Matrix Games for Modern Wargaming
Developments in Professional and Educational Wargames
Innovations in Wargaming Volume 2
John Curry and Tim Price MBE
ORASJE
BRCKO
POSAVINA
NATO
Croat
Refugees

Elizabeth (Ellie) Bartels

16 October 2017

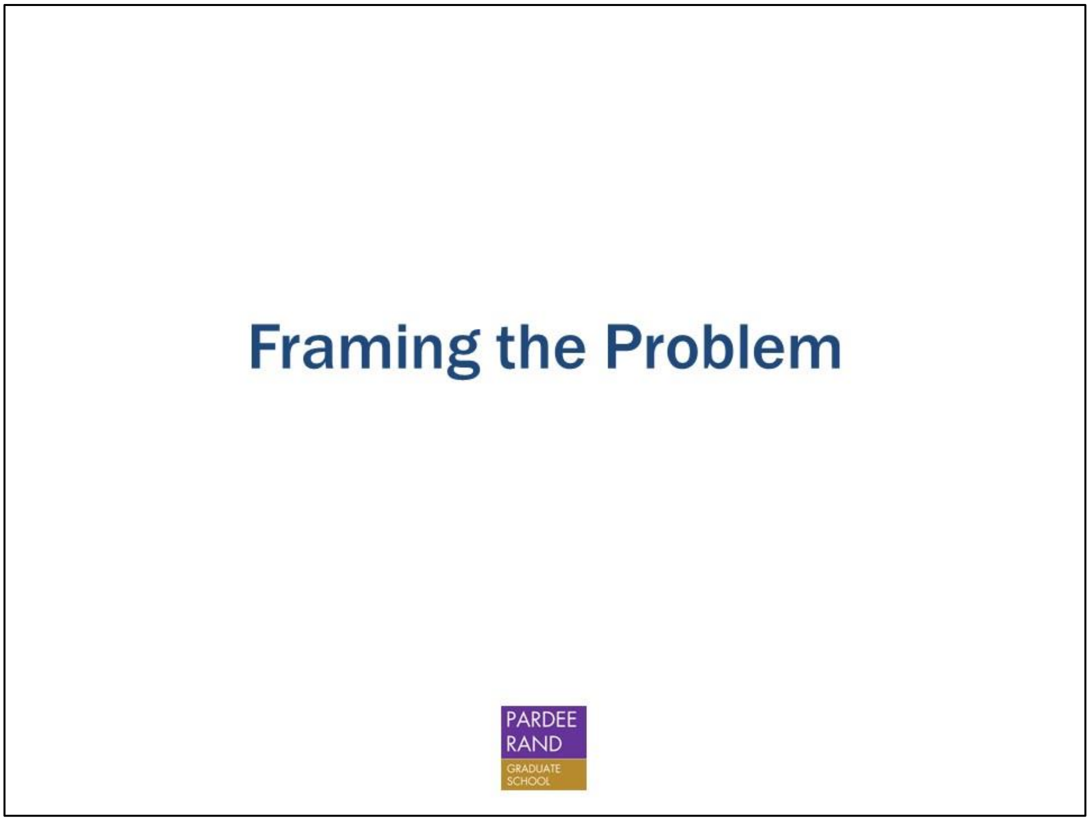
PARDEE RAND GRADUATE SCHOOL



Overview

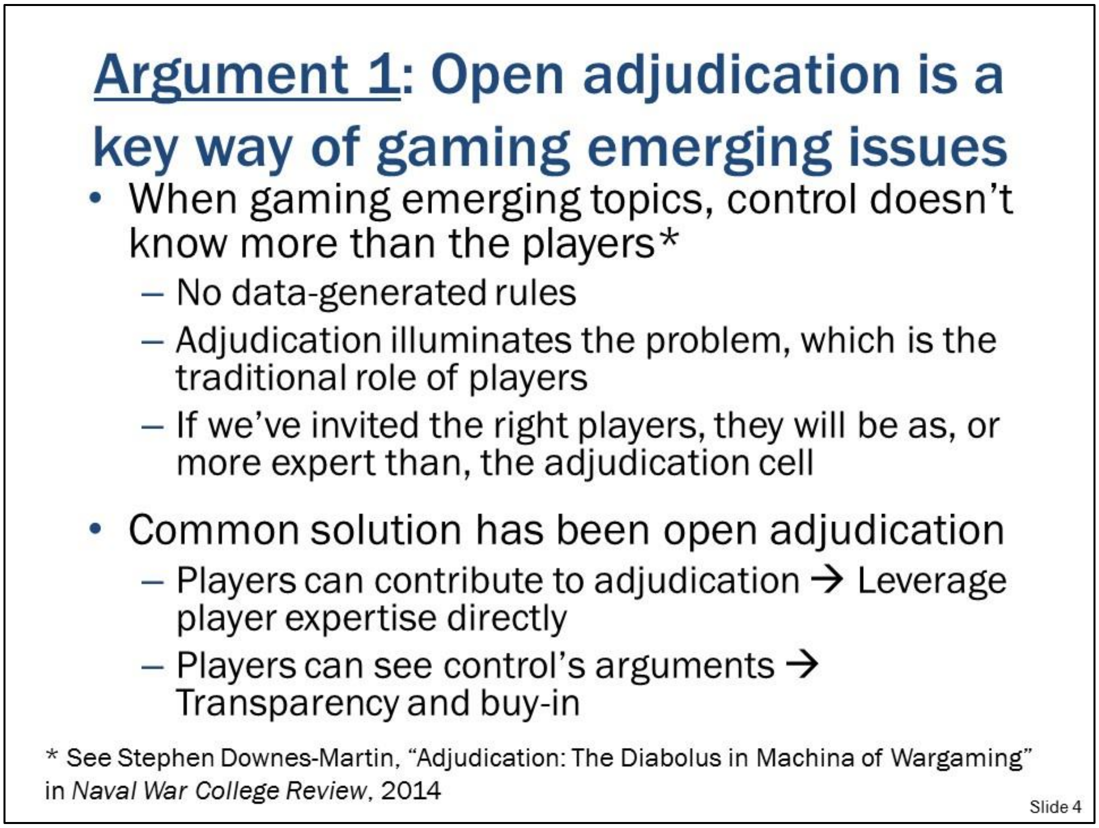
- Framing the Problem
- Anatomy of Hidden Information
- Some Thoughts on Solutions

Slide 2



Framing the Problem

PARDEE
RAND
GRADUATE
SCHOOL

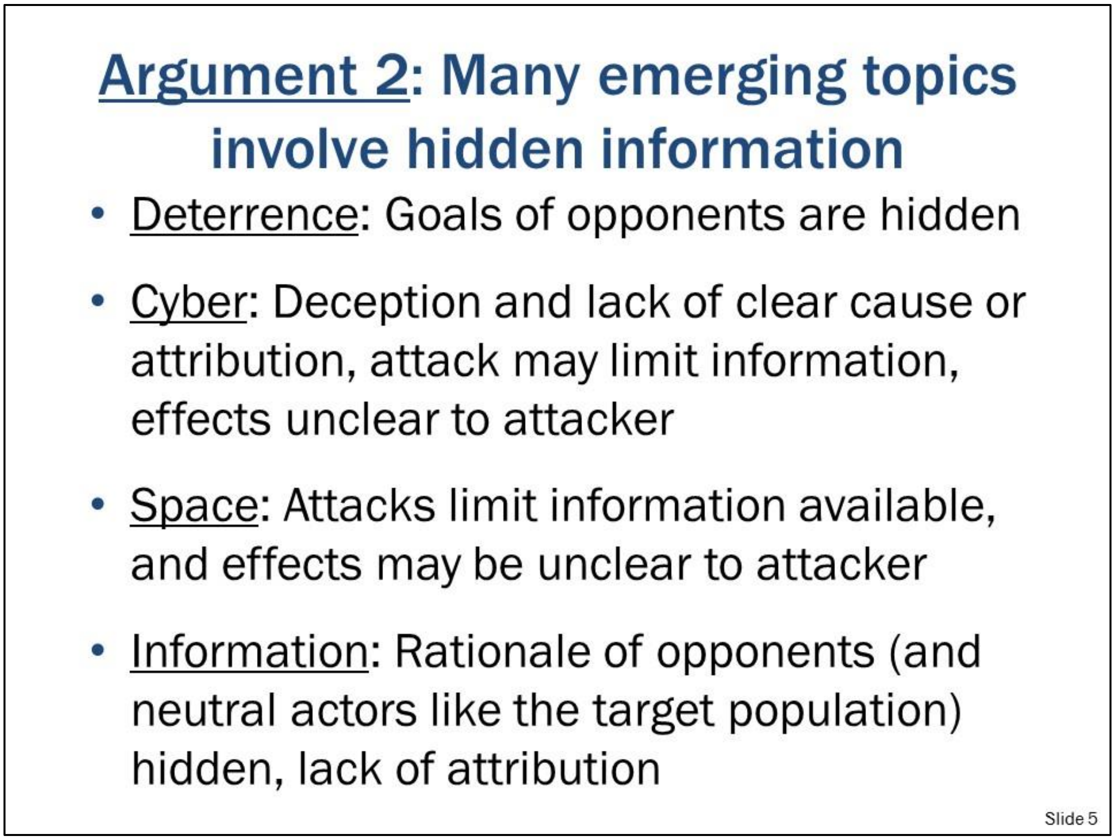


Argument 1: Open adjudication is a key way of gaming emerging issues

- When gaming emerging topics, control doesn't know more than the players*
  - No data-generated rules
  - Adjudication illuminates the problem, which is the traditional role of players
  - If we've invited the right players, they will be as, or more expert than, the adjudication cell
- Common solution has been open adjudication
  - Players can contribute to adjudication → Leverage player expertise directly
  - Players can see control's arguments → Transparency and buy-in

* See Stephen Downes-Martin, "Adjudication: The Diabolus in Machina of Wargaming" in *Naval War College Review*, 2014

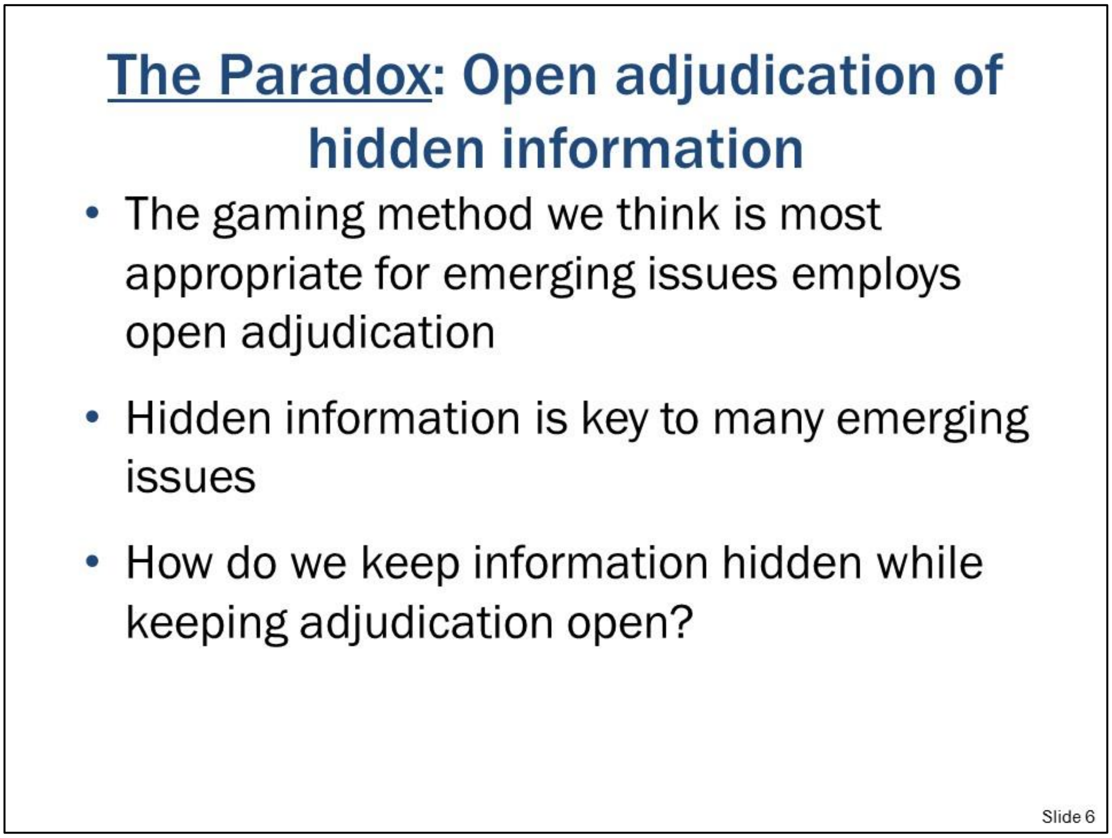
Slide 4



Argument 2: Many emerging topics involve hidden information

- Deterrence: Goals of opponents are hidden
- Cyber: Deception and lack of clear cause or attribution, attack may limit information, effects unclear to attacker
- Space: Attacks limit information available, and effects may be unclear to attacker
- Information: Rationale of opponents (and neutral actors like the target population) hidden, lack of attribution

Slide 5



The Paradox: Open adjudication of hidden information

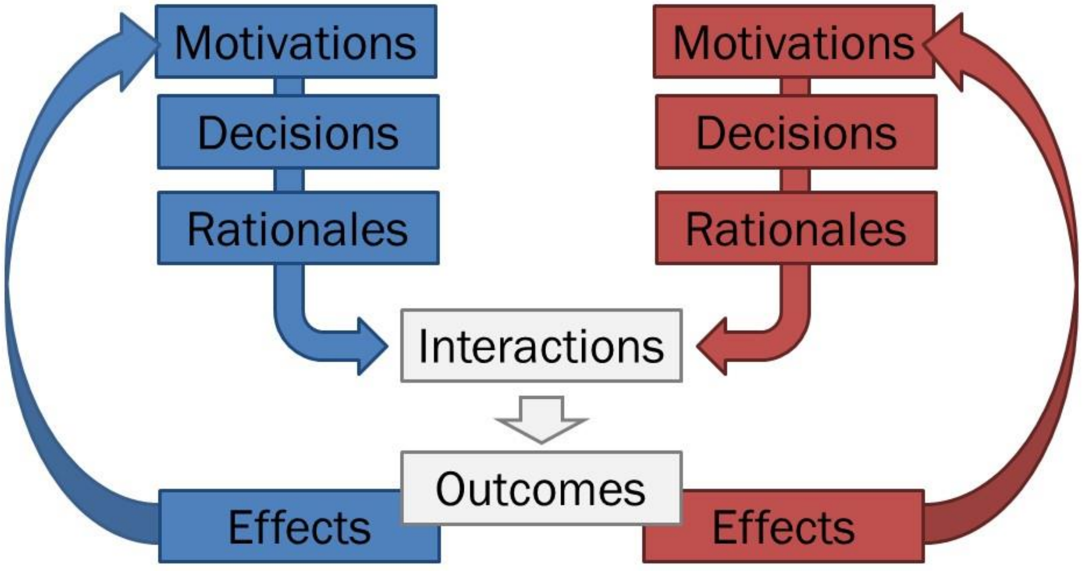
- The gaming method we think is most appropriate for emerging issues employs open adjudication
- Hidden information is key to many emerging issues
- How do we keep information hidden while keeping adjudication open?

Slide 6

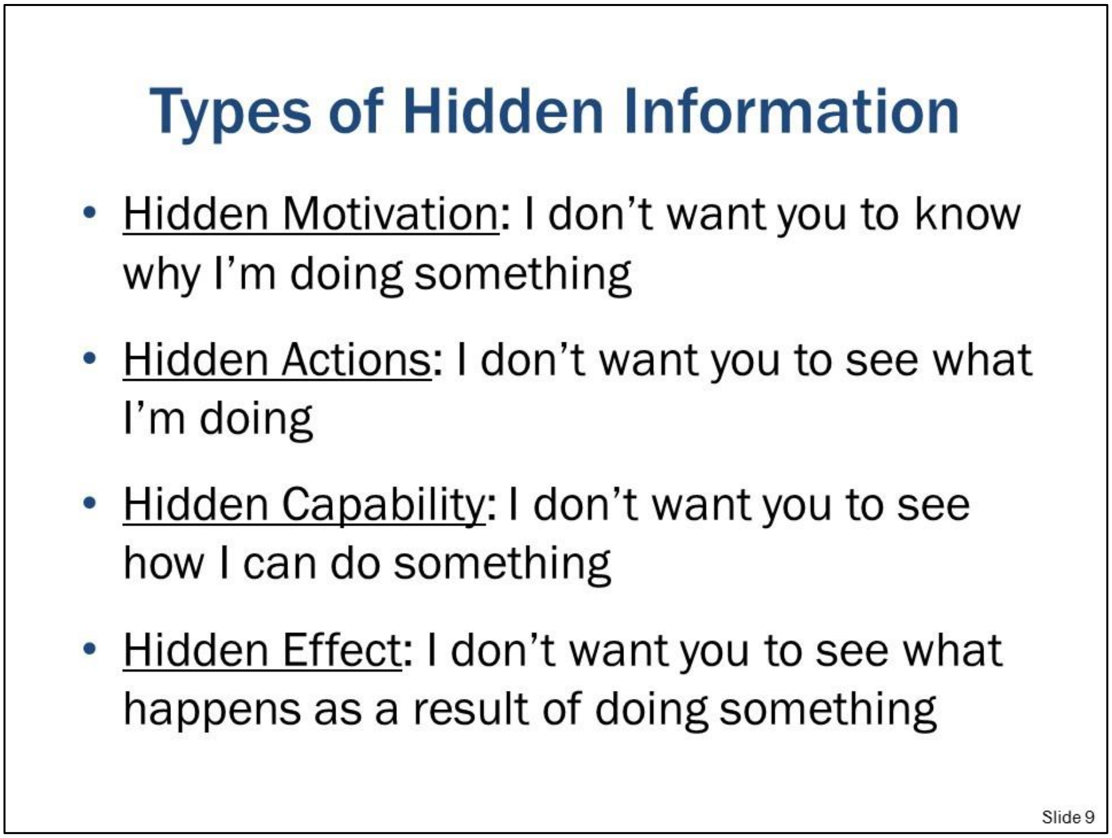
Anatomy of Hidden Information

PARDEE
RAND
GRADUATE
SCHOOL

What information is in a game?



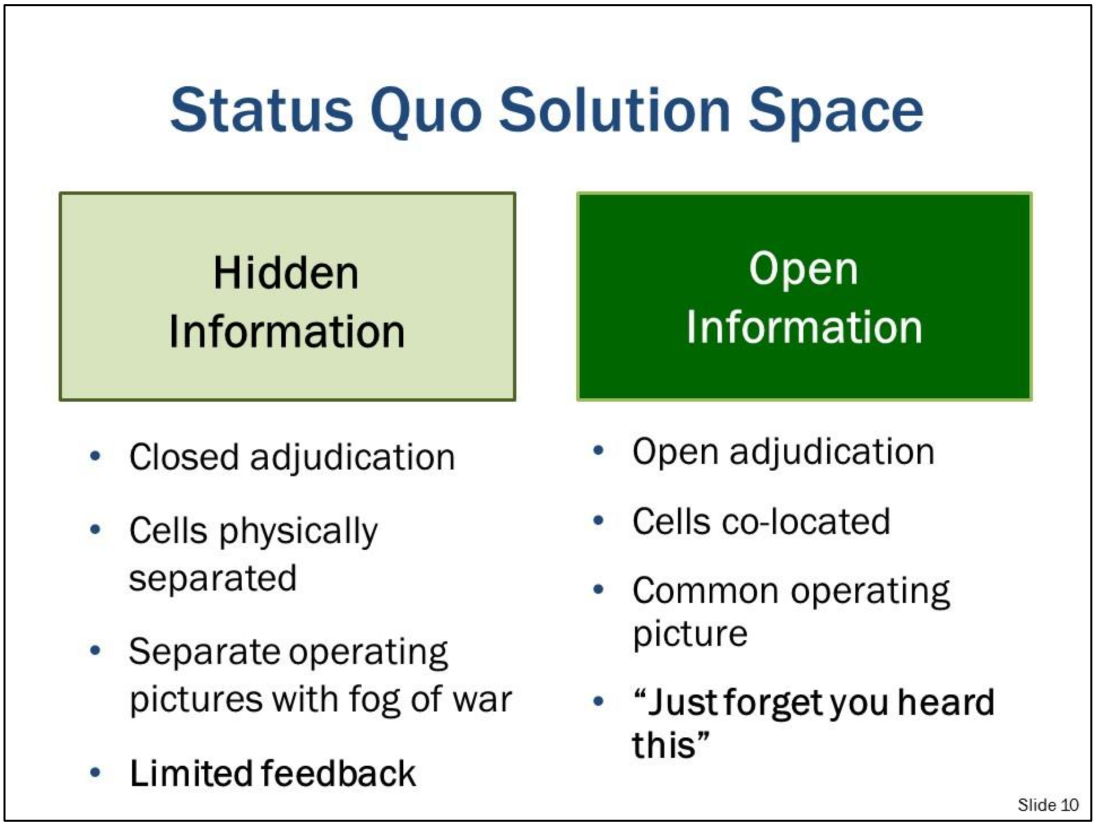
Slide 8



Types of Hidden Information

- Hidden Motivation: I don't want you to know why I'm doing something
- Hidden Actions: I don't want you to see what I'm doing
- Hidden Capability: I don't want you to see how I can do something
- Hidden Effect: I don't want you to see what happens as a result of doing something

Slide 9



Status Quo Solution Space

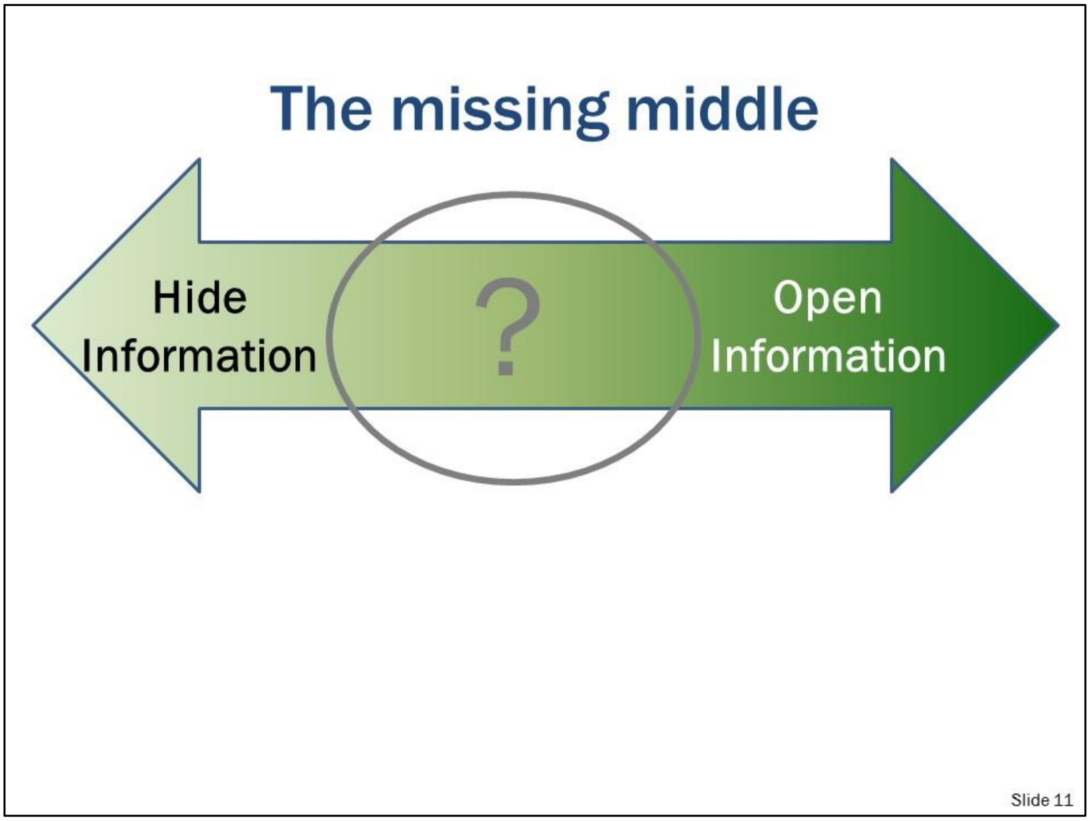
Hidden Information

- Closed adjudication
- Cells physically separated
- Separate operating pictures with fog of war
- Limited feedback

Open Information

- Open adjudication
- Cells co-located
- Common operating picture
- "Just forget you heard this"

Slide 10

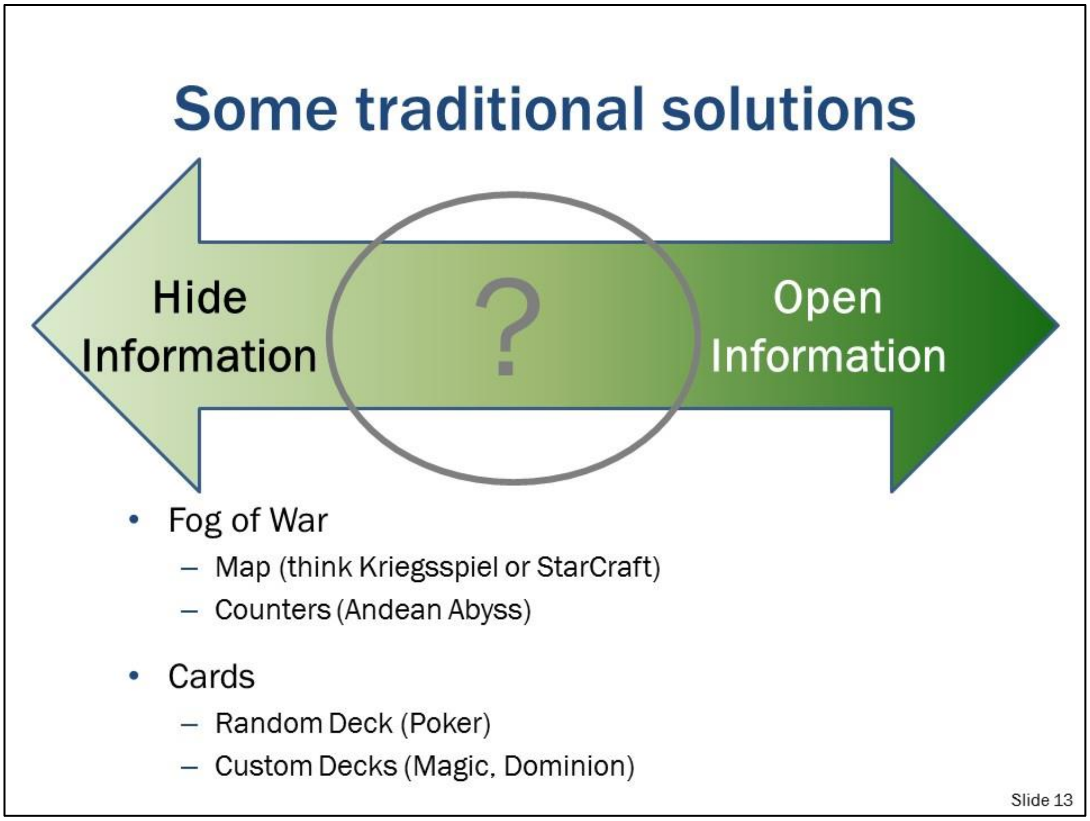


The missing middle

Slide 11

Fumbling towards Solutions

PARDEE RAND GRADUATE SCHOOL



Some traditional solutions

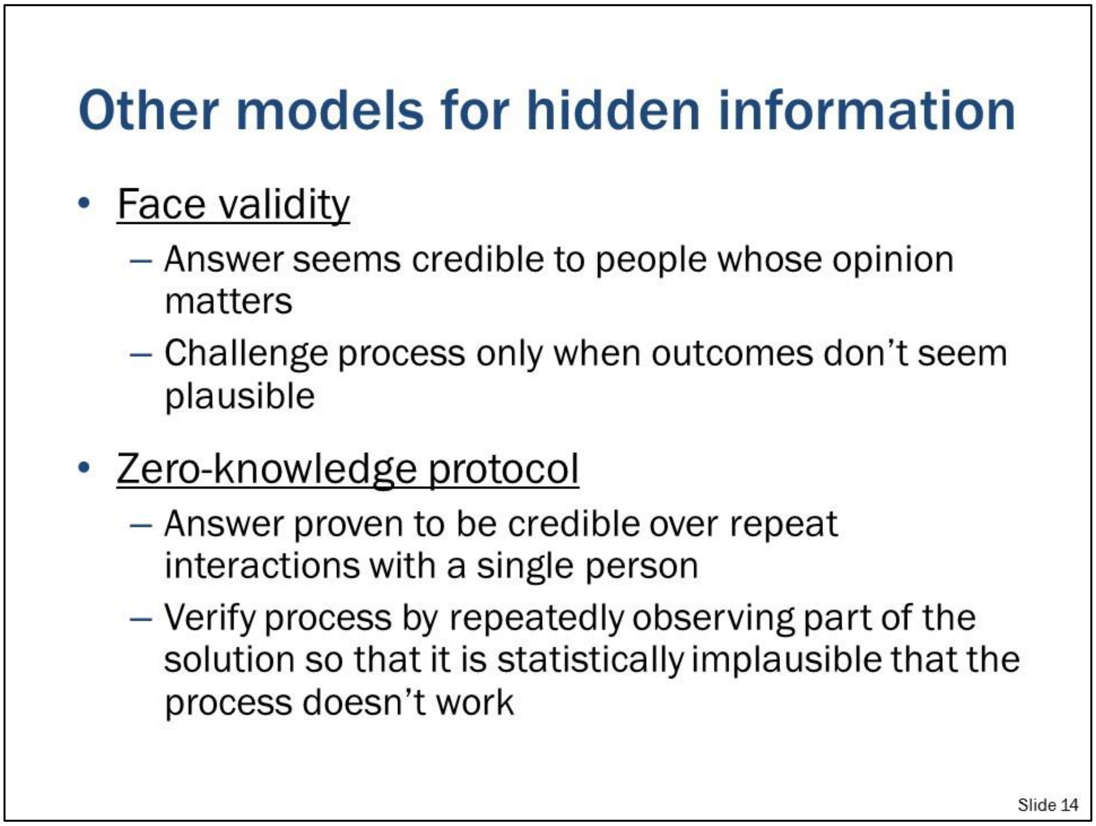
Hide Information

?

Open Information

- Fog of War
  - Map (think Kriegsspiel or StarCraft)
  - Counters (Andean Abyss)
- Cards
  - Random Deck (Poker)
  - Custom Decks (Magic, Dominion)

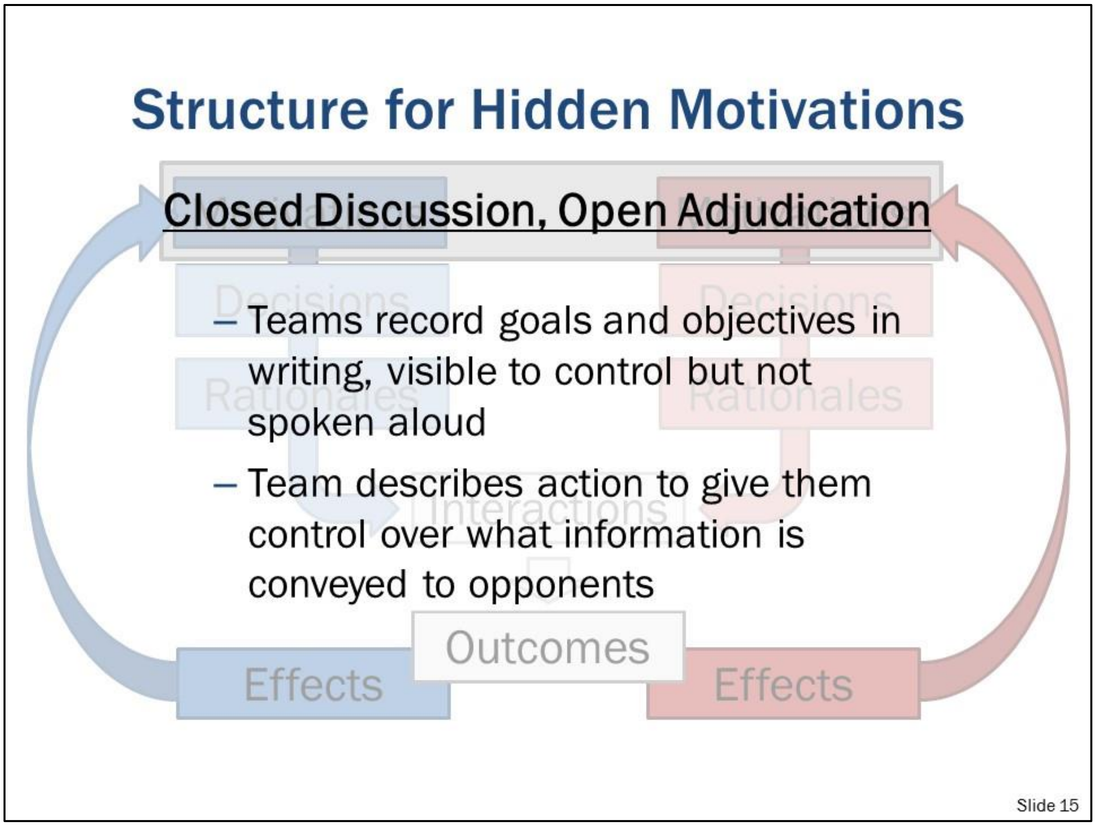
Slide 13



Other models for hidden information

- Face validity
  - Answer seems credible to people whose opinion matters
  - Challenge process only when outcomes don't seem plausible
- Zero-knowledge protocol
  - Answer proven to be credible over repeat interactions with a single person
  - Verify process by repeatedly observing part of the solution so that it is statistically implausible that the process doesn't work

Slide 14



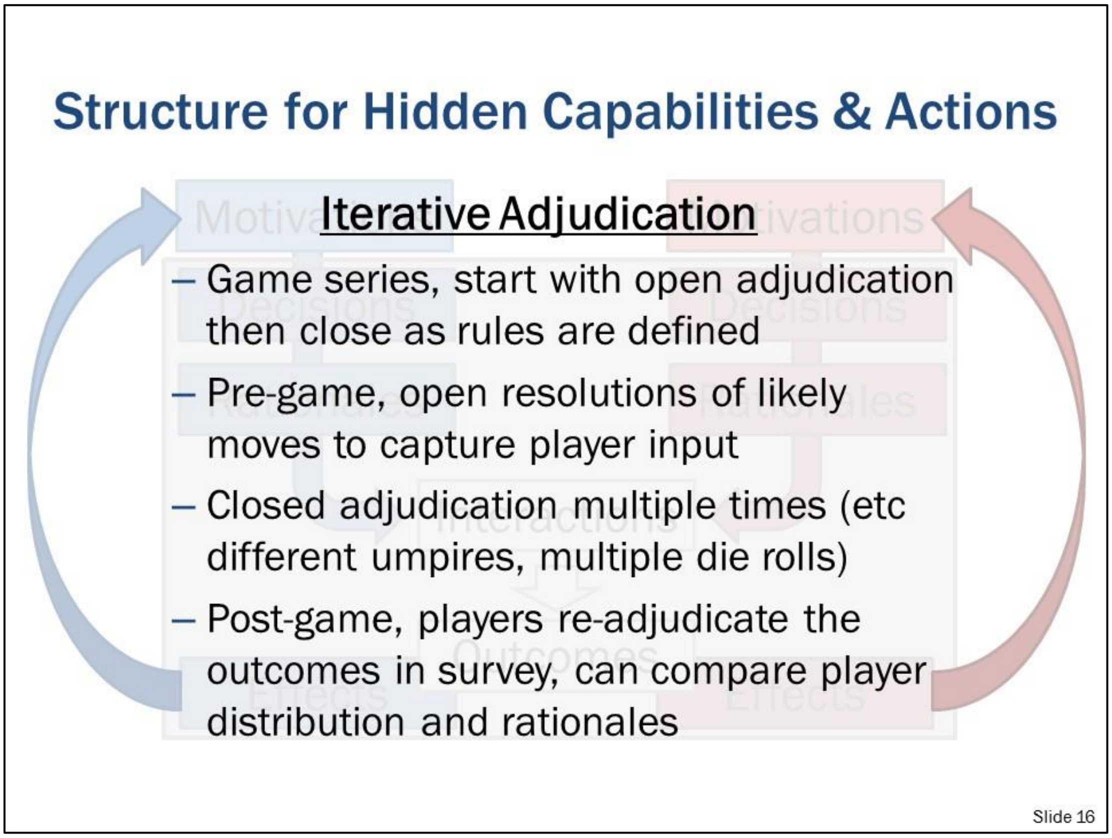
Decisions
Decisions
Rationales
Rationales
Interactions
Outcomes
Effects
Effects

Structure for Hidden Motivations

Closed Discussion, Open Adjudication

- – Teams record goals and objectives in writing, visible to control but not spoken aloud
- – Team describes action to give them control over what information is conveyed to opponents

Slide 15



Motivations
Motivations
Decisions
Decisions
Rationales
Rationales
Interactions
Outcomes
Effects
Effects

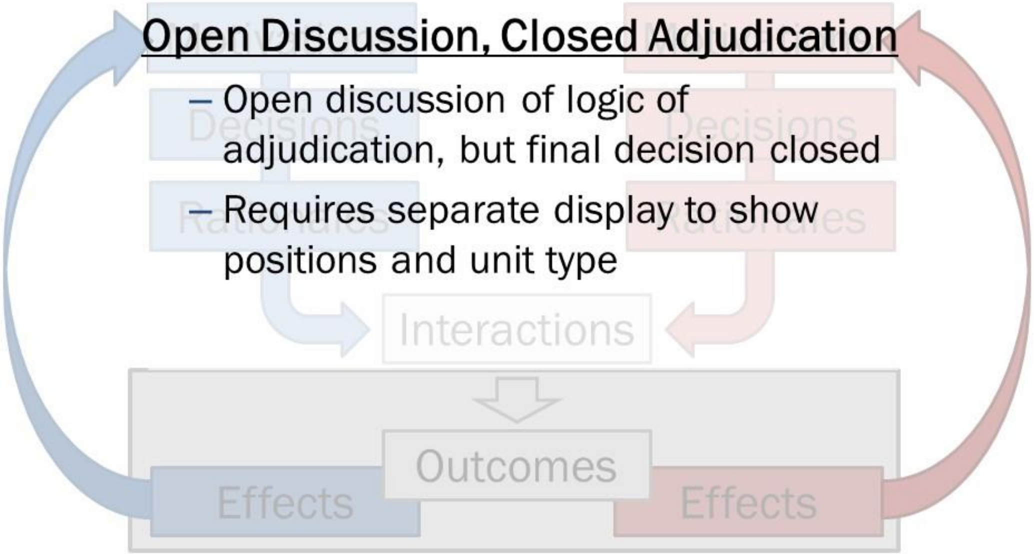
Structure for Hidden Capabilities & Actions

Iterative Adjudication

- – Game series, start with open adjudication then close as rules are defined
- – Pre-game, open resolutions of likely moves to capture player input
- – Closed adjudication multiple times (etc different umpires, multiple die rolls)
- – Post-game, players re-adjudicate the outcomes in survey, can compare player distribution and rationales

Slide 16

Structure for Hidden Effects



<u>Open Discussion, Closed Adjudication</u>

- Open discussion of logic of adjudication, but final decision closed
- Requires separate display to show positions and unit type

Slide 17

PARDEE RAND
GRADUATE SCHOOL

C. Phil Pournelle: LTSG Marinus Platform

Presentation Summary

Mr. Pournelle's discussion on the Marinus distributed and asynchronous gaming platform provided clear novice-level background information on current use of the platform and how it is moving forward. The demonstration scenario consisted of the U.S.-Japan alliance, Korean Peninsula theater, and Senkaku islands as applied to war gaming. Mr. Pournelle drew attention to the importance of integrating assessment of the actions of Green (allied) forces into complex game play, especially in scenarios where the interests or strategic goals of Blue and Green may diverge. The presentation also underscored the challenge of integrating cyber into game play.

Mr. Pournelle was wary of the inclusion of cyber effects into game play, due to their potential to distract from or disrupt exercise of traditional kinetic forces. His desire to "put it in its own sandbox so it doesn't overtake our sandbox," was in contrast to the presentations by Ms. Helm and Ms. Bartels. The Marinus platform is a vendor offering for web-based gaming with strategy and tactics for land, sea, and air positions that are presented in a standardized mapped view.

Long Term Strategy Group & The Marinus Platform

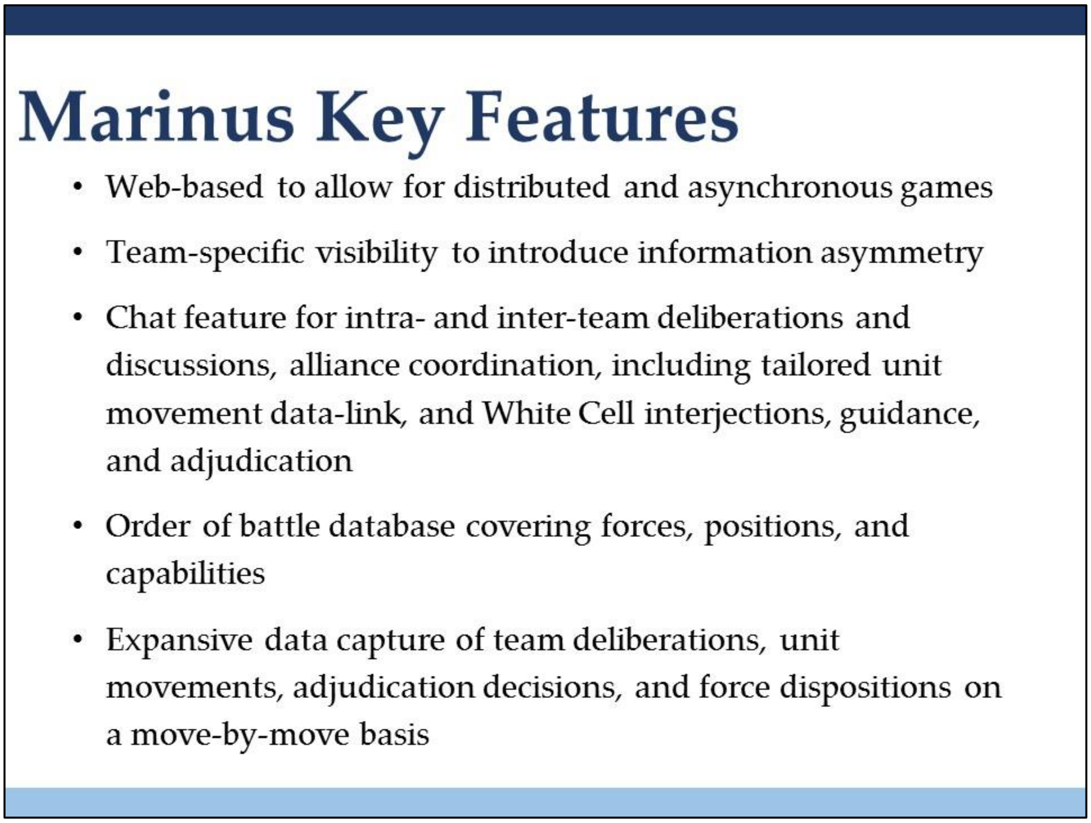
October 2017

Long Term Strategy Group

LTSG

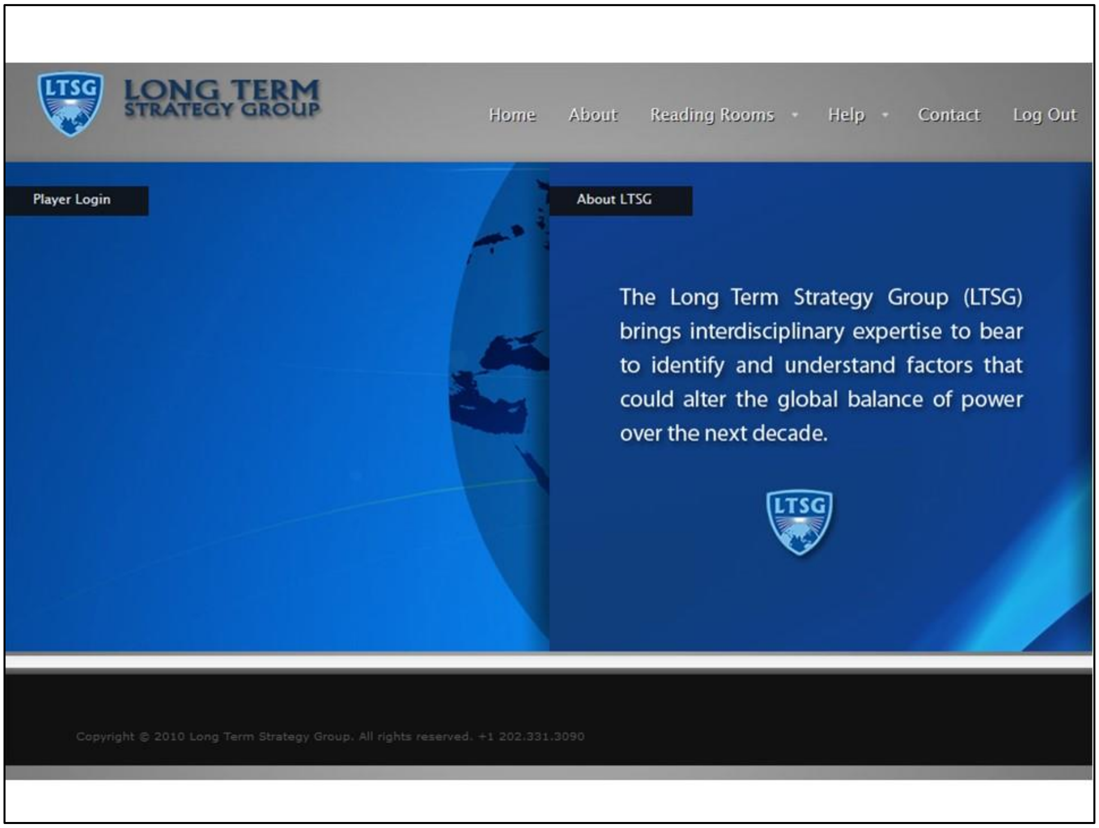
Long Term Strategy Group | inquiries@ltstrategy.com | (202) 331-3090

LTSG's Marinus wargame platform



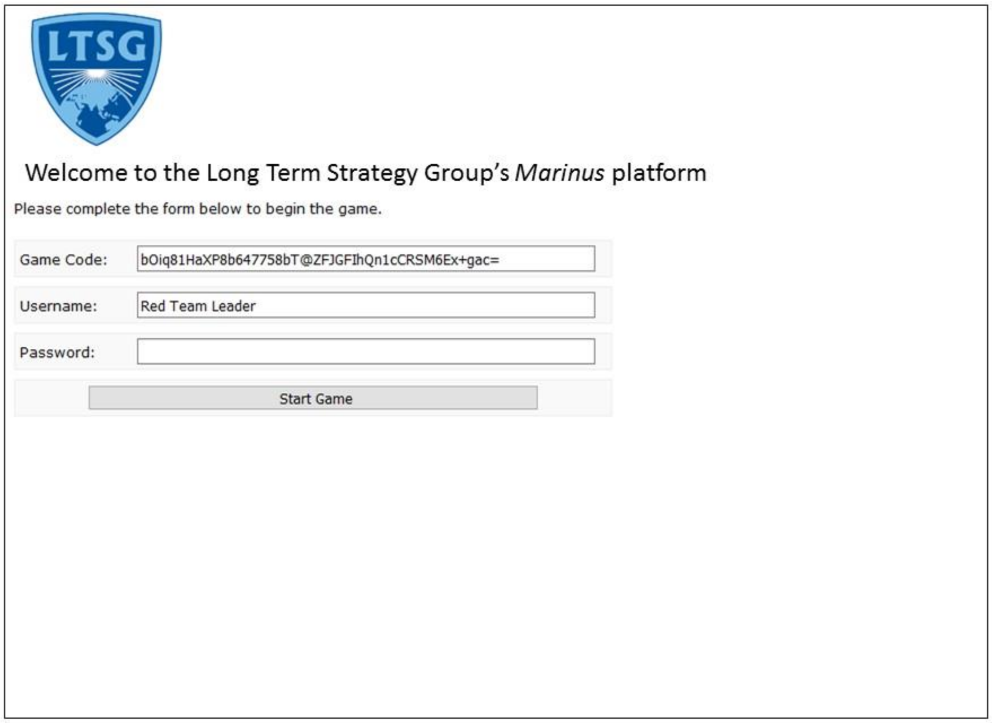
Marinus Key Features

- Web-based to allow for distributed and asynchronous games
- Team-specific visibility to introduce information asymmetry
- Chat feature for intra- and inter-team deliberations and discussions, alliance coordination, including tailored unit movement data-link, and White Cell interjections, guidance, and adjudication
- Order of battle database covering forces, positions, and capabilities
- Expansive data capture of team deliberations, unit movements, adjudication decisions, and force dispositions on a move-by-move basis



The Long Term Strategy Group (LTSG) brings interdisciplinary expertise to bear to identify and understand factors that could alter the global balance of power over the next decade.

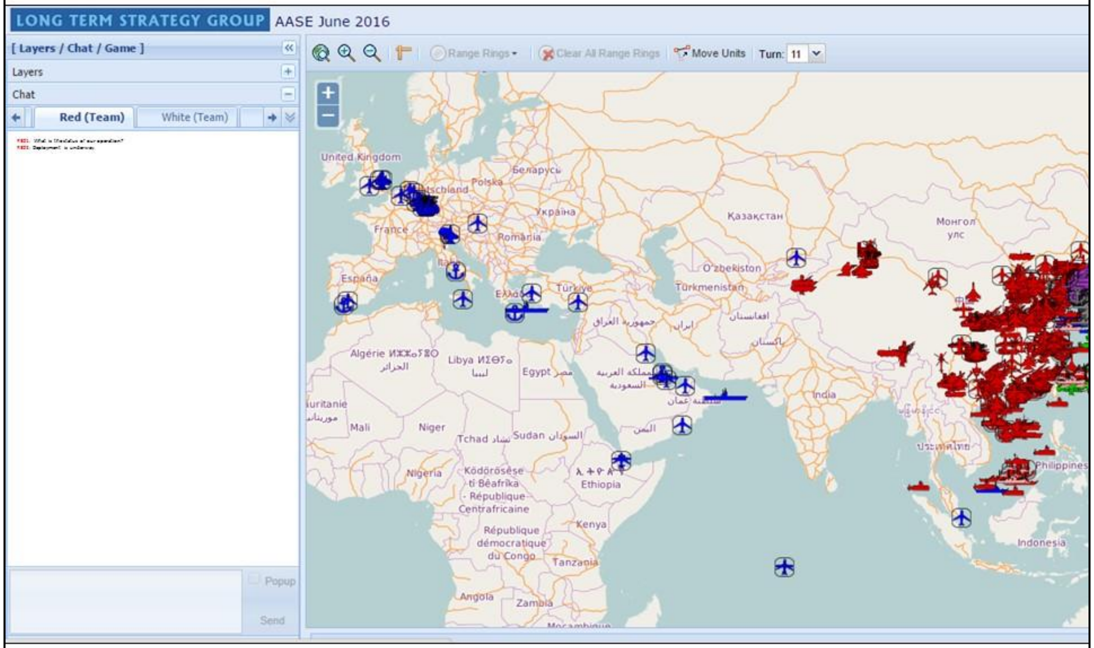
Copyright © 2010 Long Term Strategy Group. All rights reserved. +1 202.331.3090



Welcome to the Long Term Strategy Group's *Marinus* platform

Please complete the form below to begin the game.

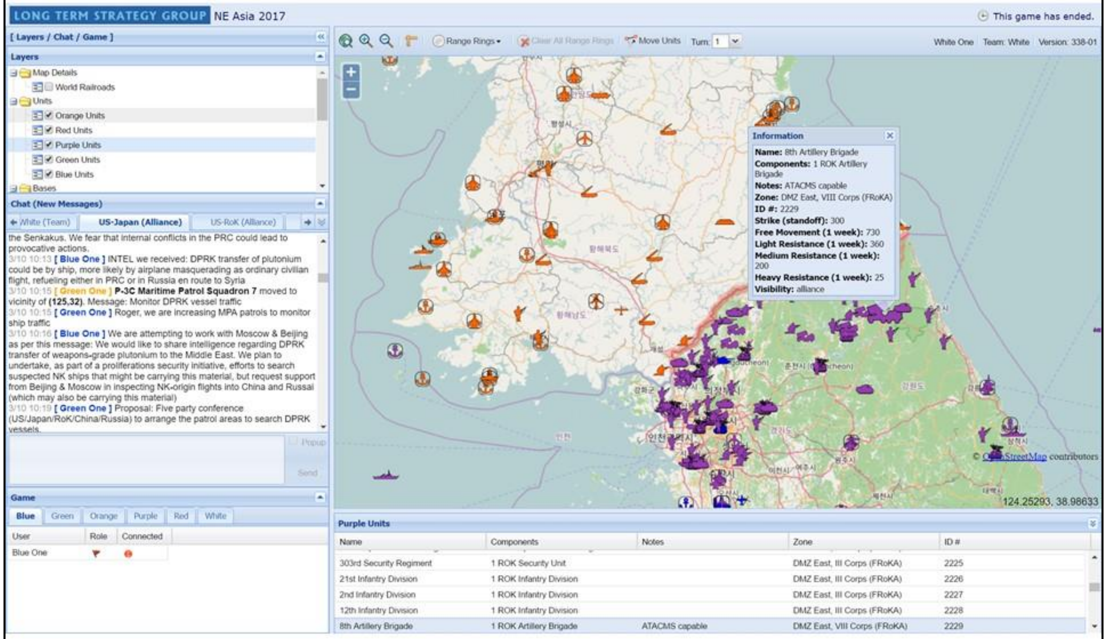
Game Code:	bOiq81HaXP8b647758bT@ZFJGFIhQn1cCRSM6Ex+gac=
Username:	Red Team Leader
Password:	



LONG TERM STRATEGY GROUP AASE June 2016

RED: What is the status of our operation?
RED: Deployment is underway.

Turn: 11



the Senkakus. We fear that internal conflicts in the PRC could lead to provocative actions.

3/10 10:13 [Blue One] INTEL we received: DPRK transfer of plutonium could be by ship, more likely by airplane masquerading as ordinary civilian flight, refueling either in PRC or in Russia en route to Syria

3/10 10:15 [Green One] **P-3C Maritime Patrol Squadron 7** moved to vicinity of **(125,32)**. Message: Monitor DPRK vessel traffic

3/10 10:15 [Green One] Roger, we are increasing MPA patrols to monitor ship traffic

3/10 10:16 [Blue One] We are attempting to work with Moscow & Beijing as per this message: We would like to share intelligence regarding DPRK transfer of weapons-grade plutonium to the Middle East. We plan to undertake, as part of a proliferations security initiative, efforts to search suspected NK ships that might be carrying this material, but request support from Beijing & Moscow in inspecting NK-origin flights into China and Russai (which may also be carrying this material)

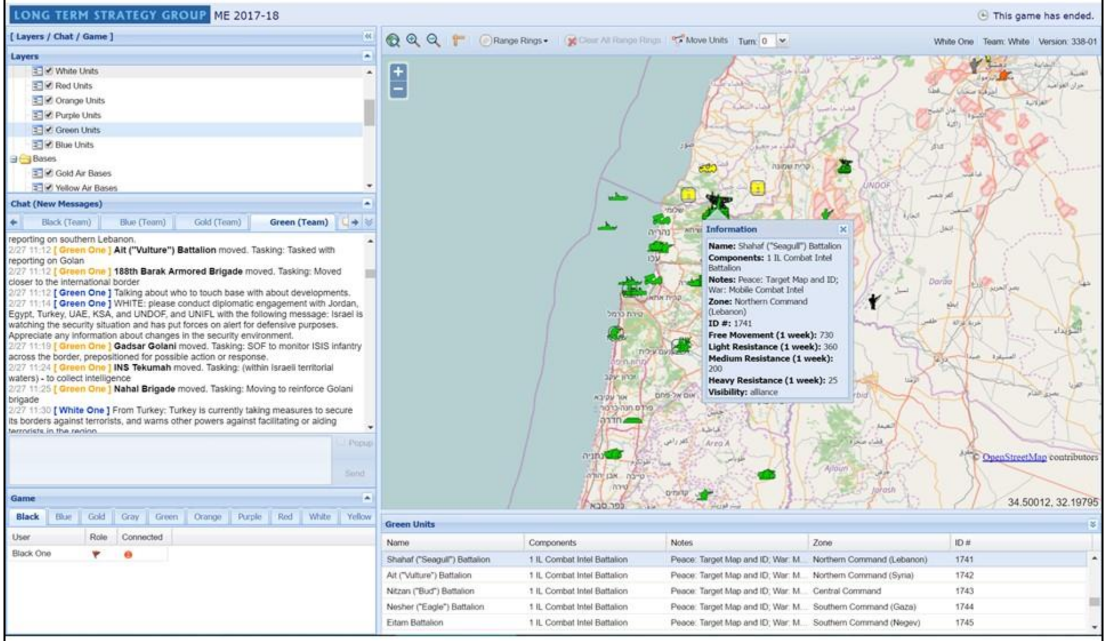
3/10 10:19 [Green One] Proposal: Five party conference (US/Japan/RoK/China/Russia) to arrange the patrol areas to search DPRK vessels.

Information

Name: 8th Artillery Brigade
Components: 1 ROK Artillery Brigade
Notes: ATACMS capable
Zone: DMZ East, VIII Corps (FRoKA)
ID #: 2229
Strike (standoff): 300
Free Movement (1 week): 730
Light Resistance (1 week): 360
Medium Resistance (1 week): 200
Heavy Resistance (1 week): 25
Visibility: alliance

Purple Units

Name	Components	Notes	Zone	ID #
303rd Security Regiment	1 ROK Security Unit		DMZ East, III Corps (FRoKA)	2225
21st Infantry Division	1 ROK Infantry Division		DMZ East, III Corps (FRoKA)	2226
2nd Infantry Division	1 ROK Infantry Division		DMZ East, III Corps (FRoKA)	2227
12th Infantry Division	1 ROK Infantry Division		DMZ East, III Corps (FRoKA)	2228
8th Artillery Brigade	1 ROK Artillery Brigade	ATACMS capable	DMZ East, VIII Corps (FRoKA)	2229



reporting on southern Lebanon.

2/27 11:12 [Green One] **Ait ("Vulture") Battalion** moved. Tasking: Tasked with reporting on Golan

2/27 11:12 [Green One] **188th Barak Armored Brigade** moved. Tasking: Moved closer to the international border

2/27 11:12 [Green One] Talking about who to touch base with about developments.

2/27 11:14 [Green One] WHITE: please conduct diplomatic engagement with Jordan, Egypt, Turkey, UAE, KSA, and UNDOF, and UNIFL with the following message: Israel is watching the security situation and has put forces on alert for defensive purposes. Appreciate any information about changes in the security environment.

2/27 11:19 [Green One] **Gadsar Golani** moved. Tasking: SOF to monitor ISIS infantry across the border, prepositioned for possible action or response.

2/27 11:24 [Green One] **INS Tekumah** moved. Tasking: (within Israeli territorial waters) - to collect intelligence

2/27 11:25 [Green One] **Nahal Brigade** moved. Tasking: Moving to reinforce Golani brigade

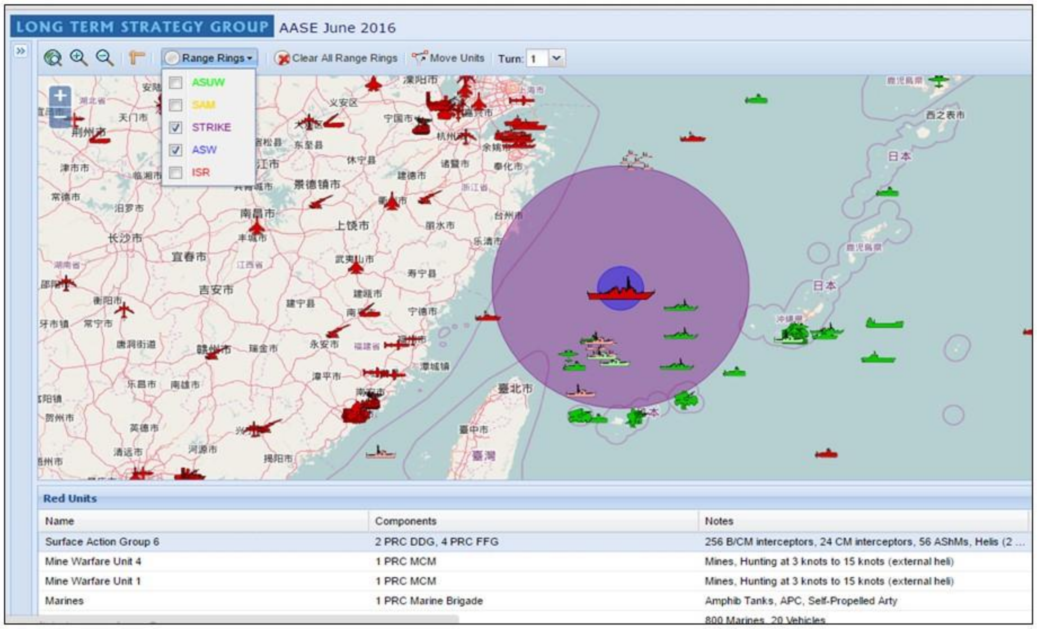
2/27 11:30 [White One] From Turkey: Turkey is currently taking measures to secure its borders against terrorists, and warns other powers against facilitating or aiding terrorists in the region

Information

Name: Shahaf ("Seagull") Battalion
Components: 1 IL Combat Intel Battalion
Notes: Peace: Target Map and ID; War: Mobile Combat Intel
Zone: Northern Command (Lebanon)
ID #: 1741
Free Movement (1 week): 730
Light Resistance (1 week): 360
Medium Resistance (1 week): 200
Heavy Resistance (1 week): 25
Visibility: alliance

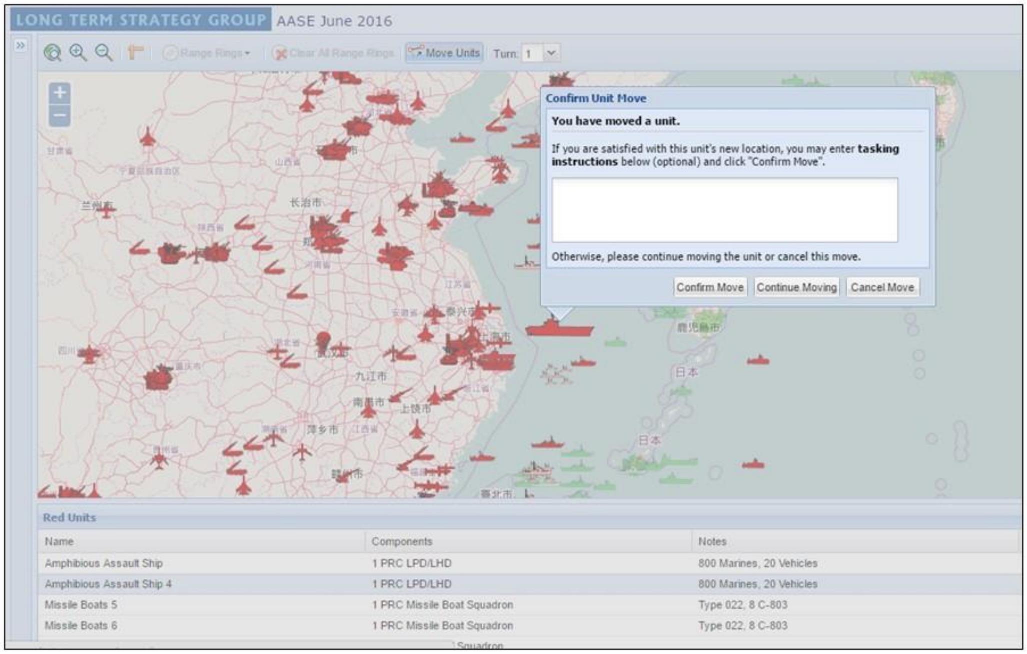
Green Units

Name	Components	Notes	Zone	ID #
Shahaf ("Seagull") Battalion	1 IL Combat Intel Battalion	Peace: Target Map and ID; War: M...	Northern Command (Lebanon)	1741
Ait ("Vulture") Battalion	1 IL Combat Intel Battalion	Peace: Target Map and ID; War: M...	Northern Command (Syria)	1742
Nitzan ("Bud") Battalion	1 IL Combat Intel Battalion	Peace: Target Map and ID; War: M...	Central Command	1743
Nesher ("Eagle") Battalion	1 IL Combat Intel Battalion	Peace: Target Map and ID; War: M...	Southern Command (Gaza)	1744
Eitam Battalion	1 IL Combat Intel Battalion	Peace: Target Map and ID; War: M...	Southern Command (Negev)	1745



Red Units

Name	Components	Notes
Surface Action Group 6	2 PRC DDG, 4 PRC FFG	256 B/CM interceptors, 24 CM interceptors, 56 AShMs, Helis (2 ...
Mine Warfare Unit 4	1 PRC MCM	Mines, Hunting at 3 knots to 15 knots (external heli)
Mine Warfare Unit 1	1 PRC MCM	Mines, Hunting at 3 knots to 15 knots (external heli)
Marines	1 PRC Marine Brigade	Amphib Tanks, APC, Self-Propelled Arty
		800 Marines, 20 Vehicles



Confirm Unit Move

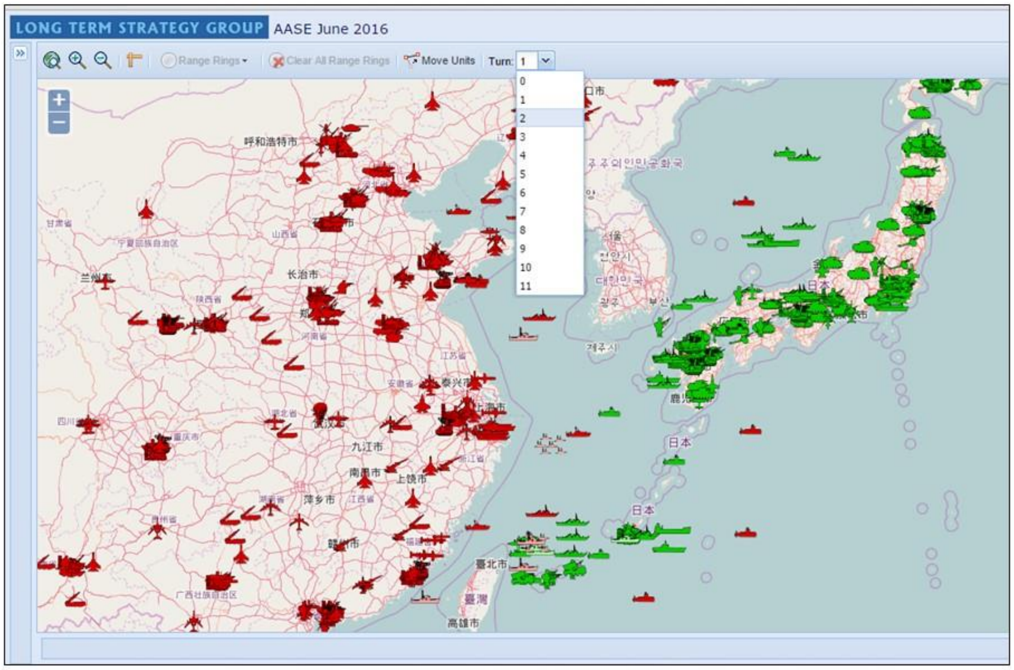
You have moved a unit.

If you are satisfied with this unit's new location, you may enter **tasking instructions** below (optional) and click "Confirm Move".

Otherwise, please continue moving the unit or cancel this move.

Red Units

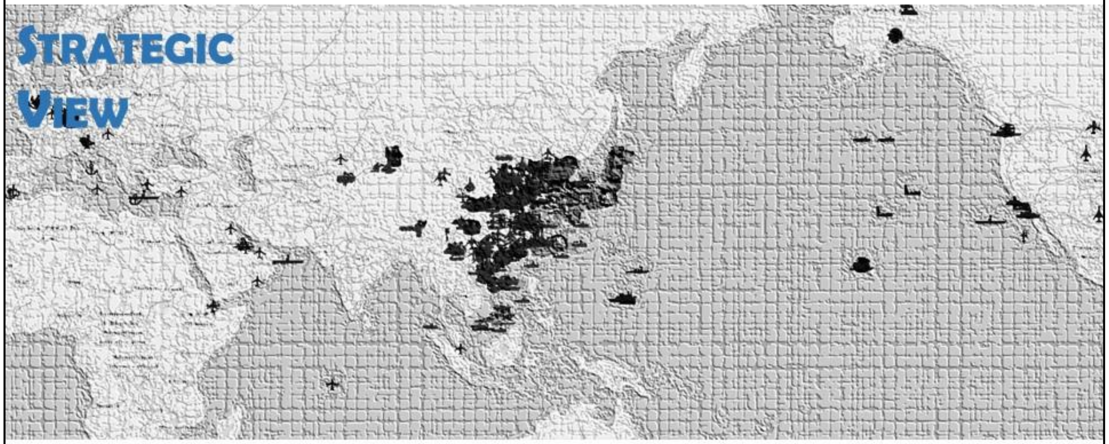
Name	Components	Notes
Amphibious Assault Ship	1 PRC LPD/LHD	800 Marines, 20 Vehicles
Amphibious Assault Ship 4	1 PRC LPD/LHD	800 Marines, 20 Vehicles
Missile Boats 5	1 PRC Missile Boat Squadron	Type 022, 8 C-803
Missile Boats 6	1 PRC Missile Boat Squadron	Type 022, 8 C-803
	Squadron	



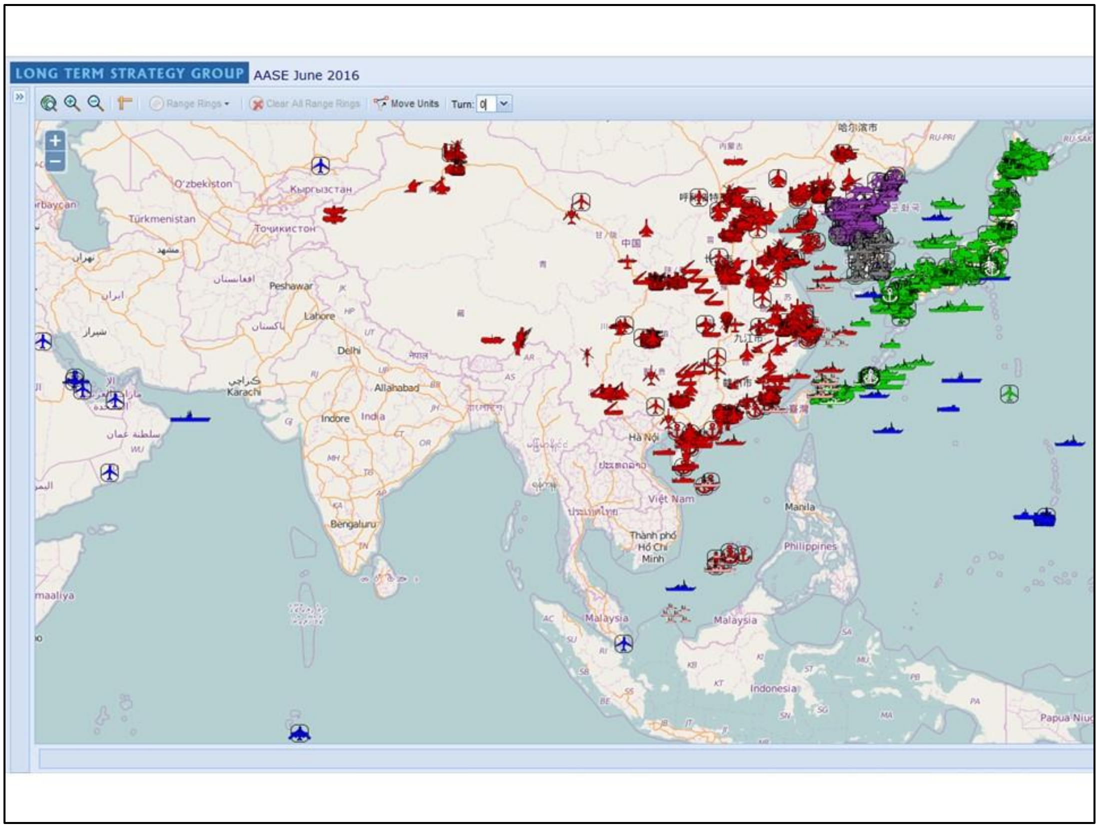
a Marinus game
flipbook

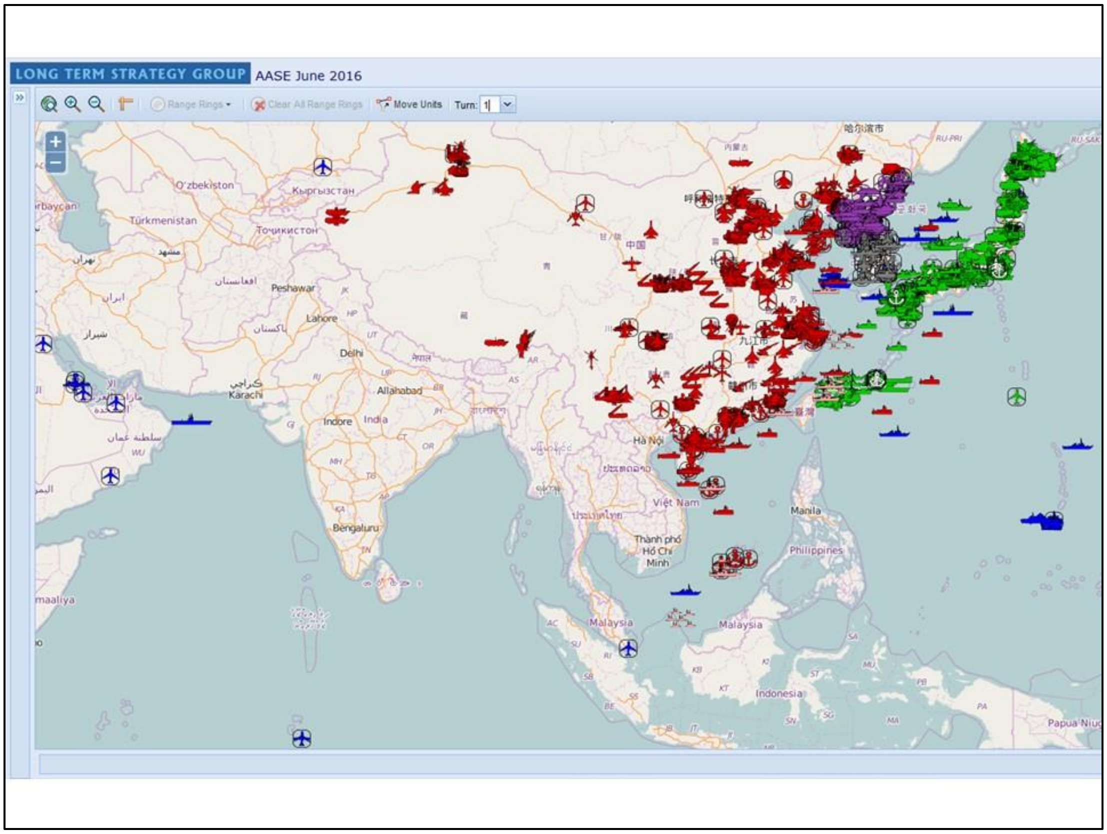
US-Japan Alliance Pol-Mil Wargame

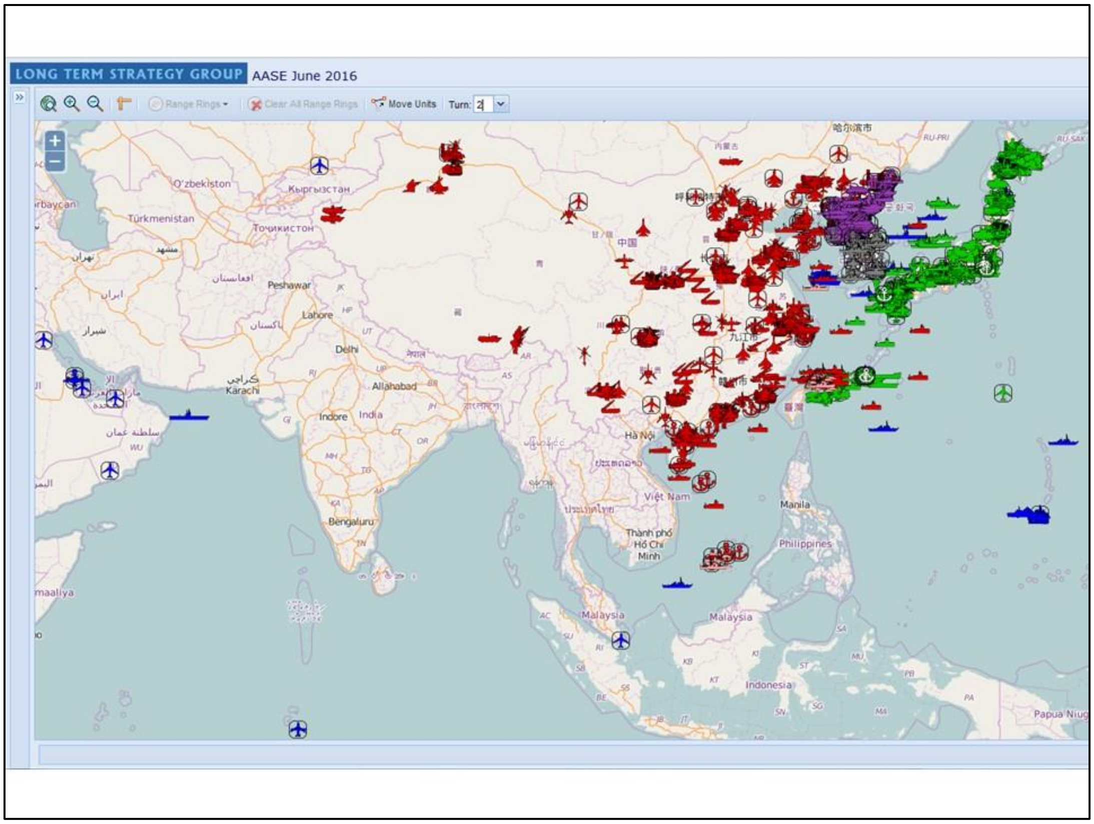
2016

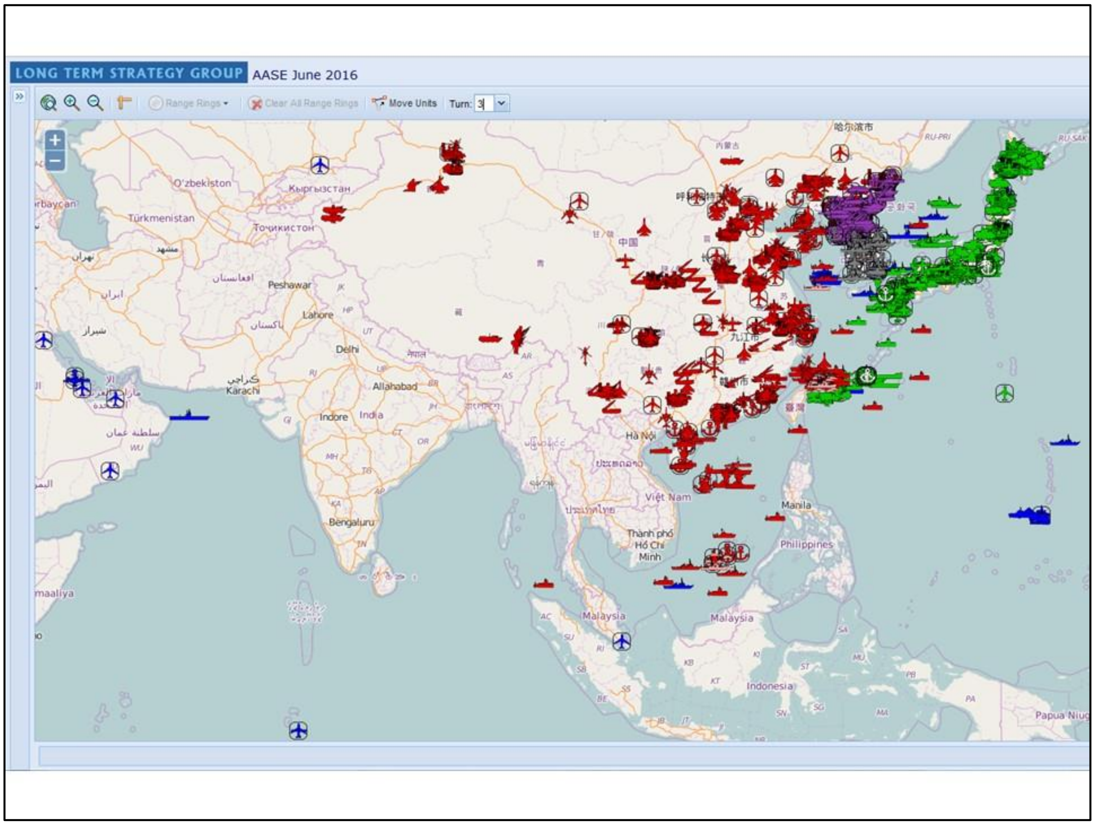


Strategic View

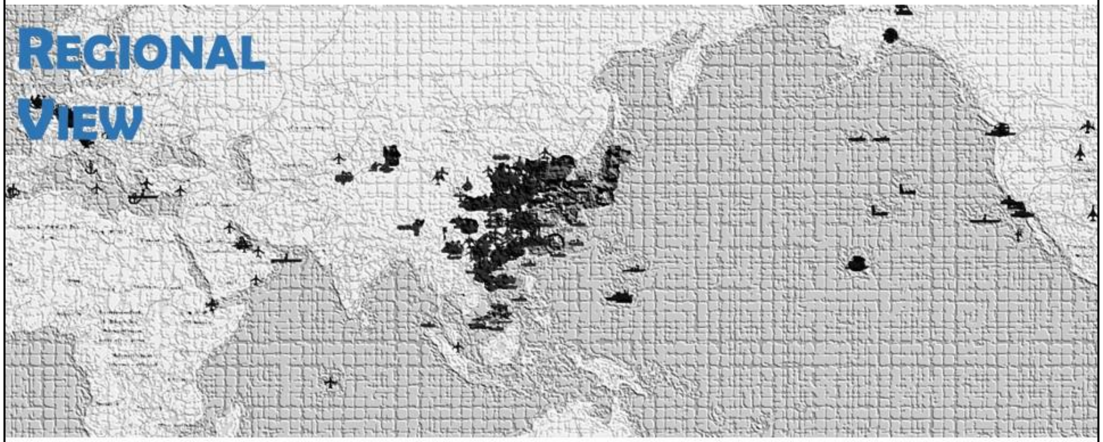

LONG TERM STRATEGY GROUP
AASE June 2016
Range Rings
Clear All Range Rings
Move Units
Turn: 0
O'zbekiston
Кыргызстан
Türkmenistan
Тоҷикистон
Peshawar
Lahore
Delhi
Karachi
Allahabad
Indore
India
Bengaluru
Hà Nội
Việt Nam
Thành phố Hồ Chí Minh
Manila
Philippines
Malaysia
Indonesia
Papua Niu
maaliya

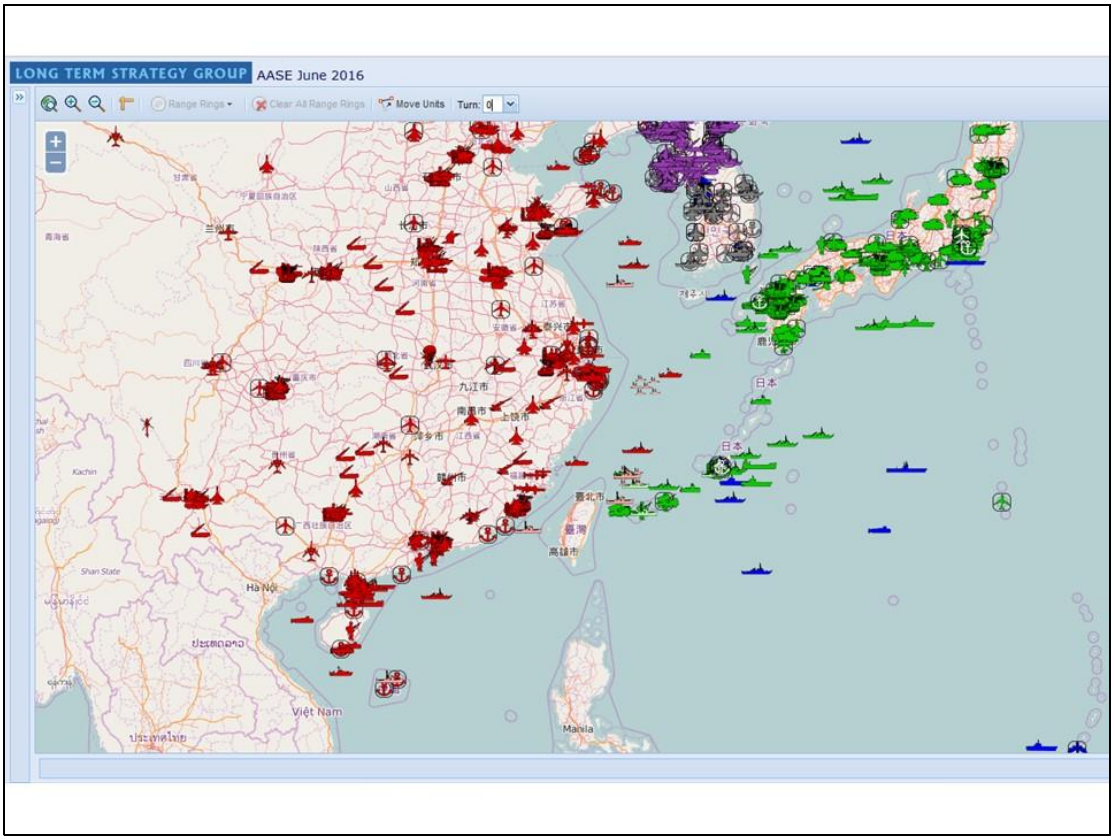

LONG TERM STRATEGY GROUP
AASE June 2016
Range Rings
Clear All Range Rings
Move Units
Turn: 1
O'zbekiston
Кыргызстан
Türkmenistan
Тоҷикистон
Peshawar
Lahore
Delhi
Karachi
Allahabad
Indore
India
Bengaluru
Hà Nội
Việt Nam
Thành phố Hồ Chí Minh
Manila
Philippines
Malaysia
Indonesia
Papua Niu
maaliya


LONG TERM STRATEGY GROUP
AASE June 2016
Range Rings
Clear All Range Rings
Move Units
Turn: 2
O'zbekiston
Türkmenistan
Кыргызстан
Тоҷикистон
Peshawar
Lahore
Delhi
Karachi
Allahabad
Indore
India
Bengaluru
中国
Hà Nội
Việt Nam
Thành phố Hồ Chí Minh
Manila
Philippines
Malaysia
Indonesia
Papua Niug
maaliya

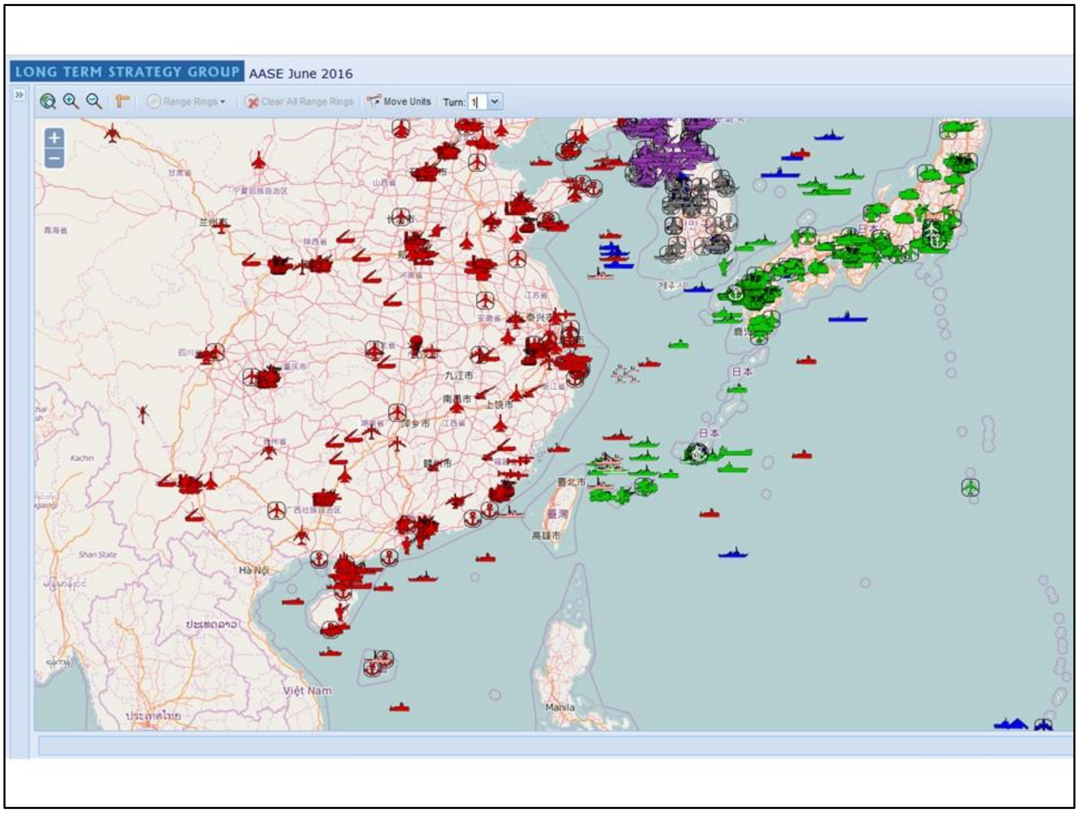

LONG TERM STRATEGY GROUP
AASE June 2016
Range Rings
Clear All Range Rings
Move Units
Turn: 3
O'zbekiston
Türkmenistan
Кыргызстан
Тоҷикистон
Peshawar
Lahore
Delhi
Karachi
Allahabad
Indore
India
Bengaluru
中国
Hà Nội
Việt Nam
Thành phố Hồ Chí Minh
Manila
Philippines
Malaysia
Indonesia
Papua Niug
maaliya

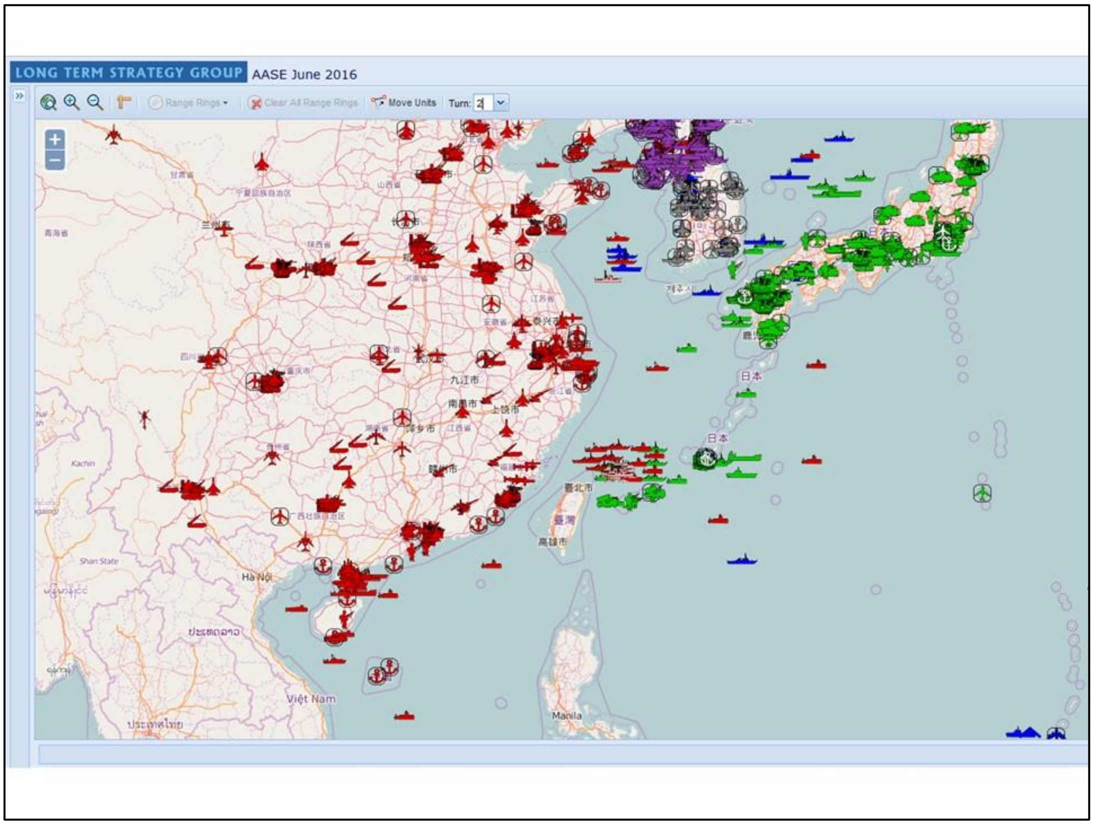
Regional View

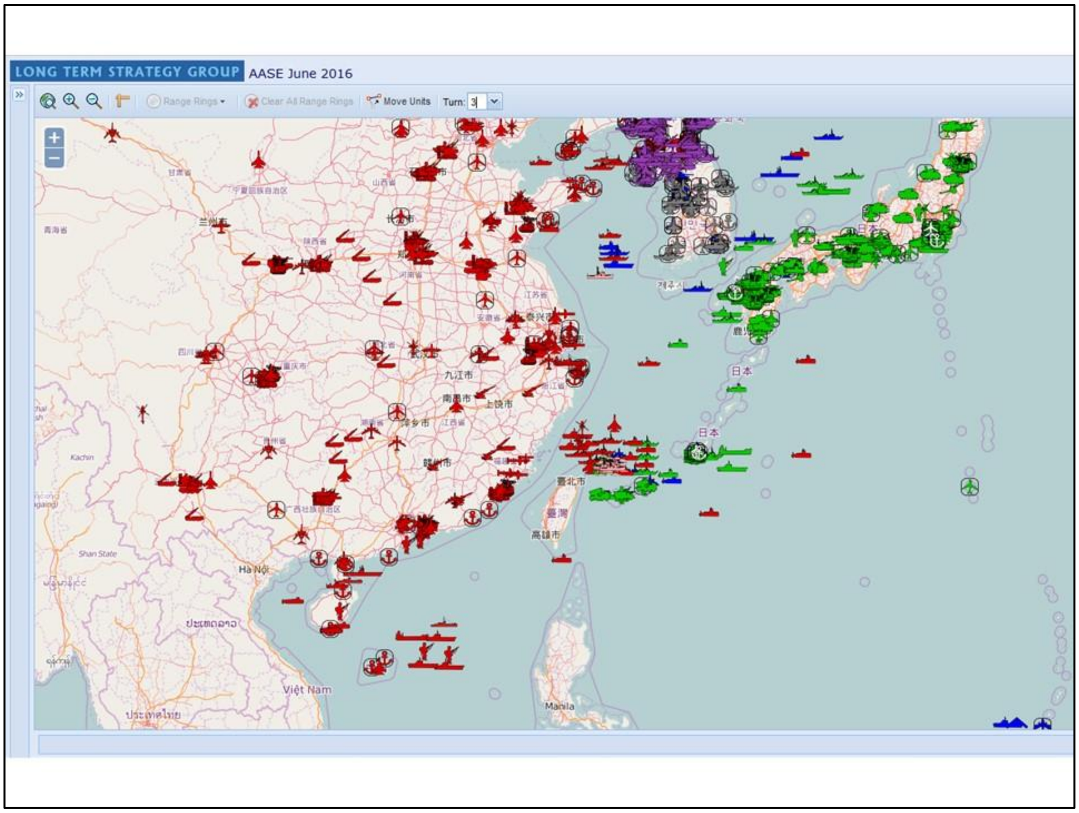




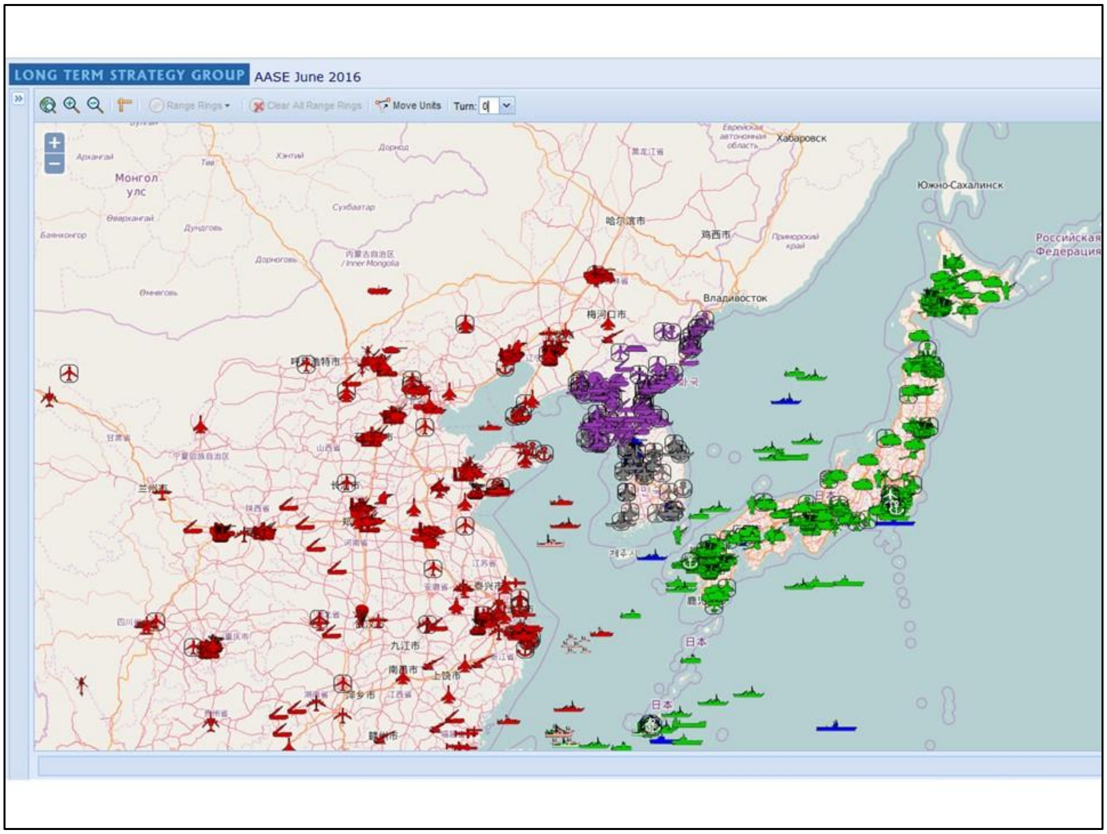
LONG TERM STRATEGY GROUP AASE June 2016


LONG TERM STRATEGY GROUP
AASE June 2016
Range Rings
Clear All Range Rings
Move Units
Turn: 1
甘肃省
兰州
青海省
四川省
九江市
南昌市
上饶市
萍乡市
台北市
台湾
高雄市
日本
Kachin
Shan State
Hà Nội
ປະເທດລາວ
Việt Nam
ประเทศไทย
Manila

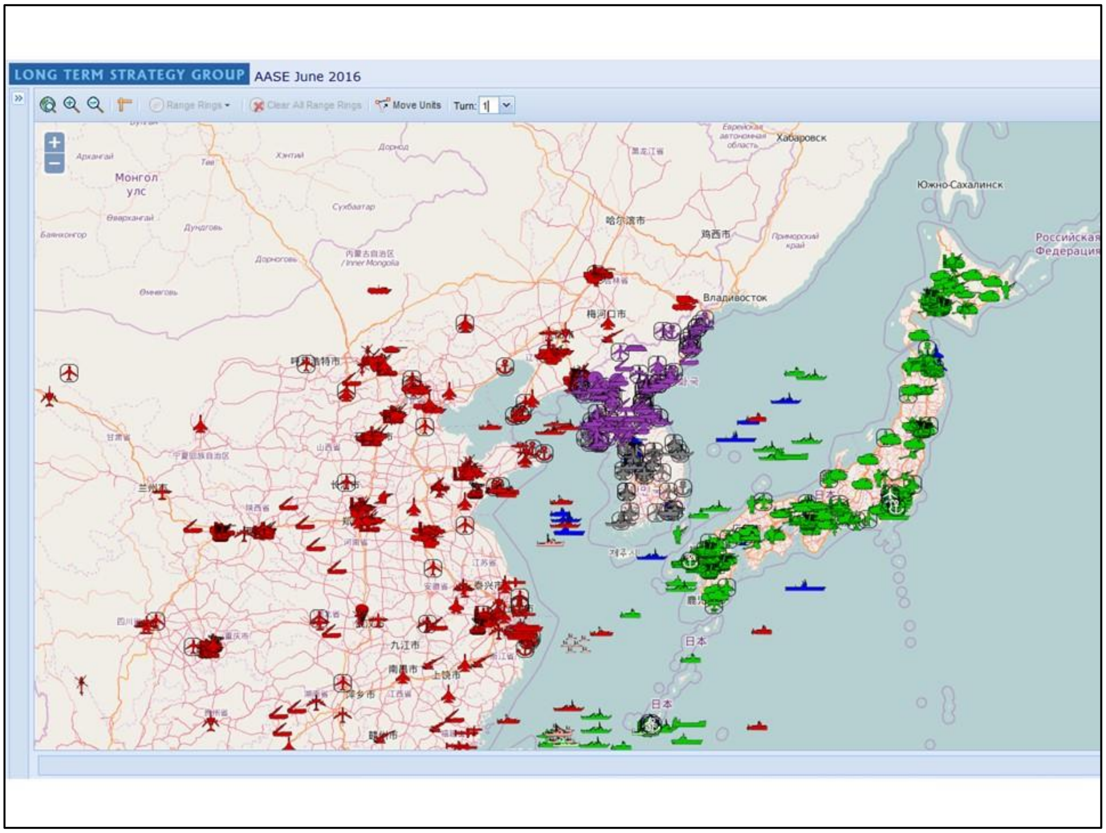

LONG TERM STRATEGY GROUP
AASE June 2016
Range Rings
Clear All Range Rings
Move Units
Turn: 2
甘肃省
兰州
青海省
四川省
九江市
南昌市
上饶市
萍乡市
台北市
台湾
高雄市
日本
Kachin
Shan State
Hà Nội
ປະເທດລາວ
Việt Nam
ประเทศไทย
Manila



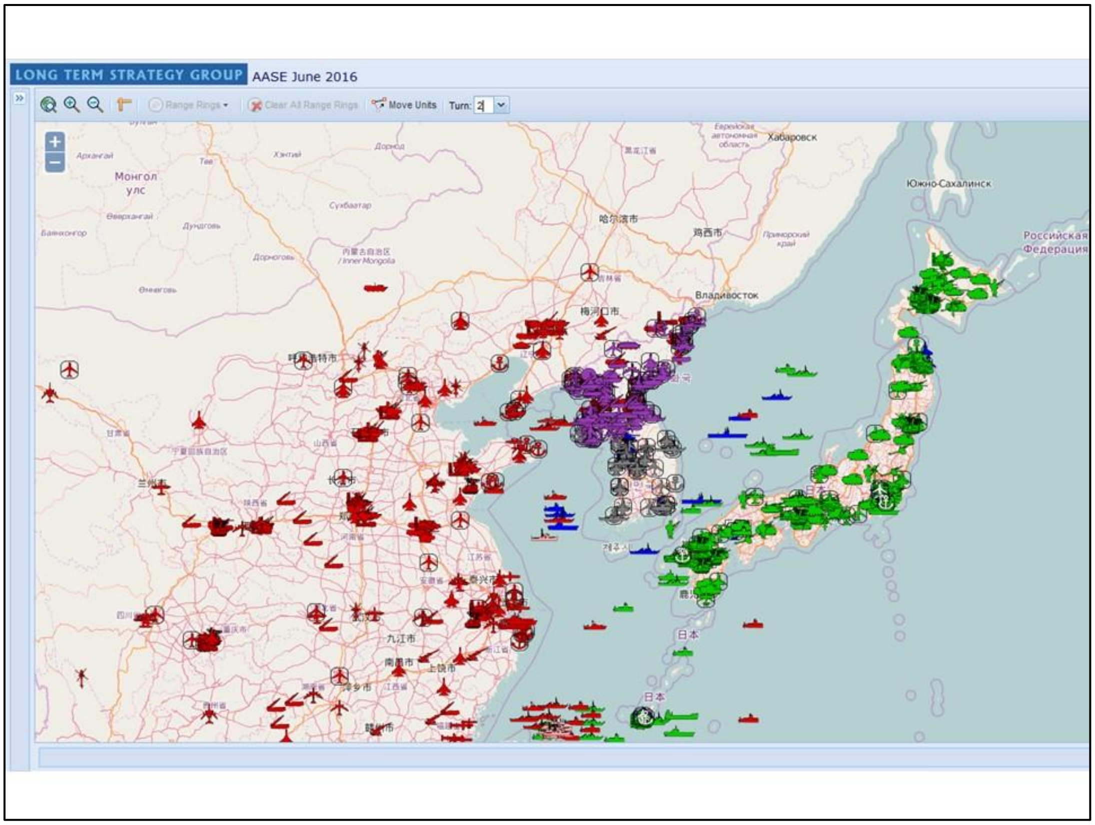
Korean Peninsula Theater View


LONG TERM STRATEGY GROUP AASE June 2016

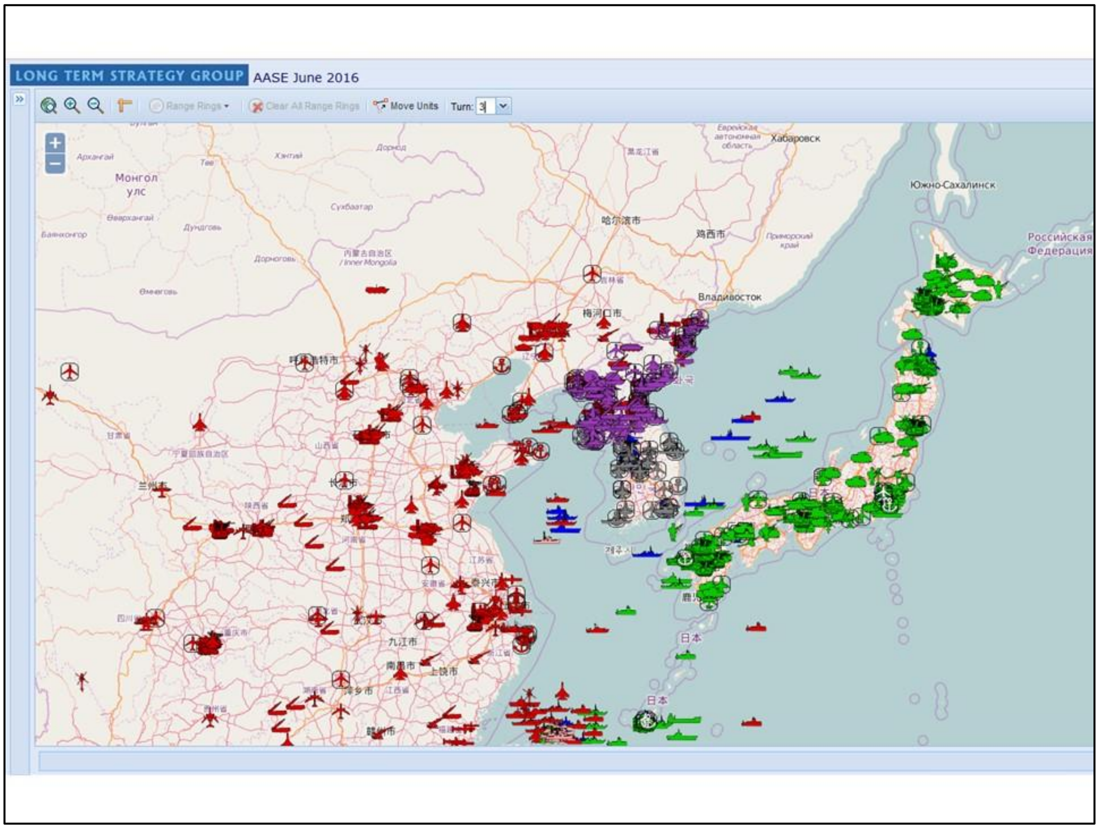
Turn: 0


LONG TERM STRATEGY GROUP AASE June 2016

Turn: 1

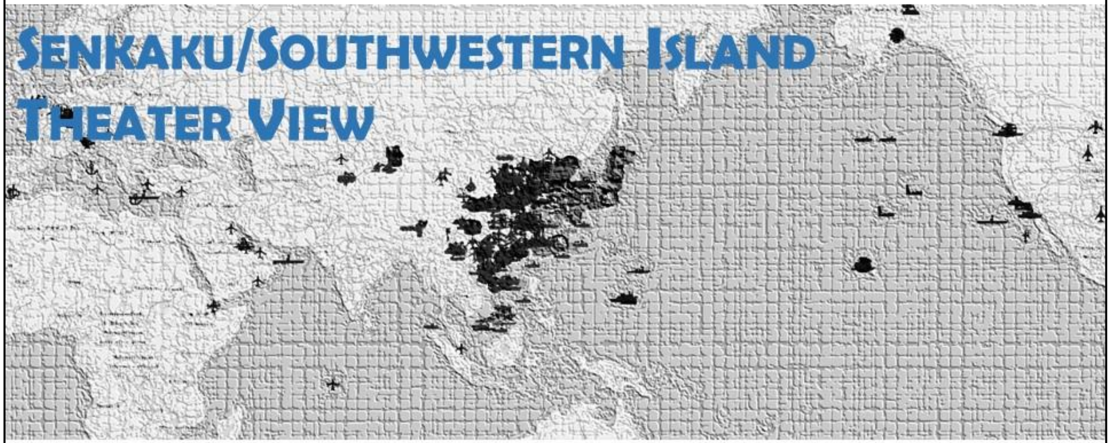

LONG TERM STRATEGY GROUP
AASE June 2016
Range Rings
Clear All Range Rings
Move Units
Монгол улс
Сухбаатар
Хабаровск
Южно-Сахалинск
Российская Федерация
Владивосток
哈尔滨市
鸡西市
梅河口市
兰州市
九江市
南昌市
上饶市
日本

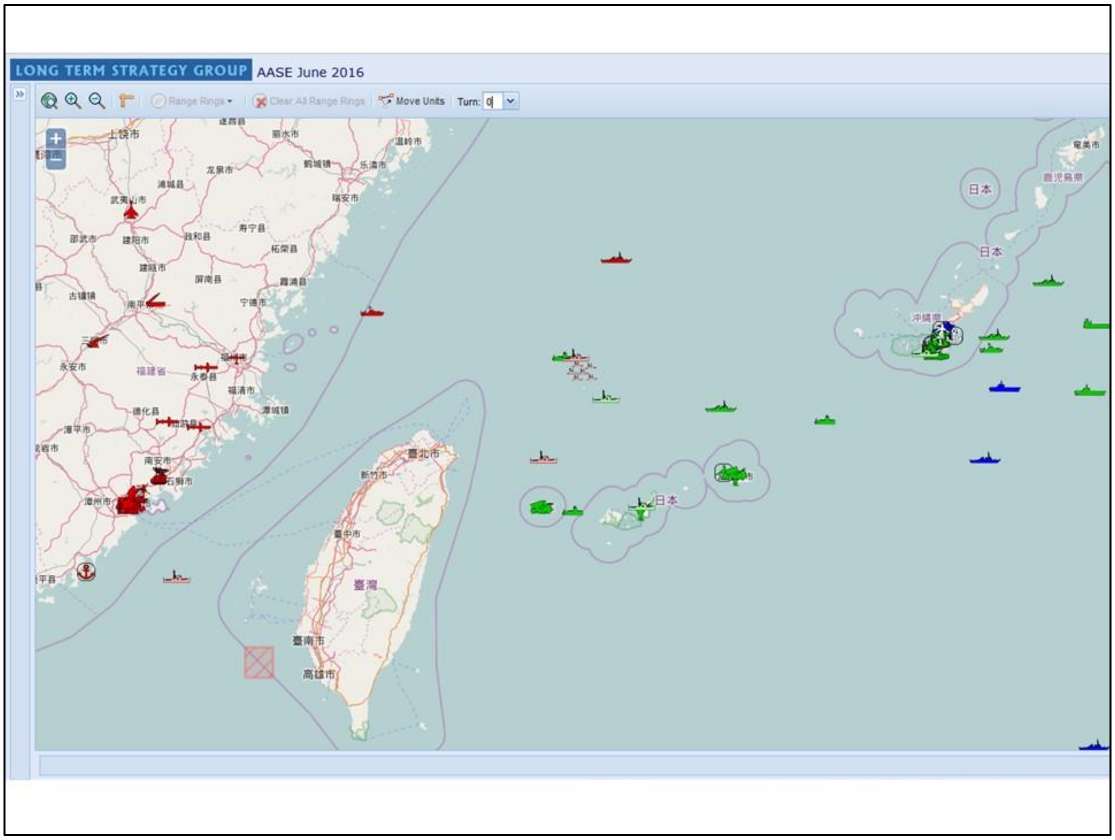
Turn: 2

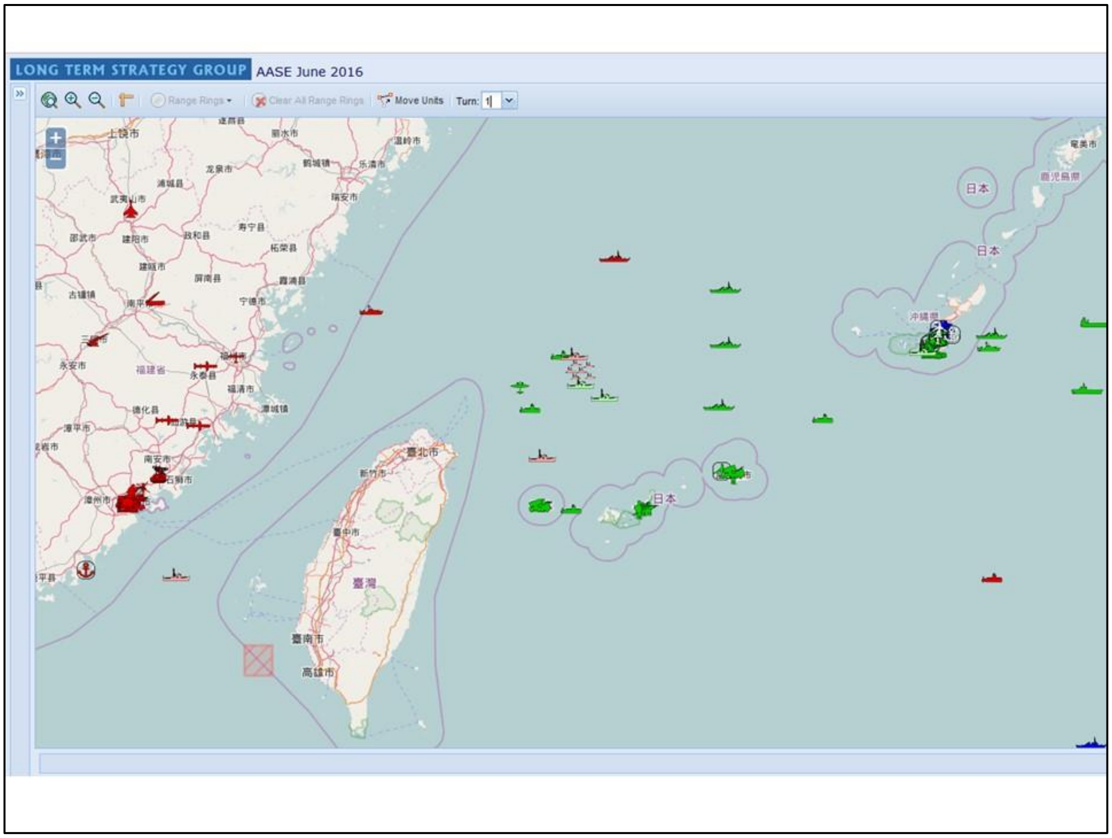

LONG TERM STRATEGY GROUP
AASE June 2016
Range Rings
Clear All Range Rings
Move Units
Монгол улс
Сухбаатар
Хабаровск
Южно-Сахалинск
Российская Федерация
Владивосток
哈尔滨市
鸡西市
梅河口市
兰州市
九江市
南昌市
上饶市
日本

Turn: 3

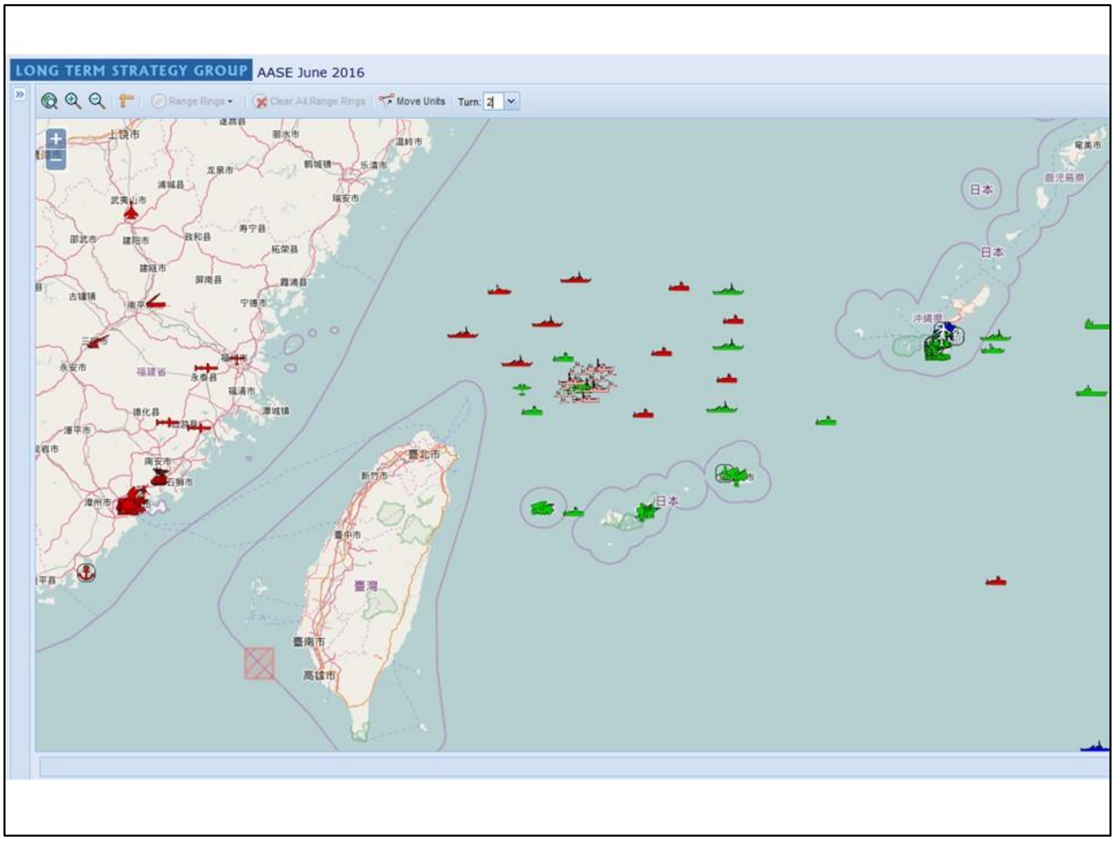
Senkaku/Southwestern Island Theater View



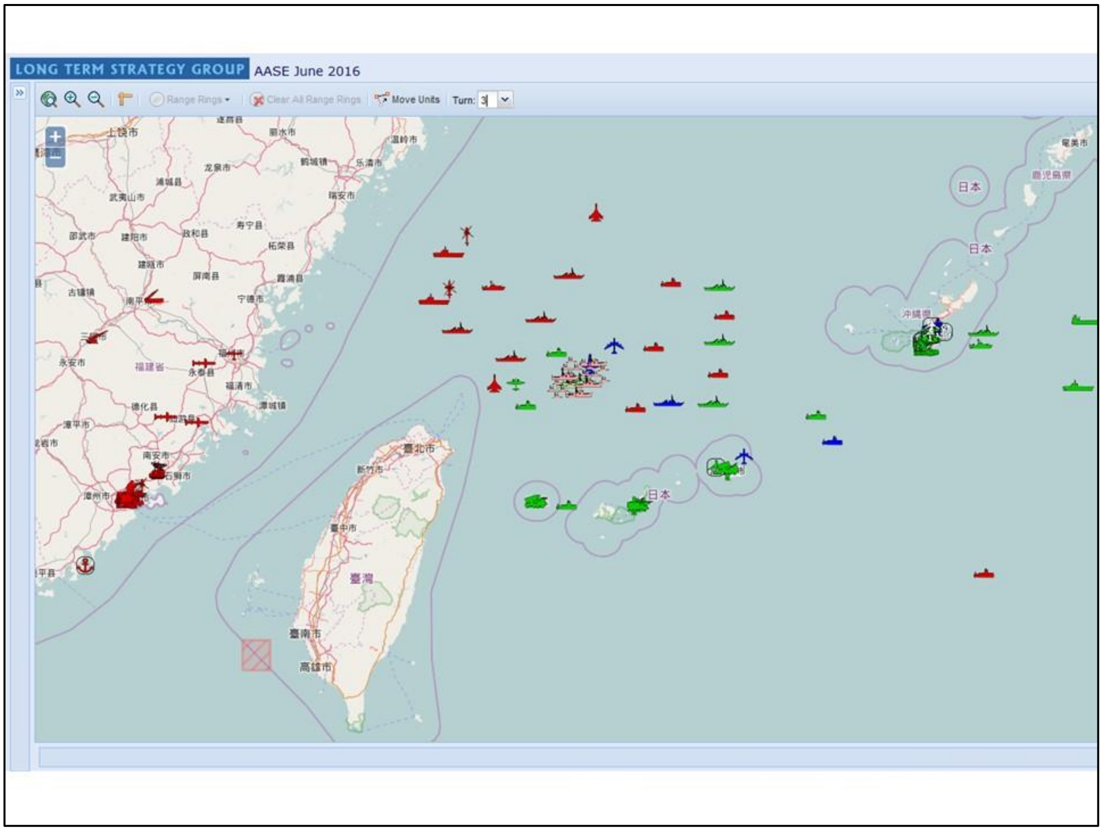


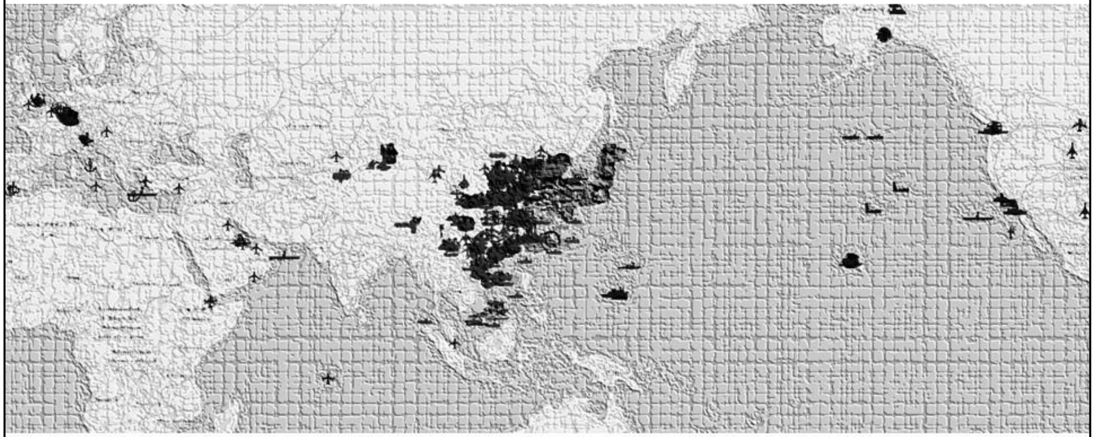

LONG TERM STRATEGY GROUP
AASE June 2016
Range Rings
Clear All Range Rings
Move Units
福建省
臺北市
新竹市
臺中市
臺灣
臺南市
高雄市
日本
沖縄県
鹿児島県
奄美市

Turn: 1


LONG TERM STRATEGY GROUP
AASE June 2016
Range Rings
Clear All Range Rings
Move Units
福建省
臺北市
新竹市
臺中市
臺灣
臺南市
高雄市
日本
沖縄県
鹿児島県
奄美市

Turn: 2


LONG TERM STRATEGY GROUP
AASE June 2016
Range Rings
Clear All Range Rings
Move Units
Turn: 3
上饶市
丽水市
温岭市
龙泉市
乐清市
瑞安市
浦城县
武夷山市
寿宁县
福建省
永安市
福清市
臺北市
新竹市
臺中市
臺灣
臺南市
高雄市
日本
沖縄県
鹿児島県
奄美市



5. Panel 3: Applications

Discussion Summary

Kathleen Conley discussed the need for C2 agility to successfully cope with changes in circumstances. She presented a methodology for designing and altering the command and C2 approach to fit the chosen operational approach. This includes changing the distribution of information, authority, and patterns of interaction. She identified tools to measure the effectiveness of particular C2 arrangements and to enable iterative improvements to the C2 approach.

Diane Schroer presented a risk assessment model for Navy operations and systems that depended upon large quantities of data, but which provided compelling evidence of what underlay failures and demonstrated where to make improvements. She emphasized how complex information is needed to overcome beliefs about extant practices.

Dr. Stephen Downes-Martin discussed methods for assessing what would be required to affect adversary decisions.

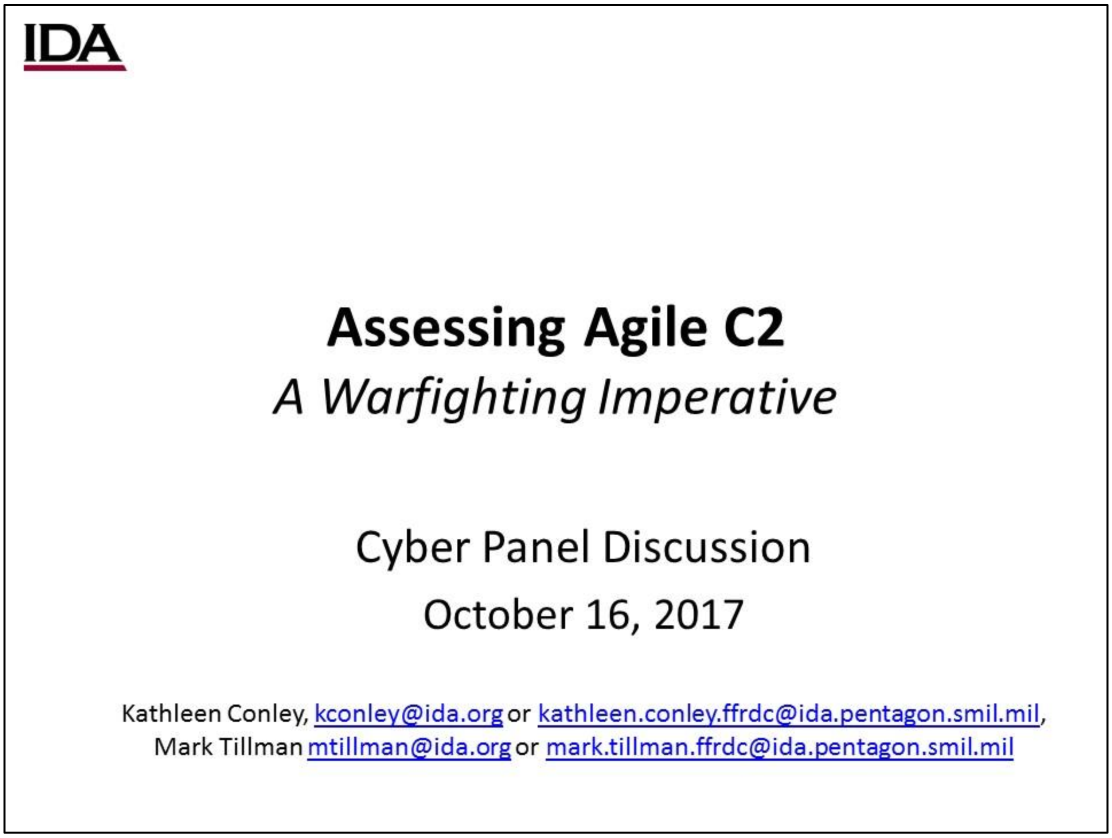
A. Kathleen Conley: Assessing Agile C2 - A Command Imperative

Presentation Summary

Ms. Conley presented an overview of the activities that together define the instantiation of a “C2 Approach,” which must be tailored to the chosen operational approach to prevail in complex or ill-structured environments. Because information systems, artificial intelligence, and cyber operations can profoundly influence the circumstances of military operations, it is important for participants in wargames and exercises to be able to explicitly understand, assess, and, if necessary, alter the C2 approach in use. Operational design principles, adapted for use in creating and updating a C2 approach that is appropriate to the circumstances, empower staffs to alter their approach in the moment to improve organizational effectiveness.

Ms. Conley also pointed out that IDA recently published a handbook that enables consideration of these factors in a structured way. The handbook addresses the concept of C2 Agility. The concept is consistent with and puts into practice the joint command and control fundamentals of Joint Publication 1, (Doctrine for the Armed Forces of the United States) (25 March 2013).

A key first step in achieving Agile C2 is the Commander’s issuance of C2 approach guidance linked to the purpose of the operation being war-gamed or exercised. This alerts the staff to the fact that C2 is not fixed but rather is a tool to enable effective decision-making. As the operational environment changes, the staff then considers what it needs to understand, identifies who has that information, and then ensures that a relationship exists that permits the information to flow to the appropriate decision maker. By iteratively assessing whether the C2 activities are effective (doing the right thing) and efficient (doing the thing right), the approach to C2 can be continually adjusted so as to accomplish the purpose of the operation.



IDA

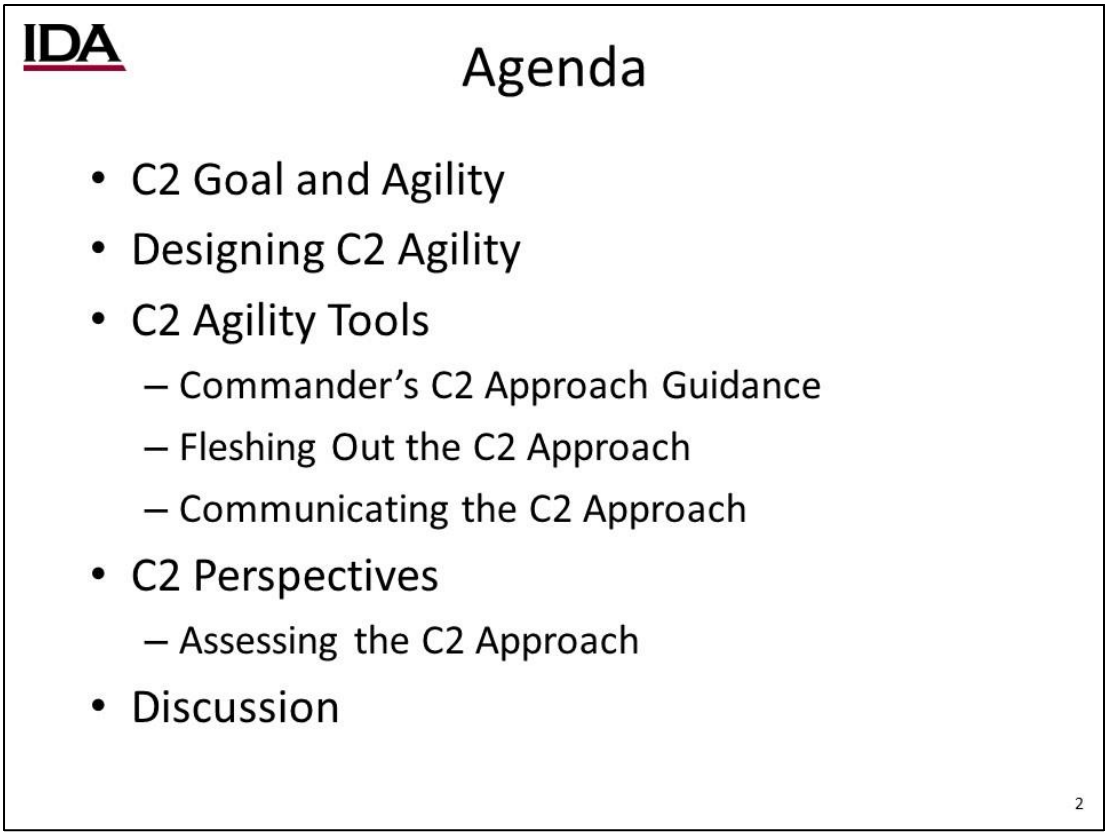
Assessing Agile C2

A Warfighting Imperative

Cyber Panel Discussion

October 16, 2017

Kathleen Conley, kconley@ida.org or kathleen.conley.ffrdc@ida.pentagon.smil.mil,
Mark Tillman mtillman@ida.org or mark.tillman.ffrdc@ida.pentagon.smil.mil

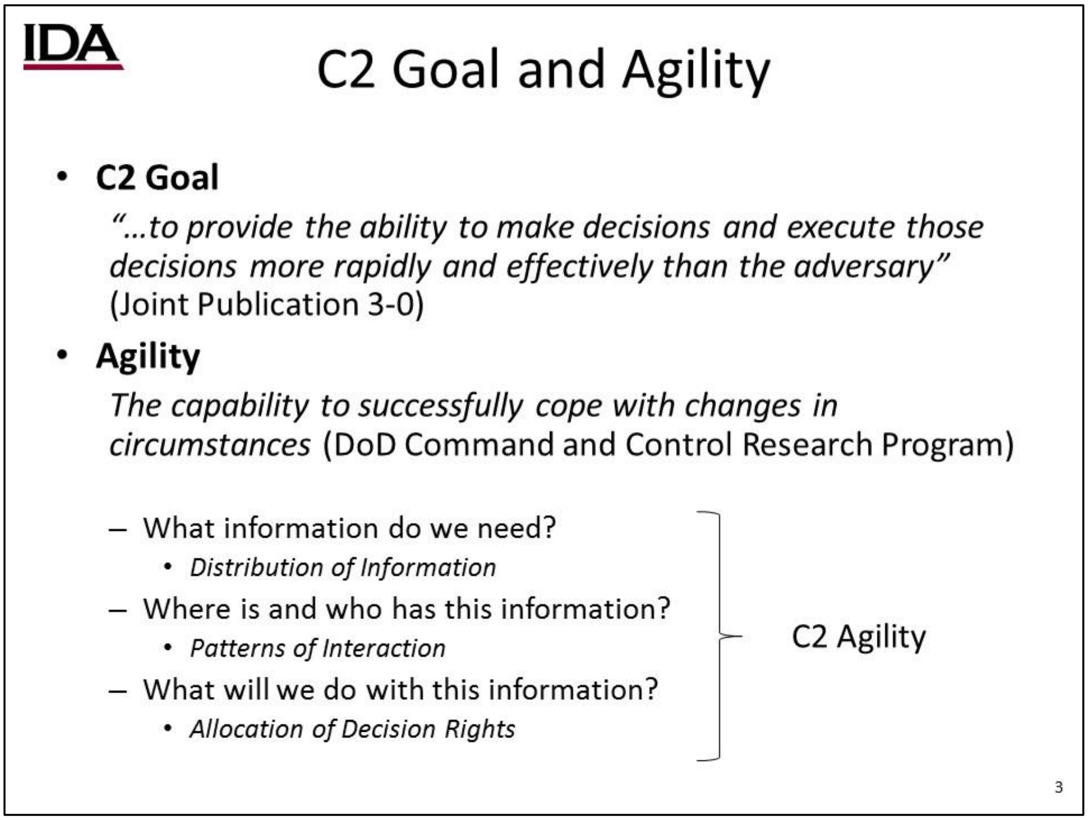


IDA

Agenda

- C2 Goal and Agility
- Designing C2 Agility
- C2 Agility Tools
  - Commander's C2 Approach Guidance
  - Fleshing Out the C2 Approach
  - Communicating the C2 Approach
- C2 Perspectives
  - Assessing the C2 Approach
- Discussion

2



IDA

C2 Goal and Agility

- **C2 Goal**

  "...to provide the ability to make decisions and execute those decisions more rapidly and effectively than the adversary" (Joint Publication 3-0)

- **Agility**

  The capability to successfully cope with changes in circumstances (DoD Command and Control Research Program)

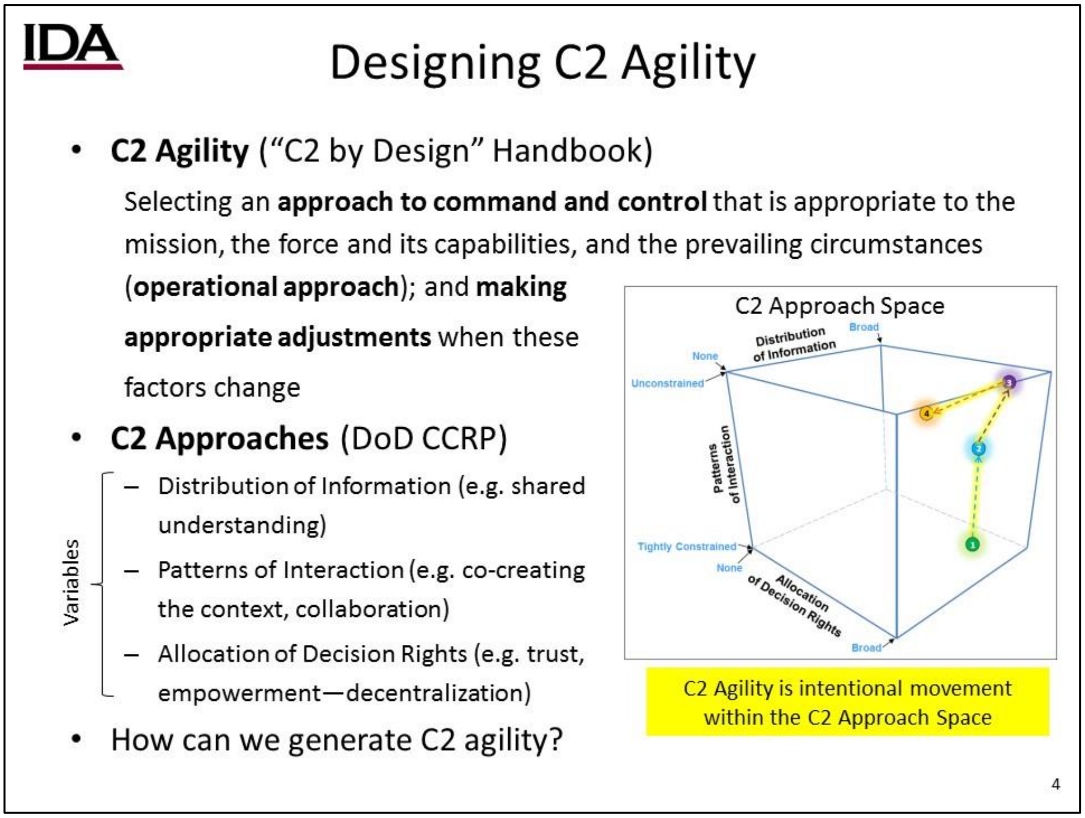
  – What information do we need?
    - *Distribution of Information*

  – Where is and who has this information?
    - *Patterns of Interaction*

  – What will we do with this information?
    - *Allocation of Decision Rights*

C2 Agility

3



IDA

Designing C2 Agility

- **C2 Agility** ("C2 by Design" Handbook)

  Selecting an **approach to command and control** that is appropriate to the mission, the force and its capabilities, and the prevailing circumstances (**operational approach**); and **making appropriate adjustments** when these factors change

- **C2 Approaches** (DoD CCRP)

  Variables
  – Distribution of Information (e.g. shared understanding)
  – Patterns of Interaction (e.g. co-creating the context, collaboration)
  – Allocation of Decision Rights (e.g. trust, empowerment—decentralization)

- How can we generate C2 agility?

C2 Approach Space

C2 Agility is intentional movement within the C2 Approach Space

4

IDA Tool: Commander's C2 Approach Guidance[2]

Designing C2 Agility starts with the Commander:

- The commander should convey that the current C2 approach may not be appropriate to the current or anticipated circumstances and **may need to change**
- Guidance should also include the commander's **understanding of the overarching purpose** for the ongoing or pending military operation
- Considering this purpose, the commander should **describe the scope and breadth of the organizations and other entities whose actions must be harmonized to achieve that purpose**

Approved for public release; distribution is unlimited.

IDA

INSTITUTE FOR DEFENSE ANALYSES

C2 by Design:
Putting Command and Control Agility
Theory Into Practice
Version 2.0

David S. Alberts
Kathleen M. Conley
Waldo D. Freeman
James H. Kurtz
Mark E. Tillman

September 2015
Approved for public release;
distribution is unlimited.
Log: H 15-000478
IDA Document NS D-5814

INSTITUTE FOR DEFENSE ANALYSES
4850 Mark Center Drive
Alexandria, Virginia 22311-1882

Approved for public release; distribution is unlimited.

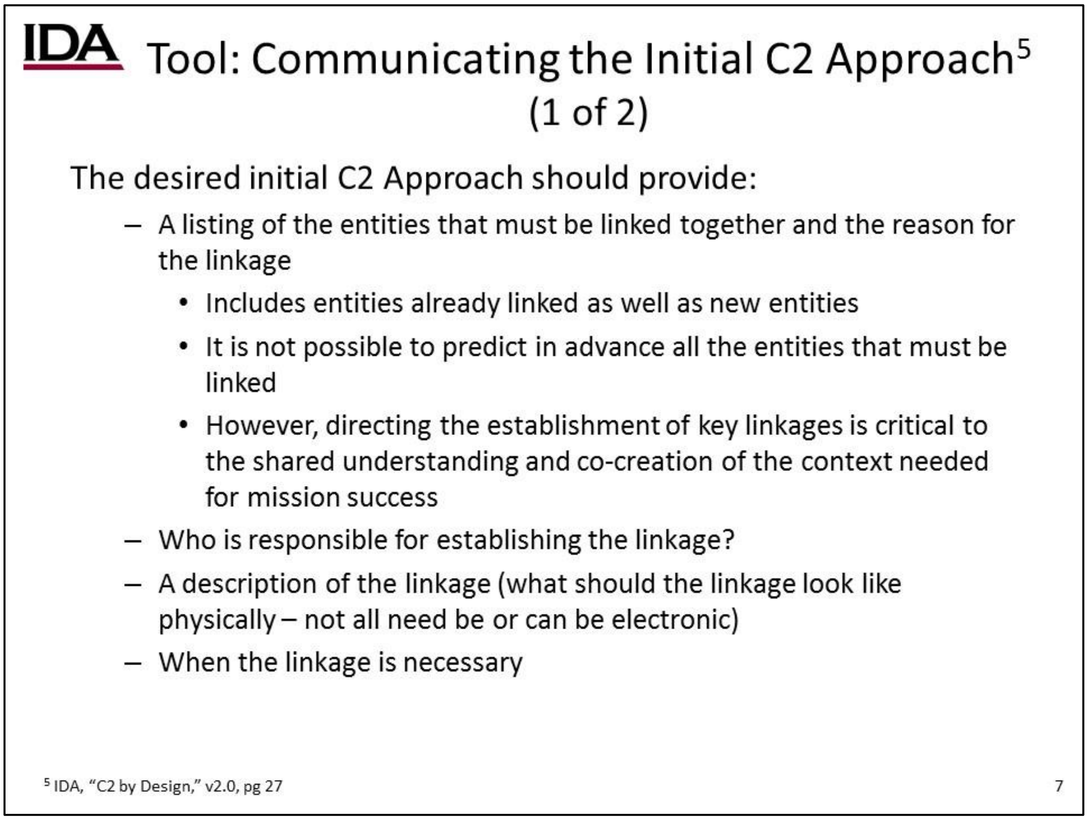
[2] Institute for Defense Analyses (IDA), "C2 by Design: Putting Command and Control Agility Theory into Practice," v2.0, September 2015, pg 23, available at http://www.dodccrp-test.org/c2-agility

IDA Tool: Fleshing Out the C2 Approach[4]

The commander's staff, subordinate commanders, and their staffs should seek answers to the following with respect to specific future decisions:

- What are we seeking to understand; how does this understanding relate to current or planned operations (relevant yet missing aspects of the circumstances and supported decisions); and how is it related to decision making?
- What then are the informational needs?
- Who might have the needed information or where do we expect to find it?
- What relationships exist with those that have or are expected to have the needed information?
- Do new relationships need to be established in order to gain the needed information?
- What types of information will need to be exchanged and how exactly will the exchange be accomplished?
- Do we have release authority to share this information in the manner expected? Do other entities have the authority to share with us?
- Are communications established and tested to ensure information can be shared in the manner expected?
- How will this new information be compiled and presented to meet the informational and decisional needs?
- How will this information support decisions necessary to enable current or future operations?

[4] IDA, "C2 by Design," v2.0, pp 24-25



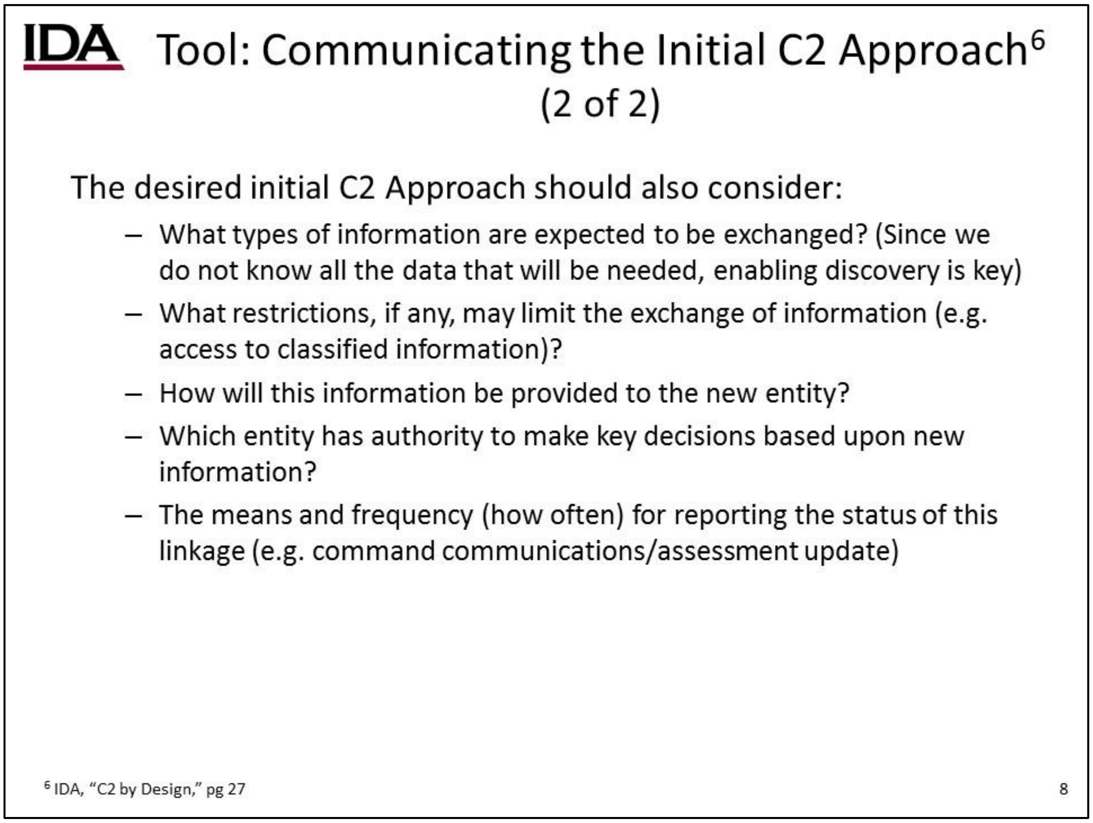
IDA Tool: Communicating the Initial C2 Approach[5] (1 of 2)

The desired initial C2 Approach should provide:

- A listing of the entities that must be linked together and the reason for the linkage
  - Includes entities already linked as well as new entities
  - It is not possible to predict in advance all the entities that must be linked
  - However, directing the establishment of key linkages is critical to the shared understanding and co-creation of the context needed for mission success
- Who is responsible for establishing the linkage?
- A description of the linkage (what should the linkage look like physically – not all need be or can be electronic)
- When the linkage is necessary

[5] IDA, "C2 by Design," v2.0, pg 27

7



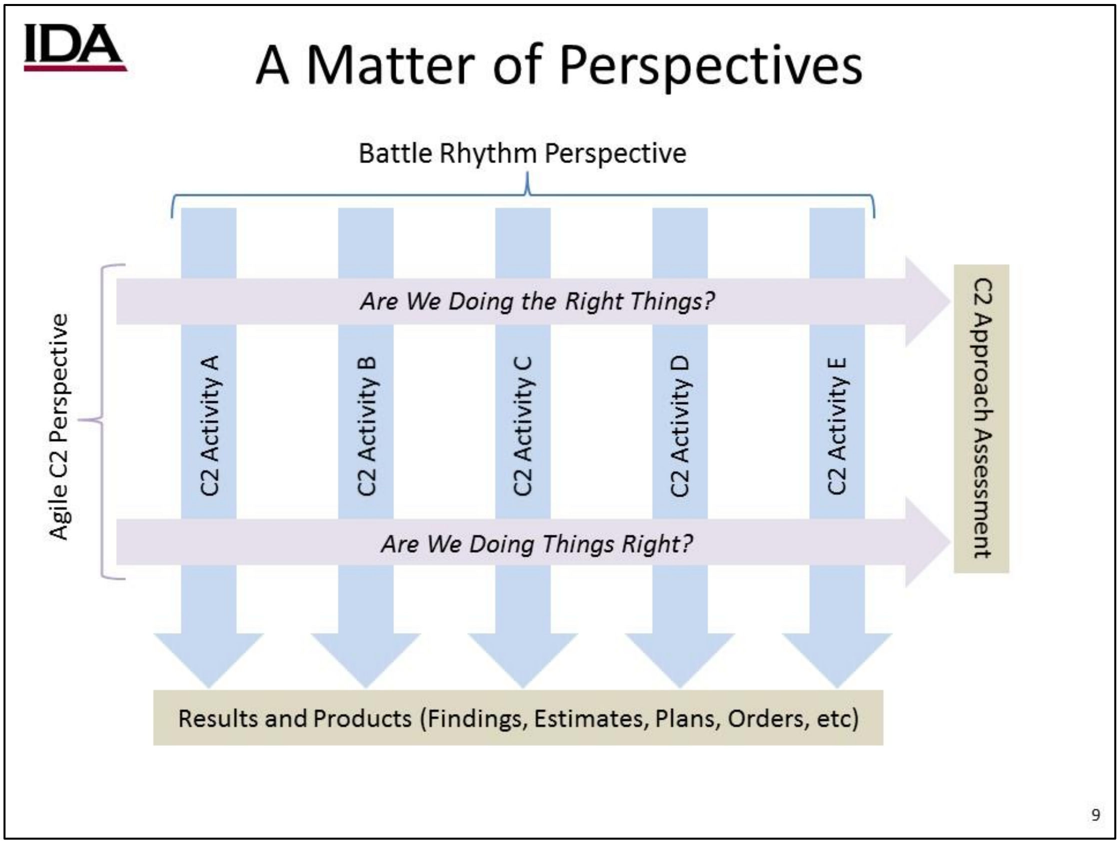
IDA Tool: Communicating the Initial C2 Approach[6] (2 of 2)

The desired initial C2 Approach should also consider:

- What types of information are expected to be exchanged? (Since we do not know all the data that will be needed, enabling discovery is key)
- What restrictions, if any, may limit the exchange of information (e.g. access to classified information)?
- How will this information be provided to the new entity?
- Which entity has authority to make key decisions based upon new information?
- The means and frequency (how often) for reporting the status of this linkage (e.g. command communications/assessment update)

[6] IDA, "C2 by Design," pg 27

8



IDA

A Matter of Perspectives

Battle Rhythm Perspective

Agile C2 Perspective

Are We Doing the Right Things?

C2 Activity A

C2 Activity B

C2 Activity C

C2 Activity D

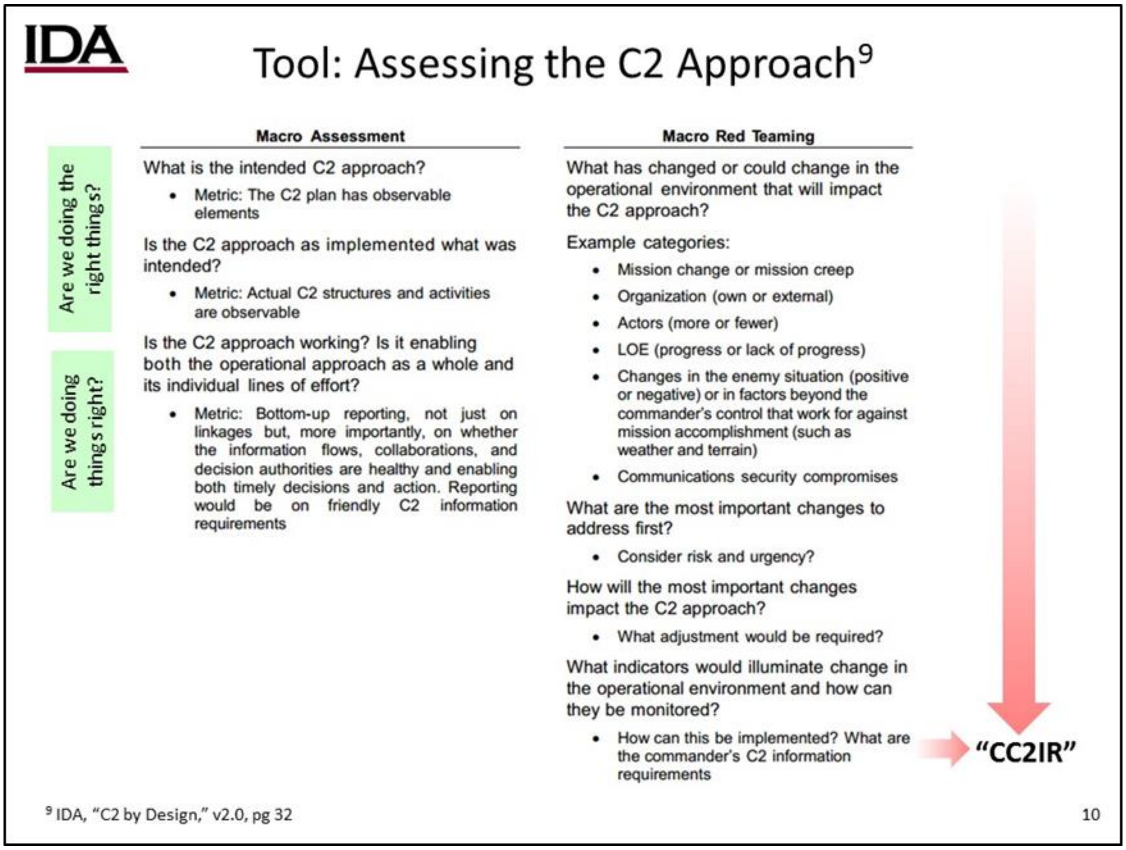
C2 Activity E

Are We Doing Things Right?

C2 Approach Assessment

Results and Products (Findings, Estimates, Plans, Orders, etc)

9



IDA

Tool: Assessing the C2 Approach[9]

Are we doing the right things?

Are we doing things right?

Macro Assessment

What is the intended C2 approach?

- Metric: The C2 plan has observable elements

Is the C2 approach as implemented what was intended?

- Metric: Actual C2 structures and activities are observable

Is the C2 approach working? Is it enabling both the operational approach as a whole and its individual lines of effort?

- Metric: Bottom-up reporting, not just on linkages but, more importantly, on whether the information flows, collaborations, and decision authorities are healthy and enabling both timely decisions and action. Reporting would be on friendly C2 information requirements

Macro Red Teaming

What has changed or could change in the operational environment that will impact the C2 approach?

Example categories:

- Mission change or mission creep
- Organization (own or external)
- Actors (more or fewer)
- LOE (progress or lack of progress)
- Changes in the enemy situation (positive or negative) or in factors beyond the commander's control that work for against mission accomplishment (such as weather and terrain)
- Communications security compromises

What are the most important changes to address first?

- Consider risk and urgency?

How will the most important changes impact the C2 approach?

- What adjustment would be required?

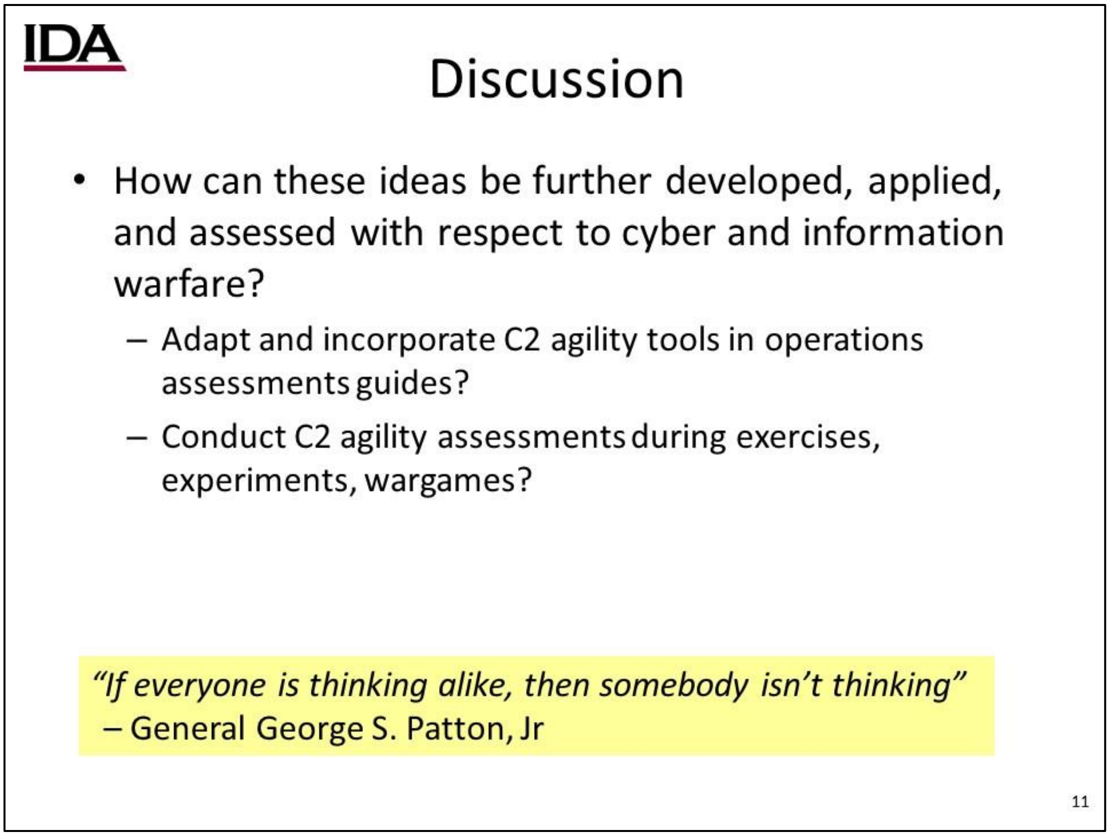
What indicators would illuminate change in the operational environment and how can they be monitored?

- How can this be implemented? What are the commander's C2 information requirements

"CC2IR"

[9] IDA, "C2 by Design," v2.0, pg 32

10

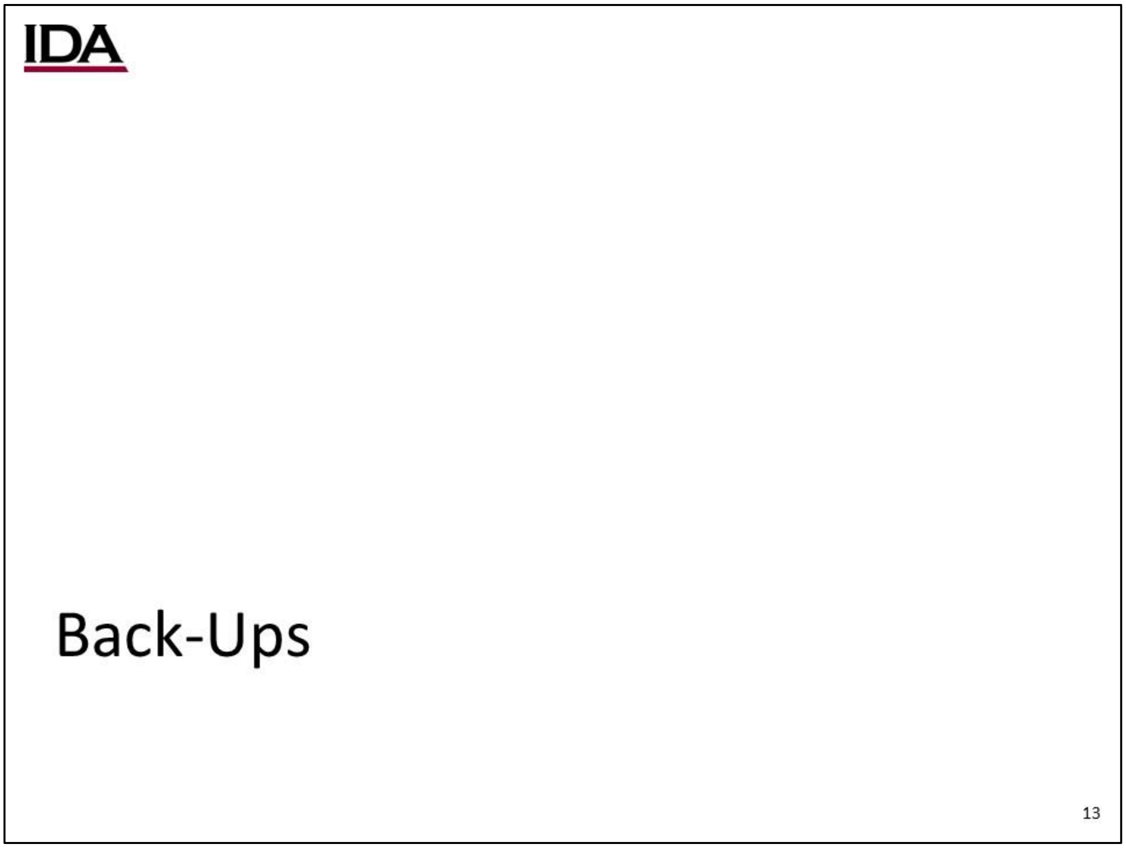


Discussion

- How can these ideas be further developed, applied, and assessed with respect to cyber and information warfare?
  - Adapt and incorporate C2 agility tools in operations assessments guides?
  - Conduct C2 agility assessments during exercises, experiments, wargames?

"If everyone is thinking alike, then somebody isn't thinking"
– General George S. Patton, Jr

Questions and Concerns



IDA

Back-Ups

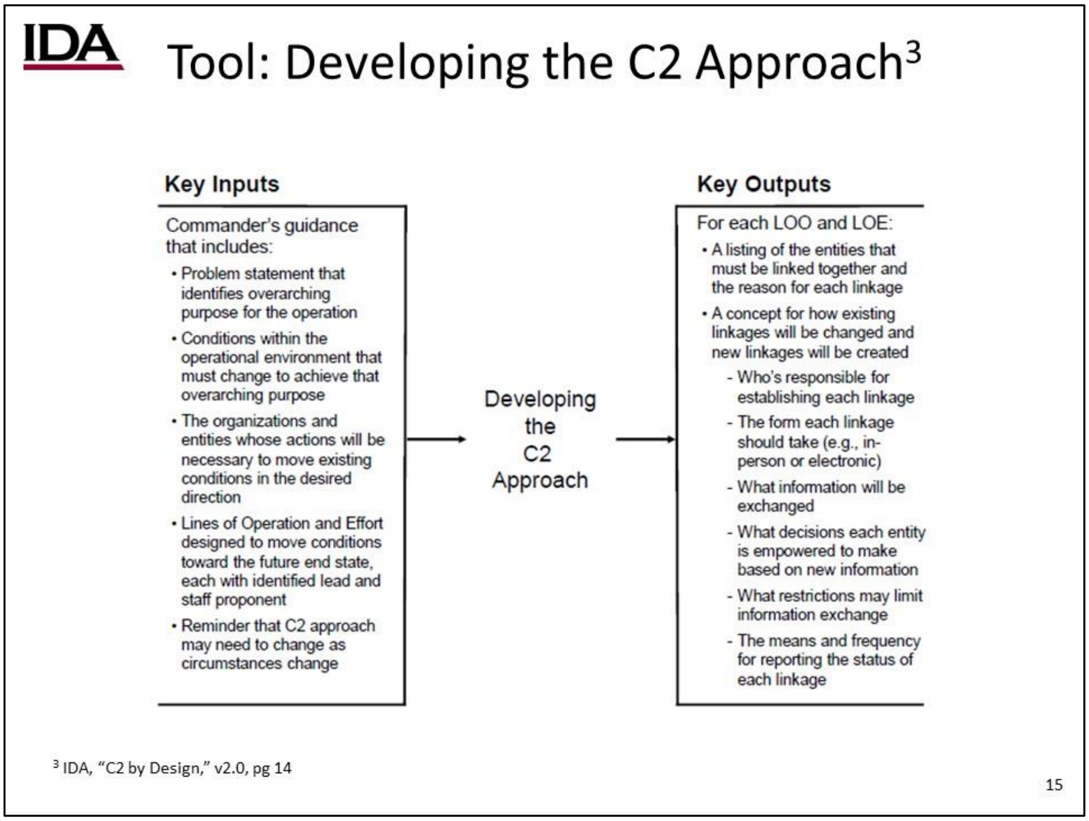
13

IDA

Agenda

- C2 Goal and Agility
- Designing C2 Agility
- C2 Agility Tools
  - Commander’s C2 Approach Guidance
  - Developing and Fleshing Out the C2 Approach
  - Communicating the C2 Approach
- C2 Perspectives
  - Assessing the C2 Approach
  - Righting the C2 Approach
- Discussion

14



IDA

Tool: Developing the C2 Approach[3]

Key Inputs

Commander's guidance that includes:

- Problem statement that identifies overarching purpose for the operation
- Conditions within the operational environment that must change to achieve that overarching purpose
- The organizations and entities whose actions will be necessary to move existing conditions in the desired direction
- Lines of Operation and Effort designed to move conditions toward the future end state, each with identified lead and staff proponent
- Reminder that C2 approach may need to change as circumstances change

Developing the C2 Approach

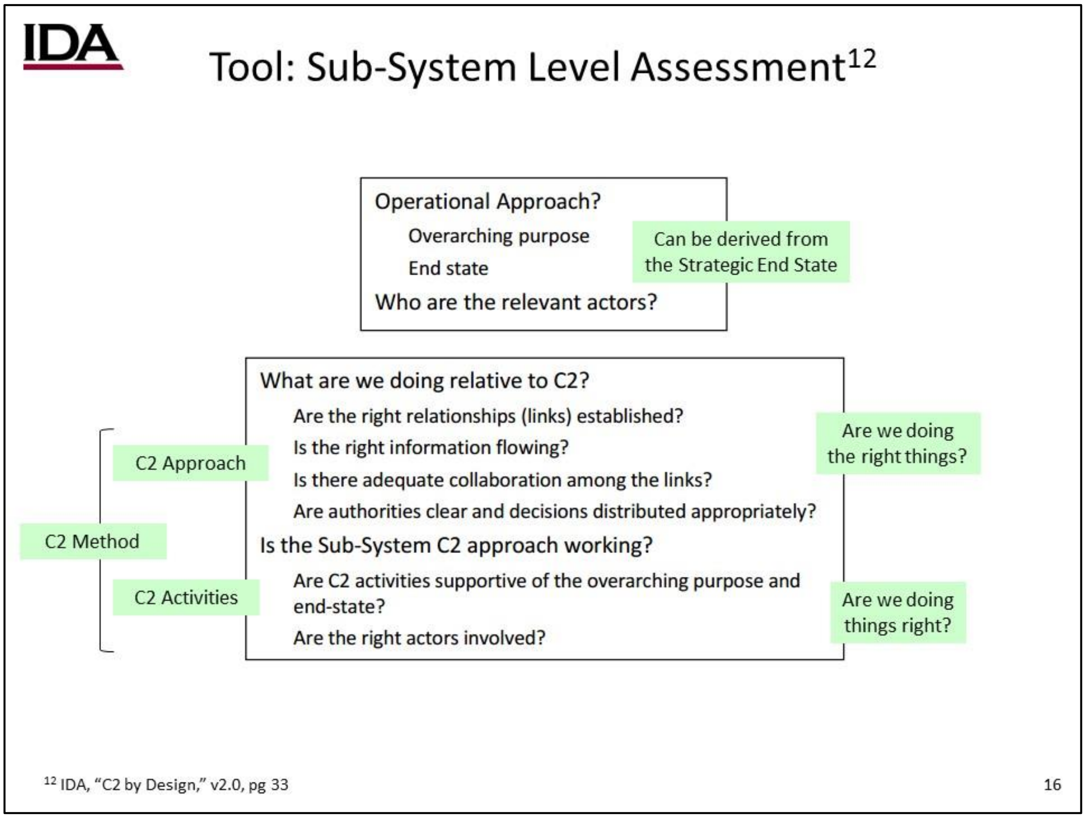
Key Outputs

For each LOO and LOE:

- A listing of the entities that must be linked together and the reason for each linkage
- A concept for how existing linkages will be changed and new linkages will be created
  - Who's responsible for establishing each linkage
  - The form each linkage should take (e.g., in-person or electronic)
  - What information will be exchanged
  - What decisions each entity is empowered to make based on new information
  - What restrictions may limit information exchange
  - The means and frequency for reporting the status of each linkage

[3] IDA, "C2 by Design," v2.0, pg 14

15



IDA

Tool: Sub-System Level Assessment[12]

Operational Approach?

Overarching purpose

End state

Can be derived from the Strategic End State

Who are the relevant actors?

What are we doing relative to C2?

Are the right relationships (links) established?

Is the right information flowing?

Is there adequate collaboration among the links?

Are authorities clear and decisions distributed appropriately?

Are we doing the right things?

Is the Sub-System C2 approach working?

Are C2 activities supportive of the overarching purpose and end-state?

Are the right actors involved?

Are we doing things right?

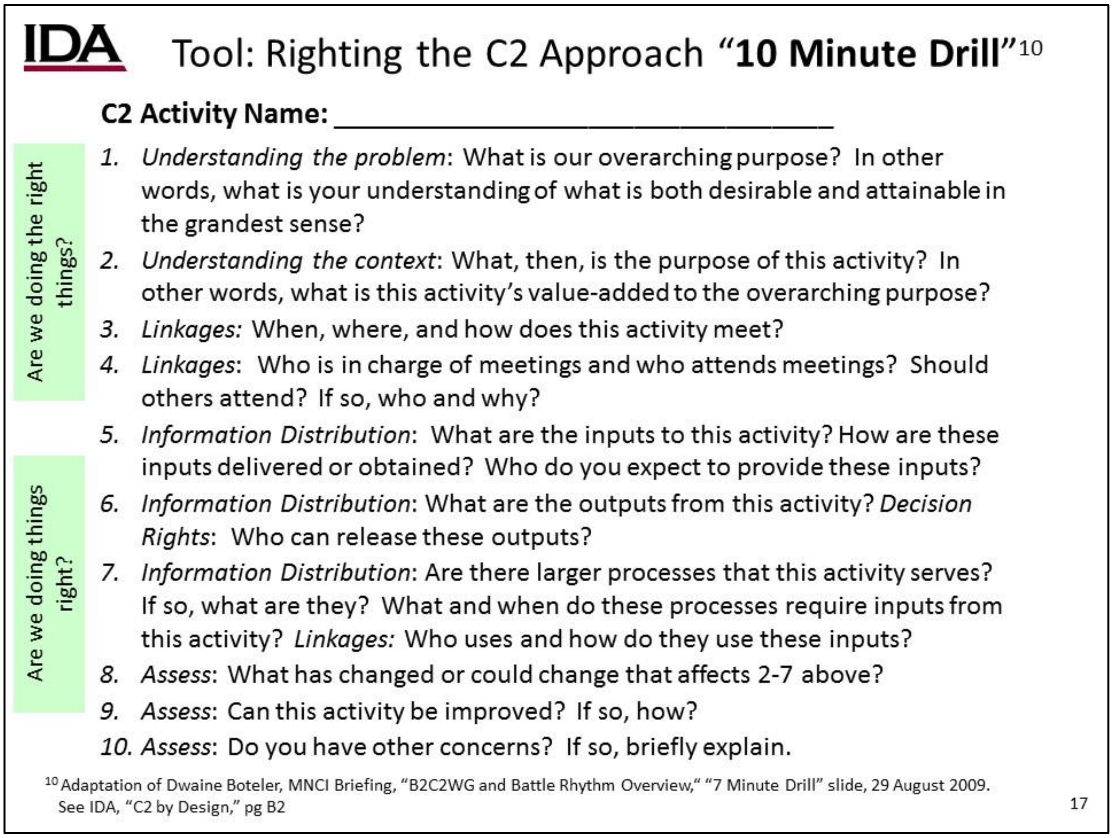
C2 Method

C2 Approach

C2 Activities

[12] IDA, "C2 by Design," v2.0, pg 33

16



IDA

Tool: Righting the C2 Approach "**10 Minute Drill**"[10]

C2 Activity Name: ________________________________

Are we doing the right things?

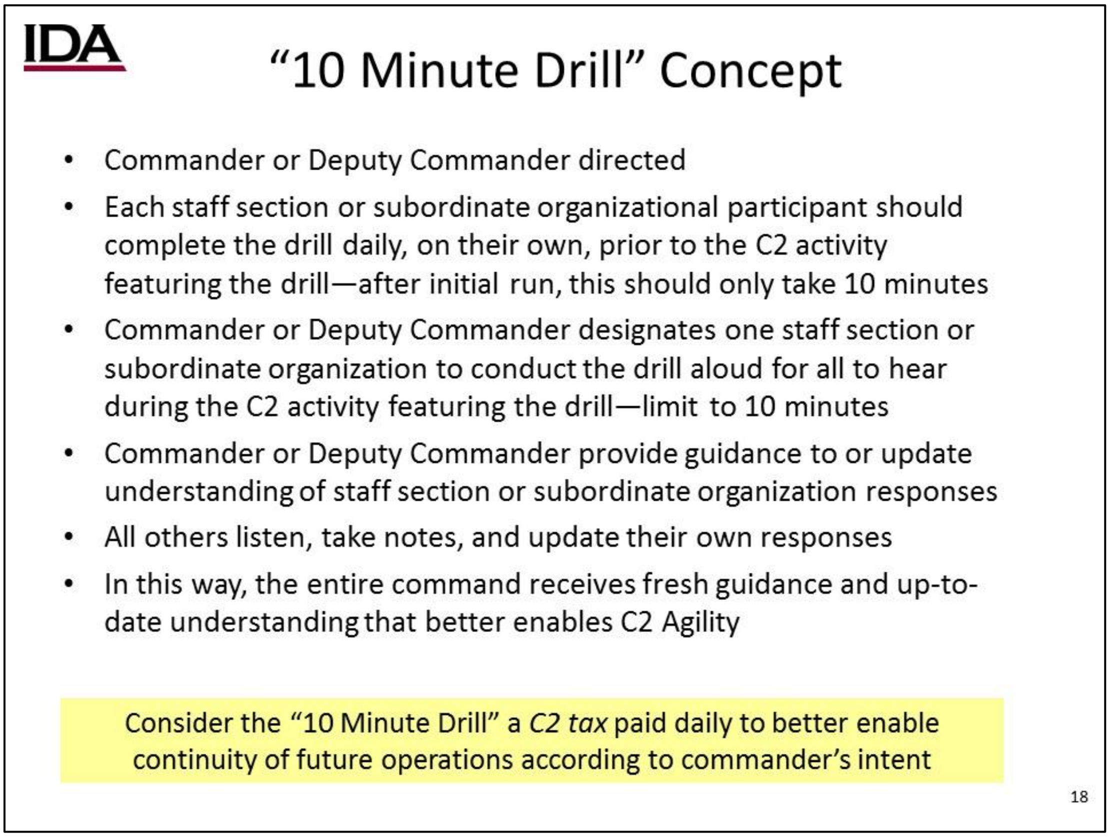
1. *Understanding the problem*: What is our overarching purpose? In other words, what is your understanding of what is both desirable and attainable in the grandest sense?
2. *Understanding the context*: What, then, is the purpose of this activity? In other words, what is this activity's value-added to the overarching purpose?
3. *Linkages:* When, where, and how does this activity meet?
4. *Linkages*: Who is in charge of meetings and who attends meetings? Should others attend? If so, who and why?

Are we doing things right?

5. *Information Distribution*: What are the inputs to this activity? How are these inputs delivered or obtained? Who do you expect to provide these inputs?
6. *Information Distribution*: What are the outputs from this activity? *Decision Rights*: Who can release these outputs?
7. *Information Distribution*: Are there larger processes that this activity serves? If so, what are they? What and when do these processes require inputs from this activity? *Linkages:* Who uses and how do they use these inputs?
8. *Assess*: What has changed or could change that affects 2-7 above?
9. *Assess*: Can this activity be improved? If so, how?
10. *Assess*: Do you have other concerns? If so, briefly explain.

[10] Adaptation of Dwaine Boteler, MNCI Briefing, "B2C2WG and Battle Rhythm Overview," "7 Minute Drill" slide, 29 August 2009. See IDA, "C2 by Design," pg B2

17



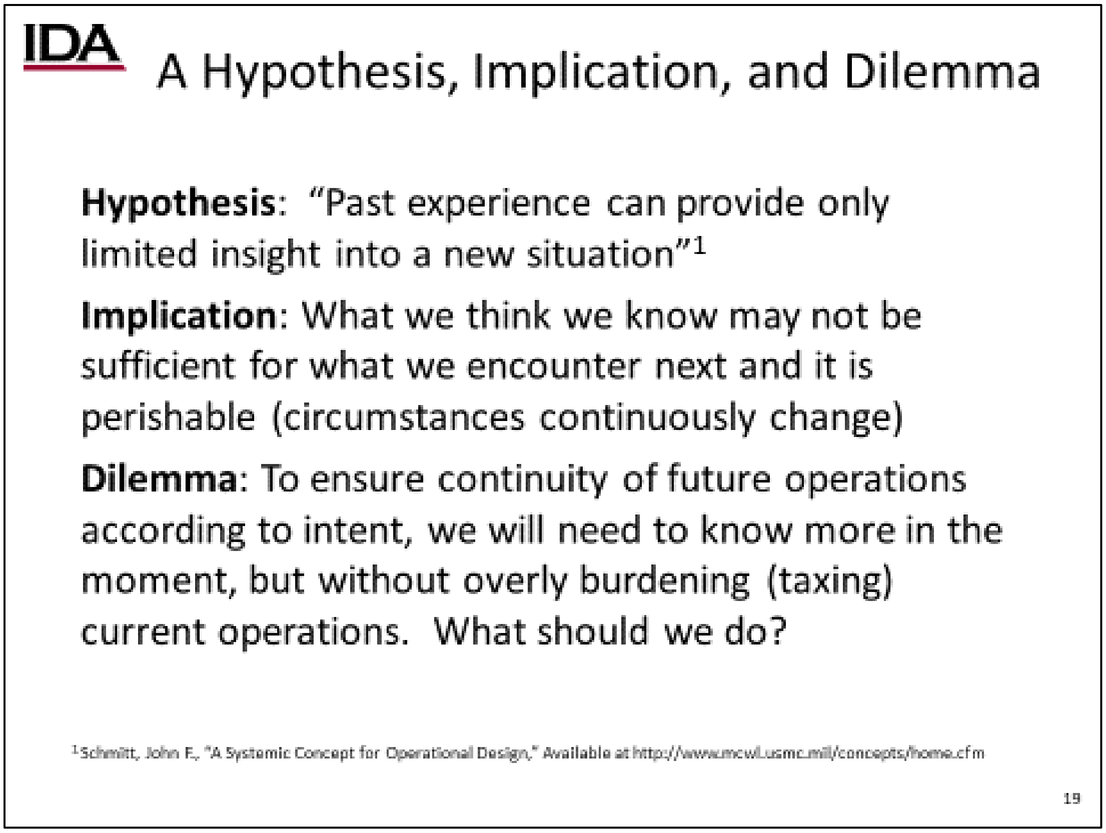
IDA

"10 Minute Drill" Concept

- Commander or Deputy Commander directed
- Each staff section or subordinate organizational participant should complete the drill daily, on their own, prior to the C2 activity featuring the drill—after initial run, this should only take 10 minutes
- Commander or Deputy Commander designates one staff section or subordinate organization to conduct the drill aloud for all to hear during the C2 activity featuring the drill—limit to 10 minutes
- Commander or Deputy Commander provide guidance to or update understanding of staff section or subordinate organization responses
- All others listen, take notes, and update their own responses
- In this way, the entire command receives fresh guidance and up-to-date understanding that better enables C2 Agility

Consider the "10 Minute Drill" a *C2 tax* paid daily to better enable continuity of future operations according to commander's intent

18



IDA

A Hypothesis, Implication, and Dilemma

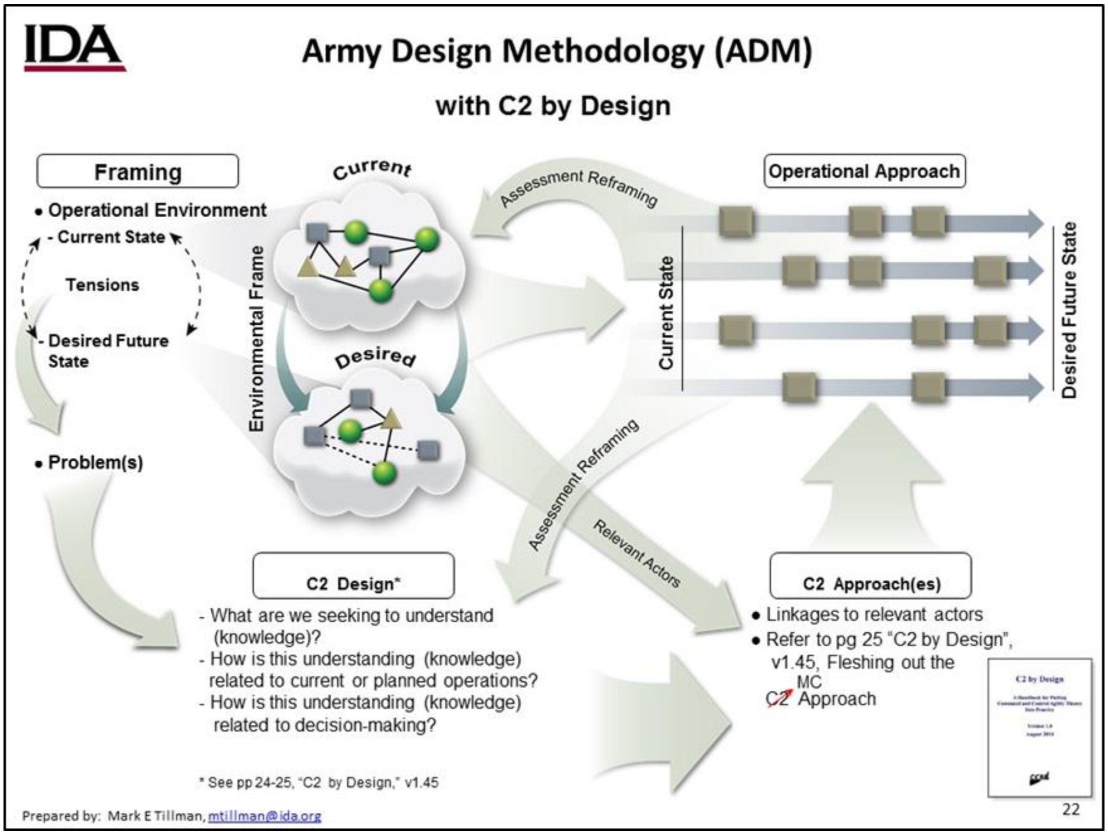
Hypothesis: "Past experience can provide only limited insight into a new situation"[1]

Implication: What we think we know may not be sufficient for what we encounter next and it is perishable (circumstances continuously change)

Dilemma: To ensure continuity of future operations according to intent, we will need to know more in the moment, but without overly burdening (taxing) current operations. What should we do?

[1] Schmitt, John F., "A Systemic Concept for Operational Design," Available at http://www.mcwl.usmc.mil/concepts/home.cfm

19



IDA

Army Design Methodology (ADM)

with C2 by Design

Framing

- Operational Environment
  - Current State
  - Tensions
  - Desired Future State
- Problem(s)

C2 Design*

- What are we seeking to understand (knowledge)?
- How is this understanding (knowledge) related to current or planned operations?
- How is this understanding (knowledge) related to decision-making?

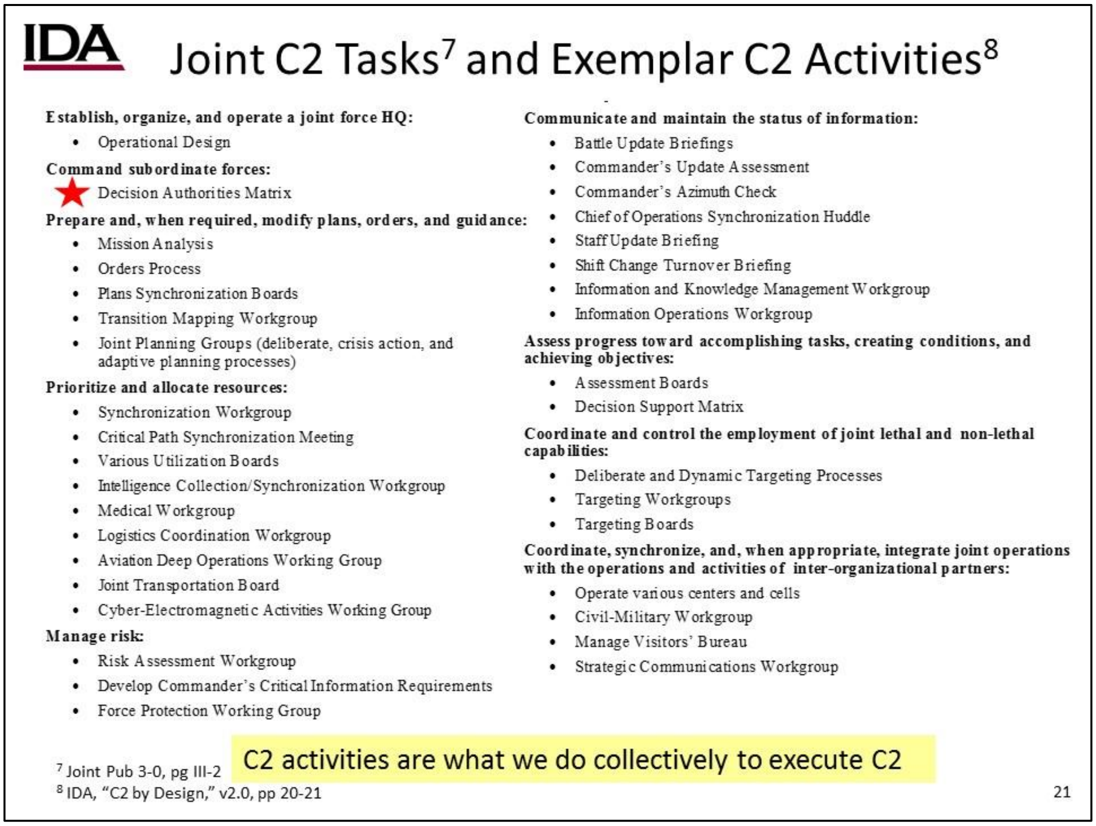
C2 Approach(es)

- Linkages to relevant actors
- Refer to pg 25 "C2 by Design", v1.45, Fleshing out the ~~C2~~ MC Approach

* See pp 24-25, "C2 by Design," v1.45

Prepared by: Mark E Tillman, mtillman@ida.org

22



IDA

Joint C2 Tasks[7] and Exemplar C2 Activities[8]

Establish, organize, and operate a joint force HQ:

- Operational Design

Command subordinate forces:

★ Decision Authorities Matrix

Prepare and, when required, modify plans, orders, and guidance:

- Mission Analysis
- Orders Process
- Plans Synchronization Boards
- Transition Mapping Workgroup
- Joint Planning Groups (deliberate, crisis action, and adaptive planning processes)

Prioritize and allocate resources:

- Synchronization Workgroup
- Critical Path Synchronization Meeting
- Various Utilization Boards
- Intelligence Collection/Synchronization Workgroup
- Medical Workgroup
- Logistics Coordination Workgroup
- Aviation Deep Operations Working Group
- Joint Transportation Board
- Cyber-Electromagnetic Activities Working Group

Manage risk:

- Risk Assessment Workgroup
- Develop Commander's Critical Information Requirements
- Force Protection Working Group

Communicate and maintain the status of information:

- Battle Update Briefings
- Commander's Update Assessment
- Commander's Azimuth Check
- Chief of Operations Synchronization Huddle
- Staff Update Briefing
- Shift Change Turnover Briefing
- Information and Knowledge Management Workgroup
- Information Operations Workgroup

Assess progress toward accomplishing tasks, creating conditions, and achieving objectives:

- Assessment Boards
- Decision Support Matrix

Coordinate and control the employment of joint lethal and non-lethal capabilities:

- Deliberate and Dynamic Targeting Processes
- Targeting Workgroups
- Targeting Boards

Coordinate, synchronize, and, when appropriate, integrate joint operations with the operations and activities of inter-organizational partners:

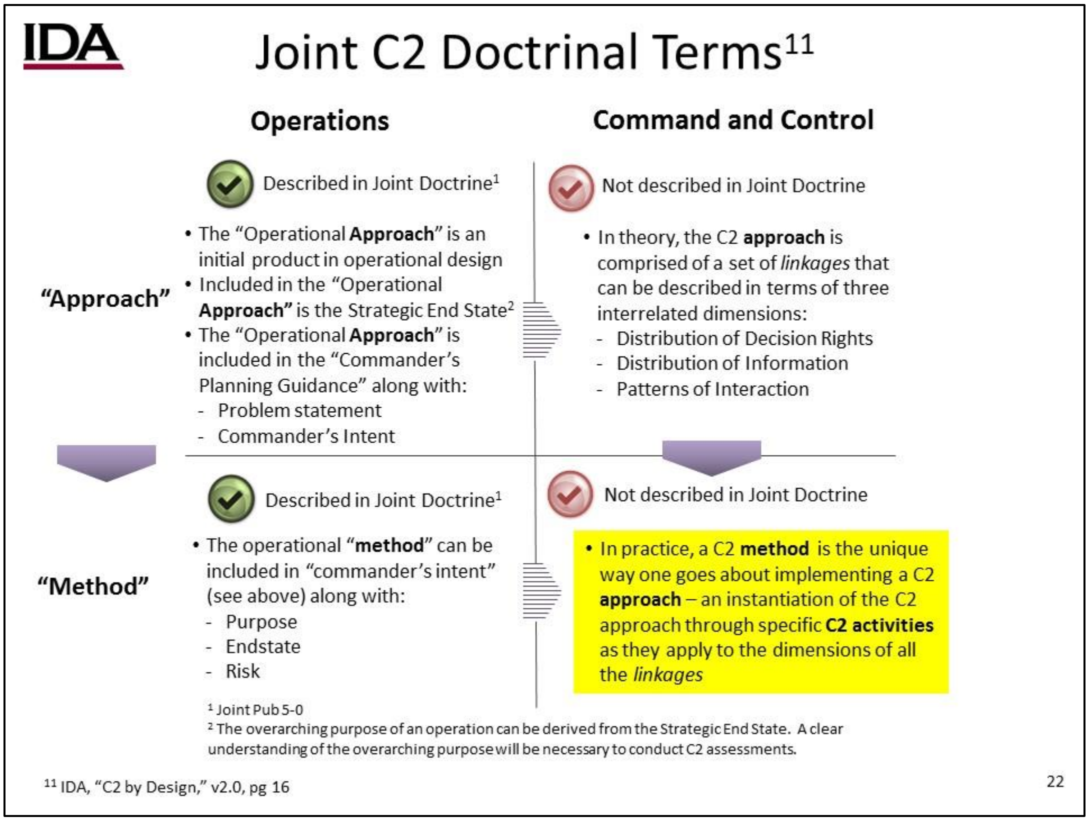
- Operate various centers and cells
- Civil-Military Workgroup
- Manage Visitors' Bureau
- Strategic Communications Workgroup

C2 activities are what we do collectively to execute C2

[7] Joint Pub 3-0, pg III-2

[8] IDA, "C2 by Design," v2.0, pp 20-21

21



IDA

Joint C2 Doctrinal Terms[11]

Operations

Command and Control

"Approach"

Operations: ✓ Described in Joint Doctrine[1]

- The "Operational **Approach**" is an initial product in operational design
- Included in the "Operational **Approach"** is the Strategic End State[2]
- The "Operational **Approach**" is included in the "Commander's Planning Guidance" along with:
  - Problem statement
  - Commander's Intent

Command and Control: ✓ Not described in Joint Doctrine

- In theory, the C2 **approach** is comprised of a set of *linkages* that can be described in terms of three interrelated dimensions:
  - Distribution of Decision Rights
  - Distribution of Information
  - Patterns of Interaction

"Method"

Operations: ✓ Described in Joint Doctrine[1]

- The operational **"method"** can be included in "commander's intent" (see above) along with:
  - Purpose
  - Endstate
  - Risk

Command and Control: ✓ Not described in Joint Doctrine

- In practice, a C2 **method** is the unique way one goes about implementing a C2 **approach** – an instantiation of the C2 approach through specific **C2 activities** as they apply to the dimensions of all the *linkages*

[1] Joint Pub 5-0

[2] The overarching purpose of an operation can be derived from the Strategic End State. A clear understanding of the overarching purpose will be necessary to conduct C2 assessments.

[11] IDA, "C2 by Design," v2.0, pg 16

22

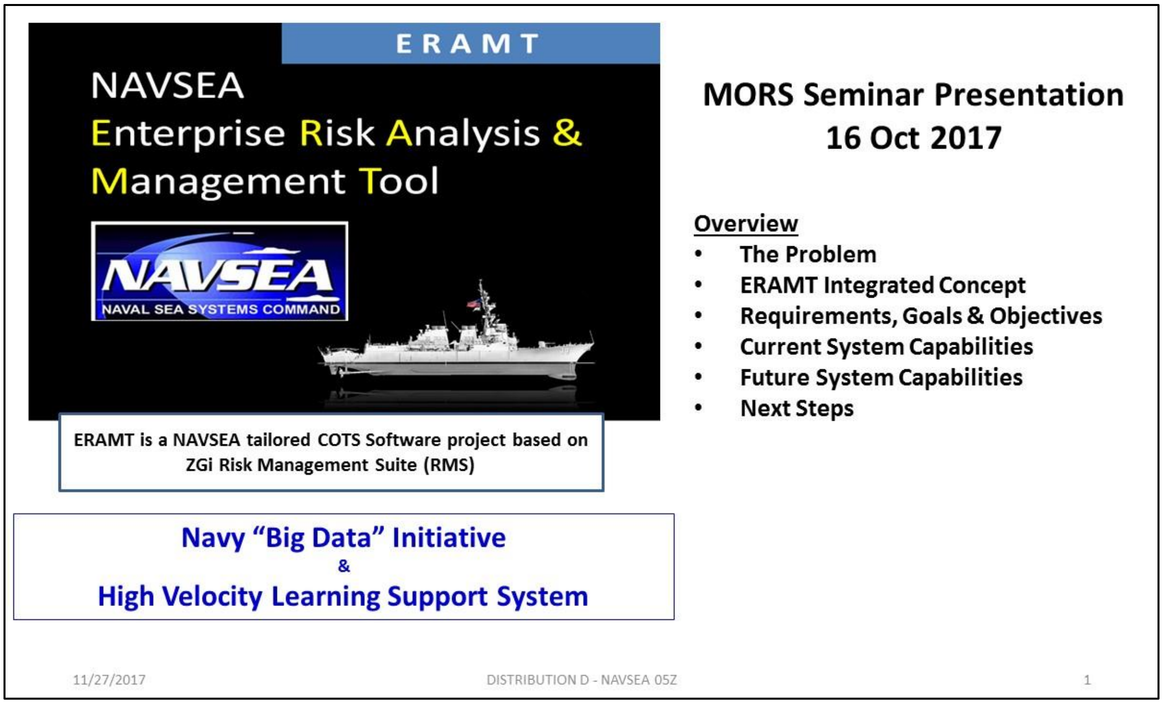
B. Diane Schroer: Enterprise Risk Analysis and Management Tool (ERAMT)

Presentation Summary

Ms. Schroer's topic focused on the concept of using big data to analyze risks across disciplines and how to achieve a unified model from the current silos. Her approach echoed discussions on the semantic overlap between areas of risk, cyber, operational, and project/mission. The ERAMT is an attempt to bridge the gaps and get an overall risk dashboard.

Leadership has repeatedly requested this capability, but delivery has been difficult. Ms. Schroer captured the challenges to leadership, weighing the risks of potential courses of action when similar terminology from slightly different disciplines often doesn't mean exactly the same thing in context. These semantic miscommunications undermine accurate decision-making. She explained how this can result in a lack of congruency and affect data modeling. This discussion of maturity in managing and visualizing risk through data would be an excellent topic for follow-on exploration.

She followed her problem definition (outdated risk identification methodology) with a high-level solution (automation). However, when a variety of "Big Data" analytics sets are available, this can pose a problem for leadership, resulting in "paralysis by analysis." Ms. Schroer proposes the ERAMT based on its successful implementation in the Naval Sea Systems Command (NAVSEA). Discussion centered on the data flow process, which results in linking with rule sets that provide a risk cluster assessment as final product. Applying these techniques seems sound and should be pursued at all levels.



ERAMT

NAVSEA
Enterprise Risk Analysis &
Management Tool

NAVSEA
NAVAL SEA SYSTEMS COMMAND

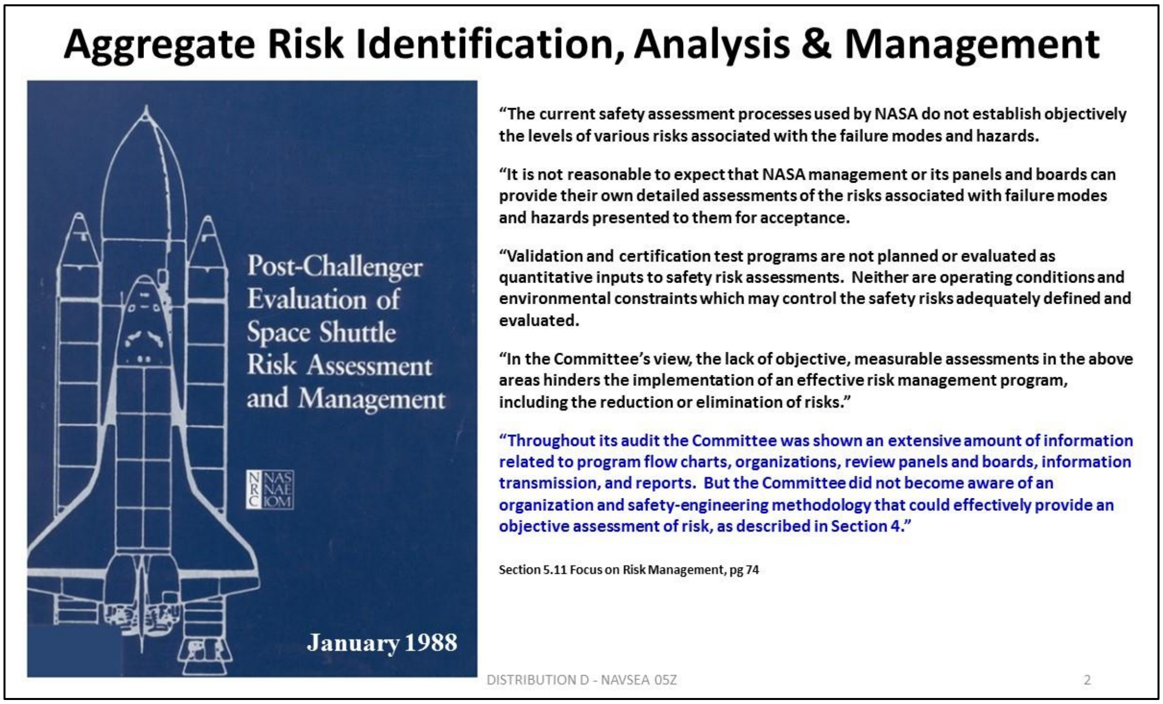
ERAMT is a NAVSEA tailored COTS Software project based on ZGi Risk Management Suite (RMS)

Navy "Big Data" Initiative
&
High Velocity Learning Support System

MORS Seminar Presentation
16 Oct 2017

Overview

- The Problem
- ERAMT Integrated Concept
- Requirements, Goals & Objectives
- Current System Capabilities
- Future System Capabilities
- Next Steps



Aggregate Risk Identification, Analysis & Management

Post-Challenger
Evaluation of
Space Shuttle
Risk Assessment
and Management
NRC NAS NAE IOM
January 1988

"The current safety assessment processes used by NASA do not establish objectively the levels of various risks associated with the failure modes and hazards.

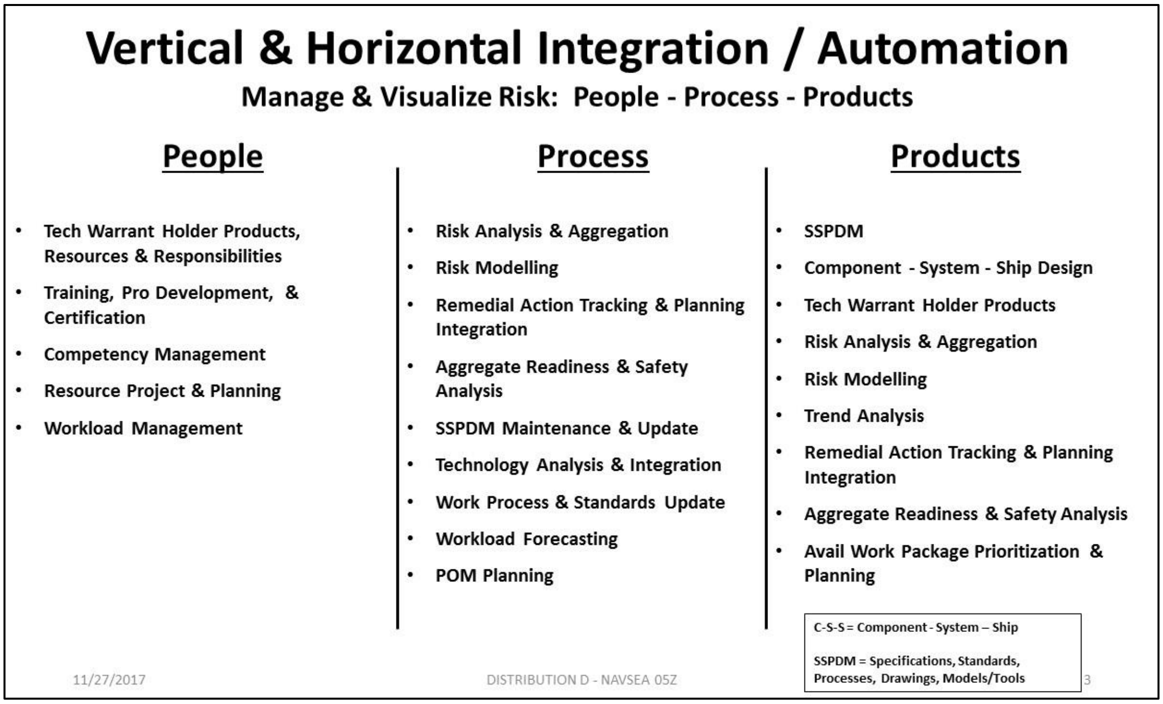
"It is not reasonable to expect that NASA management or its panels and boards can provide their own detailed assessments of the risks associated with failure modes and hazards presented to them for acceptance.

"Validation and certification test programs are not planned or evaluated as quantitative inputs to safety risk assessments. Neither are operating conditions and environmental constraints which may control the safety risks adequately defined and evaluated.

"In the Committee's view, the lack of objective, measurable assessments in the above areas hinders the implementation of an effective risk management program, including the reduction or elimination of risks."

"Throughout its audit the Committee was shown an extensive amount of information related to program flow charts, organizations, review panels and boards, information transmission, and reports. But the Committee did not become aware of an organization and safety-engineering methodology that could effectively provide an objective assessment of risk, as described in Section 4."

Section 5.11 Focus on Risk Management, pg 74



Vertical & Horizontal Integration / Automation

Manage & Visualize Risk: People - Process - Products

People

- Tech Warrant Holder Products, Resources & Responsibilities
- Training, Pro Development, & Certification
- Competency Management
- Resource Project & Planning
- Workload Management

Process

- Risk Analysis & Aggregation
- Risk Modelling
- Remedial Action Tracking & Planning Integration
- Aggregate Readiness & Safety Analysis
- SSPDM Maintenance & Update
- Technology Analysis & Integration
- Work Process & Standards Update
- Workload Forecasting
- POM Planning

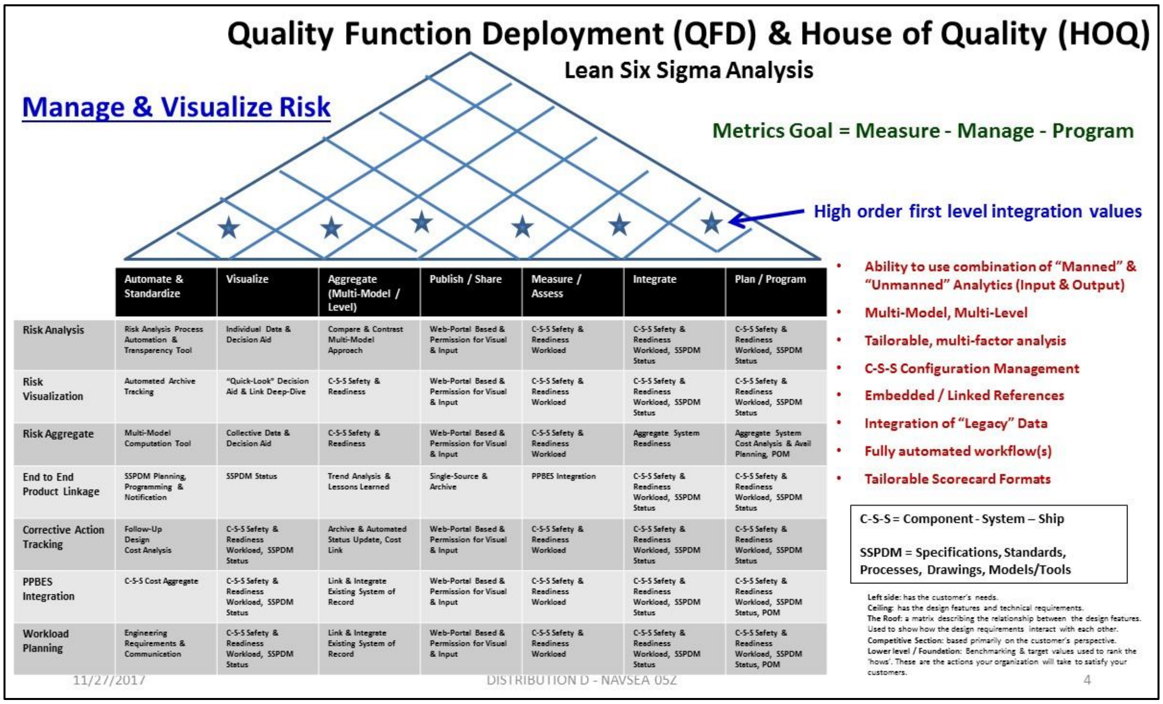
Products

- SSPDM
- Component - System - Ship Design
- Tech Warrant Holder Products
- Risk Analysis & Aggregation
- Risk Modelling
- Trend Analysis
- Remedial Action Tracking & Planning Integration
- Aggregate Readiness & Safety Analysis
- Avail Work Package Prioritization & Planning

C-S-S = Component - System – Ship

SSPDM = Specifications, Standards, Processes, Drawings, Models/Tools

11/27/2017 DISTRIBUTION D - NAVSEA 05Z 3



Quality Function Deployment (QFD) & House of Quality (HOQ)

Lean Six Sigma Analysis

Manage & Visualize Risk

Metrics Goal = Measure - Manage - Program

	Automate & Standardize	Visualize	Aggregate (Multi-Model / Level)	Publish / Share	Measure / Assess	Integrate	Plan / Program
Risk Analysis	Risk Analysis Process Automation & Transparency Tool	Individual Data & Decision Aid	Compare & Contrast Multi-Model Approach	Web-Portal Based & Permission for Visual & Input	C-S-S Safety & Readiness Workload	C-S-S Safety & Readiness Workload, SSPDM Status	C-S-S Safety & Readiness Workload, SSPDM Status
Risk Visualization	Automated Archive Tracking	"Quick-Look" Decision Aid & Link Deep-Dive	C-S-S Safety & Readiness	Web-Portal Based & Permission for Visual & Input	C-S-S Safety & Readiness Workload	C-S-S Safety & Readiness Workload, SSPDM Status	C-S-S Safety & Readiness Workload, SSPDM Status
Risk Aggregate	Multi-Model Computation Tool	Collective Data & Decision Aid	C-S-S Safety & Readiness	Web-Portal Based & Permission for Visual & Input	C-S-S Safety & Readiness Workload	Aggregate System Readiness	Aggregate System Cost Analysis & Avail Planning, POM
End to End Product Linkage	SSPDM Planning, Programming & Notification	SSPDM Status	Trend Analysis & Lessons Learned	Single-Source & Archive	PPBES Integration	C-S-S Safety & Readiness Workload, SSPDM Status	C-S-S Safety & Readiness Workload, SSPDM Status
Corrective Action Tracking	Follow-Up Design Cost Analysis	C-S-S Safety & Readiness Workload, SSPDM Status	Archive & Automated Status Update, Cost Link	Web-Portal Based & Permission for Visual & Input	C-S-S Safety & Readiness Workload	C-S-S Safety & Readiness Workload, SSPDM Status	C-S-S Safety & Readiness Workload, SSPDM Status
PPBES Integration	C-S-S Cost Aggregate	C-S-S Safety & Readiness Workload, SSPDM Status	Link & Integrate Existing System of Record	Web-Portal Based & Permission for Visual & Input	C-S-S Safety & Readiness Workload	C-S-S Safety & Readiness Workload, SSPDM Status	C-S-S Safety & Readiness Workload, SSPDM Status, POM
Workload Planning	Engineering Requirements & Communication	C-S-S Safety & Readiness Workload, SSPDM Status	Link & Integrate Existing System of Record	Web-Portal Based & Permission for Visual & Input	C-S-S Safety & Readiness Workload	C-S-S Safety & Readiness Workload, SSPDM Status	C-S-S Safety & Readiness Workload, SSPDM Status, POM

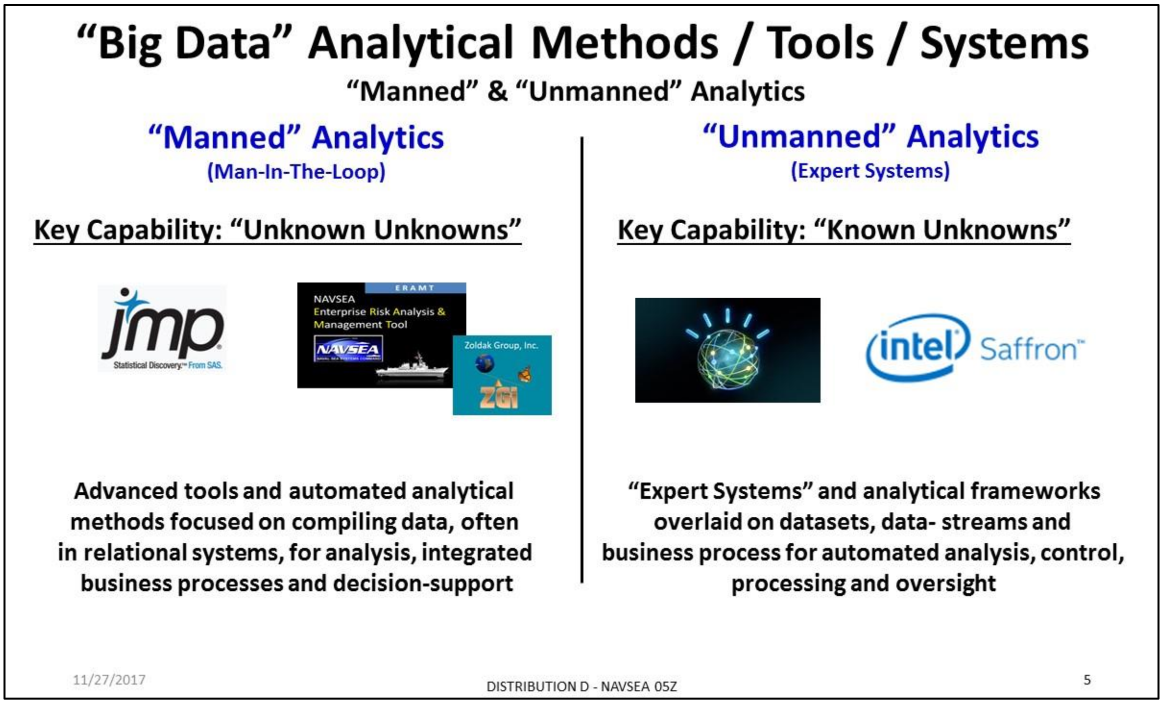
- Ability to use combination of "Manned" & "Unmanned" Analytics (Input & Output)
- Multi-Model, Multi-Level
- Tailorable, multi-factor analysis
- C-S-S Configuration Management
- Embedded / Linked References
- Integration of "Legacy" Data
- Fully automated workflow(s)
- Tailorable Scorecard Formats

C-S-S = Component - System – Ship

SSPDM = Specifications, Standards, Processes, Drawings, Models/Tools

Left side: has the customer's needs.
Ceiling: has the design features and technical requirements.
The Roof: a matrix describing the relationship between the design features. Used to show how the design requirements interact with each other.
Competitive Section: based primarily on the customer's perspective.
Lower level / Foundation: Benchmarking & target values used to rank the 'hows'. These are the actions your organization will take to satisfy your customers.

11/27/2017 DISTRIBUTION D - NAVSEA 05Z 4



"Big Data" Analytical Methods / Tools / Systems

"Manned" & "Unmanned" Analytics

"Manned" Analytics

(Man-In-The-Loop)

Key Capability: "Unknown Unknowns"

jmp
Statistical Discovery. From SAS.
ERAMT
NAVSEA
Enterprise Risk Analysis & Management Tool
NAVSEA
Zoldak Group, Inc.
ZGI

Advanced tools and automated analytical methods focused on compiling data, often in relational systems, for analysis, integrated business processes and decision-support

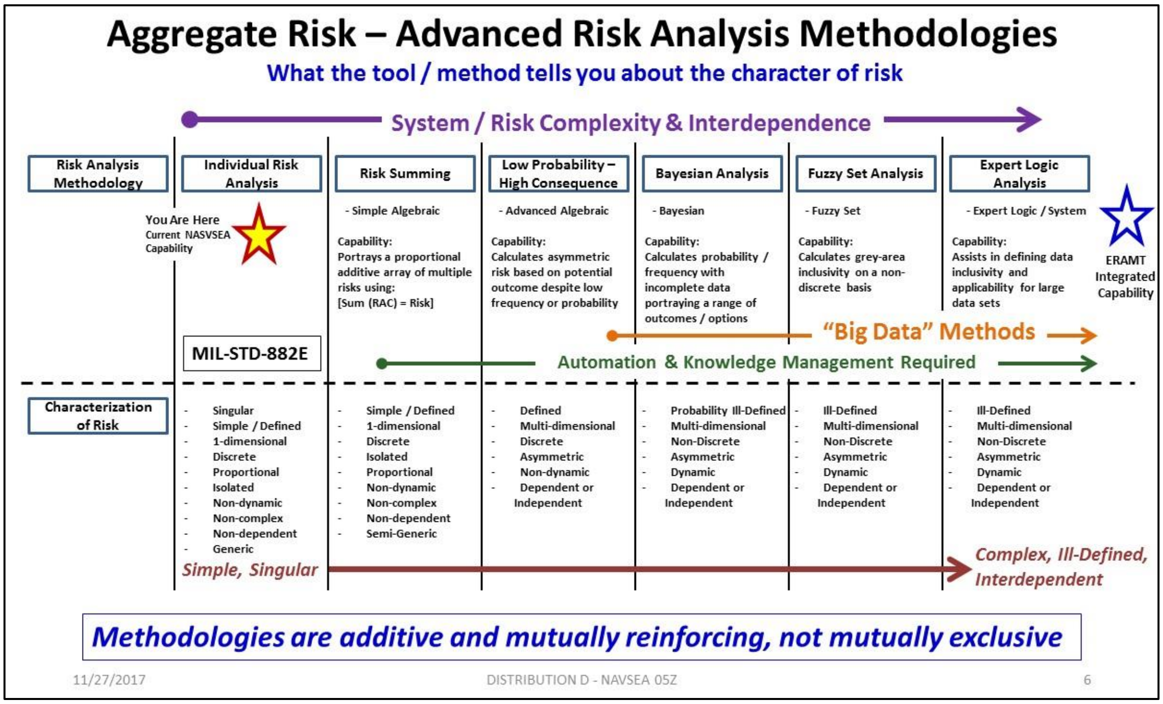
"Unmanned" Analytics

(Expert Systems)

Key Capability: "Known Unknowns"

"Expert Systems" and analytical frameworks overlaid on datasets, data- streams and business process for automated analysis, control, processing and oversight

11/27/2017 DISTRIBUTION D - NAVSEA 05Z 5



Aggregate Risk – Advanced Risk Analysis Methodologies

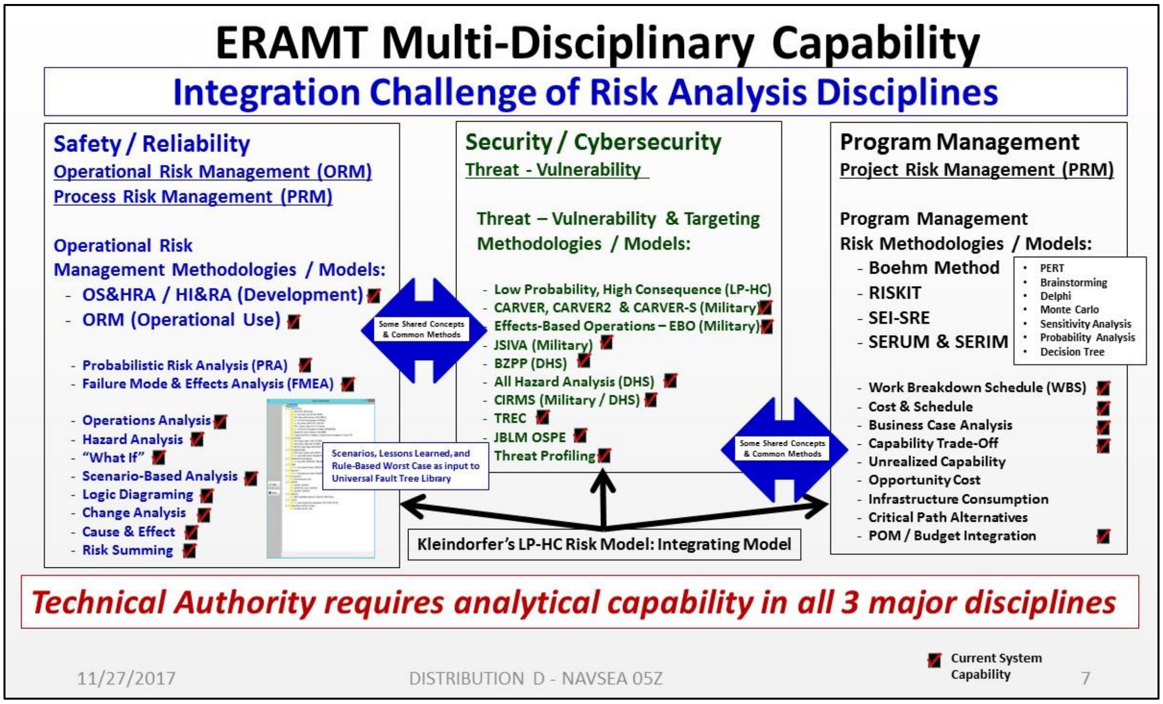
What the tool / method tells you about the character of risk

System / Risk Complexity & Interdependence
You Are Here
Current NASVSEA Capability
MIL-STD-882E
ERAMT Integrated Capability
"Big Data" Methods
Automation & Knowledge Management Required
Simple, Singular
Complex, Ill-Defined, Interdependent

Risk Analysis Methodology	Individual Risk Analysis	Risk Summing	Low Probability – High Consequence	Bayesian Analysis	Fuzzy Set Analysis	Expert Logic Analysis
		- Simple Algebraic	- Advanced Algebraic	- Bayesian	- Fuzzy Set	- Expert Logic / System
		Capability: Portrays a proportional additive array of multiple risks using: [Sum (RAC) = Risk]	Capability: Calculates asymmetric risk based on potential outcome despite low frequency or probability	Capability: Calculates probability / frequency with incomplete data portraying a range of outcomes / options	Capability: Calculates grey-area inclusivity on a non-discrete basis	Capability: Assists in defining data inclusivity and applicability for large data sets
Characterization of Risk	- Singular - Simple / Defined - 1-dimensional - Discrete - Proportional - Isolated - Non-dynamic - Non-complex - Non-dependent - Generic	- Simple / Defined - 1-dimensional - Discrete - Isolated - Proportional - Non-dynamic - Non-complex - Non-dependent - Semi-Generic	- Defined - Multi-dimensional - Discrete - Asymmetric - Non-dynamic - Dependent or Independent	- Probability Ill-Defined - Multi-dimensional - Non-Discrete - Asymmetric - Dynamic - Dependent or Independent	- Ill-Defined - Multi-dimensional - Non-Discrete - Asymmetric - Dynamic - Dependent or Independent	- Ill-Defined - Multi-dimensional - Non-Discrete - Asymmetric - Dynamic - Dependent or Independent

Methodologies are additive and mutually reinforcing, not mutually exclusive

11/27/2017 DISTRIBUTION D - NAVSEA 05Z 6



ERAMT Multi-Disciplinary Capability

Integration Challenge of Risk Analysis Disciplines

Safety / Reliability

Operational Risk Management (ORM)

Process Risk Management (PRM)

Operational Risk Management Methodologies / Models:

- OS&HRA / HI&RA (Development) ☑
- ORM (Operational Use) ☑

- Probabilistic Risk Analysis (PRA) ☑
- Failure Mode & Effects Analysis (FMEA) ☑

- Operations Analysis ☑
- Hazard Analysis ☑
- "What If" ☑
- Scenario-Based Analysis ☑
- Logic Diagraming ☑
- Change Analysis ☑
- Cause & Effect ☑
- Risk Summing ☑

Scenarios, Lessons Learned, and Rule-Based Worst Case as input to Universal Fault Tree Library

Security / Cybersecurity

Threat - Vulnerability

Threat – Vulnerability & Targeting Methodologies / Models:

- Low Probability, High Consequence (LP-HC)
- CARVER, CARVER2 & CARVER-S (Military) ☑
- Effects-Based Operations – EBO (Military) ☑
- JSIVA (Military) ☑
- BZPP (DHS) ☑
- All Hazard Analysis (DHS) ☑
- CIRMS (Military / DHS) ☑
- TREC ☑
- JBLM OSPE ☑
- Threat Profiling ☑

Program Management

Project Risk Management (PRM)

Program Management Risk Methodologies / Models:

- Boehm Method
- RISKIT
- SEI-SRE
- SERUM & SERIM

- PERT
- Brainstorming
- Delphi
- Monte Carlo
- Sensitivity Analysis
- Probability Analysis
- Decision Tree

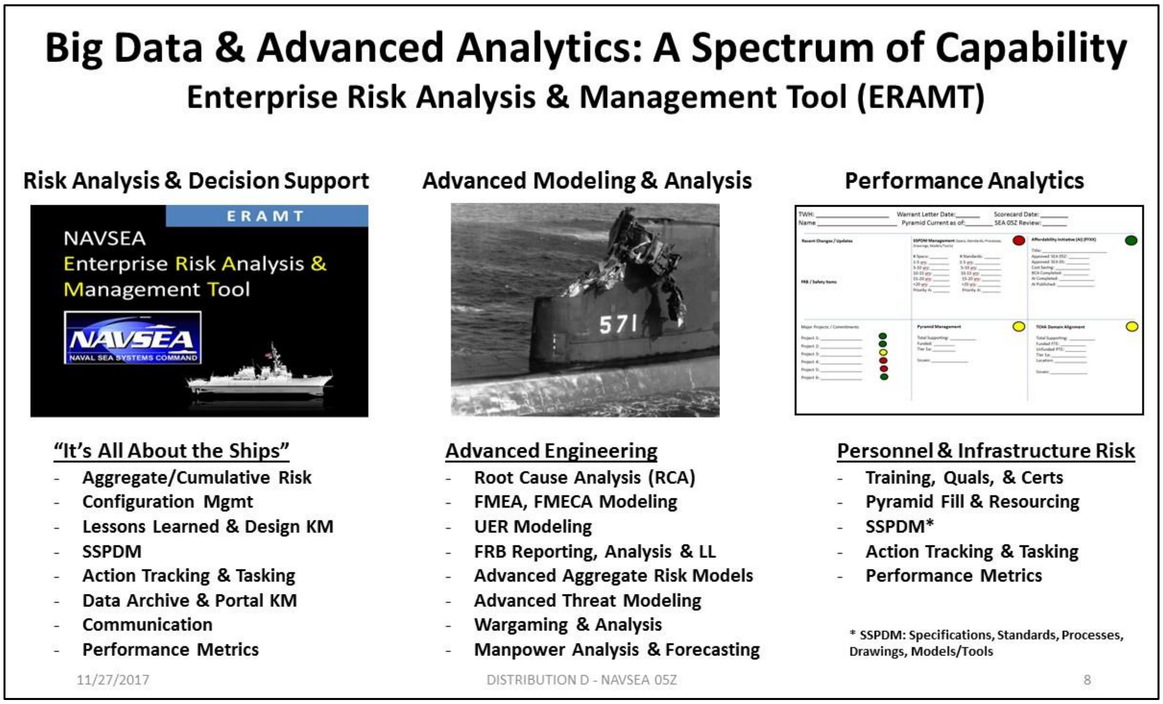
- Work Breakdown Schedule (WBS) ☑
- Cost & Schedule ☑
- Business Case Analysis ☑
- Capability Trade-Off ☑
- Unrealized Capability
- Opportunity Cost
- Infrastructure Consumption
- Critical Path Alternatives
- POM / Budget Integration ☑

Some Shared Concepts & Common Methods
Some Shared Concepts & Common Methods

Kleindorfer's LP-HC Risk Model: Integrating Model

Technical Authority requires analytical capability in all 3 major disciplines

☑ Current System Capability



Big Data & Advanced Analytics: A Spectrum of Capability

Enterprise Risk Analysis & Management Tool (ERAMT)

Risk Analysis & Decision Support

ERAMT
NAVSEA
Enterprise Risk Analysis & Management Tool
NAVSEA
NAVAL SEA SYSTEMS COMMAND

"It's All About the Ships"

- Aggregate/Cumulative Risk
- Configuration Mgmt
- Lessons Learned & Design KM
- SSPDM
- Action Tracking & Tasking
- Data Archive & Portal KM
- Communication
- Performance Metrics

Advanced Modeling & Analysis

571

Advanced Engineering

- Root Cause Analysis (RCA)
- FMEA, FMECA Modeling
- UER Modeling
- FRB Reporting, Analysis & LL
- Advanced Aggregate Risk Models
- Advanced Threat Modeling
- Wargaming & Analysis
- Manpower Analysis & Forecasting

Performance Analytics

Personnel & Infrastructure Risk

- Training, Quals, & Certs
- Pyramid Fill & Resourcing
- SSPDM*
- Action Tracking & Tasking
- Performance Metrics

* SSPDM: Specifications, Standards, Processes, Drawings, Models/Tools

Aggregate Risk – Ship Scorecard

Ship / System Aggregate Risk Analysis & Visibility

Example Dashboard

Class __DDG-51__ Ship __DDG-51__ USS Arleigh Burke

Risk Model / Methodology	Individual	Risk Sum	LP - HC	Bayesian	ORM	FMECA	RCA
Ship Aggregate Risk:							

ESWBS	100 - 199	200 - 299	300 - 399	400 - 499	500 - 599	600 - 699	700 - 799	800 - 899	900 - 999	
DFS	🟨 100 - 199	🟨 200 - 299	🟩 300 - 399	🟩 400 - 499	🟩 500 - 599	🟩 600 - 699	🟨 700 - 799	🟩 800 - 899	🟩 900 - 999	🟨
SCD	🟨 100 - 199	🟩 200 - 299	🟨 300 - 399	🟨 400 - 499	🟩 500 - 599	🟩 600 - 699	🟩 700 - 799	🟩 800 - 899	🟩 900 - 999	🟨
Advisories	🟩 100 - 199	🟥 200 - 299	🟩 300 - 399	🟨 400 - 499	🟩 500 - 599	🟩 600 - 699	🟩 700 - 799	🟩 800 - 899	🟩 900 - 999	🟥
FRB / Safety	🟨 100 - 199	🟩 200 - 299	🟩 300 - 399	🟩 400 - 499	🟩 500 - 599	🟩 600 - 699	🟩 700 - 799	🟩 800 - 899	🟩 900 - 999	🟨
Warfare	🟩 100 - 199	🟨 200 - 299	🟩 300 - 399	🟩 400 - 499	🟩 500 - 599	🟩 600 - 699	🟩 700 - 799	🟩 800 - 899	🟩 900 - 999	🟨
Cyber	🟩 100 - 199	🟨 200 - 299	🟩 300 - 399	🟩 400 - 499	🟩 500 - 599	🟩 600 - 699	🟩 700 - 799	🟩 800 - 899	🟩 900 - 999	🟨

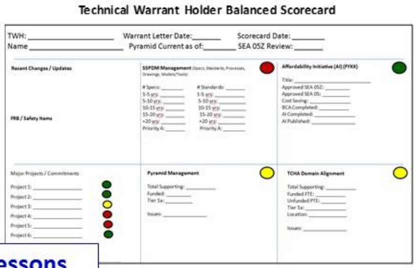
Recent History – Major Events / Casualties / Risk Factors

Automated TWH Balanced Scorecard

Automates & Aggregates Risk for Key Engineering Basics

Automated Performance Metrics & Reporting for 7 Key Areas

- Safety Items
- Specifications, Standards, Processes, Drawings, & Models/Tools (SSPDM)
- Affordability Initiatives
- Ongoing Projects / Commitments
- Pyramid Management
- TCHA Domain Management/Integration
- Training, Qualifications & Certifications



Technical Warrant Holder Balanced Scorecard

TWH: ____________ Warrant Letter Date:______ Scorecard Date: _______
Name ____________ Pyramid Current as of:_______ SEA 05Z Review: _______

Recent Changes / Updates

FRB / Safety Items

SSPDM Management (Specs, Standards, Processes, Drawings, Models/Tools) 🔴

Specs: ______ # Standards: ______
1-5 yrs: ______ 1-5 yrs: ______
5-10 yrs: ______ 5-10 yrs: ______
10-15 yrs: ______ 10-15 yrs: ______
15-20 yrs: ______ 15-20 yrs: ______
+20 yrs: ______ +20 yrs: ______
Priority A: ______ Priority A: ______

Affordability Initiative (AI) (FYXX) 🟢

Title: ____________
Approved SEA 05Z: ______
Approved SEA 05: ______
Cost Saving: ______
BCA Completed: ______
AI Completed: ______
AI Published: ______

Major Projects / Commitments

Project 1: ____________ 🟢
Project 2: ____________ 🟢
Project 3: ____________ 🟡
Project 4: ____________ 🔴
Project 5: ____________ 🔴
Project 6: ____________ 🟢

Pyramid Management 🟡

Total Supporting: ______
Funded: ______
Tier 1a: ______

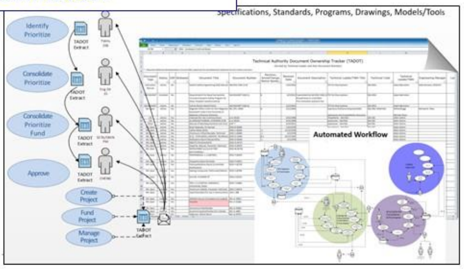
Issues: ______

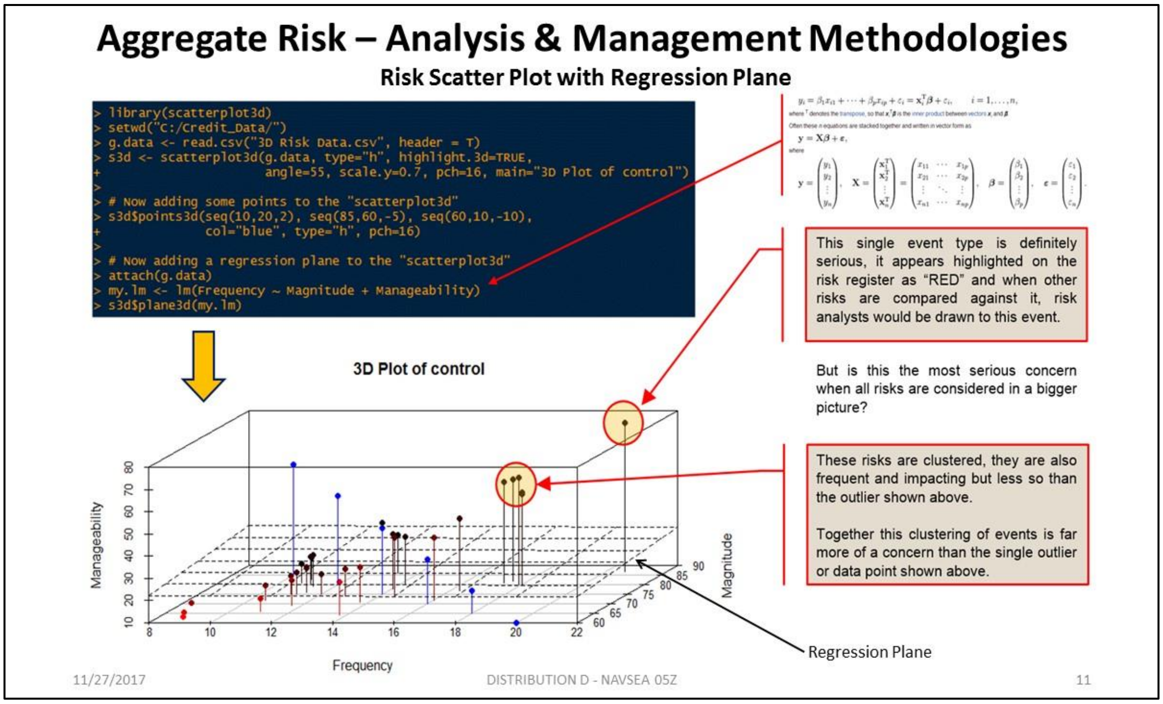
TCHA Domain Alignment 🟡

Total Supporting: ______
Funded FTE: ______
Unfunded FTE: ______
Tier 1a: ______
Location: ______

Issues: ______

Automated Workflow & Lessons Learned Dissemination





Aggregate Risk – Analysis & Management Methodologies

Risk Scatter Plot with Regression Plane

```
> library(scatterplot3d)
> setwd("C:/Credit_Data/")
> g.data <- read.csv("3D Risk Data.csv", header = T)
> s3d <- scatterplot3d(g.data, type="h", highlight.3d=TRUE,
+                      angle=55, scale.y=0.7, pch=16, main="3D Plot of control")
>
> # Now adding some points to the "scatterplot3d"
> s3d$points3d(seq(10,20,2), seq(85,60,-5), seq(60,10,-10),
+              col="blue", type="h", pch=16)
>
> # Now adding a regression plane to the "scatterplot3d"
> attach(g.data)
> my.lm <- lm(Frequency ~ Magnitude + Manageability)
> s3d$plane3d(my.lm)
```

$$y_i = \beta_1 x_{i1} + \cdots + \beta_p x_{ip} + \varepsilon_i = \mathbf{x}_i^{\mathsf T}\boldsymbol\beta + \varepsilon_i, \qquad i = 1, \ldots, n,$$

where $^{\mathsf T}$ denotes the transpose, so that $\mathbf{x}_i^{\mathsf T}\boldsymbol\beta$ is the inner product between vectors $\mathbf{x}_i$ and $\boldsymbol\beta$.

Often these n equations are stacked together and written in vector form as

$$\mathbf{y} = X\boldsymbol\beta + \boldsymbol\varepsilon,$$

where

$$\mathbf{y} = \begin{pmatrix} y_1 \\ y_2 \\ \vdots \\ y_n \end{pmatrix}, \quad X = \begin{pmatrix} \mathbf{x}_1^{\mathsf T} \\ \mathbf{x}_2^{\mathsf T} \\ \vdots \\ \mathbf{x}_n^{\mathsf T} \end{pmatrix} = \begin{pmatrix} x_{11} & \cdots & x_{1p} \\ x_{21} & \cdots & x_{2p} \\ \vdots & \ddots & \vdots \\ x_{n1} & \cdots & x_{np} \end{pmatrix}, \quad \boldsymbol\beta = \begin{pmatrix} \beta_1 \\ \beta_2 \\ \vdots \\ \beta_p \end{pmatrix}, \quad \boldsymbol\varepsilon = \begin{pmatrix} \varepsilon_1 \\ \varepsilon_2 \\ \vdots \\ \varepsilon_n \end{pmatrix}.$$

This single event type is definitely serious, it appears highlighted on the risk register as "RED" and when other risks are compared against it, risk analysts would be drawn to this event.

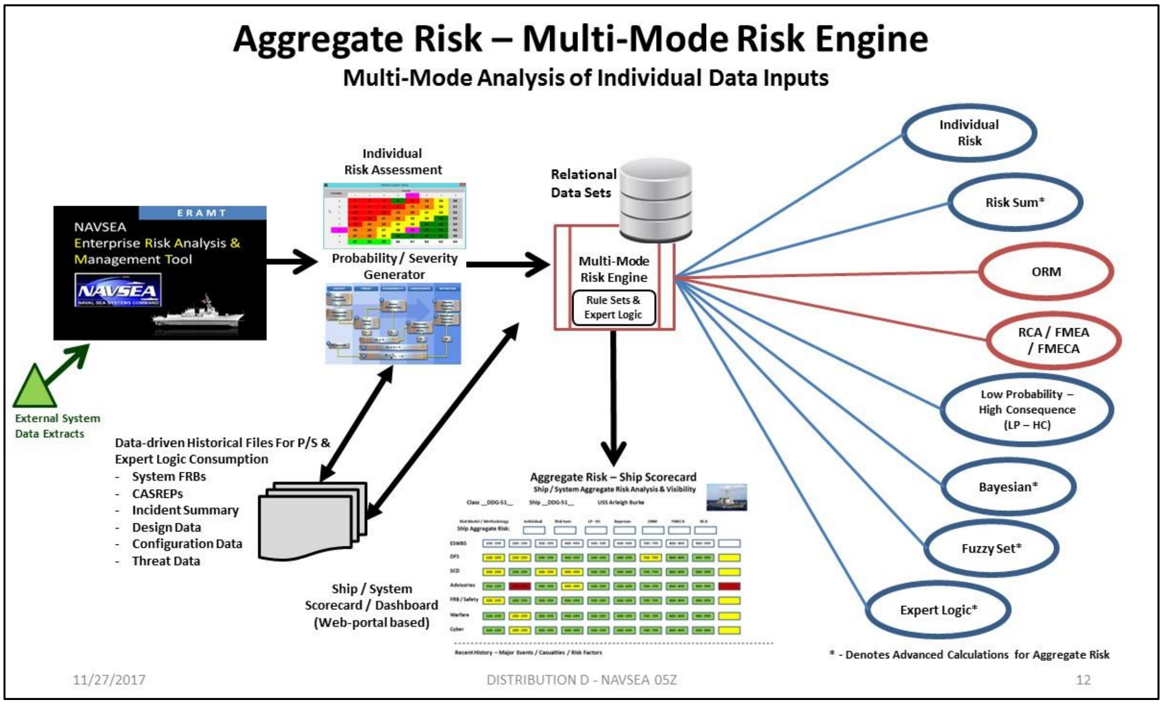
But is this the most serious concern when all risks are considered in a bigger picture?

These risks are clustered, they are also frequent and impacting but less so than the outlier shown above.

Together this clustering of events is far more of a concern than the single outlier or data point shown above.

Regression Plane

11/27/2017 DISTRIBUTION D - NAVSEA 05Z 11



Aggregate Risk – Multi-Mode Risk Engine

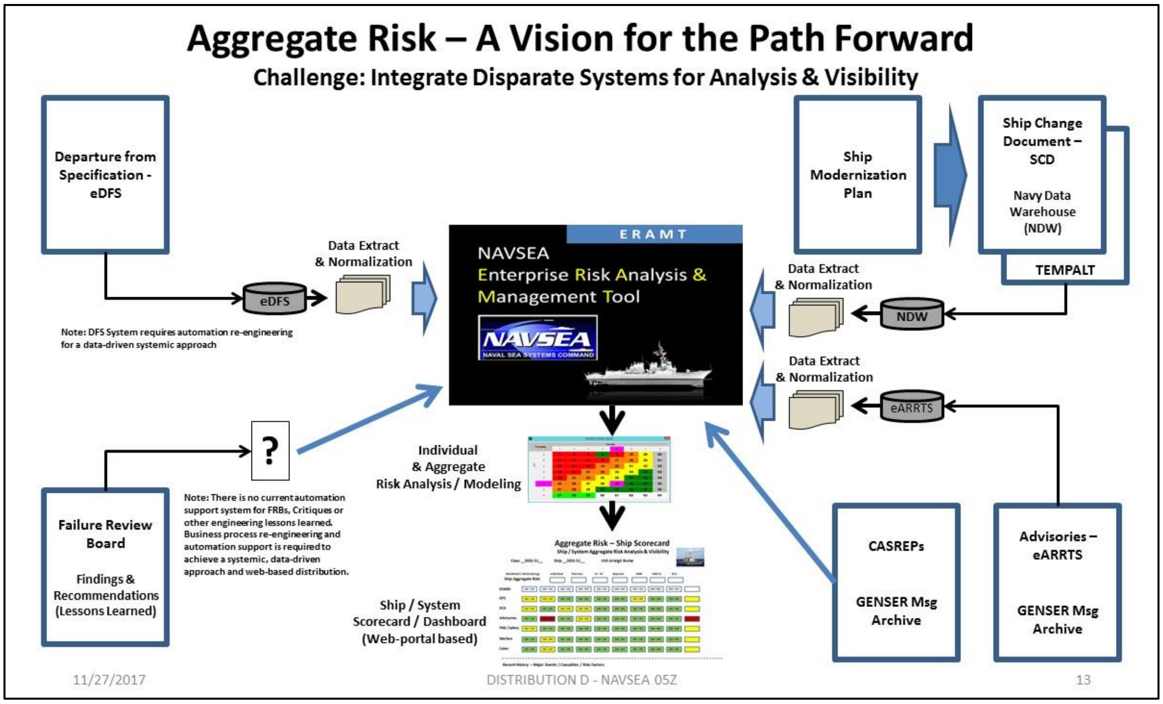
Multi-Mode Analysis of Individual Data Inputs

Data-driven Historical Files For P/S & Expert Logic Consumption

- System FRBs
- CASREPs
- Incident Summary
- Design Data
- Configuration Data
- Threat Data

* - Denotes Advanced Calculations for Aggregate Risk

11/27/2017 DISTRIBUTION D - NAVSEA 05Z 12



Aggregate Risk – A Vision for the Path Forward

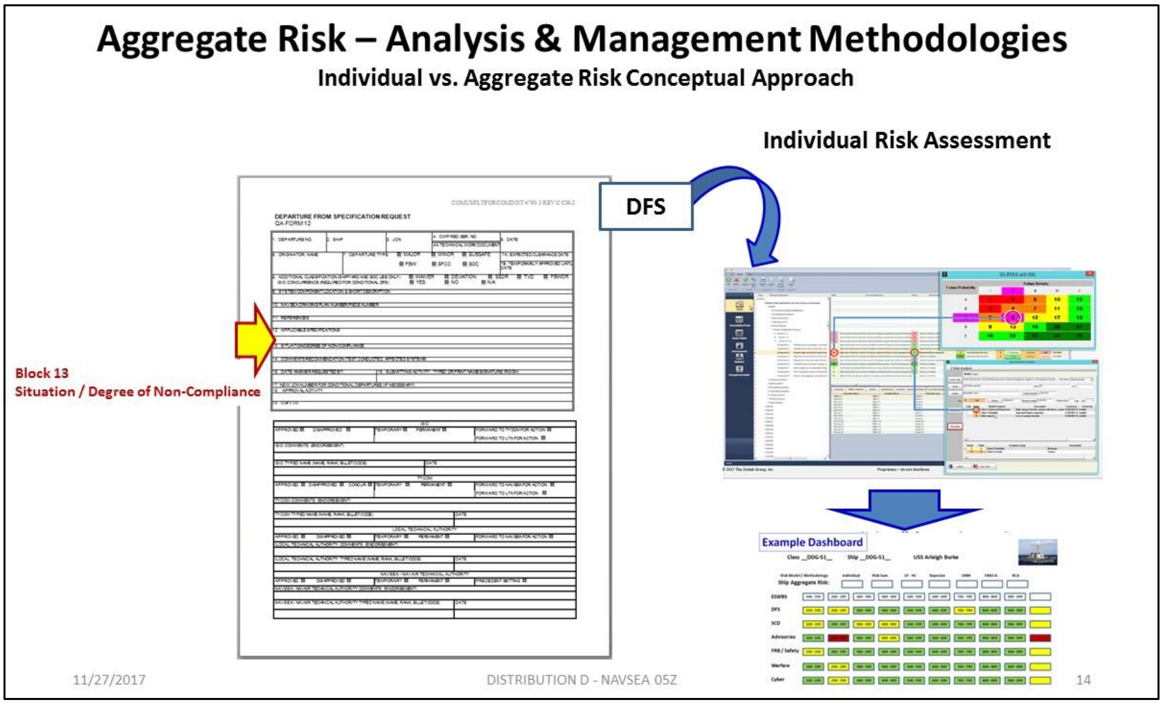
Challenge: Integrate Disparate Systems for Analysis & Visibility

Departure from Specification - eDFS
eDFS
Data Extract & Normalization
ERAMT
NAVSEA Enterprise Risk Analysis & Management Tool
NAVSEA
NAVAL SEA SYSTEMS COMMAND
Ship Modernization Plan
Ship Change Document – SCD
Navy Data Warehouse (NDW)
TEMPALT
Data Extract & Normalization
NDW
Data Extract & Normalization
eARRTS
?
Individual & Aggregate Risk Analysis / Modeling
Aggregate Risk – Ship Scorecard
Ship / System Aggregate Risk Analysis & Visibility
Ship / System Scorecard / Dashboard (Web-portal based)
Failure Review Board
Findings & Recommendations (Lessons Learned)
CASREPs
GENSER Msg Archive
Advisories – eARRTS
GENSER Msg Archive

Note: DFS System requires automation re-engineering for a data-driven systemic approach

Note: There is no current automation support system for FRBs, Critiques or other engineering lessons learned. Business process re-engineering and automation support is required to achieve a systemic, data-driven approach and web-based distribution.

11/27/2017 DISTRIBUTION D - NAVSEA 05Z 13



Aggregate Risk – Analysis & Management Methodologies

Individual vs. Aggregate Risk Conceptual Approach

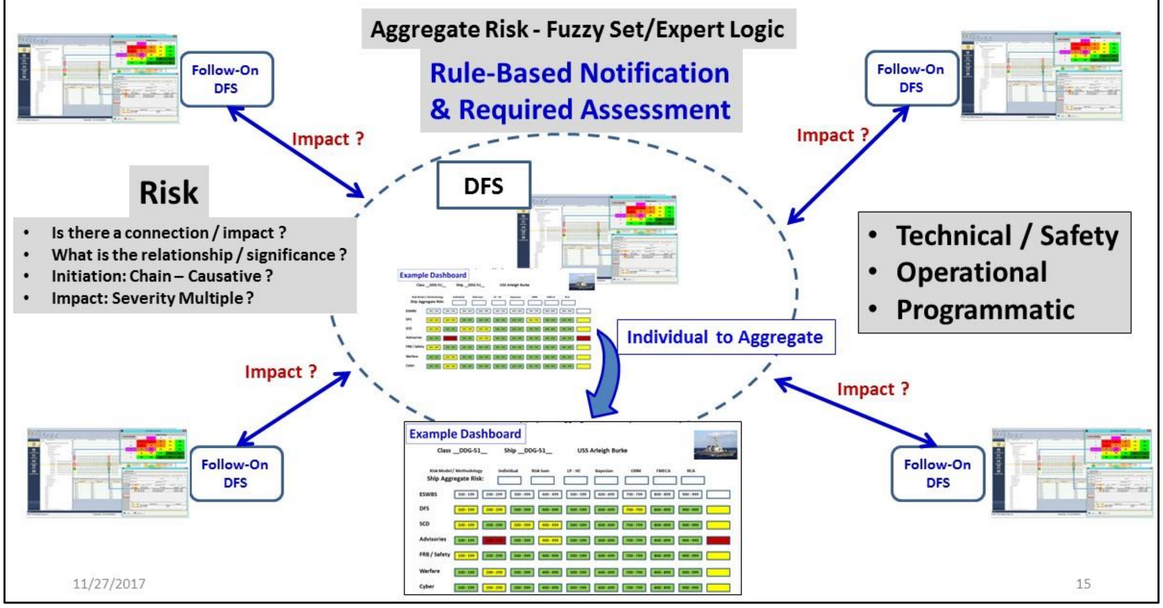
Individual Risk Assessment

Block 13
Situation / Degree of Non-Compliance

11/27/2017 DISTRIBUTION D - NAVSEA 05Z 14

Aggregate Risk – Analysis & Management Methodologies

DFS Individual vs. Aggregate Risk - Conceptual Approach



Aggregate Risk - Fuzzy Set/Expert Logic

Rule-Based Notification & Required Assessment

Risk

- Is there a connection / impact ?
- What is the relationship / significance ?
- Initiation: Chain – Causative ?
- Impact: Severity Multiple ?

- Technical / Safety
- Operational
- Programmatic

Example Dashboard

Class __DDG-51__ Ship __DDG-51__ USS Arleigh Burke

Risk Model / Methodology: Individual, Risk Sum, LP - HC, Bayesian, ORM, FMECA, RCA

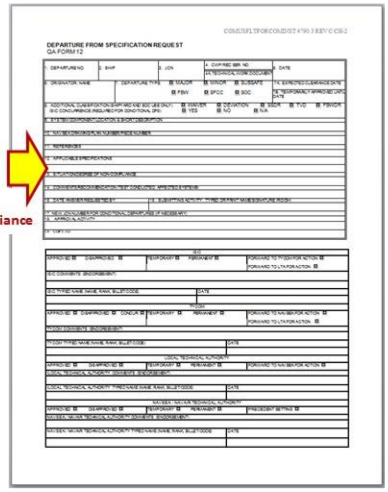
Ship Aggregate Risk:

ESWBS	100 - 199	200 - 299	300 - 399	400 - 499	500 - 599	600 - 699	700 - 799	800 - 899	900 - 999	
DFS	🟨 100 - 199	🟨 200 - 299	🟩 300 - 399	🟩 400 - 499	🟩 500 - 599	🟩 600 - 699	🟨 700 - 799	🟩 800 - 899	🟩 900 - 999	🟨
SCD	🟨 100 - 199	🟩 200 - 299	🟨 300 - 399	🟨 400 - 499	🟩 500 - 599	🟩 600 - 699	🟩 700 - 799	🟩 800 - 899	🟩 900 - 999	🟨
Advisories	🟩 100 - 199	🟥 200 - 299	🟩 300 - 399	🟨 400 - 499	🟩 500 - 599	🟩 600 - 699	🟩 700 - 799	🟩 800 - 899	🟩 900 - 999	🟥
FRB / Safety	🟨 100 - 199	🟩 200 - 299	🟩 300 - 399	🟩 400 - 499	🟩 500 - 599	🟩 600 - 699	🟩 700 - 799	🟩 800 - 899	🟩 900 - 999	🟨
Warfare	🟩 100 - 199	🟨 200 - 299	🟩 300 - 399	🟩 400 - 499	🟩 500 - 599	🟩 600 - 699	🟩 700 - 799	🟩 800 - 899	🟩 900 - 999	🟨
Cyber	🟩 100 - 199	🟨 200 - 299	🟩 300 - 399	🟩 400 - 499	🟩 500 - 599	🟩 600 - 699	🟩 700 - 799	🟩 800 - 899	🟩 900 - 999	🟨

Aggregate Risk – Analysis & Management Methodologies

DFS Aggregate Risk

DFS / eDFS must be data-driven



COMUSFLTFORCOMINST 4790.3 REV C CH-2

DEPARTURE FROM SPECIFICATION REQUEST
QA FORM 12

1. DEPARTURE NO. 2. SHIP 3. JCN 4. CWP REC SER. NO. 4A. TECHNICAL WORK DOCUMENT 5. DATE

6. ORIGINATOR NAME 7. DEPARTURE TYPE ☒ MAJOR ☒ MINOR ☒ SUBSAFE ☒ FBW ☒ SPCC ☒ SOC 7A. EXPECTED CLEARANCE DATE 7B. TEMPORARILY APPROVED UNTIL DATE

8. ADDITIONAL CLASSIFICATION (SHIPYARD AND SOC USE ONLY) ☒ WAIVER ☒ DEVIATION ☒ SSDR ☒ TYC ☒ FSWOR
ISIC CONCURRENCE (REQUIRED FOR CONDITIONAL DFS) ☒ YES ☒ NO ☒ N/A

9. SYSTEM/COMPONENT/LOCATION & SHORT DESCRIPTION

10. NAVSEA DRAWING/PLAN NUMBER/PIECE NUMBER

11. REFERENCES

12. APPLICABLE SPECIFICATIONS

13. SITUATION/DEGREE OF NON-COMPLIANCE

14. COMMENTS/RECOMMENDATION/TEST CONDUCTED, AFFECTED SYSTEMS

15. DATE ANSWER REQUESTED BY 16. SUBMITTING ACTIVITY, TYPED OR PRINT NAME/SIGNATURE /ROOM

17. NEW JCN/NUMBER FOR CONDITIONAL DEPARTURES (IF NECESSARY)

18. APPROVAL ACTIVITY

19. COPY TO

ISIC
APPROVED ☒ DISAPPROVED ☒ TEMPORARY ☒ PERMANENT ☒ FORWARD TO TYCOM FOR ACTION ☒ FORWARD TO LTA FOR ACTION ☒
ISIC COMMENTS (ENDORSEMENT)
ISIC TYPED NAME (NAME, RANK, BILLET CODE) DATE

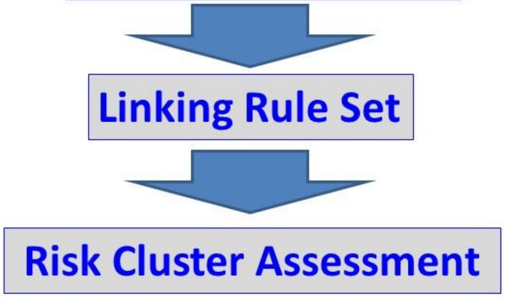
TYCOM
APPROVED ☒ DISAPPROVED ☒ CONCUR ☒ TEMPORARY ☒ PERMANENT ☒ FORWARD TO NAVSEA FOR ACTION ☒ FORWARD TO LTA FOR ACTION ☒
TYCOM COMMENTS (ENDORSEMENT)
TYCOM TYPED NAME (NAME, RANK, BILLET CODE) DATE

LOCAL TECHNICAL AUTHORITY
APPROVED ☒ DISAPPROVED ☒ TEMPORARY ☒ PERMANENT ☒ FORWARD TO NAVSEA FOR ACTION ☒
LOCAL TECHNICAL AUTHORITY COMMENTS (ENDORSEMENT)
LOCAL TECHNICAL AUTHORITY TYPED NAME (NAME, RANK, BILLET CODE) DATE

NAVSEA / NAVAIR TECHNICAL AUTHORITY
APPROVED ☒ DISAPPROVED ☒ TEMPORARY ☒ PERMANENT ☒ PRECEDENT SETTING ☒
NAVSEA / NAVAIR TECHNICAL AUTHORITY COMMENTS (ENDORSEMENT)
NAVSEA / NAVAIR TECHNICAL AUTHORITY TYPED NAME (NAME, RANK, BILLET CODE) DATE

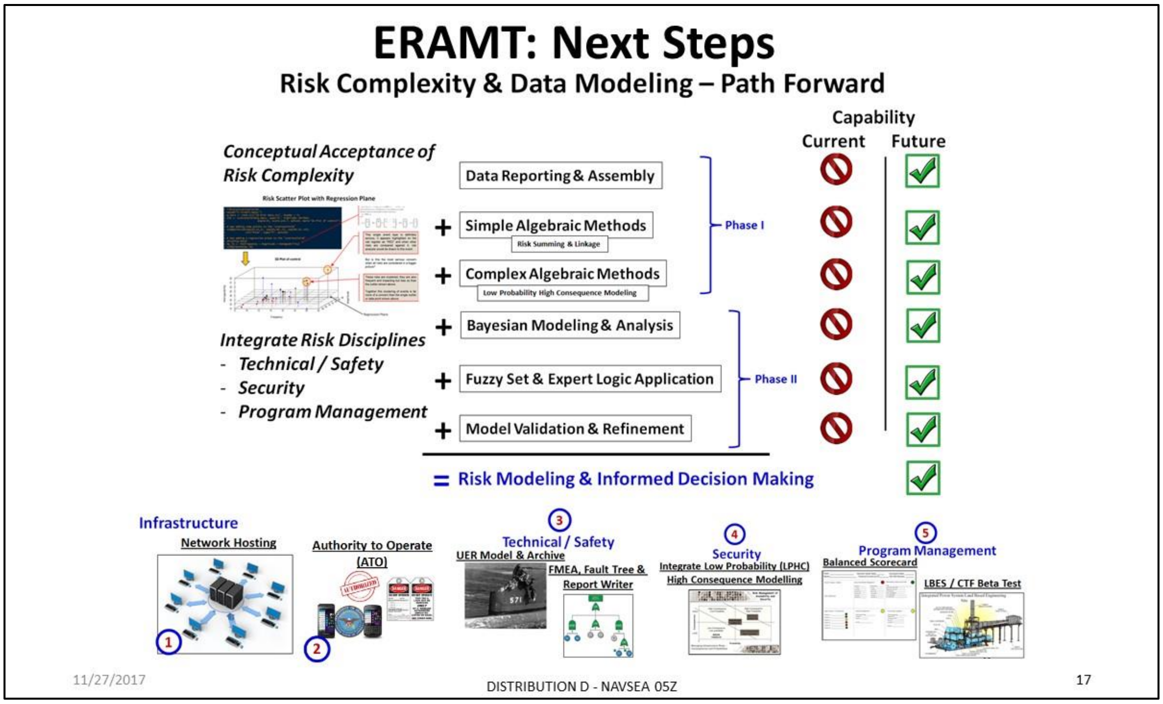
Block 13
Situation / Degree of Non-Compliance

- New, automated form
- Drop-down menus
- NASA "Big Sheet" equivalent
- ERAMT automated workflow
- Leap from individual to aggregate risk



Linking Rule Set

Risk Cluster Assessment



ERAMT: Next Steps

Risk Complexity & Data Modeling – Path Forward

Conceptual Acceptance of Risk Complexity

Integrate Risk Disciplines
- *Technical / Safety*
- *Security*
- *Program Management*

		Capability Current	Capability Future
Data Reporting & Assembly	Phase I	⊘	✓
+ Simple Algebraic Methods Risk Summing & Linkage		⊘	✓
+ Complex Algebraic Methods Low Probability High Consequence Modeling		⊘	✓
+ Bayesian Modeling & Analysis	Phase II	⊘	✓
+ Fuzzy Set & Expert Logic Application		⊘	✓
+ Model Validation & Refinement		⊘	✓
= Risk Modeling & Informed Decision Making			✓

Infrastructure

1 Network Hosting

2 Authority to Operate (ATO)

3 Technical / Safety
UER Model & Archive
FMEA, Fault Tree & Report Writer

4 Security
Integrate Low Probability (LPHC) High Consequence Modelling

5 Program Management
Balanced Scorecard
LBES / CTF Beta Test

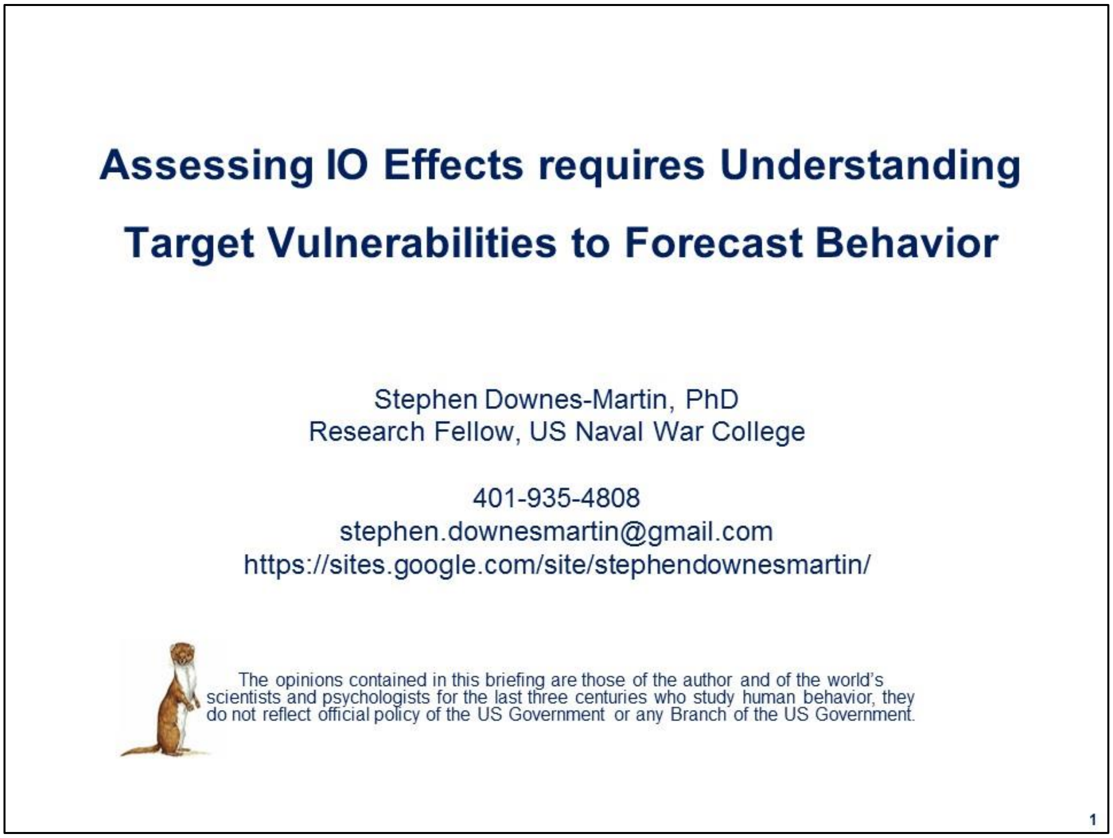
Questions?

C. Stephen Downes-Martin: Assessing IO Effects requires Understanding Target Vulnerabilities to Forecast Behavior

Presentation Summary

Mr. Downes-Martin highlighted the effects of bias and preconceived notions on gaming, doctrine, and policy-making. Information Operations (IO) are permanently ongoing, since the target is anyone and everyone. But the unanswered question remains "Was the IO successful?" since it is difficult if not impossible to determine whether the target's action would have been undertaken without the operation. However, human intelligence can help since most people's beliefs are bedrock solid and will not change even in the face of evidence proving otherwise. This is a topic worth investigating further.

Mr. Downes-Martin's presentation drew from his wide range of experience in gaming and included numerous references from his published work. His observations on cognitive bias in decision-making have clear repercussions for successful outcomes beyond just IO.



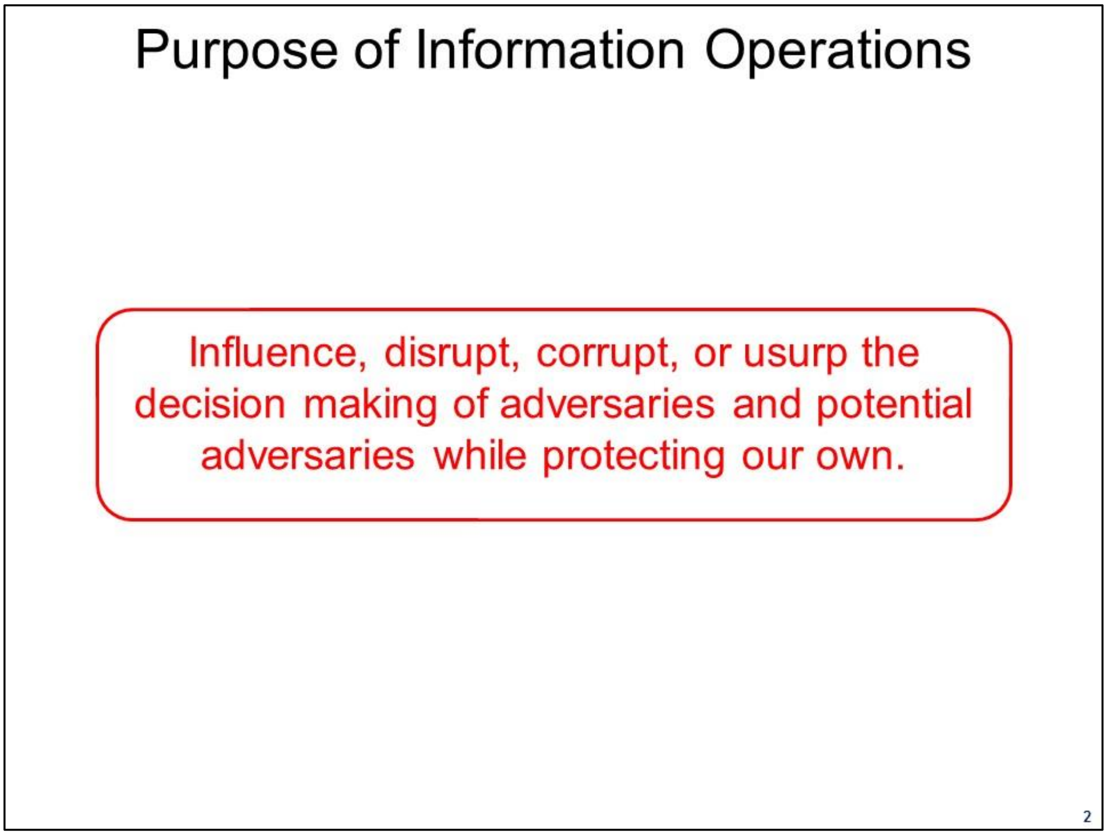
Assessing IO Effects requires Understanding Target Vulnerabilities to Forecast Behavior

Stephen Downes-Martin, PhD
Research Fellow, US Naval War College

401-935-4808
stephen.downesmartin@gmail.com
https://sites.google.com/site/stephendownesmartin/

The opinions contained in this briefing are those of the author and of the world's scientists and psychologists for the last three centuries who study human behavior, they do not reflect official policy of the US Government or any Branch of the US Government.

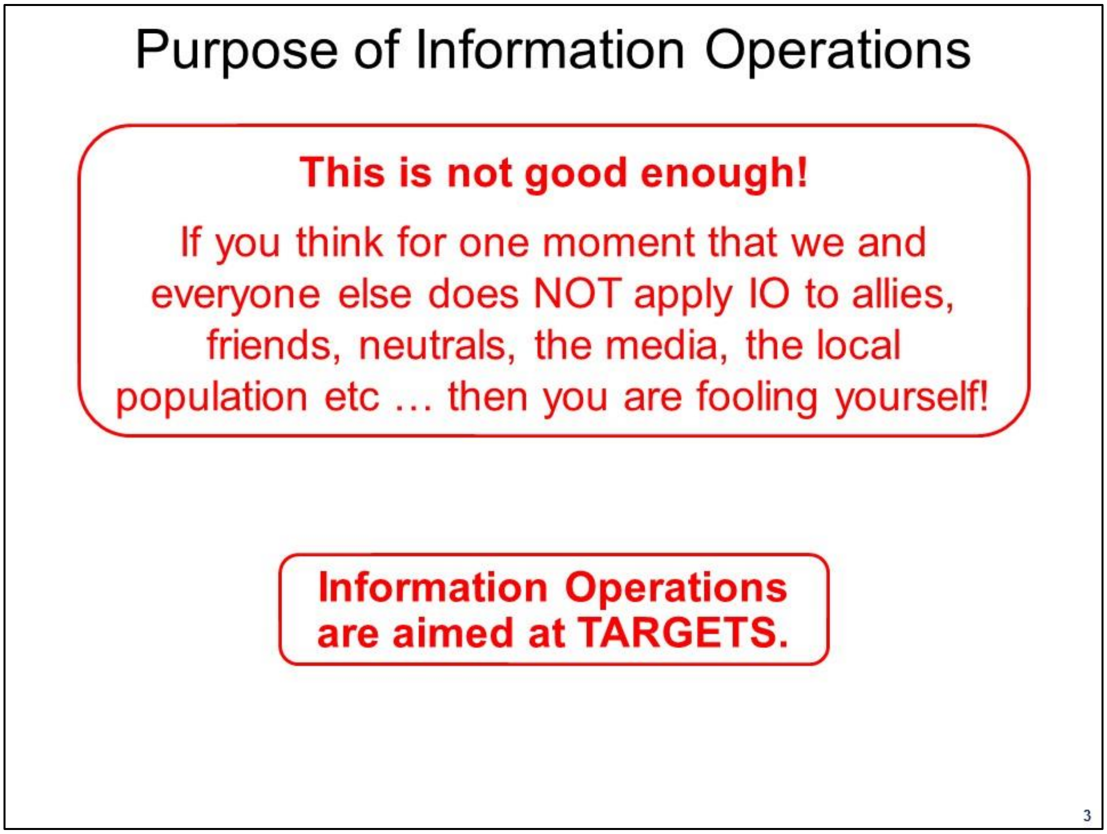
1



Purpose of Information Operations

Influence, disrupt, corrupt, or usurp the decision making of adversaries and potential adversaries while protecting our own.

2

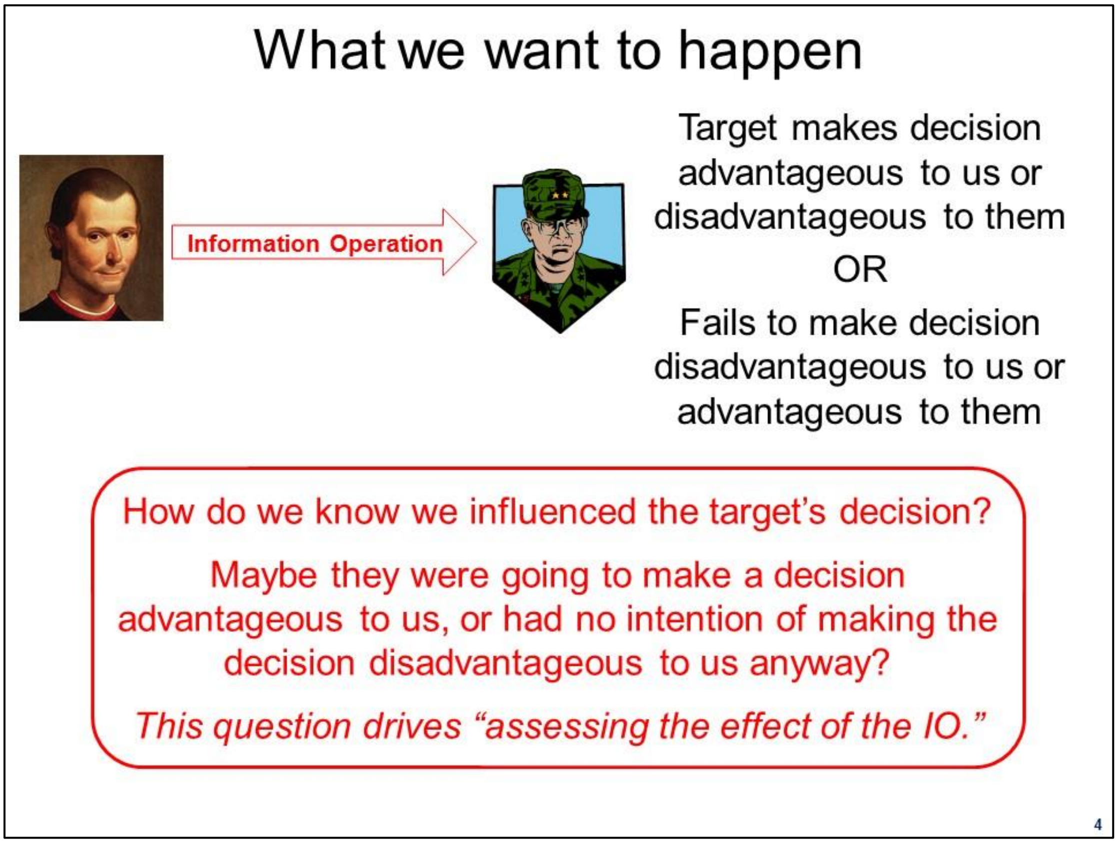


Purpose of Information Operations

This is not good enough!

If you think for one moment that we and everyone else does NOT apply IO to allies, friends, neutrals, the media, the local population etc … then you are fooling yourself!

Information Operations are aimed at TARGETS.



What we want to happen

Information Operation

Target makes decision advantageous to us or disadvantageous to them

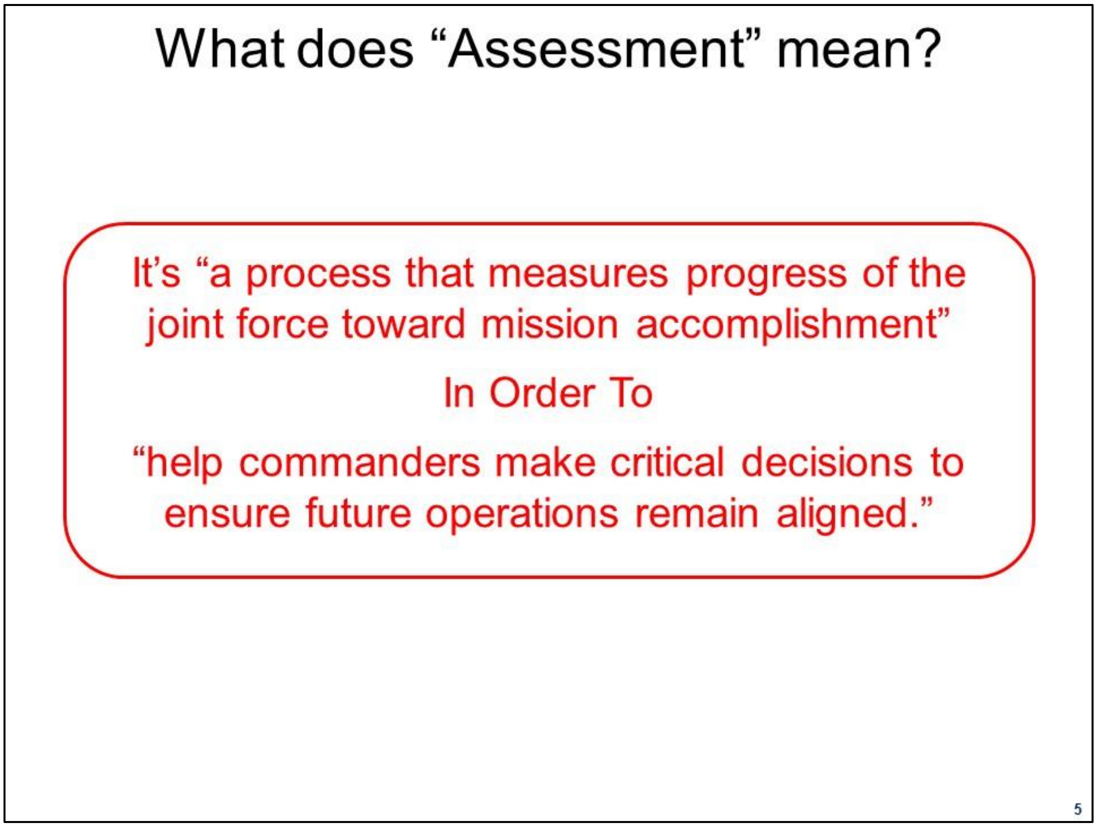
OR

Fails to make decision disadvantageous to us or advantageous to them

How do we know we influenced the target's decision?

Maybe they were going to make a decision advantageous to us, or had no intention of making the decision disadvantageous to us anyway?

This question drives "assessing the effect of the IO."

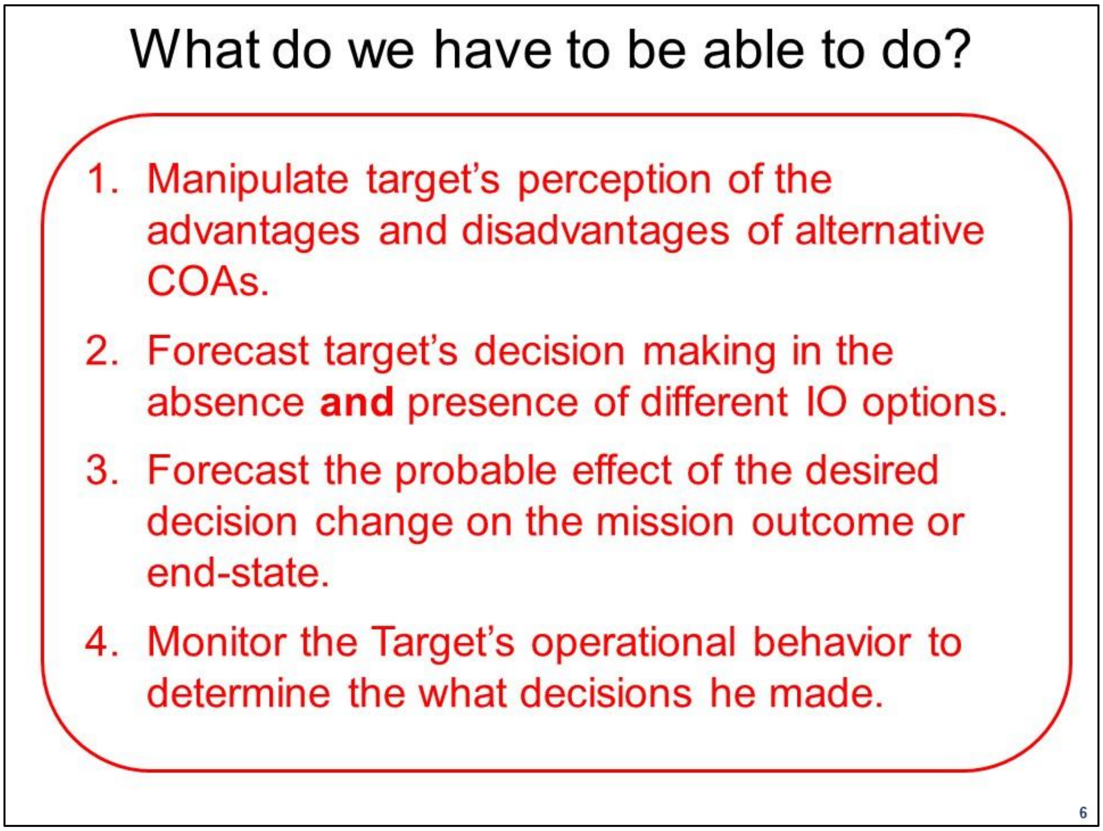


What does “Assessment” mean?

It’s “a process that measures progress of the joint force toward mission accomplishment”

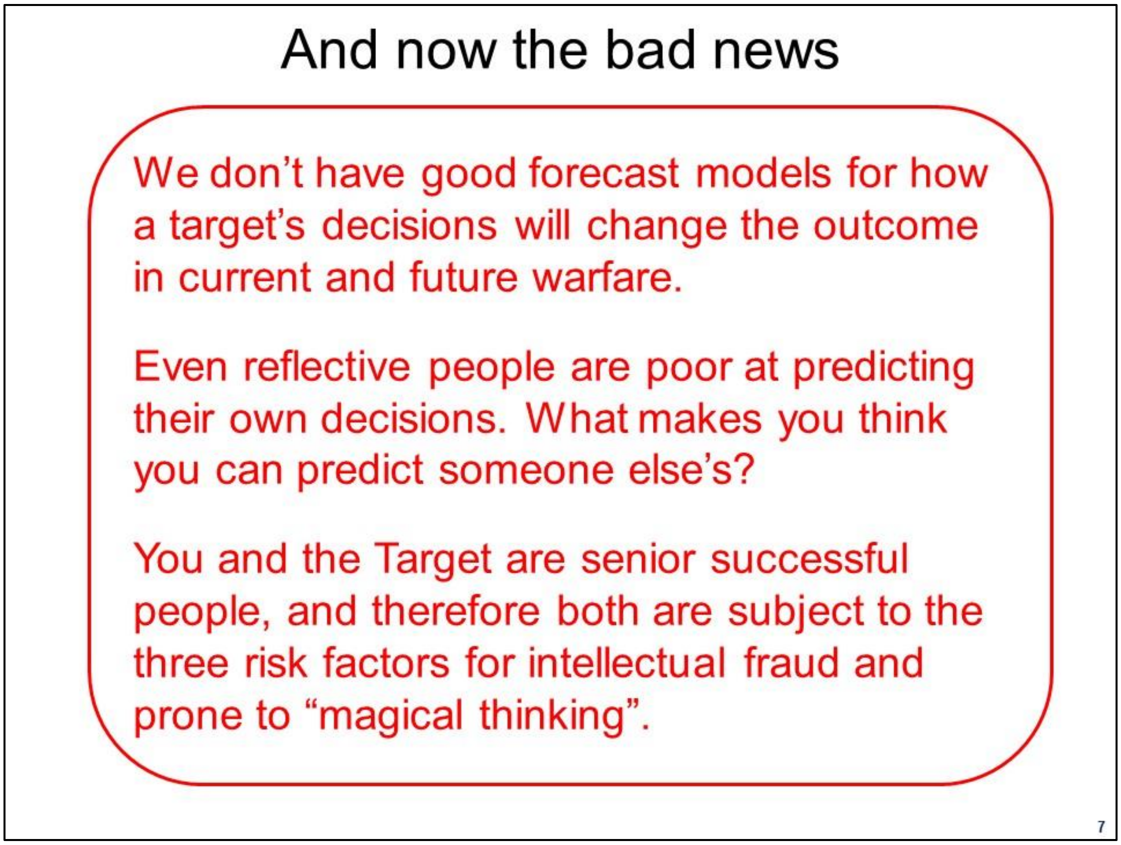
In Order To

“help commanders make critical decisions to ensure future operations remain aligned.”



What do we have to be able to do?

1. Manipulate target’s perception of the advantages and disadvantages of alternative COAs.
2. Forecast target’s decision making in the absence **and** presence of different IO options.
3. Forecast the probable effect of the desired decision change on the mission outcome or end-state.
4. Monitor the Target’s operational behavior to determine the what decisions he made.

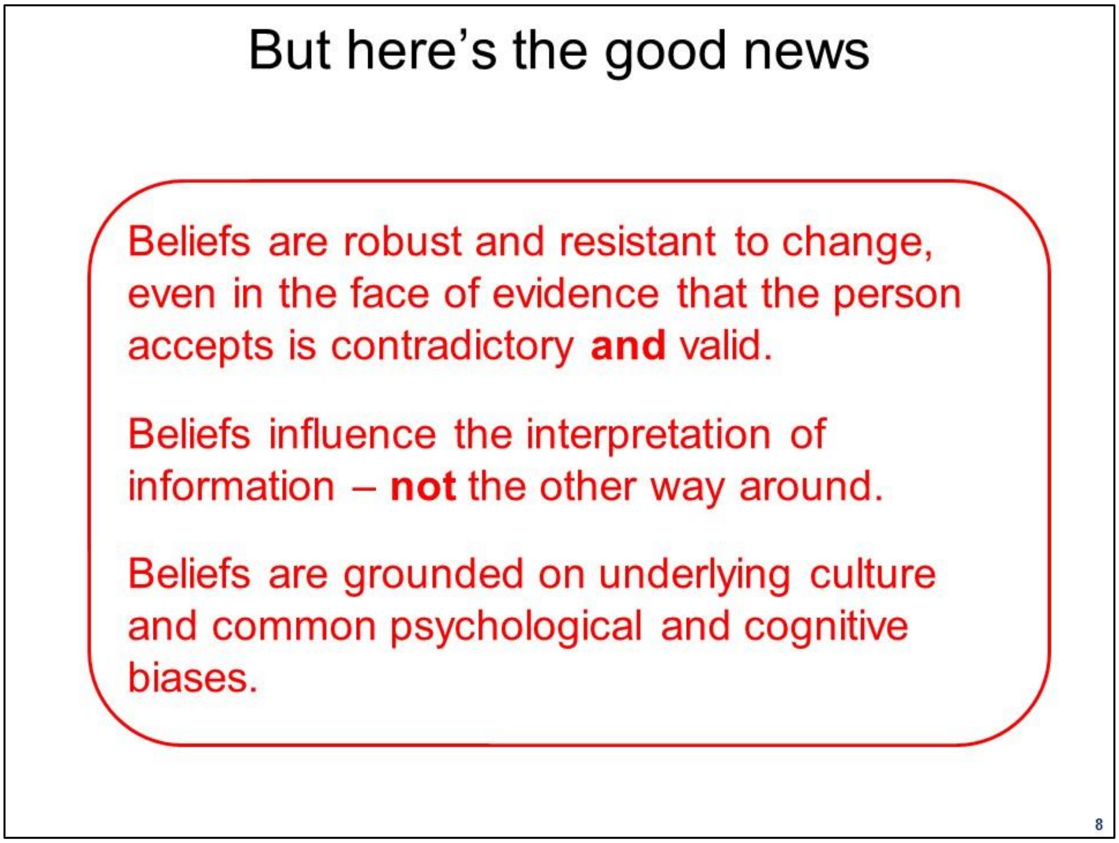


And now the bad news

We don't have good forecast models for how a target's decisions will change the outcome in current and future warfare.

Even reflective people are poor at predicting their own decisions. What makes you think you can predict someone else's?

You and the Target are senior successful people, and therefore both are subject to the three risk factors for intellectual fraud and prone to "magical thinking".

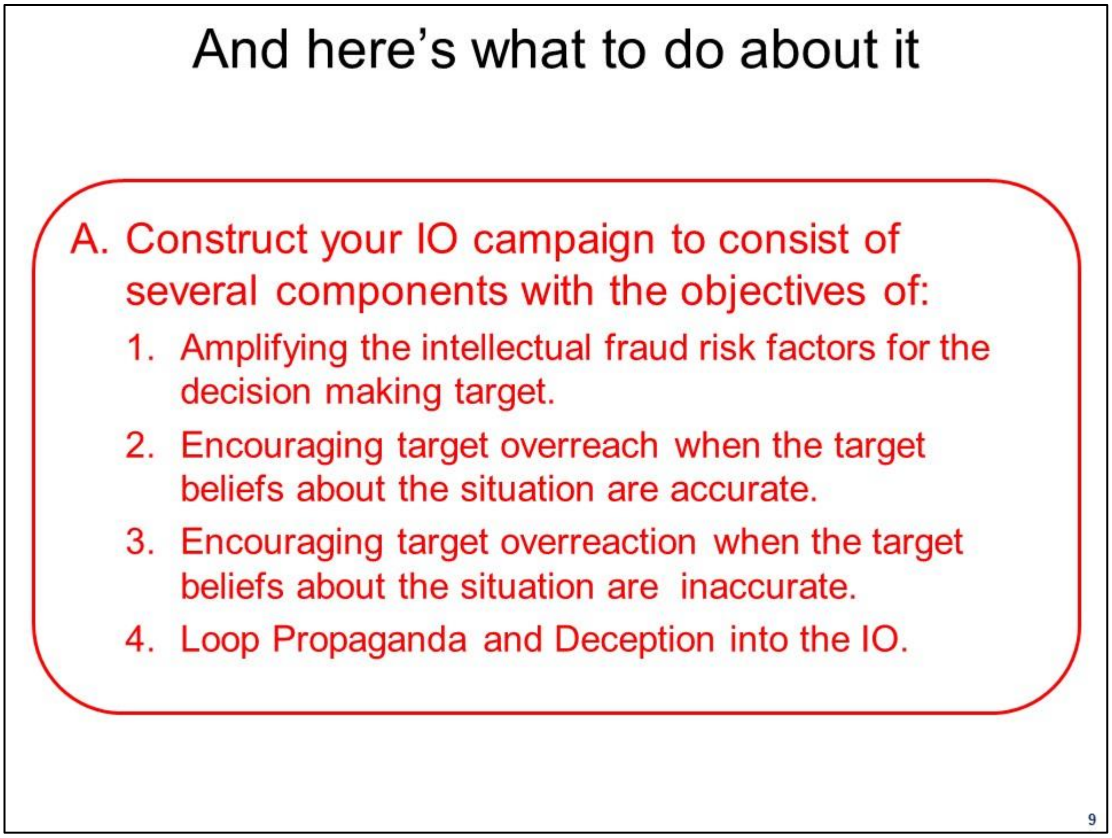


But here's the good news

Beliefs are robust and resistant to change, even in the face of evidence that the person accepts is contradictory **and** valid.

Beliefs influence the interpretation of information – **not** the other way around.

Beliefs are grounded on underlying culture and common psychological and cognitive biases.

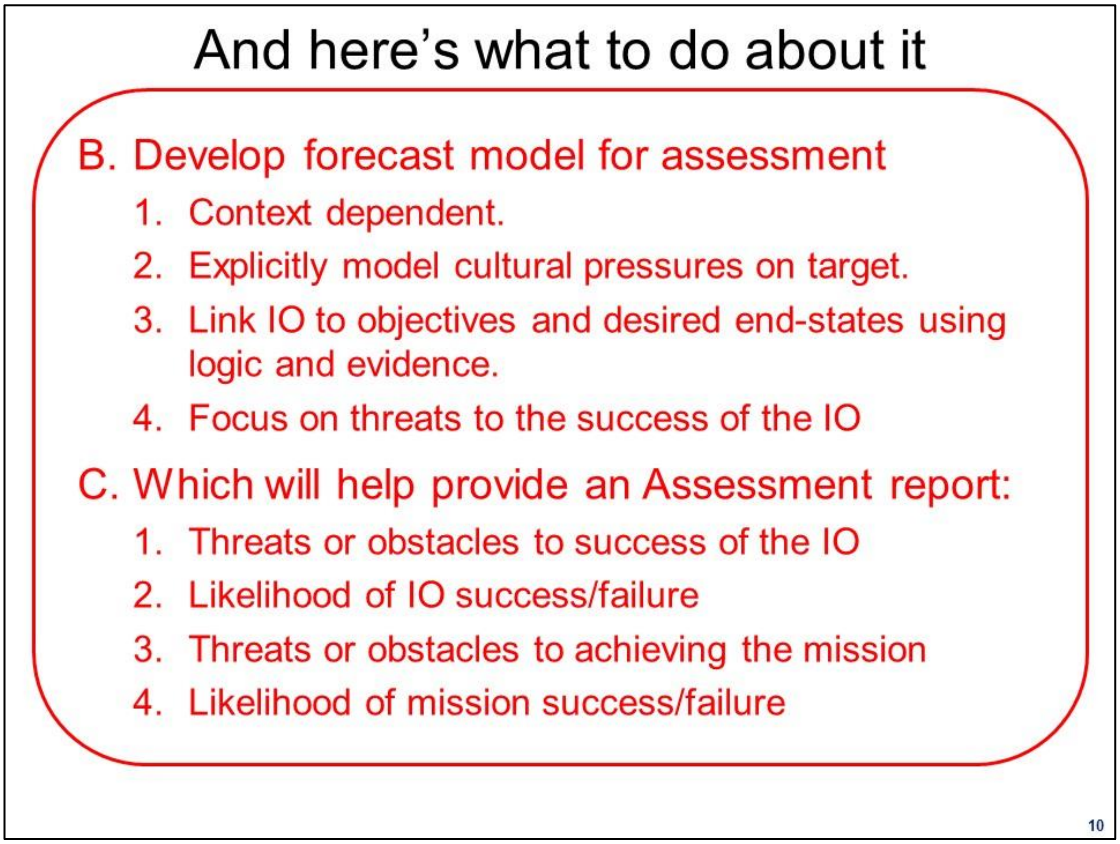


And here’s what to do about it

A. Construct your IO campaign to consist of several components with the objectives of:

1. Amplifying the intellectual fraud risk factors for the decision making target.
2. Encouraging target overreach when the target beliefs about the situation are accurate.
3. Encouraging target overreaction when the target beliefs about the situation are inaccurate.
4. Loop Propaganda and Deception into the IO.

9



And here’s what to do about it

B. Develop forecast model for assessment

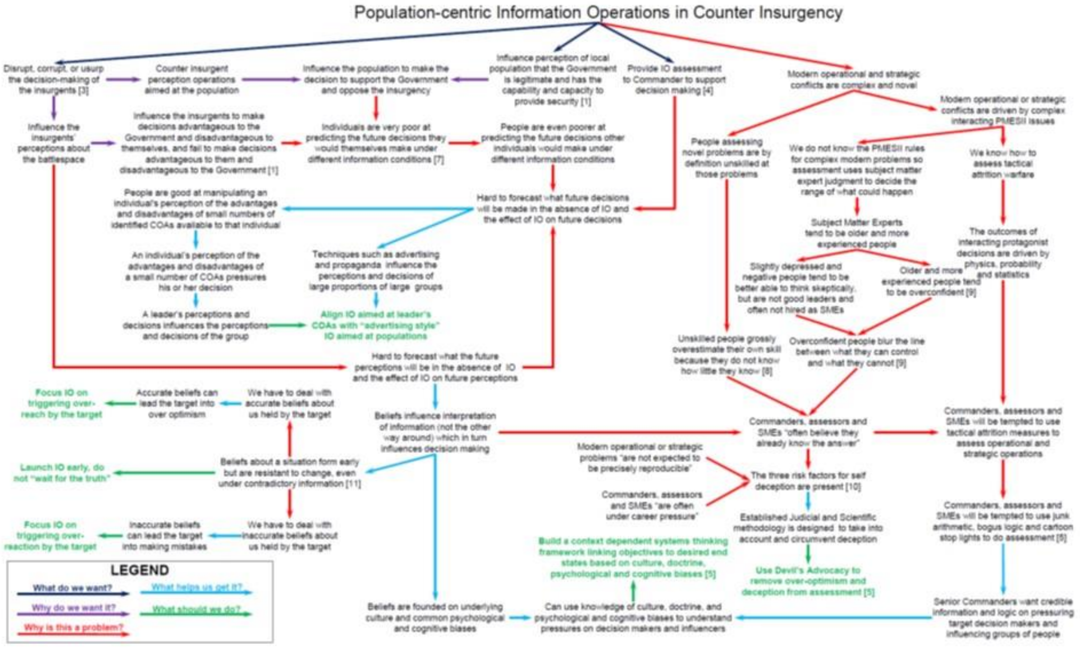
1. Context dependent.
2. Explicitly model cultural pressures on target.
3. Link IO to objectives and desired end-states using logic and evidence.
4. Focus on threats to the success of the IO

C. Which will help provide an Assessment report:

1. Threats or obstacles to success of the IO
2. Likelihood of IO success/failure
3. Threats or obstacles to achieving the mission
4. Likelihood of mission success/failure

10

Example: COIN IO Operations Framework



Population-centric Information Operations in Counter Insurgency

Disrupt, corrupt, or usurp the decision-making of the insurgents [3]

Counter insurgent perception operations aimed at the population

Influence the population to make the decision to support the Government and oppose the insurgency

Influence perception of local population that the Government is legitimate and has the capability and capacity to provide security [1]

Provide IO assessment to Commander to support decision making [4]

Modern operational and strategic conflicts are complex and novel

Modern operational or strategic conflicts are driven by complex interacting PMESII issues

Influence the insurgents' perceptions about the battlespace

Influence the insurgents to make decisions advantageous to the Government and disadvantageous to themselves, and fail to make decisions advantageous to them and disadvantageous to the Government [1]

Individuals are very poor at predicting the future decisions they would themselves make under different information conditions [7]

People are even poorer at predicting the future decisions other individuals would make under different information conditions

People assessing novel problems are by definition unskilled at those problems

We do not know the PMESII rules for complex modern problems so assessment uses subject matter expert judgment to decide the range of what could happen

We know how to assess tactical attrition warfare

People are good at manipulating an individual's perception of the advantages and disadvantages of small numbers of identified COAs available to that individual

Hard to forecast what future decisions will be made in the absence of IO and the effect of IO on future decisions

Subject Matter Experts tend to be older and more experienced people

The outcomes of interacting protagonist decisions are driven by physics, probability and statistics

An individual's perception of the advantages and disadvantages of a small number of COAs pressures his or her decision

Techniques such as advertising and propaganda influence the perceptions and decisions of large proportions of large groups

Slightly depressed and negative people tend to be better able to think skeptically, but are not good leaders and often not hired as SMEs

Older and more experienced people tend to be overconfident [9]

A leader's perceptions and decisions influences the perceptions and decisions of the group

Align IO aimed at leader's COAs with "advertising style" IO aimed at populations

Unskilled people grossly overestimate their own skill because they do not know how little they know [8]

Overconfident people blur the line between what they can control and what they cannot [9]

Hard to forecast what the future perceptions will be in the absence of IO and the effect of IO on future perceptions

Focus IO on triggering over-reach by the target

Accurate beliefs can lead the target into over optimism

We have to deal with accurate beliefs about us held by the target

Beliefs influence interpretation of information (not the other way around) which in turn influences decision making

Commanders, assessors and SMEs "often believe they already know the answer"

Commanders, assessors and SMEs will be tempted to use tactical attrition measures to assess operational and strategic operations

Launch IO early, do not "wait for the truth"

Beliefs about a situation form early but are resistant to change, even under contradictory information [11]

Modern operational or strategic problems "are not expected to be precisely reproducible"

The three risk factors for self deception are present [10]

Commanders, assessors and SMEs "are often under career pressure"

Focus IO on triggering over-reaction by the target

Inaccurate beliefs can lead the target into making mistakes

We have to deal with inaccurate beliefs about us held by the target

Established Judicial and Scientific methodology is designed to take into account and circumvent deception

Commanders, assessors and SMEs will be tempted to use junk arithmetic, bogus logic and cartoon stop lights to do assessment [5]

Build a context dependent systems thinking framework linking objectives to desired end states based on culture, doctrine, psychological and cognitive biases [5]

Use Devil's Advocacy to remove over-optimism and deception from assessment [5]

LEGEND

What do we want?

What helps us get it?

Why do we want it?

What should we do?

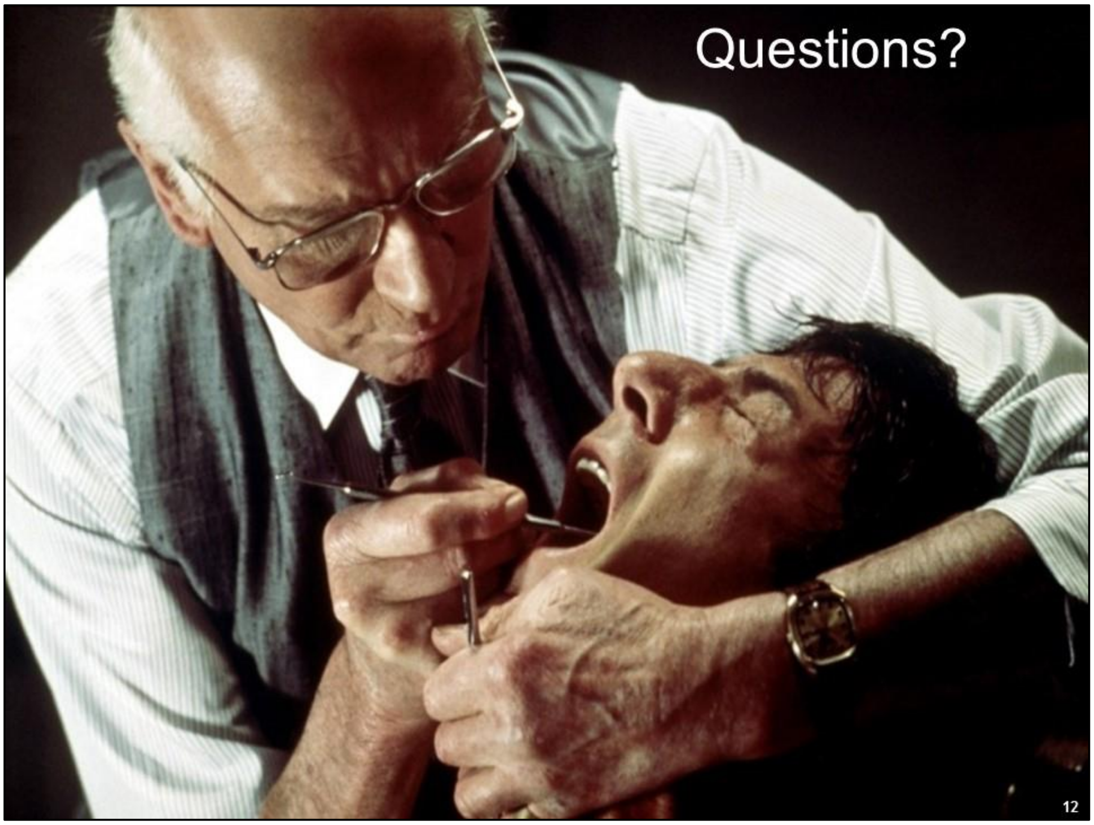
Why is this a problem?

Beliefs are founded on underlying culture and common psychological and cognitive biases

Can use knowledge of culture, doctrine, and psychological and cognitive biases to understand pressures on decision makers and influencers

Senior Commanders want credible information and logic on pressuring target decision makers and influencing groups of people

11



Questions?

12

Appendix A
Panelist Biographies

Elizabeth Bartels is a Ph.D student at the Pardee RAND Graduate School studying policy analysis. Her work seeks to improve games use in national security policy analysis by systematically documenting existing approaches and developing new tools. She also works as a game designer and analyst, specializing in games that explore novel topics or integrate other analytical techniques. She has a B.A. from the University of Chicago and an M.S. from the Massachusetts Institute of Technology in Political Science. Before coming to RAND, she worked as a game designer and national security analyst at the National Defense University and Caerus Associates.

Dr. John J. Borsi is an Operations Research Analyst in the Strategic Analysis and Wargaming Division of OSD CAPE (Analysis Integration). He received his B.S. in Engineering Sciences from the United States Air Force Academy, his Masters of Engineering in Operations Research and Industrial Engineering from Cornell, and his M.S. in Industrial Engineering and Ph.D. in Operations Research from Georgia Tech. At OSD CAPE, he designs and conducts wargames (tactical engagement, campaign, and strategic) across the full range of military operations, with an emphasis on analyzing UAVs, Space Communications, Cyberspace Operations, and Nuclear Command and Control. From 2001 through 2010, he was a contractor/civil servant, operations research analyst at HQAF/A9 conducting analyses on current operations and cyberspace operations. From 1980 through 2001, he was on active duty in the Air Force as an Aircraft structural test engineer, space systems logistics analyst, Assistant Professor (Air Force Institute of Technology), Mobility Ops analyst, Campaign Analysis Branch Chief, and AF Studies and Analysis Agency Chief Analyst.

Kathleen M. Conley serves as a research staff member at the Institute for Defense Analyses. Prior to joining IDA, she served as the Director of Land Forces Division, Cost Assessment and Program Evaluation (CAPE), Office of the Secretary of Defense, Washington, D.C., from August 2006 to October 2011. She was responsible for providing direction and analysis for high-level ground forces studies, as well as for articulating guidance for future service programs, assessing service program proposals, and assisting in acquisition milestone reviews. She also served as the Director of CAPE's Projection Forces Division from 2003 to 2006, where she led several major mobility capability and requirement studies.

After her commissioning as an officer in the U.S. Air Force 1980, she attended Cornell University followed by pilot training. Following an initial assignment as a C-141 aircraft commander at Norton Air Force Base, California, she completed a variety of operational and staff assignments, including Air Staff training officer, joint exercise planner, C-141 and C-17 operations officer, and T-1A squadron commander, culminating with her assignment as the Chief of Special Air Missions in the Office of the Vice Chief of Staff, United States Air Force. She retired in the grade of colonel.

Her education includes a Bachelor of Science Degree in Operations Research, Management, and Humanities from the United States Air Force Academy (distinguished graduate), a Master of Science Degree in Operations Research from Cornell University, and a Master of Arts Degree in National Security and Strategic Studies from the Naval War College. Her professional military education includes Squadron Officers School, College of Naval Command and Staff (graduated with highest distinction), Armed Forces Staff College, and National Defense Fellow at Harvard University's John M. Olin Institute for Strategic Studies.

While on active duty, Ms. Conley was awarded the Legion of Merit, the Defense Meritorious Service Medal (two awards), the Meritorious Service Medal (four awards), the Joint Service Commendation Medal, and the Air Force Commendation Medal. She is a command pilot with more than 3,200 hours in a variety of military aircraft.

Dr. Stephen Downes-Martin is a Senior Research Fellow at the U.S. Naval War College, a Senior Associate of the Center on Irregular Warfare and Armed Groups, and an independent scholar researching, teaching, and supporting wargaming, game theory, confrontation analysis, systems thinking, decision support and analysis, negotiation analysis, and deception and assessments methods applied to problems at the strategic, operational, and tactical levels of warfare and business. A research focus is on how to manipulate such methods to deceive decision makers, how decision makers misuse such methods to deceive themselves, and how to detect such attempts and protect decision makers from them. He works with and for a wide variety of government, military, aerospace, academic, and commercial organizations in the United States and internationally.

Dr. John Hanley earned his doctorate in operations research and management science at Yale University, writing his dissertation *On Wargaming*. A former U.S. Navy nuclear submarine officer and fleet exercise analyst employing military modeling to conduct campaign analyses, he used gaming extensively during his service with the first eighteen Chief of Naval Operations Strategic Studies Groups as an analyst, Program Director, and Deputy Director. He also served as Special Assistant to Commander in Chief, U.S. Forces Pacific; in the Office of the Secretary of Defense (Offices of Force Transformation; Acquisition, Technology and Logistics; and Strategy); and as Deputy Director of the Joint

Advanced Warfighting Program at the Institute for Defense Analyses. Retiring from government in 2012 after serving as Director for Strategy at the Office of the Director of National Intelligence, he is now an independent consultant.

Stephanie Helm specializes in information operations, cyberspace operations, and strategic communication support for war gaming and other defense security projects as an employee of Network Simulation and Technologies, Incorporated. She is also Adjunct Faculty at the Naval War College, teaching electives in her area of expertise.

Mrs. Helm retired from active duty in the U.S. Navy as a Captain, Special Duty Information Warfare. During her naval career, she specialized in information warfare and cryptology, and was designated as Joint Specialty Officer. Her assignments included Military Professor in the Joint Military Operations Department of the Naval War College; Staff Officer assignments on OPNAV N3/N5, Second Fleet, USCENTCOM, and National Security Agency staffs; Commanding Officer of the Naval Security Group Activity, Norfolk, Virginia; and various cryptologic assignments in Maine, Italy, California, and Virginia.

Mrs. Helm was a Fellow at the Massachusetts Institute of Technology Seminar XXI program. She earned her Master of Arts Degree in National Security and Strategic Studies from the Naval War College and a Bachelor of Arts degree in Slavic Languages and Literature at the University of California.

Lieutenant Commander Connor S. McLemore graduated from the U.S. Naval Academy in 2000 with a Bachelor of Science in Mechanical Engineering. He was designated a Naval Flight Officer in 2002. Upon completion of flight training, he reported to his first fleet assignment with the "Sun Kings" of Carrier Command and Control Squadron 116 (VAW-116) aboard USS *Constellation* (CV 64). While at VAW-116, he deployed to the Persian Gulf in support of Operations *Southern Watch* and *Iraqi Freedom*, accumulating over 150 flight hours during major combat operations. In 2004, he deployed aboard USS *Abraham Lincoln* (CVN 72) to the Indian Ocean and Western Pacific in support of the humanitarian Operation *Unified Assistance*.

In 2007, he returned to VAW-116 as Weapons and Tactics Instructor and was designated a CVW-2 Dynamic Strike Lead deployed aboard USS *Abraham Lincoln* (CVN 72). While at VAW-116, he deployed to the Arabian Gulf and Gulf of Oman in support of Operations *Iraqi Freedom* and *Enduring Freedom*.

In 2010, Lieutenant Commander McLemore completed an Operations Research Master's Degree at the Naval Postgraduate School in Monterey, California. His thesis was awarded the Military Operations Research Society Stephen A. Tisdale Graduate Research Award.

In January 2011, Lieutenant Commander McLemore assumed duties as Plans Officer on the staff of Commander, Combined Joint Special Operations Air Component (CJSOAC) in Al-Udied, Qatar. While there, he completed a National Security and Strategic Studies Masters Degree with distinction from the Naval War College in Newport, Rhode Island.

In October 2011, Lieutenant Commander McLemore joined Tactical Air Control Squadron (TACRON) 12, Detachment Alfa, in Okinawa, Japan, deployed aboard USS *Bonhomme Richard* (LHD 6). While at TACRON 12, he deployed regularly to Korea, Australia, and the Philippines for major exercises and was the lead Navy Air Officer in the Joint Task Force 505 Headquarters in support of Philippine Typhoon relief; the humanitarian Operation *Damayan*.

In May 2014, Lieutenant Commander McLemore returned to the Naval Postgraduate School as a Military Assistant Professor of Operations Research and the Operations Research Program Officer. In June 2017, Lieutenant Commander McLemore joined the Office of the Chief of Naval Operations (OPNAV) Assessments Division (N81) as the Integrated Fires Section Head.

Lieutenant Commander McLemore is a graduate of the Navy Fighter Weapons School (Topgun), Naval Aviation Safety Officer School, and Naval Strike and Air Warfare Center's Advanced Mission Commander Course (AMCC).

Stephen Olechnowicz is a Research Staff Member with the Institute for Defense Analyses (IDA) where he leads and participates in research examining the use of scientific and technical information in the execution of national and Defense security programs, cyberspace workforce challenges, and acquisition of capabilities. He works with the DoD Chief Information, the Military Services, USCYBERCOM, National Security Agency, and Defense Information Systems Agency on matters relating to cybersecurity, cyberspace workforce development, cyberspace operations, nuclear command and control, and Insider Threat. Stephen is a significant contributor to the just-released NIST Special Publication 800-181 National Initiative for Cybersecurity Education (NICE) Cybersecurity Workforce Framework and to the Draft Cybersecurity Curricula 2017 Guidelines for Post-Secondary Degree Programs. He is a retired Navy Nuclear Submarine Officer and served three years in the then Office of Secretary of Defense Program Analyses and Evaluation. He holds a Master of Science in Operations Research from the Naval Postgraduate School and is a member of the Military Operations Research Society and IEEE.

Commander Phil Pournelle (Retired) retired after 26 years in the U.S. Navy as a Surface Warfare Officer, contingency planner, and Operations Analyst. At sea, he served as an Electronics Material Officer, Electronic Warfare Officer, Aegis Fire Control Officer (missile systems), Tactical Action Officer, and Operations Officer. He served on cruisers, destroyers, amphibious ships, and as the Executive Officer aboard an experimental High Speed Vessel. He served as the Future Plans (contingencies) Officer at Expeditionary Strike Group Five (ESG-5) in the Central Command area of responsibility.

He served for three years on the Navy headquarters staff (OPNAV N-81) where he conducted Campaign Analysis employing Modeling and Simulation (M&S) and was the founding director of the Navy's World Class Modeling program. He served for three years at the Office of the Secretary of Defense's Cost Assessment and Program Evaluation (CAPE) where he did mobility and Naval warfare analysis. He served for five years as advisor to the Director of the Office of Net Assessment. He has a master's degree in Operations Analysis from the Naval Postgraduate School in Monterey, California. He was the chair of the 2016 Military Operations Research Society's Wargaming Workshop and will be the Chair of the forthcoming 2017 Workshop. He is now Senior Director for Gaming and Analysis at the Long Term Strategy Group.

REPORT DOCUMENTATION PAGE	*Form Approved* *OMB No. 0704-0188*

Public reporting burden for this collection of information is estimated to average 1 hour per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing this collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden to Department of Defense, Washington Headquarters Services, Directorate for Information Operations and Reports (0704-0188), 1215 Jefferson Davis Highway, Suite 1204, Arlington, VA 22202-4302. Respondents should be aware that notwithstanding any other provision of law, no person shall be subject to any penalty for failing to comply with a collection of information if it does not display a currently valid OMB control number. **PLEASE DO NOT RETURN YOUR FORM TO THE ABOVE ADDRESS.**

1. REPORT DATE (DD-MM-YY) 11/00/17	2. REPORT TYPE Non-Standard	3. DATES COVERED (From – To)

4. TITLE AND SUBTITLE Assessing Information Effects Workshop Proceedings	5a. CONTRACT NUMBER HQ0034-14-D-0001
	5b. GRANT NUMBER
	5c. PROGRAM ELEMENT NUMBERS
6. AUTHOR(S) Stephen M. Olechnowicz, John T. Hanley, Jr., John A. Cordero, G. Lee Kennedy	5d. PROJECT NUMBER C5107
	5e. TASK NUMBER
	5f. WORK UNIT NUMBER
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESSES Institute for Defense Analyses 4850 Mark Center Drive Alexandria, VA 22311-1882	8. PERFORMING ORGANIZATION REPORT NUMBER NS D-8858
9. SPONSORING / MONITORING AGENCY NAME(S) AND ADDRESS(ES) Institute for Defense Analyses	10. SPONSOR'S / MONITOR'S ACRONYM IDA
	11. SPONSOR'S / MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION / AVAILABILITY STATEMENT

Approved for public release; distribution is unlimited.

13. SUPPLEMENTARY NOTES

Project Leader: Stephen M. Olechnowicz

14. ABSTRACT

On October 16, 2017, representatives from the Institute for Defense Analyses (IDA), the Office of Secretary of Defense for Cost Analysis and Program Evaluation (OSD CAPE), the US Naval War College, the Chief of Naval Operations Assessments Division (OPNAV N81), academia, and industry met at IDA in Alexandria, Virginia for a half-day workshop to foster dialog on assessing information. The topics addressed in this workshop offer ideas on how to model the effects of information through a variety of analytical efforts to gain insight on a potential adversary's behavior in cyber and information warfare. This document contains the proceedings of the workshop.

15. SUBJECT TERMS

Simulations; information operations; modeling and simulation; war gaming; information effects in warfare

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	Unlimited	118	19b. TELEPHONE NUMBER (Include Area Code)