NPS MDP Study
Outbrief Schedule, 1 JUN 2005

0800-0815 Introductions

0815-0915 Background/Results

0930-1015 Cargo Inspection System (Land)

1030-1130 Cargo Inspection System (Sea)

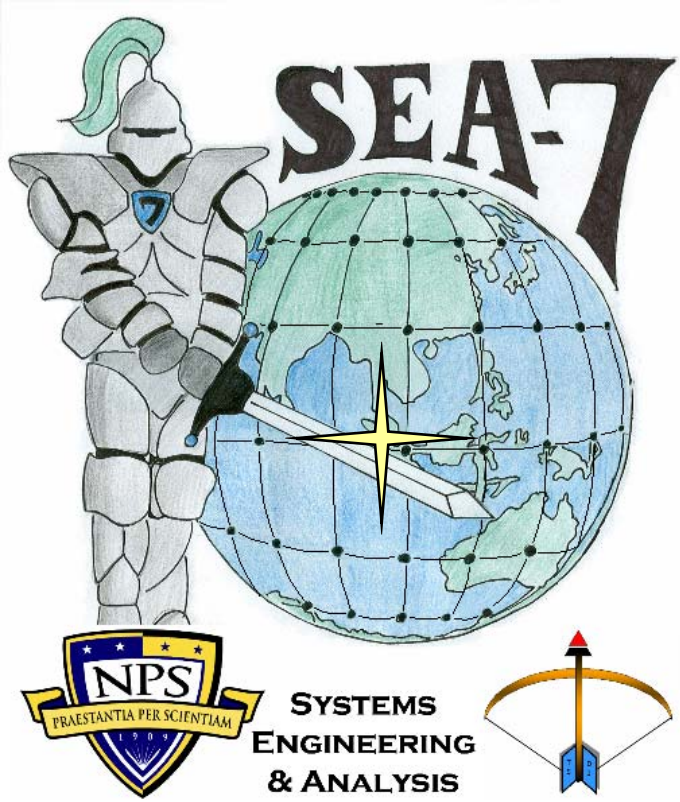
1130-1230 LUNCH

1230-1330 Sensor System

1345-1445 C3I System

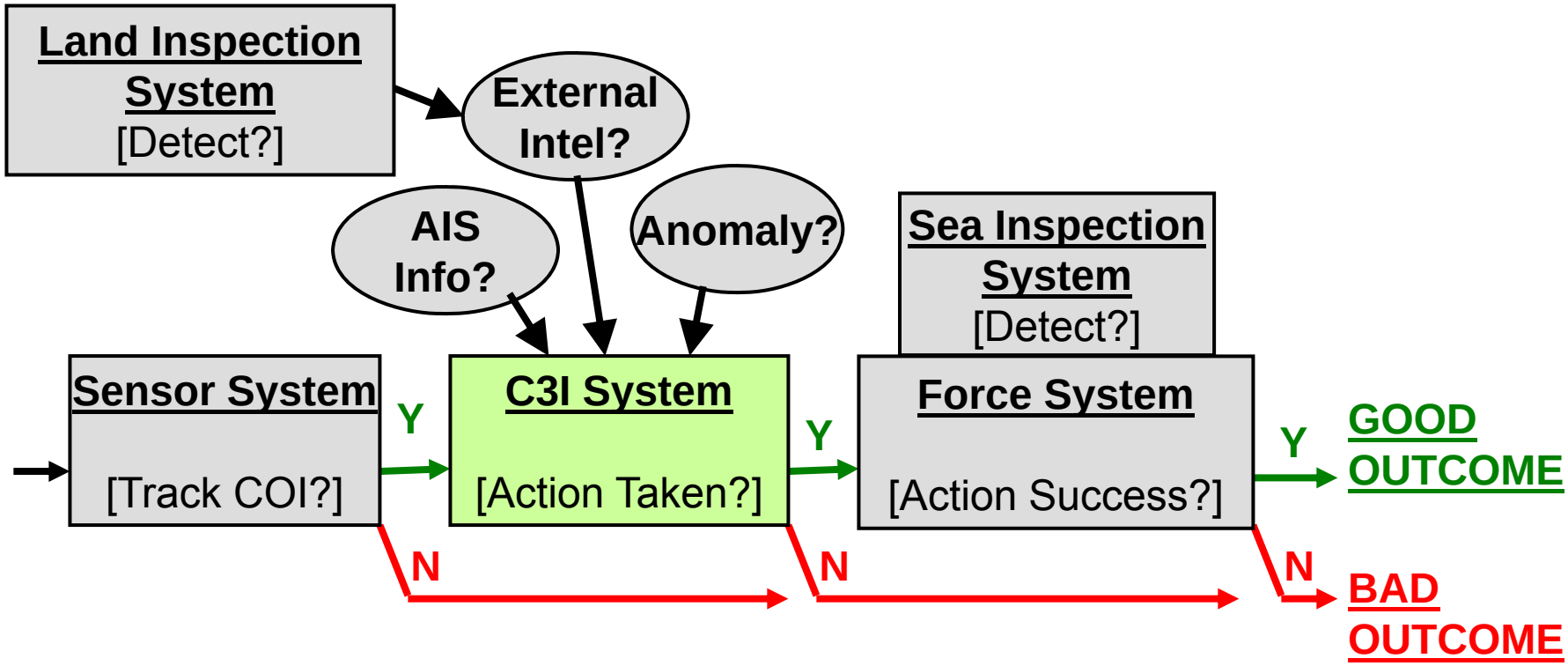
1500-1600 Response Force System

C3I Group



MAJ Russ A. Wyllie, USA

MDP System
Operational Architecture



C3I Agenda

- Objectives/Requirements
- Functional Decomposition
- Alternatives (TDSI)
- Design Factors
- Model Overview
- Results
- Insights/Recommendations

NPS MDP Study System Insights

Sensors

- Current System is inefficient – better performance available at same cost

C3I

- Common Operating Picture and Data Fusion Centers drive C3I performance

Force Response

- Current Sea Marshal program is effective
- Point defense is key to protecting merchant ships from attack

C3I Group Objectives

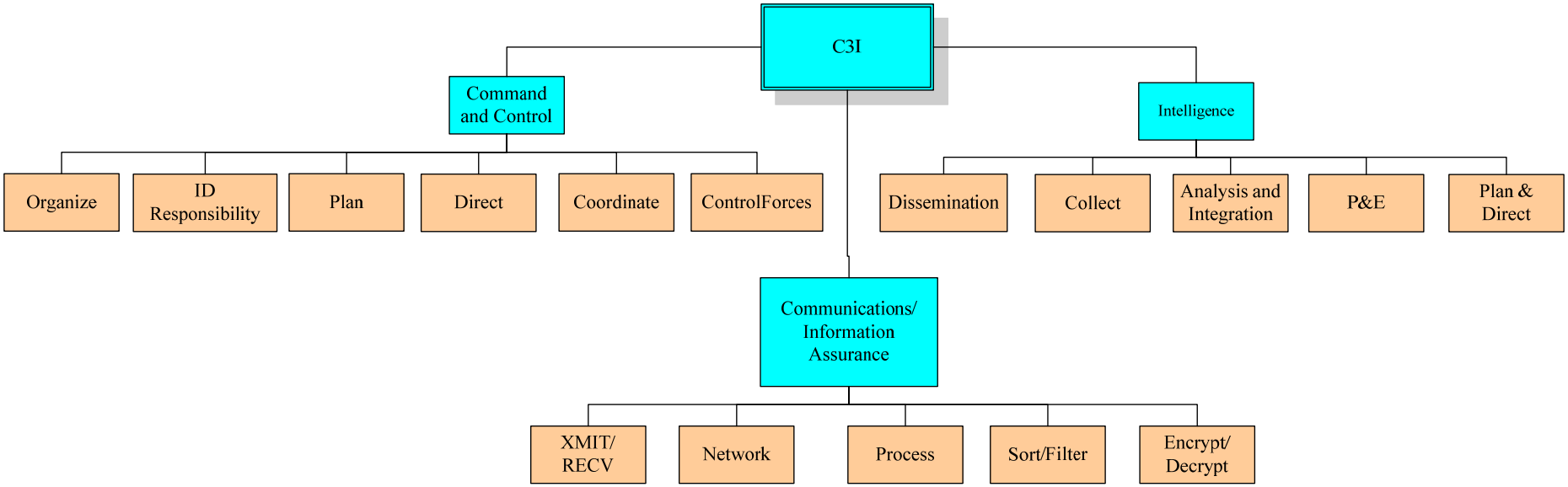
- Evaluate Command and Control and Intelligence (data fusion) System Capabilities
- Identify Communications network components linking Sensors and C3I system
- Identify appropriate level of Information Assurance for MDP system.
- Recommend system alternatives to improve C3I performance.

C3I System Requirements

- Minimum Analysis Time (Required to make Decision)
- Maximum Correct Decision
  - % P(Decide Act | Trigger Event)
- Minimum Incorrect Decision
  - % P(Decide Act | No Trigger Event)
- Communications Network Available 24/7

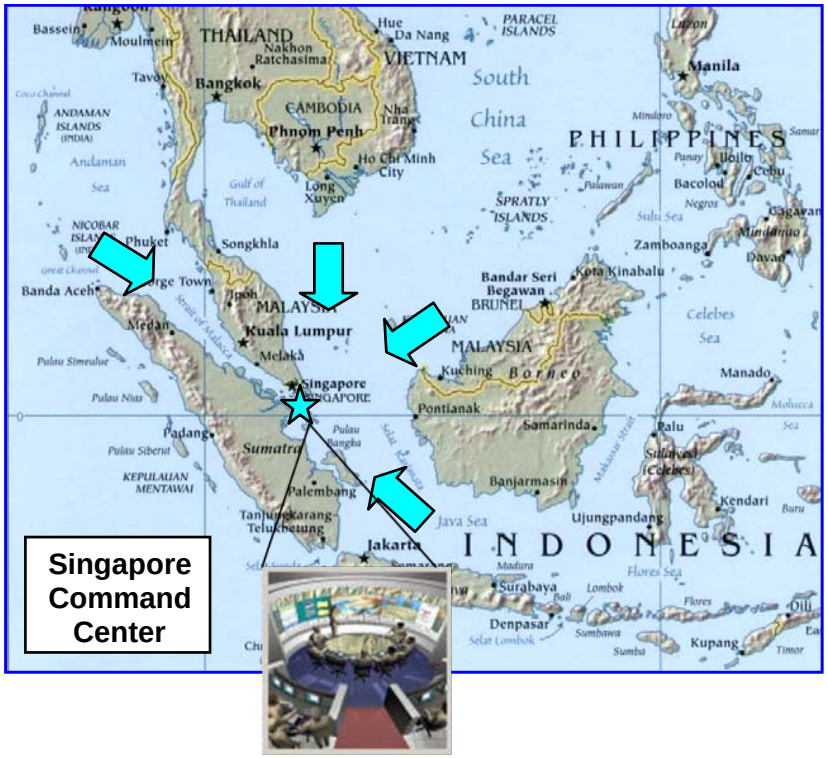
C3I Functional Decomposition

High Level Functions and Sub-Functions



“As–Is” C3I System

- **Singapore Primary Maritime Domain C2/Intel**
  - Independent Operations
  - Territorial Responsibility
- **Reliance on Electronic Intelligence Collection**
  - Sensor Data
  - Limited Correlation
  - Sequential Processing and Queuing
- **Communications**
  - Fixed infrastructure
  - Non-redundant



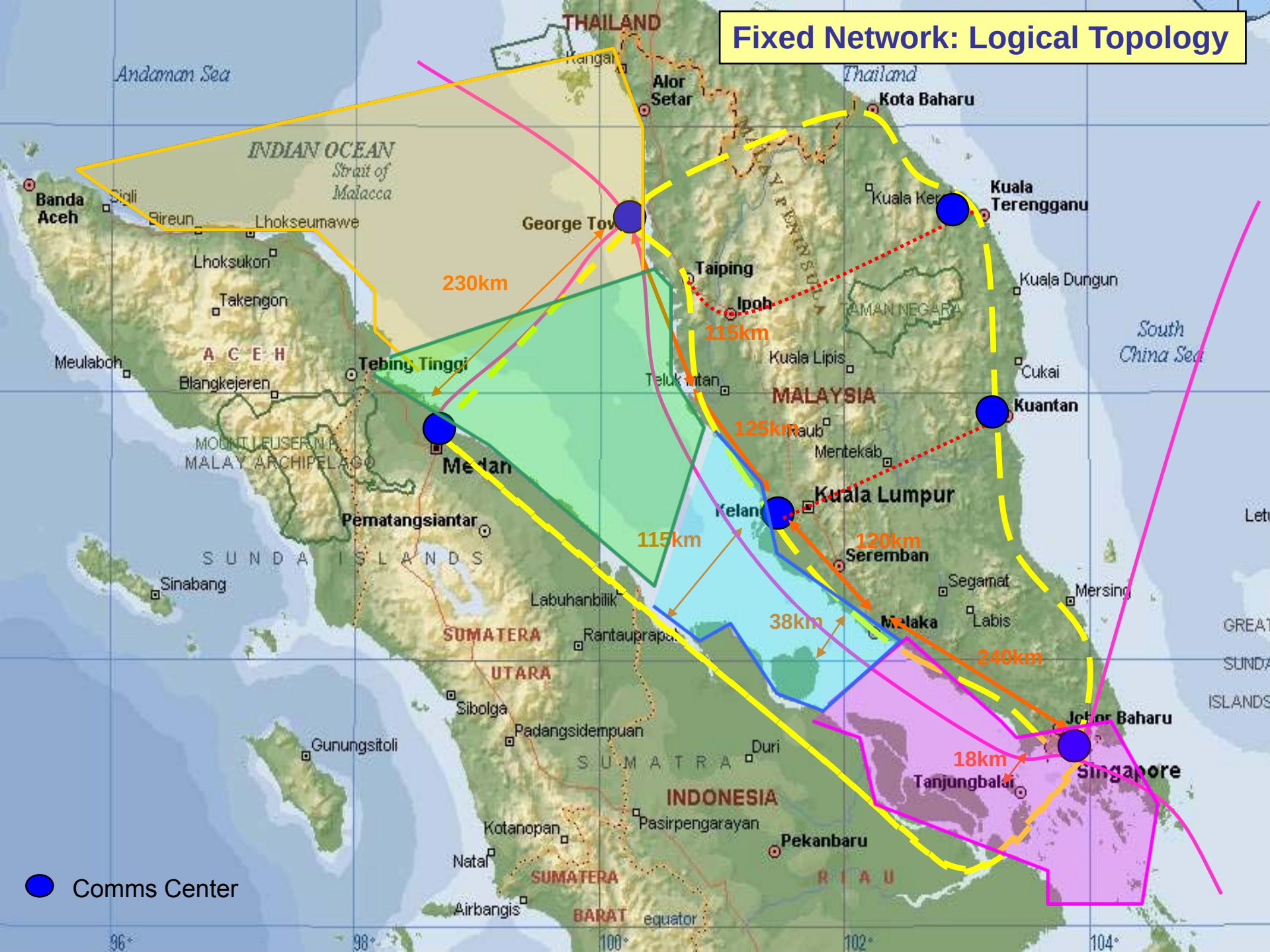
C3I Alternatives Generation

Communications Brief

By
TDSI Comms Track

Members:
Tat Lee, LIM
Hong Siang, TEO
Cheng Kiat, TEO
Swee Jin, KOH

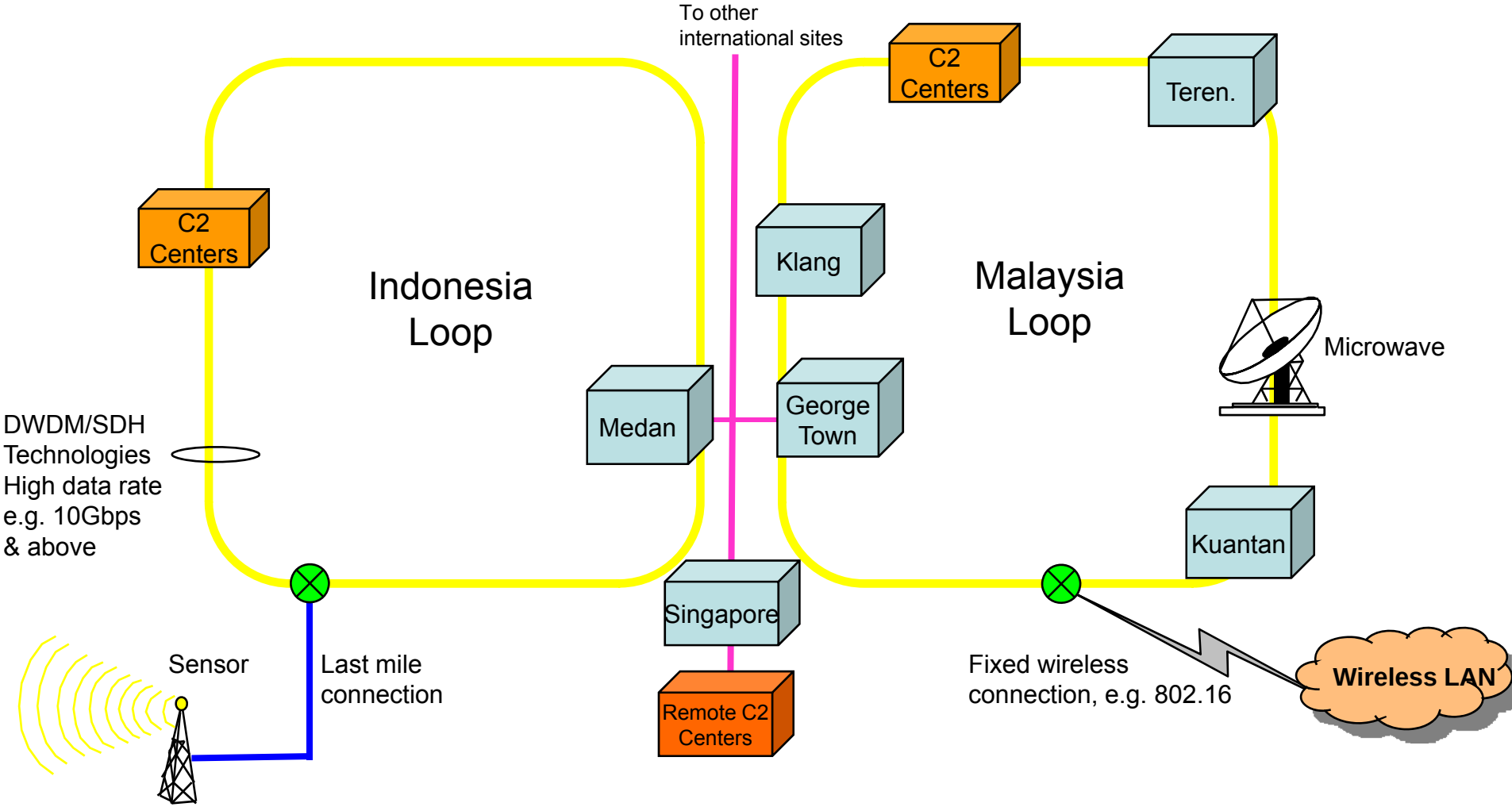
Fixed Network: Logical Topology



Comms Center

Fixed Network: Logical Topology

Backbone Fiber Optics Infrastructure



Fixed Network

Alternative Communications Link (Microwave)

- Preferred frequency 7.5 GHz, proposed link distance per hop of < 30 km.
- Alternate frequency 15 GHz, proposed link distance per hop of < 10 km.
  - Shorter distance per hop => more equipment
  - Lower availability rates (99.9%)

	Frequency	7.5 GHz	Wavelength	0.04m	Frequency	15 GHz	Wavelength	0.02m
Dist (km)	Availability (Rainfall)	Downtime (seconds)	Availability (Terrain)	Downtime (seconds)	Availability (Rainfall)	Downtime (seconds)	Availability (Terrain)	Downtime (seconds)
10	>99.993%	<181	100.000%	1	99.9259%	1920	100.000%	3
20	>99.993%	<181	99.9993%	35	99.8265%	4497	99.9985%	80
30	99.9910%	232	99.9949%	264	99.7417%	6694	99.9883%	608
40	99.9871%	334	99.9786%	1111	99.6670%	8630	99.9506%	2563
50	99.9832%	435	99.9346%	3390	99.5988%	10399	99.8491%	7821
60	99.9794%	534	99.8373%	8435	99.5348%	12059	99.6246%	19461

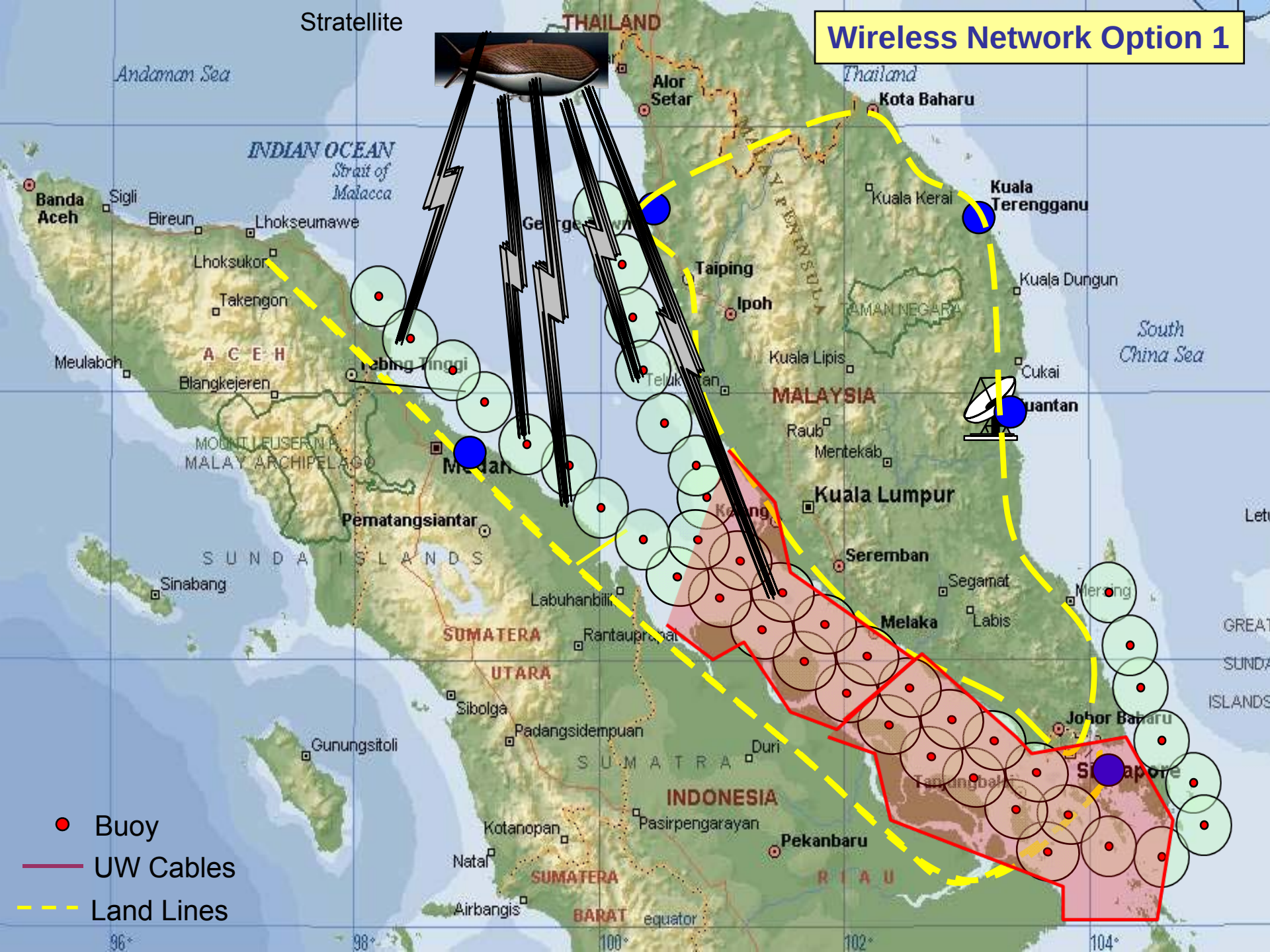
Parameters:
Antenna Size:1.2m
Antenna Gain: 37.5dB
Tx Power: 25dBm
ERP: 60.7dBm

Calculations based on:
-Climate: Maritime temperate, coastal or high humidity and temperate climatic regions
-Rainfall Zone: P (145mm/hr)

Wireless Network Topology

- **Concept 1: Buoys as Wireless LAN Base Stations**
  - Buoys deployed along the straits
    - Solar powered
  - **Backhaul options:**
    - Fixed Wireless e.g. 802.16
      - Point-to-point wireless links to shore
      - "Stratellite" as rebro-stations
    - U/W cables provide power and connectivity
  - **Limitations:** May require many cells, high cost
  - **Strengths:** Ubiquitous network coverage

Wireless Network Option 1



Wireless Network Topology

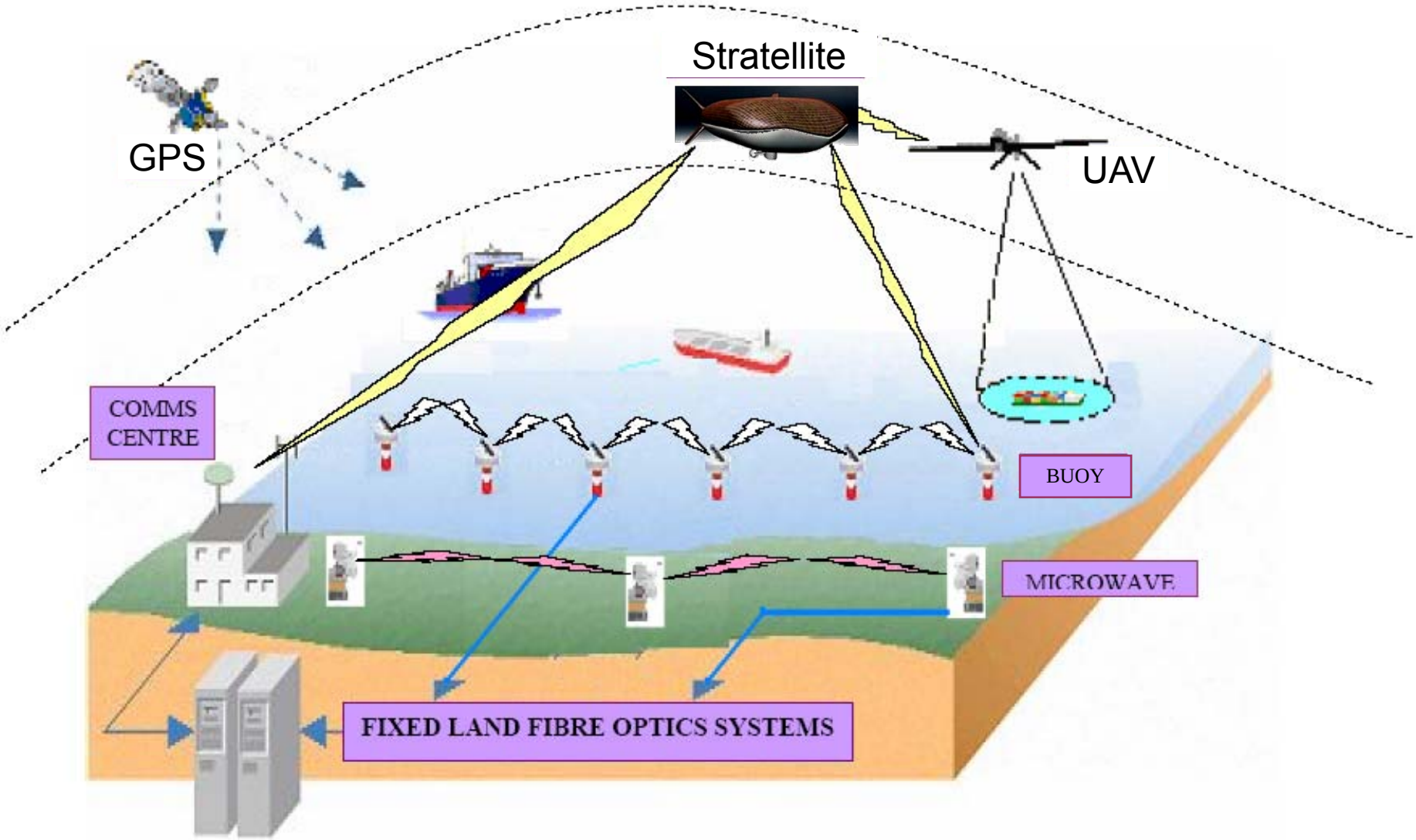
- **Concept 2: Ad-hoc Network via mobile platforms**
  - Mainly used to support task force
  - Wireless LAN Breadcrumb supported by UAV as routing nodes to fixed wireless nodes (e.g. 802.16)
  - **Limitations:** No permanent coverage
  - **Strengths:** Cheap and proven prototype

Bandwidth Requirements

- Baseline Network Bandwidth (per C2 site/ sector COMCEN)
  - Radars (Assume 20 sites)
  - Automatic Identification System (AIS) (2 channels)
  - Voice & Data (30 channels)
- Ad-hoc Network Bandwidth (Task force)
  - Image (video/IR)
    - Assume 5 UAV in a region at any one time
    - Frame rate – 30 frames/sec (NTSC)
  - Voice & Data (Assume 20 platforms with 2 channels)

- Estimated backbone bandwidth requirement:
  - Approx 250Mbps (c.f. OC-3: 155Mbps)
  - Excess bandwidth for RCMS, VPN, SCADA, etc.
- Scalable Fiber Optic Network Technology
  - Up to multiples of OC-3 in one OC-48 (aka STM-16) ring

Conceptual Communications Linkages



Information Assurance Strategy : Defense in Depth

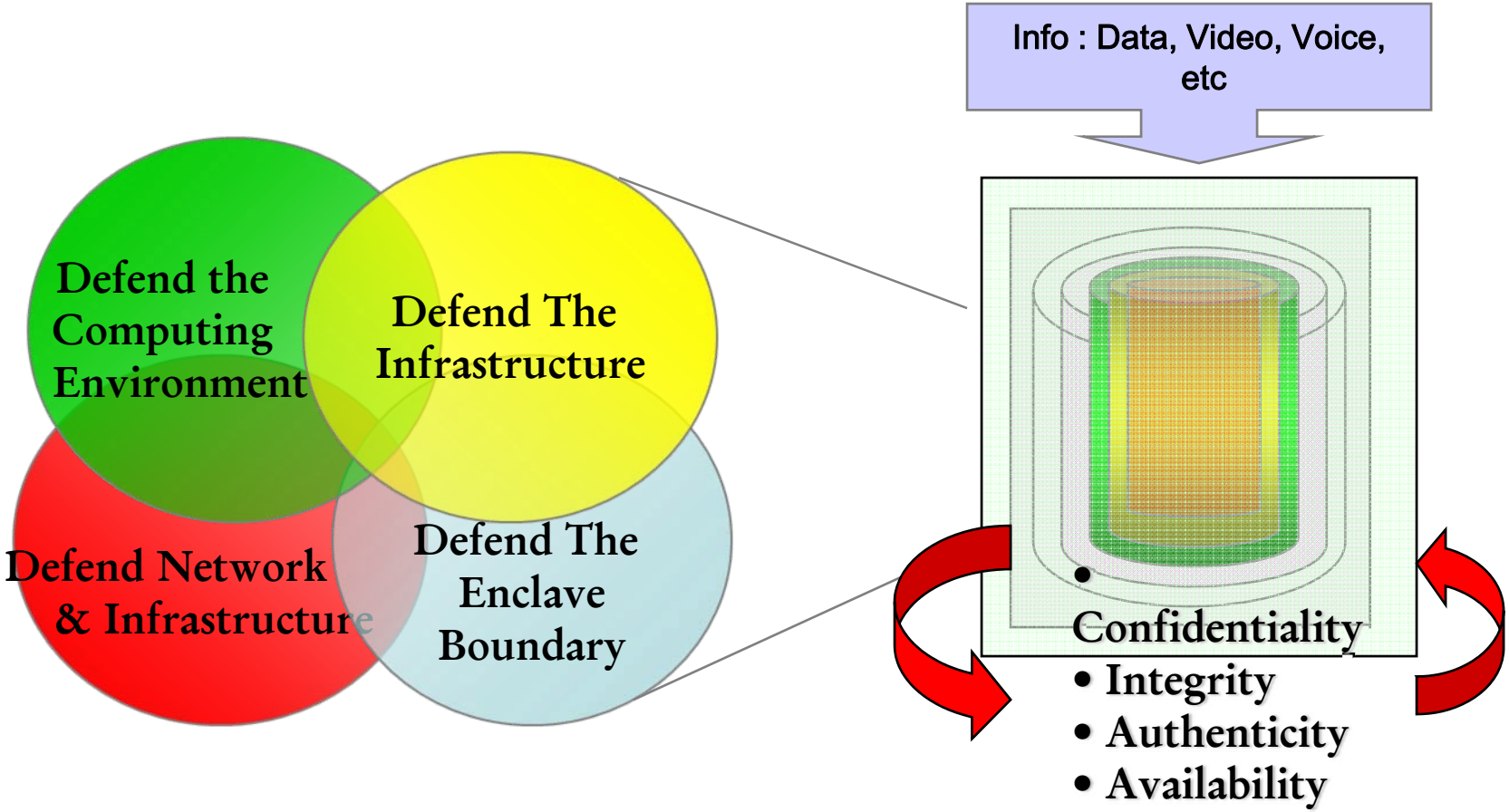
Presented by : CPT CHAY CHUA

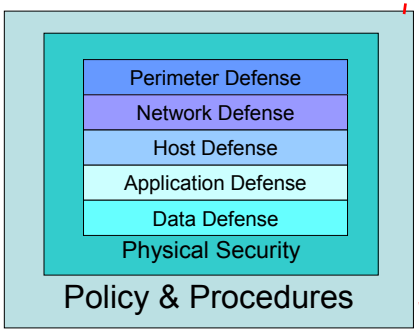
Team Members: Mr CheeMun Ng
: Mr NaiKwan Tan

Information Assurance

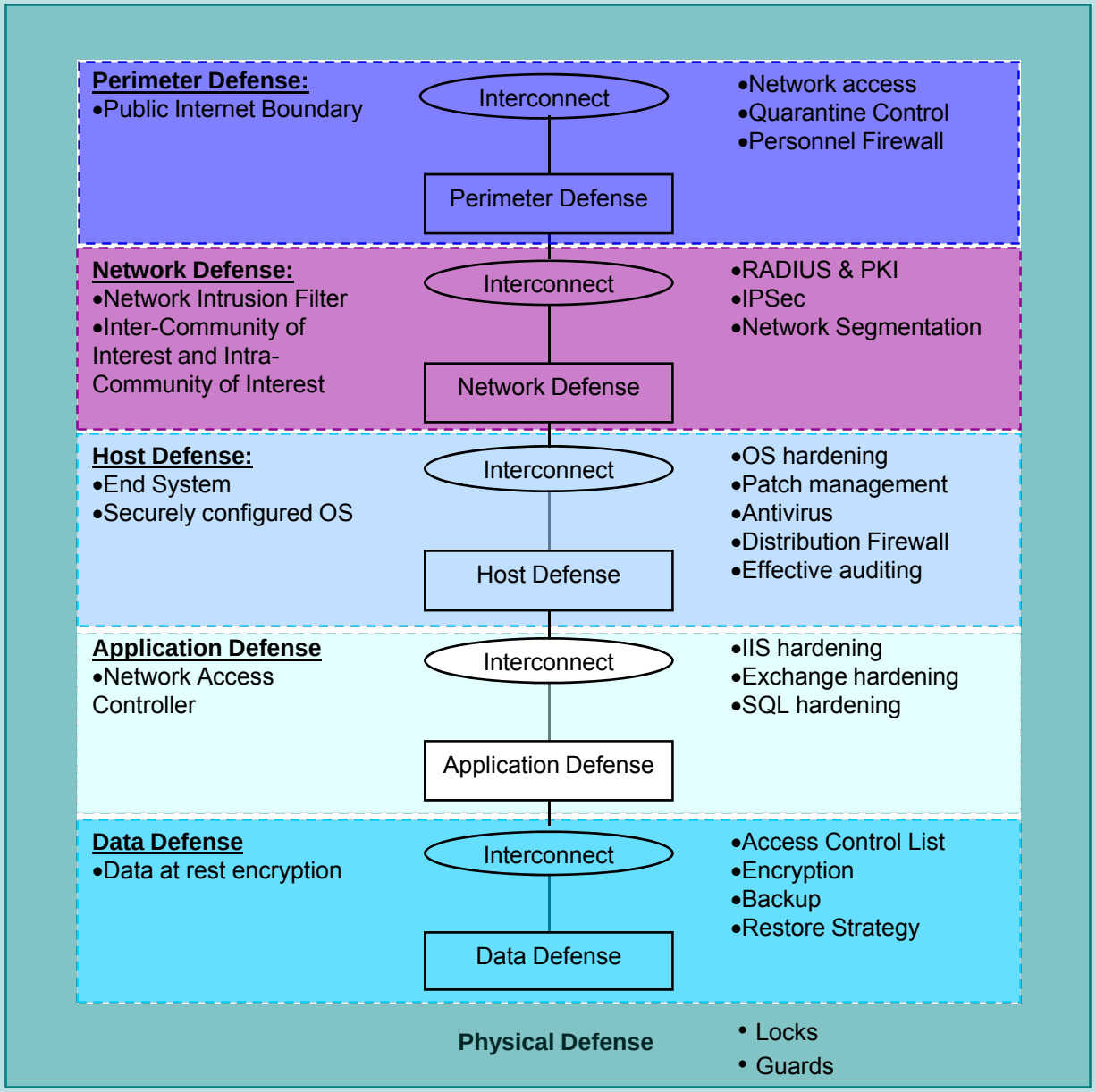
IA Strategy: Defense In Depth

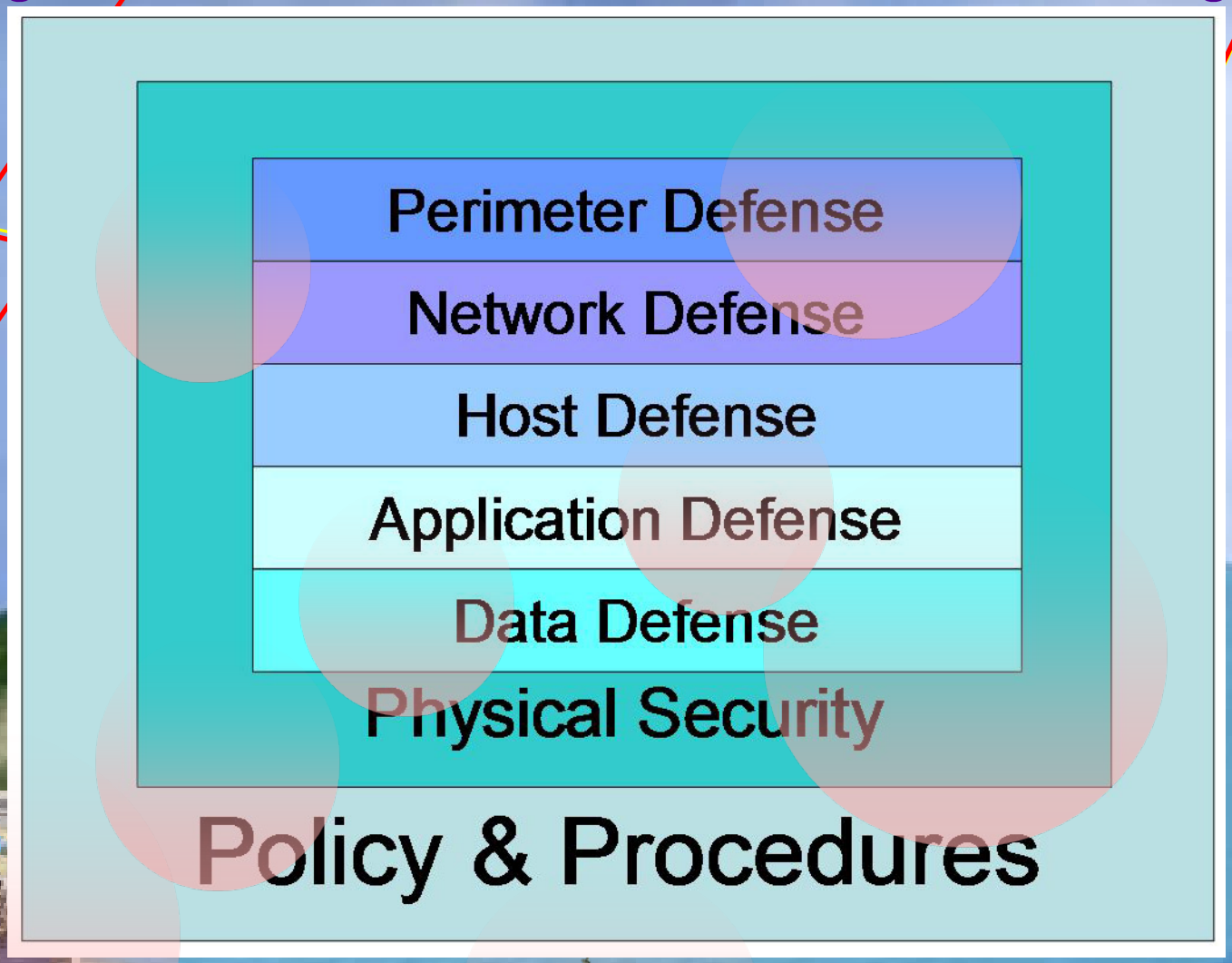
- Layers of Defense
- Overlapping Layers of Protection



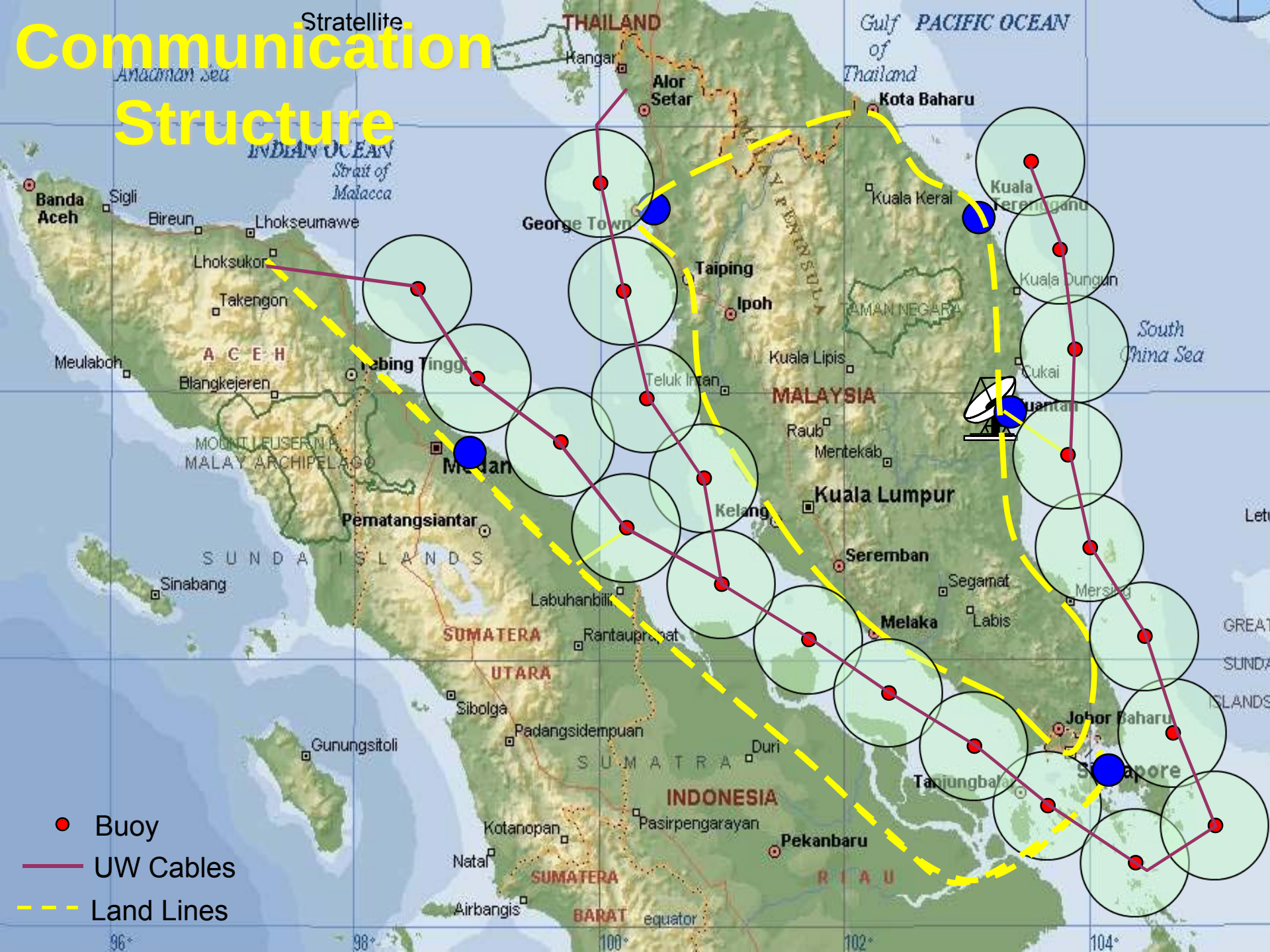


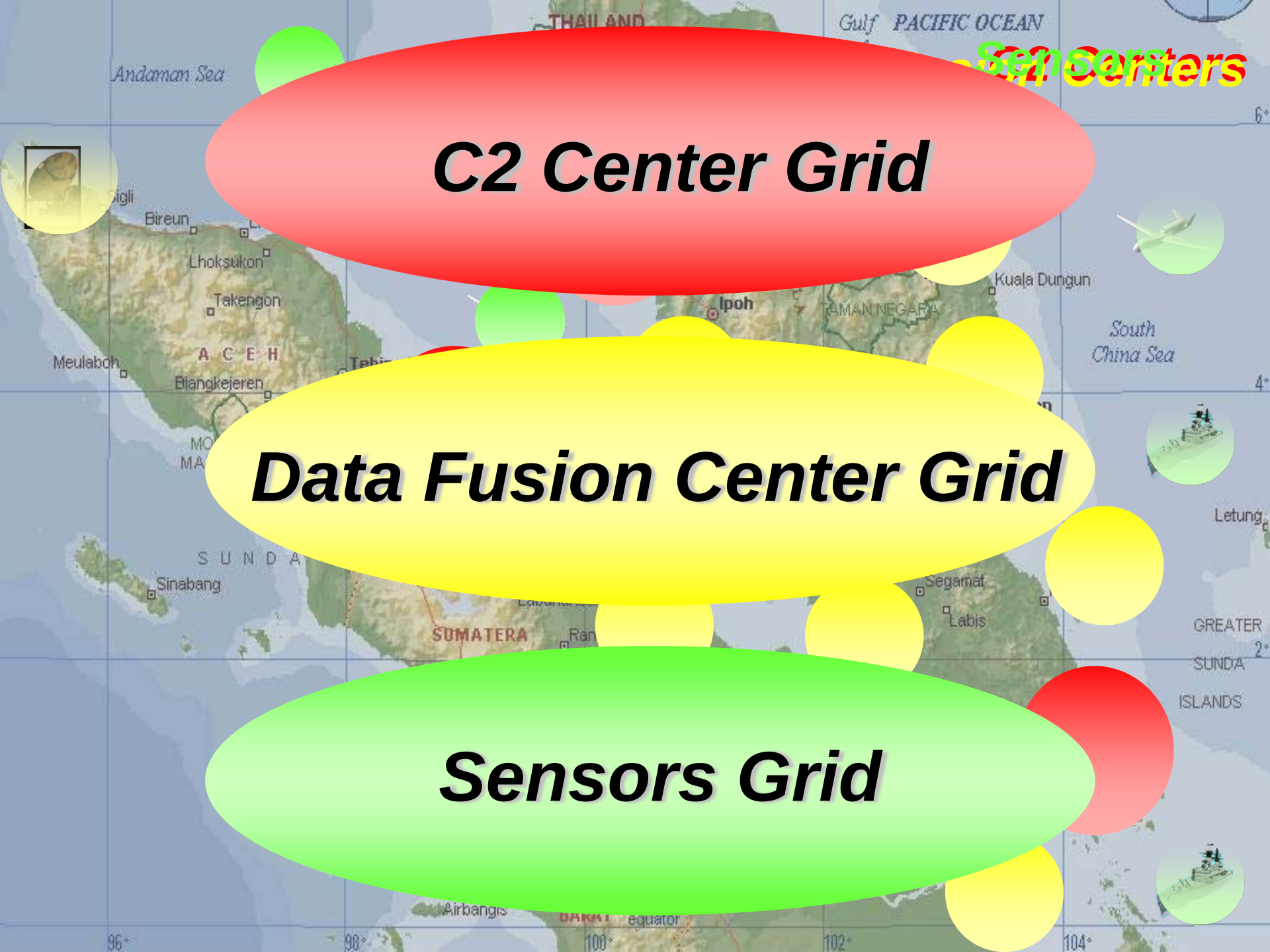
Defense in Depth Security Model



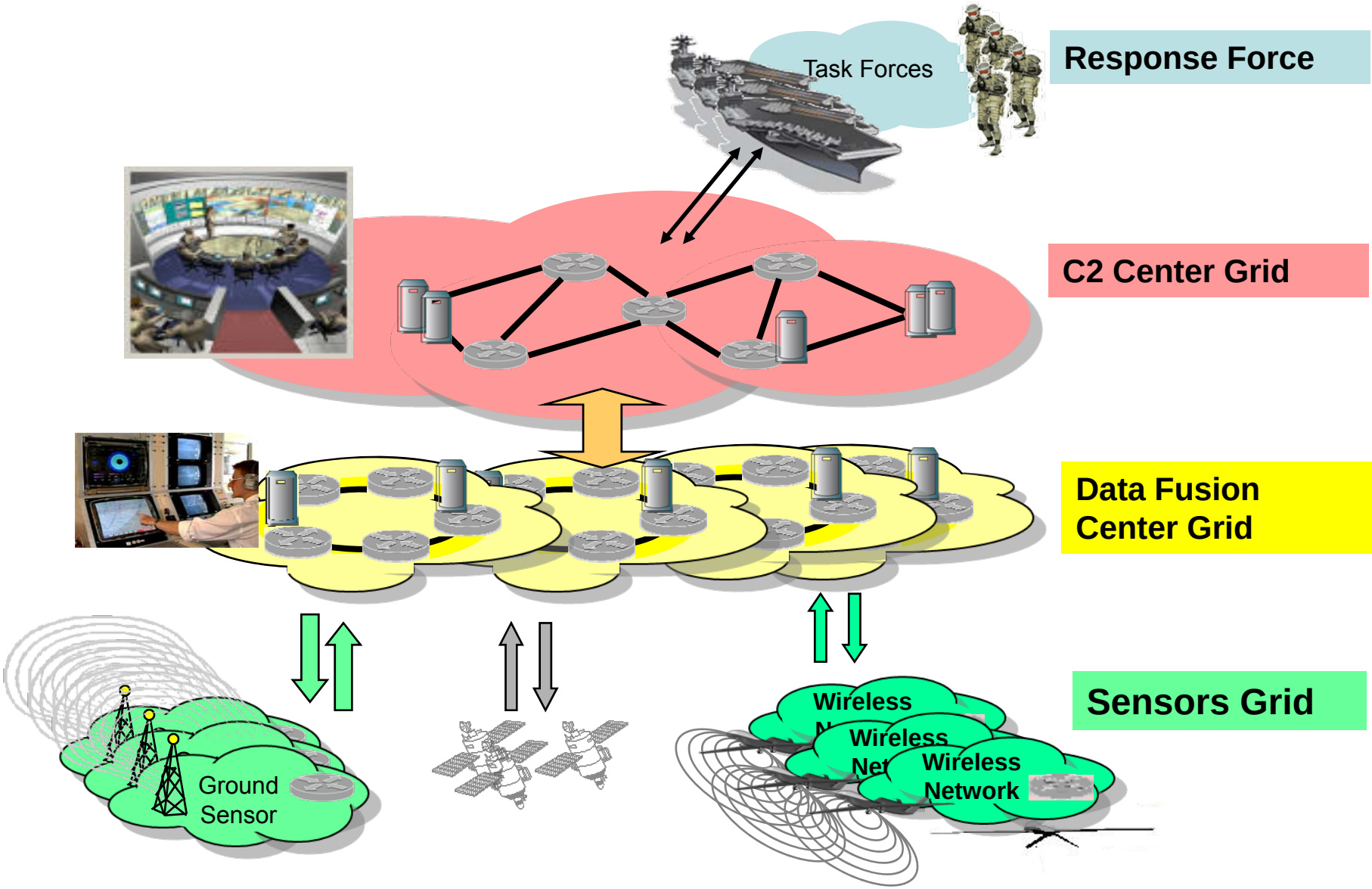

Perimeter Defense
Network Defense
Host Defense
Application Defense
Data Defense
Physical Security
Policy & Procedures

Communication Structure




C2 Center Grid
Data Fusion Center Grid
Sensors Grid
Andaman Sea
Gulf
PACIFIC OCEAN
Bireun
Lhoksukon
Takengon
Meulaboh
A C E H
Blangkejeren
Ipoh
Kuala Dungun
South
China Sea
Letung
S U N D A
Sinabang
SUMATERA
Segamat
Labis
GREATER
SUNDA
ISLANDS
Airbangis
equator
96°
98°
100°
102°
104°

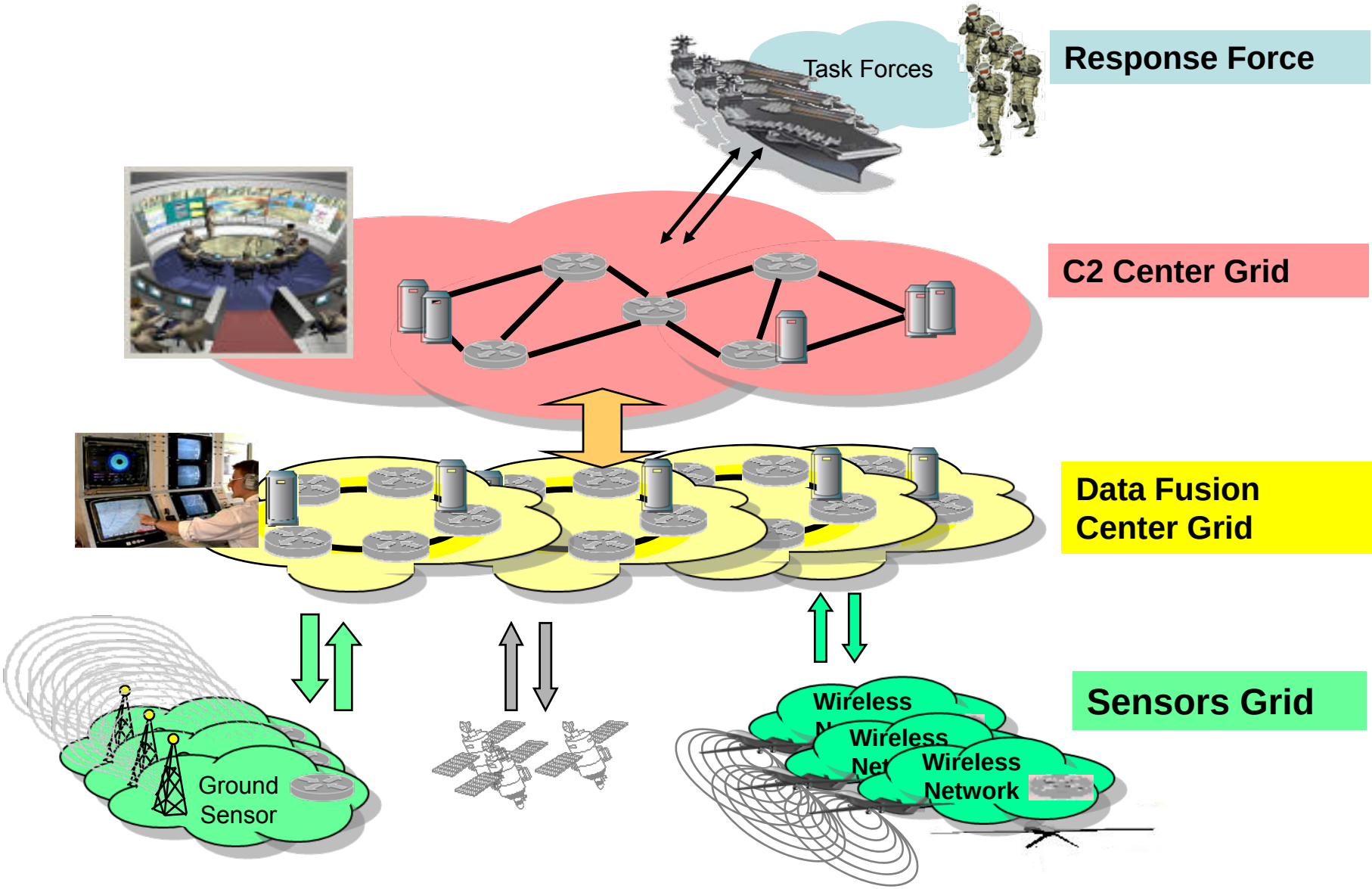
Logical Connectivity



Potential Cyber Threats

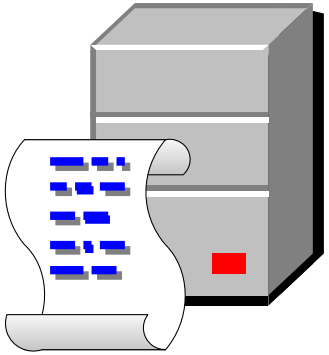
- **Categories of threats:**
  - ***Malicious Programs*** – Malevolent programs reproduce self to move between systems without authorization, or subvert the system by providing trap-doors into the systems.
  - ***Users' Error***– Authorized user may create unintentional errors that cause breakdown to the whole system/operations.
  - ***Professional Hackers*** – Seasonal attackers who break into systems for vandalism or theft of information
  - ***Criminals*** – Trespassers who read and distort information without granted authority.
  - ***Terrorists*** – Organized hacking and eavesdropping on network traffic to gather/steal intelligence for their destructive attacks
  - ***State-Sponsored Attack*** – Hostile countries may sponsor attacks to infiltrate and sabotage the system

Logical Connectivity



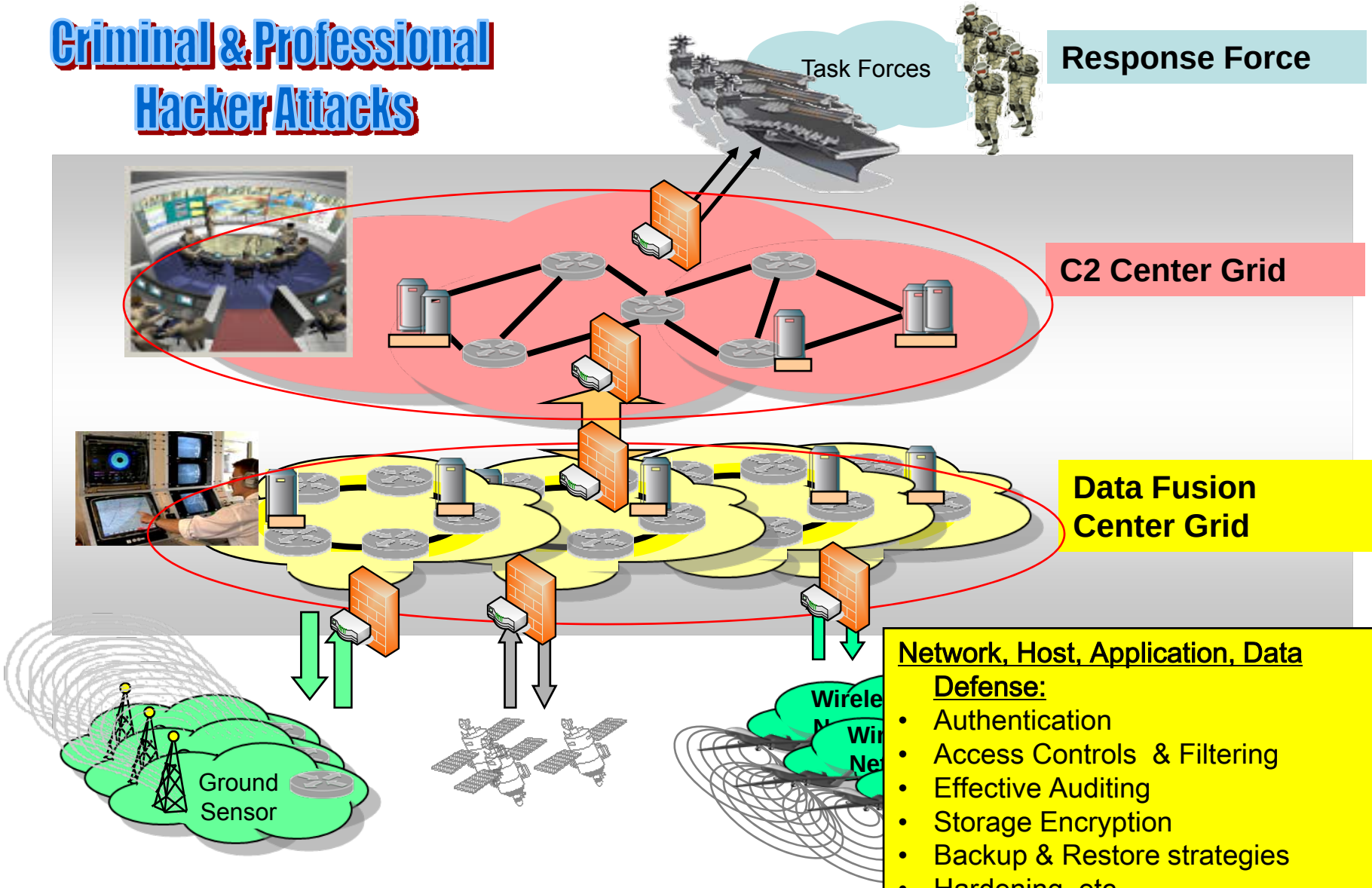
Countermeasures: Policies & Training

- **Objectives:**
  - ***Protect against Malicious Programs***
  - ***Prevent User Errors***



- **Mechanisms *:***
  - ***DoD IA Directives and implementations:***
    - ***DoD Directive 8100.1 : Global Information Grid(GIG) overarching Policy***
    - ***DoD Directive 8500.1: Information Assurance***
    - ***DoD Instruction 8500.2: IA Implementation***
    - ***DoD Instruction 8100.2 : Use of Wireless Device, Services & Technologies in DoD GIG***
  - ***Provide security training for all users***

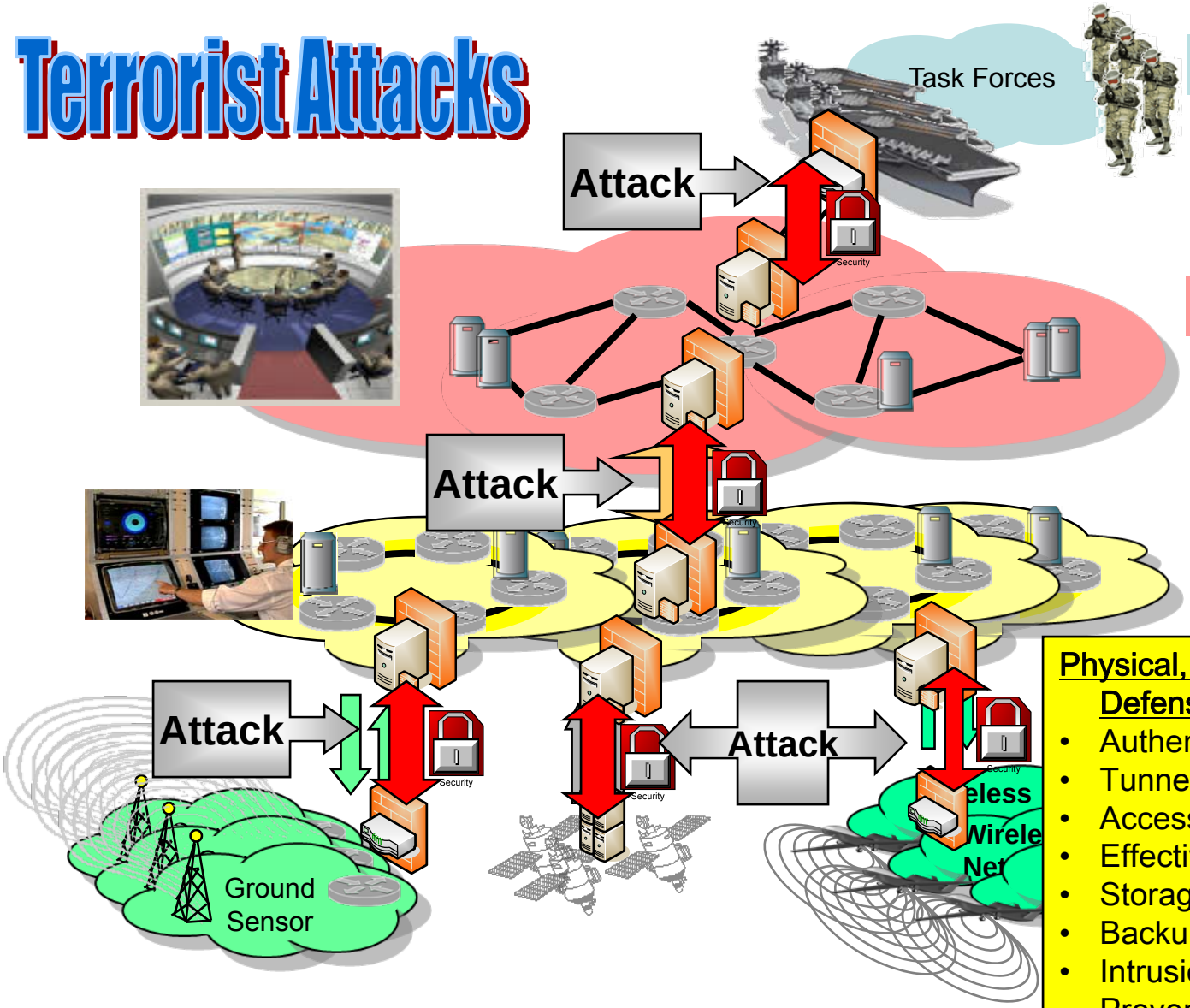
Countermeasures Against Criminal & Professional Hacker Attacks



Network, Host, Application, Data Defense:

- Authentication
- Access Controls & Filtering
- Effective Auditing
- Storage Encryption
- Backup & Restore strategies
- Hardening, etc..

Countermeasures Against Terrorist Attacks



Response Force

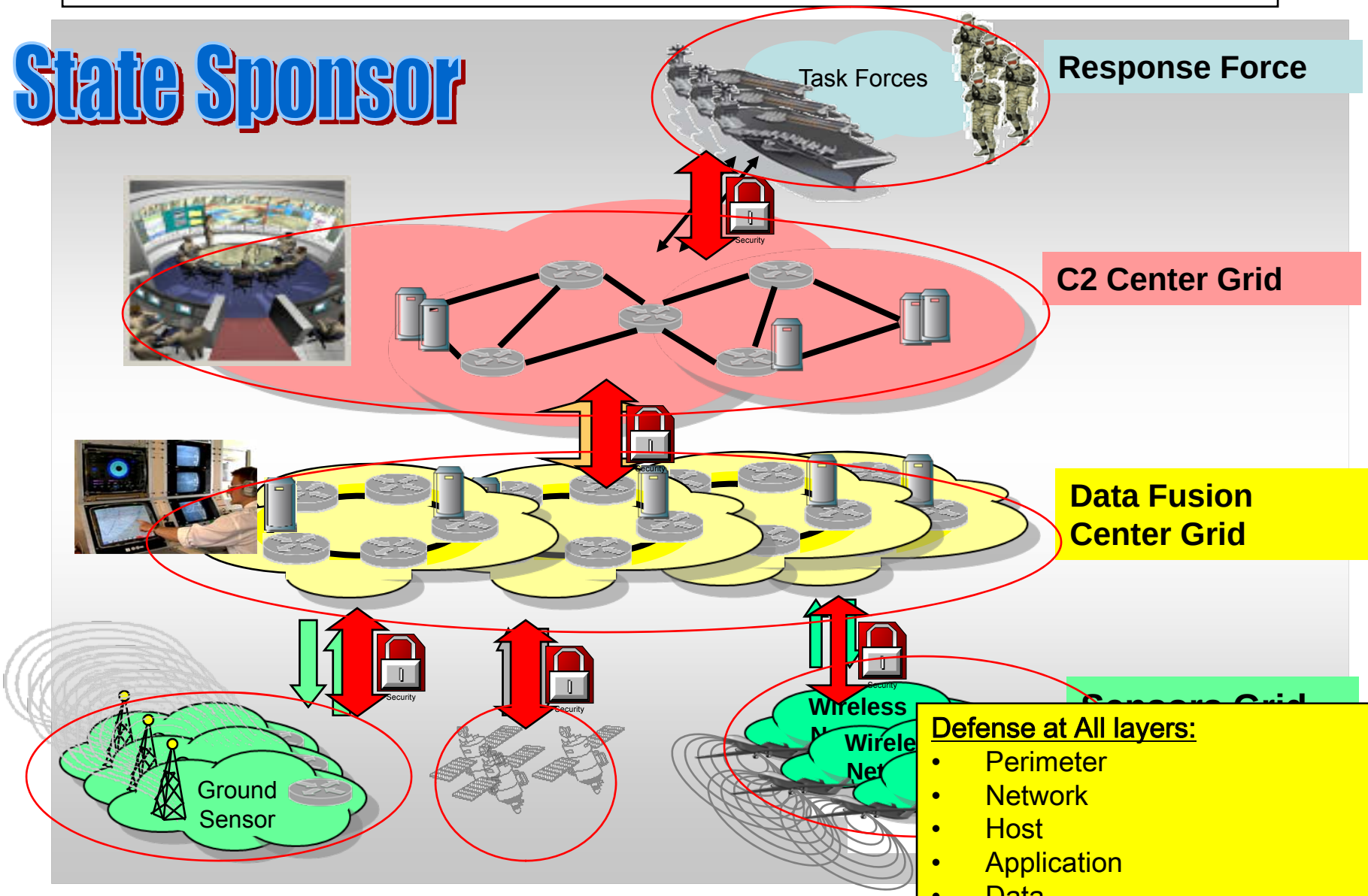
C2 Center Grid

Data Fusion Center Grid

<u>Physical, Network, Host & Data Defense:</u>

- Authentication
- Tunneling
- Access Controls & Filtering
- Effective Auditing
- Storage Encryption
- Backup
- Intrusion Detection & Prevention, etc…

Countermeasures Against State Sponsored Attacks



Defense at All layers:

- Perimeter
- Network
- Host
- Application
- Data

Summary

- **Policies and Procedure**
  - Provide End User Training
  - Increase User Awareness
  - Continuously Review Policies and Procedures to meet the new adversaries

- **Defense-in-depth strategy**
  - Secure physical and logical perimeters
  - Defend Network, Host, Application and Data

Conclusion

- **No Perfect Security**
  - Threat is pervasive and ever changing
  - Protections must evolve to meet these challenges
  - Implement layered defense to deter adversaries

Reference

- Picture from
  - homepage.mac.com/g3head/hacksgallery.html
  - http://www.cranfieldaerospace.com/applications/observer_details.htm

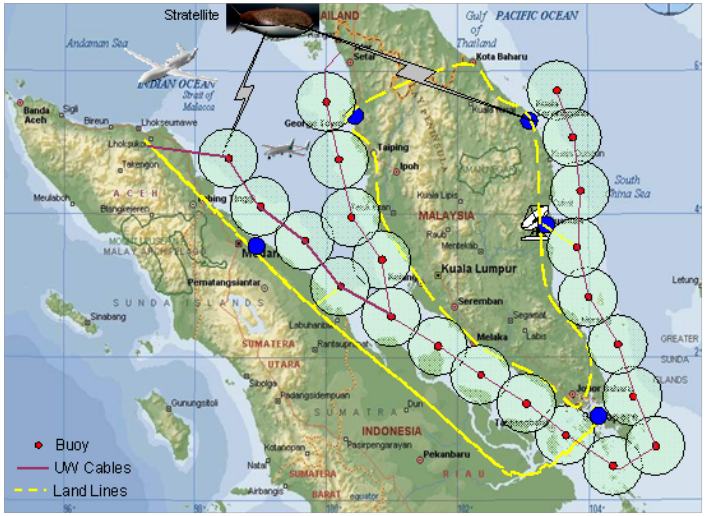
C3I Alternatives Overview

- **ALT 1: Regional Architecture**
  - Two C2/Data Fusion Center
  - Network Centric Communications
  - Reliance on Electronic Intelligence Collection

- **ALT 2: Network Centric + Data Fusion Cells**
  - Four Regional C2/Intel Centers
  - Nine Data Fusion Cells
  - Intelligence Network 13 Intel/HUMINT Collection Nodes
  - Network Centric Communications

C3I Alternative 1
Regional Architecture

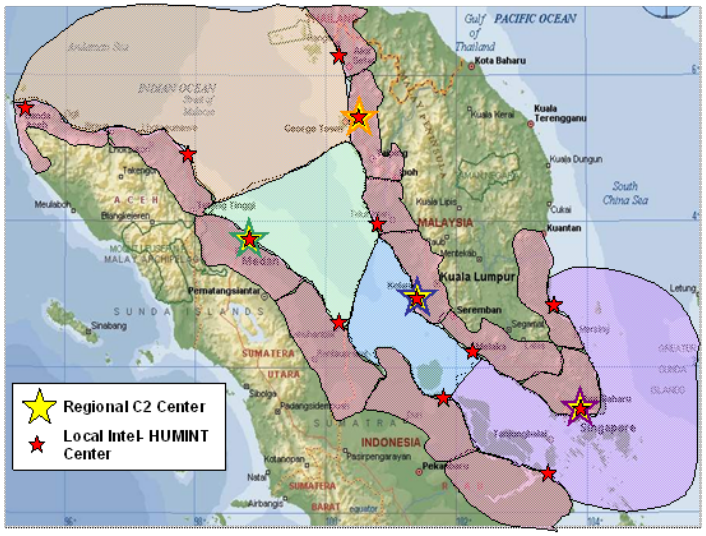
- **Two C²/Data Fusion Centers**
  - Network Centric
  - Large AOR
- **Reliance on Electronic Intelligence Collection**
  - Sensor Data
  - Sequential Processing and Queuing
- **Communications**
  - Fiber Optic Backbone, Networked Maritime Wireless Communication Buoy Stations, Stratellites
  - Unmanned fixed wing UAVs
  - Layered, graceful degradation

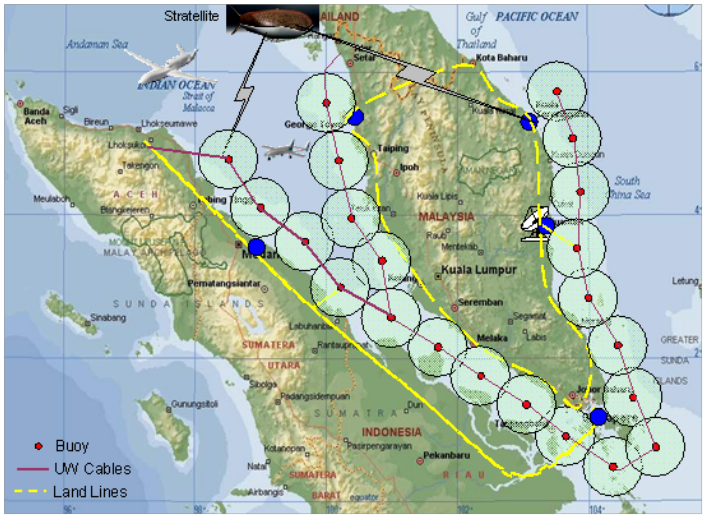


C3I Alternative 2

Network Centric + Data Fusion Cells

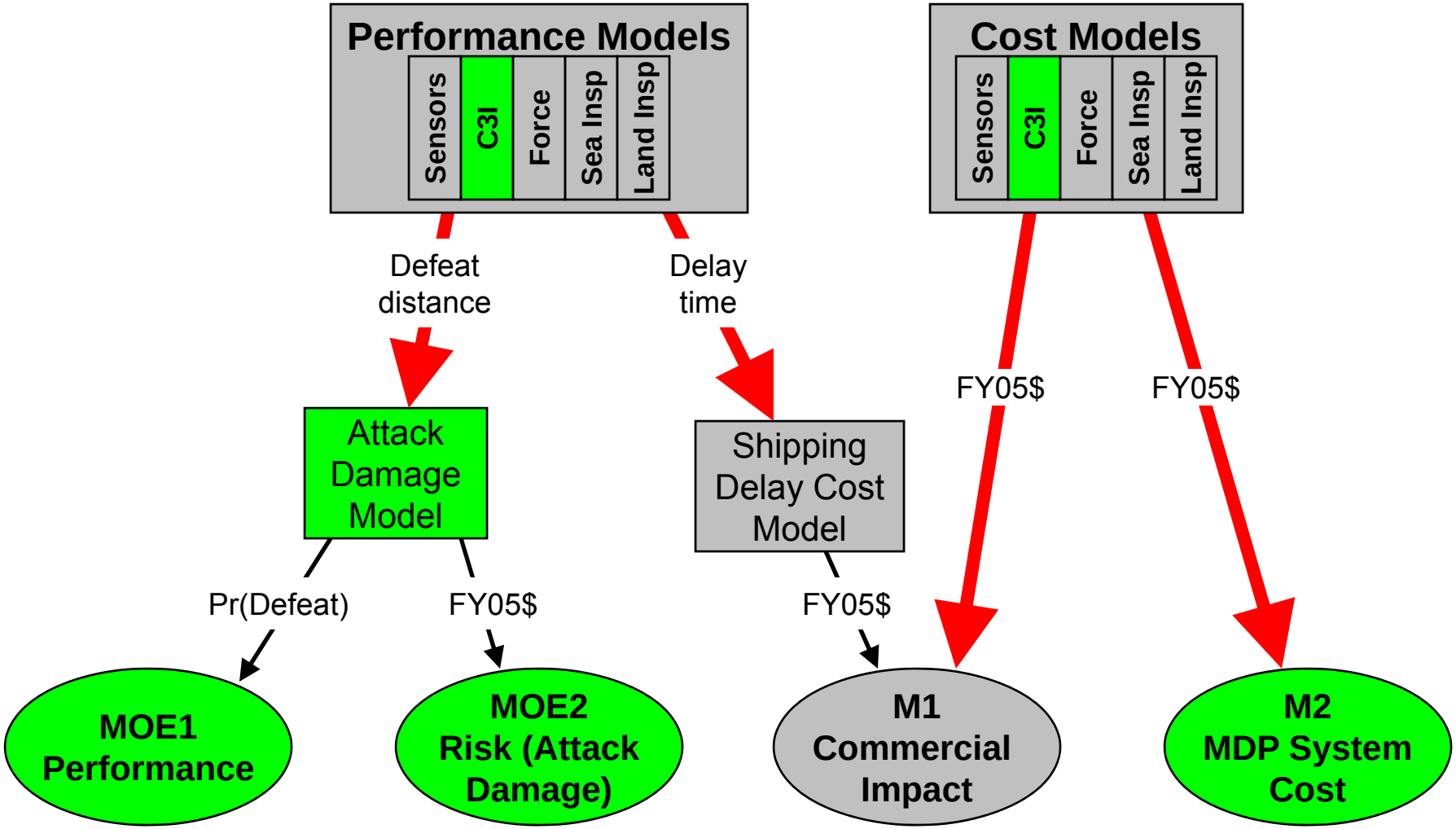
- **4 Regional C2/Intel Centers**
  - 9 Data Fusion Cells Creates CIP
  - Creates COP
  - Self-Synchronizing w/Distributed Authority
- **Intelligence Network 13 Intel/HUMINT Collection Nodes**
  - Localized Intelligence Expertise (Inland)
  - Social Networks and All-source collection
  - Maximize "Trigger Event" Opportunities
- **Communications**
  - Fiber Optic Backbone, Networked Maritime Wireless Communication Buoy Stations, Stratelites
  - Unmanned fixed wing UAVs
  - Layered, graceful degradation





C3I Modeling

Overarching Modeling Plan



C3I Model Description & Assumptions

- **Approach**
  - **Two Models; “Timely” and “Informed”**
- **Models Used**
  - **EXTEND Model**
  - **Excel**
- **Assumptions**
  - **Only one decision can be made on each track.**
  - **Delays represent automation (0) or human (>0) in the loop**
  - **Data Fusion Cells and Command and Control Centers are collocated**
  - **An “informed” decision can be modeled by probabilities and the associated assigned scores**
  - **Decisions are based upon a perceived reality**

C3I System Factors

Held Constant

- Track Quality: P(track)
- Track Quality: P(fa)
- Position Error: CEP
- Presence/Quality :
  - Intelligence
  - AIS Info
  - Sea Inspect

Varied

- # Data Fusion Cells
- # C2 Centers
- Network Centric (Y/N)
- Intel Collection Nodes

C3I Performance Model Overview

Inputs | **Outputs**

- # Data Fusion Cells
- # C2 Centers
- Network Centric (Y/N)
- Intelligence Collection Nodes

→ **C3I "Timeliness" Model** → Analysis Time

- Presence/Quality:
  - Intelligence
  - AIS Info.
  - Sea Inspection

→ **C3I "Informed" Model** → Probability Correct Decision

C3I Modeling Results

C3I Modeling Factors

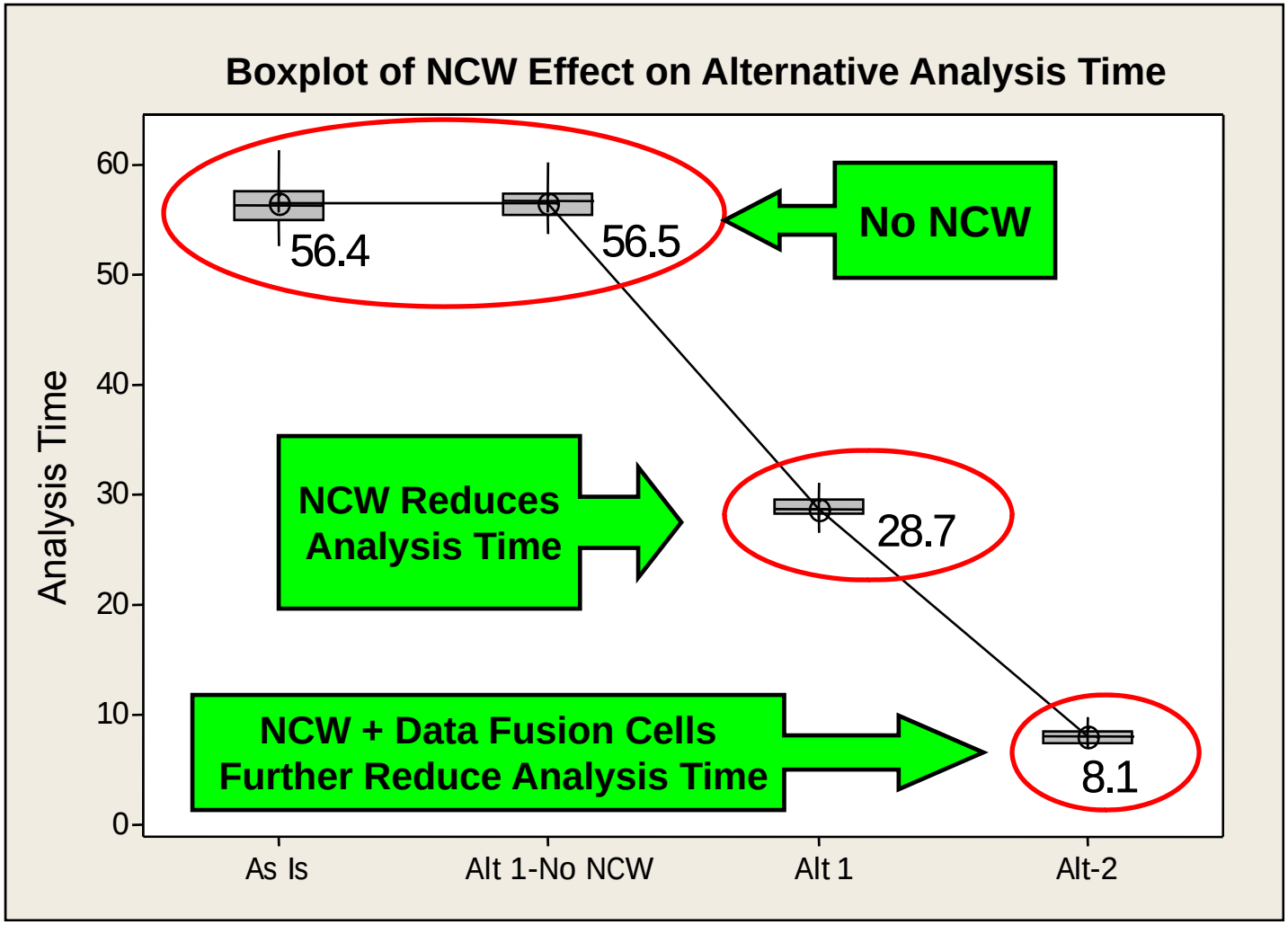
		Values		
Factors	**Values Evaluated**	**As-Is**	**Alt 1**	**Alt 2**
# C2 Centers	1,2,4	1	2	4
# Data Fusion Cells	1,2,9	1	2	9
Network Centric (Yes/No)	0,1	0	1	1
Intelligence Collection Nodes	0, 13	0	0	13
C2 Center Staffing Ratio	7:1, 5:1, 4:1	5:1	5:1	5:1

C3I Modeling Results

MOEs	As-Is	Alt 1	Alt 2
Analysis Time (Generic Time Unit)	56.40	28.70	8.10
P (Decide Act | Trigger Event)			
P(Inspect | WMD)	20%	35%	68%
P(Engage | Anomaly)	20%	35%	68%
P (Decide Act | No Trigger Event)			
P(Inspect | No WMD)	0.41%	0.32%	0.16%
P(Engage | No Anomaly)	0.49%	0.33%	0.21%
C3I System Cost (FY05$M)	541	1,593	2,922

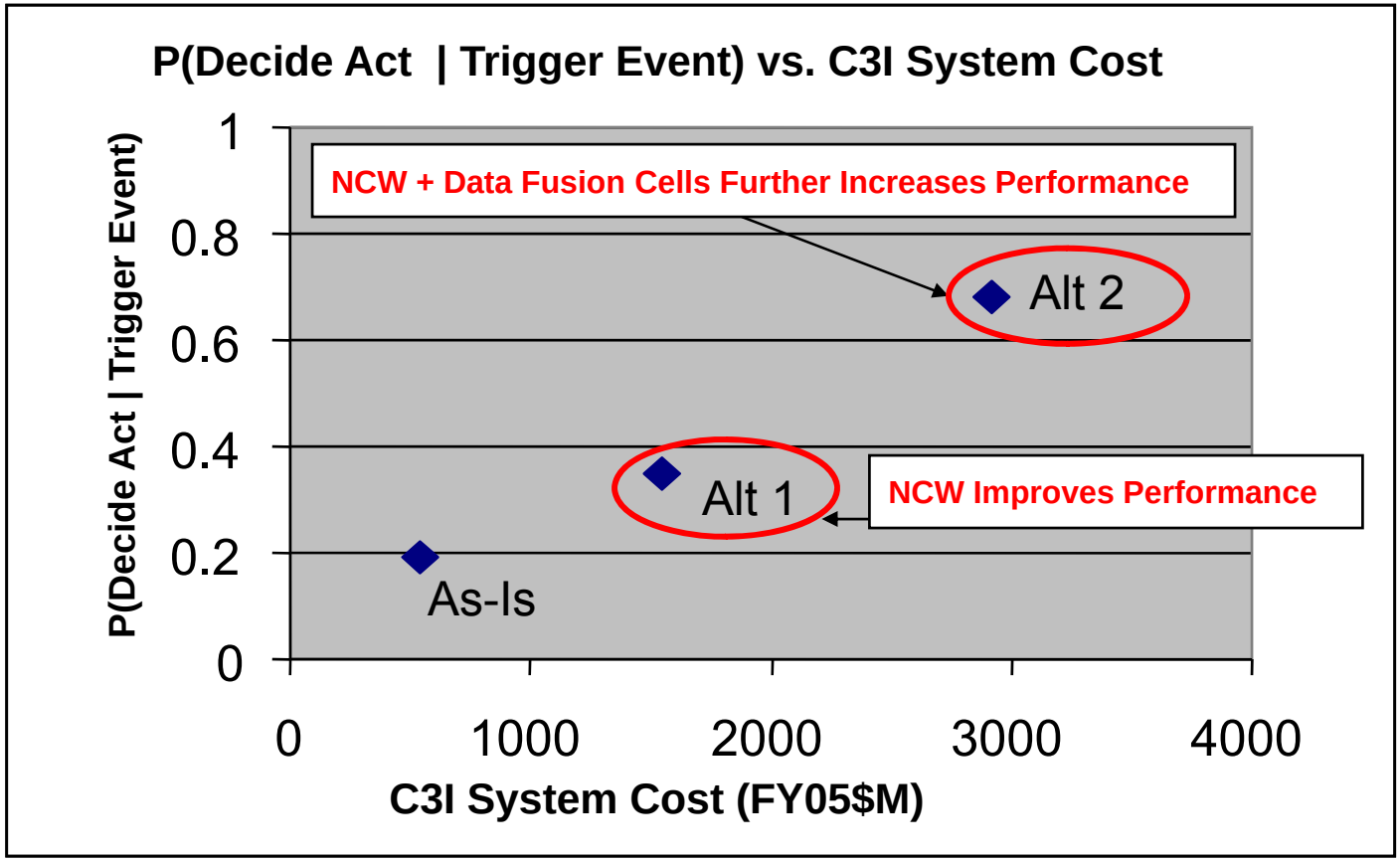
C3I Results Graphs

Timely Model Performance



C3I Results Graphs

P(Decide Act | Trigger Event) vs. Cost

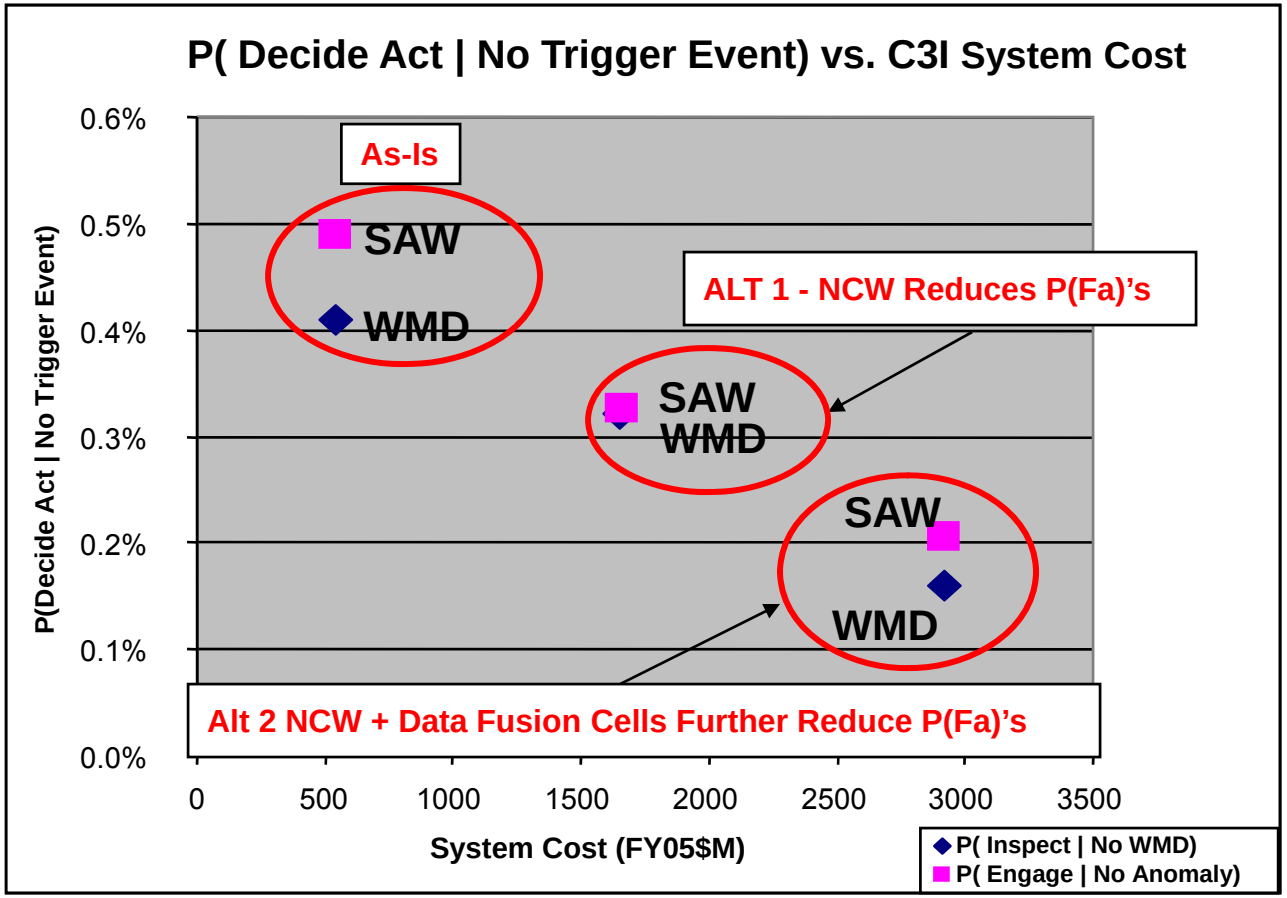


P (Decide Act | Trigger Event);

- **P (Decide Inspect | WMD)**
- **P (Decide Engage | Anomaly)**

C3I Results Graphs

P(Decide Act | No Trigger Event) vs. Cost

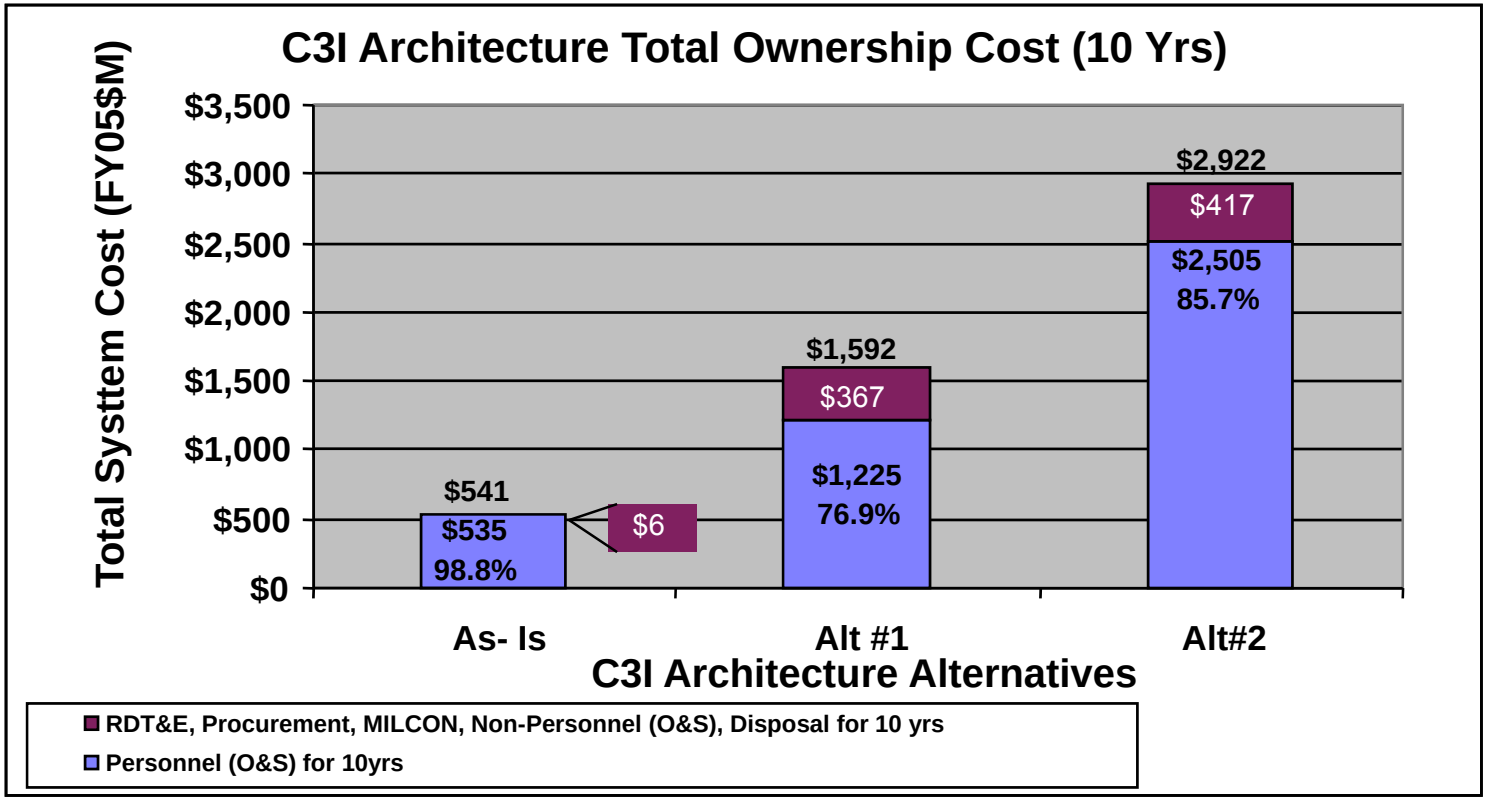


P (Decide Act | No Trigger Event);

- **P (Decide Engage | No Anomaly)**
- **P (Decide Inspect | No WMD)**

C3I Results Graphs

Staffing Cost Comparisons



Personnel Drives Cost

- **Accounts for most of Total C3I System Cost**

Insights and Recommendations

C3I Insights

- **Network Centric and Data Fusion Centers Drive C3I Improvements**
- **Network Centric C3I makes C2/Intel Center location irrelevant**
- **Decouple Analysis Time and Decision Quality to model C3I**
- **Humans still relevant in C3I process**
  - **Data Fusion**
  - **HUMINT**

RECOMMENDATIONS

- Invest Network Centric Communications System
- Invest in HUMINT
- Divide Region into “Data Fusion Cell” Regions.

C3I Group Questions ?

- SEA-7 Sensors
  - MAJ Russ Wyllie, USA
  - ENS Greg Woelfel, USN
  - ENS Alexis Wise, USN
  - Mr. David Rummler, Northrop-Grumman

- Communications Curriculum
  - MAJ Cheng Kiat Teo, RSN
  - Mr. Hong Siang Teo
  - Mr. Swee Jin Koh
  - Mr. Tat Lee Lim

- Information Assurance Curriculum
  - CPT Chay Chua, SinA
  - Mr. Chee Mun Ng
  - Mr. Nai Kwan Tan

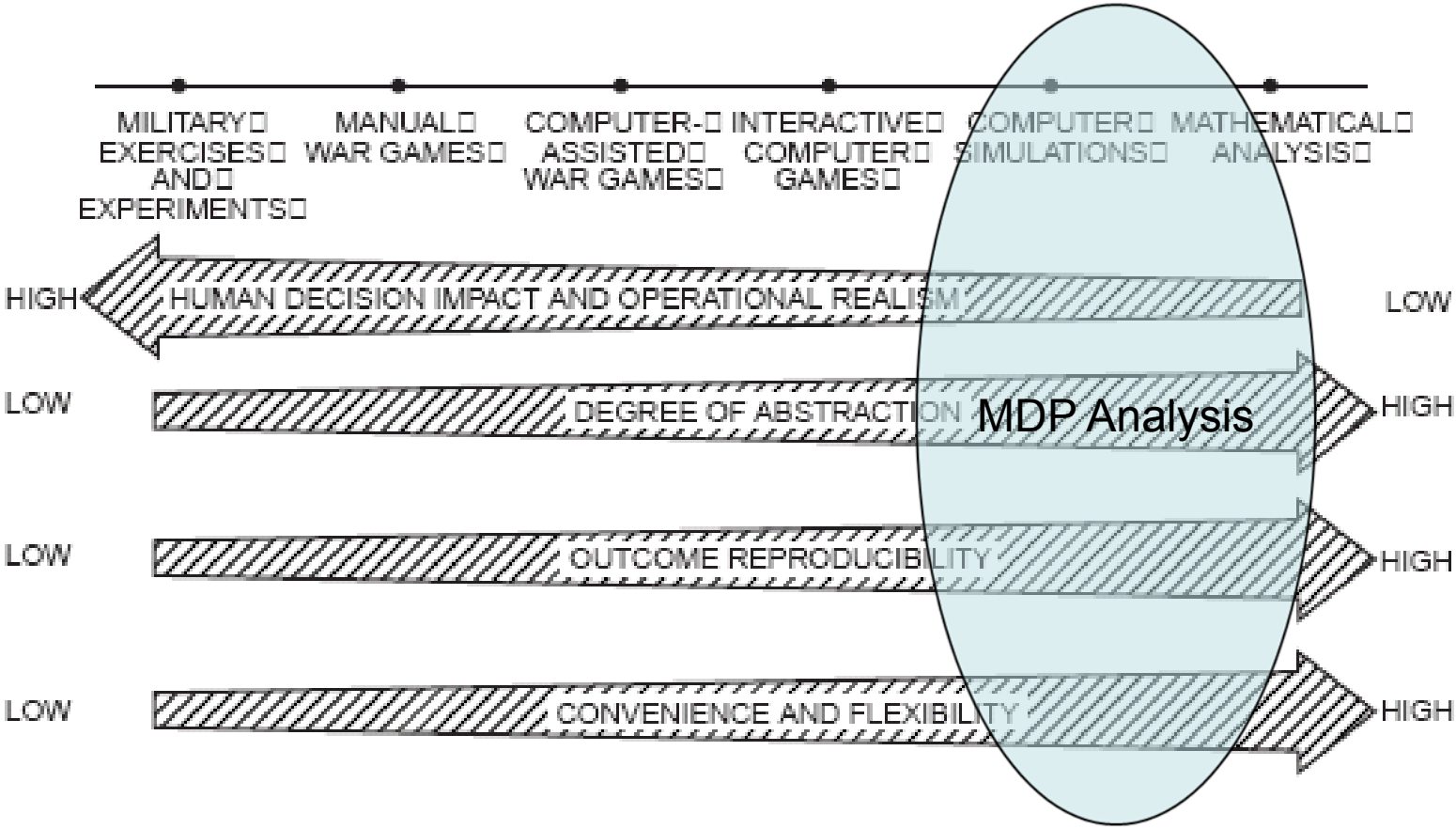
C3I Insights
Gaps

- Real time Common Operating Picture
- Consequence Assessment
- Anomaly Detection
- Modeling Human Behavior
  - Actions at various threat levels
  - Quality

C3I Insights
Future Study

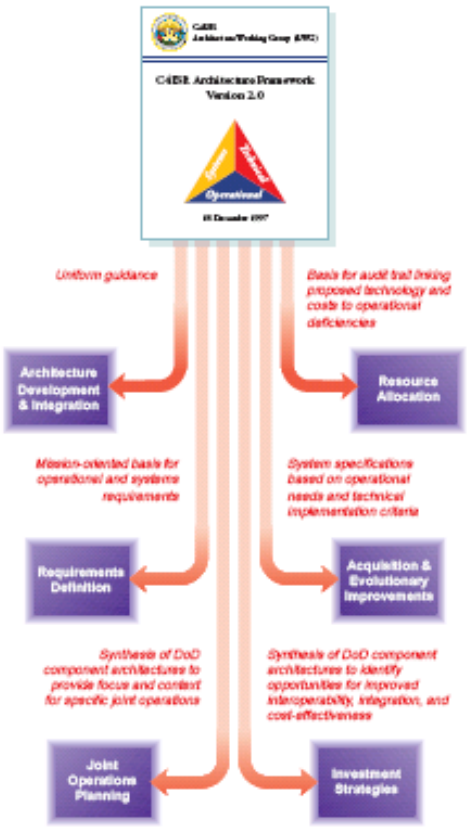
- Type II Decision (Quality) - [Tie False Alarm Rate to driving resources to $ to effectiveness]
- Test and evaluation of algorithms embedded in the data fusion are high risk to the ultimate performance of the overall MDP system.
- Complexity in the data fusion system engineering process is characterized:
  - representing the uncertainty in observations and in models of the phenomena that generate observations
  - combining non-commensurate information (e.g., the distinctive attributes in imagery, text, and signals)
  - maintaining and manipulating the enormous number of alternative ways of associating and interpreting large numbers of observations of multiple entities.
  - Staffing Ratio
- C3I Mod/Sim/Wargaming (Demonstration of Actual Human Behavior)
- Sensitivity/Cost Analysis various system component

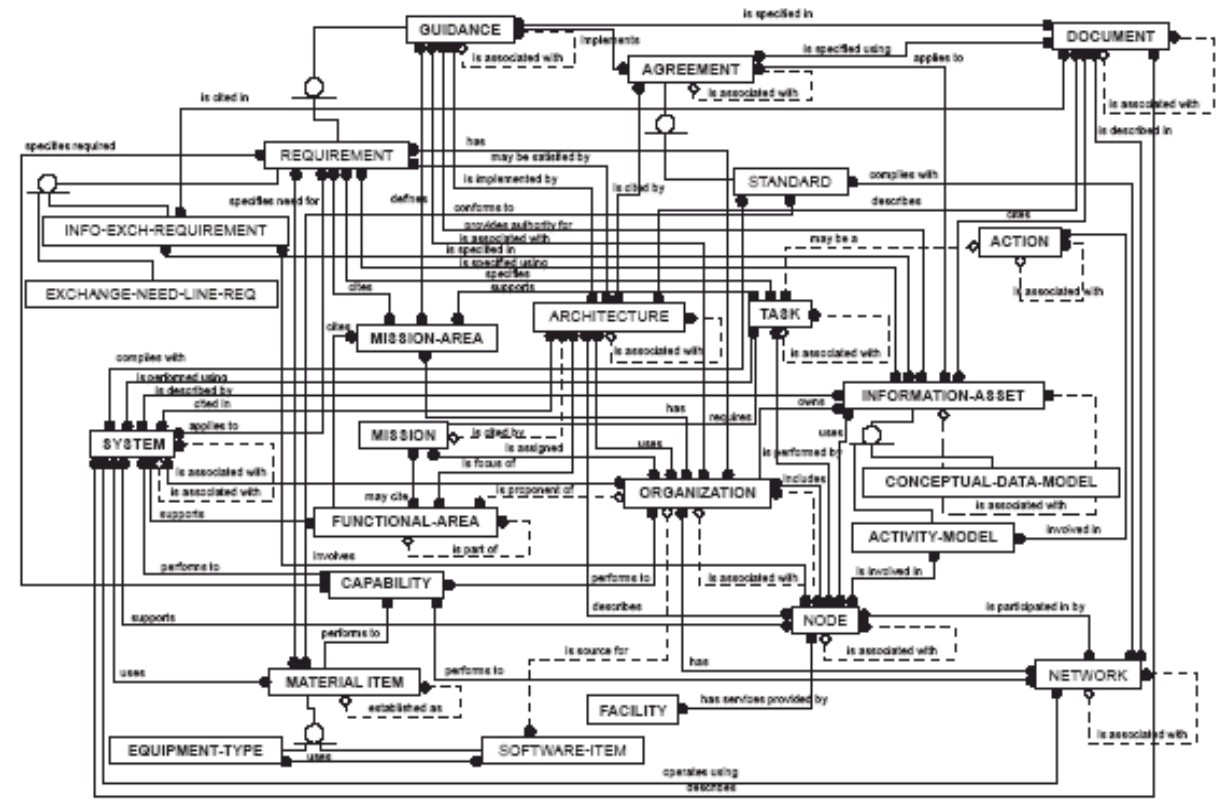
Insight C3I Modeling (Human Reality)



Further C3I MDP Systems Design Required

C4ISR Architecture Framework-Version 2.0 (1997)





NOTE: DoD standard entities are shown in bold font.

Figure 4-42. Overview of the Key Entities and Relationships for the C4ISR Core C4ISR Architecture Data Model (CADM)

Timeliness Model
Inputs and Outputs

Inputs

- Track Quality: P_{track}
- Track Quality: P_{fa}
- Position Error: CEP mean
- Position Error: CEP variance
- Traffic Density
- RAM
- WMD Probability ($P_{present}$)
- Anomaly Probability (P_{occurs})
- Information Inputs:
  - External Intel (may be HUMINT, ELINT, or other types)
  - Internal Intel: Land Inspection information
  - Internal Intel: Sea Inspection information
  - Sensor Information

Outputs

- Time to make a decision (based on gathering any three pieces of information)

Goodness Model Inputs

- Probabilities
  - $P_{\text{Receive AIS information (Y/N)}}$
  - $P_{\text{AIS information is good}}$
  - $P_{\text{Receive external intelligence (Y/N)}}$
  - $P_{\text{External intelligence is good}}$
  - $P_{\text{Receive sea inspection information (Y/N)}}$
  - $P_{\text{Sea inspection information is good}}$
  - $P_{\text{Anomaly occur?}}$
  - $P_{\text{Inspection decision error}}$
  - $P_{\text{Pass decision error}}$
- Distribution Means and Standard Deviations*
  - AIS information arrival time μ and σ
  - Sea Inspection information arrival time μ and σ
  - External intelligence information arrival time μ and σ
  - Anomaly occurrence time μ and σ

  *All information times are modeled by distributions based on scenario timelines