

An Operational Framework for Battle in Network Space

By RDL Knight

Head, Future Trends and Forecasts in Network Defence
Communication Security Establishment - Canada

and

Dr M. MacIntyre

Head, Network Information Operations
Defence R&D Canada – Ottawa

Report Documentation Page

*Form Approved
OMB No. 0704-0188*

Public reporting burden for the 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 the 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 Washington Headquarters Services, Directorate for Information Operations and Reports, 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 a penalty for failing to comply with a collection of information if it does not display a currently valid OMB control number.

| | | | |
|--|------------------------------------|---|----------------------------------|
| 1. REPORT DATE JUN 2006 | 2. REPORT TYPE | 3. DATES COVERED 00-00-2006 to 00-00-2006 | |
| 4. TITLE AND SUBTITLE An Operational Framework for Battle in Network Space | | 5a. CONTRACT NUMBER | |
| | | 5b. GRANT NUMBER | |
| | | 5c. PROGRAM ELEMENT NUMBER | |
| 6. AUTHOR(S) | | 5d. PROJECT NUMBER | |
| | | 5e. TASK NUMBER | |
| | | 5f. WORK UNIT NUMBER | |
| 7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) Defence Research and Development Canada -Ottawa,3701 Carling Avenue,Ottawa Ontario K1A 0Z4, , | | 8. PERFORMING ORGANIZATION REPORT NUMBER | |
| 9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES) | | 10. SPONSOR/MONITOR'S ACRONYM(S) | |
| | | 11. SPONSOR/MONITOR'S REPORT NUMBER(S) | |
| 12. DISTRIBUTION/AVAILABILITY STATEMENT Approved for public release; distribution unlimited | | | |
| 13. SUPPLEMENTARY NOTES The original document contains color images. | | | |
| 14. ABSTRACT | | | |
| 15. SUBJECT TERMS | | | |
| 16. SECURITY CLASSIFICATION OF: | | | 17. LIMITATION OF ABSTRACT |
| a. REPORT unclassified | b. ABSTRACT unclassified | c. THIS PAGE unclassified | 18. NUMBER OF PAGES 26 |
| | | | 19a. NAME OF RESPONSIBLE PERSON |

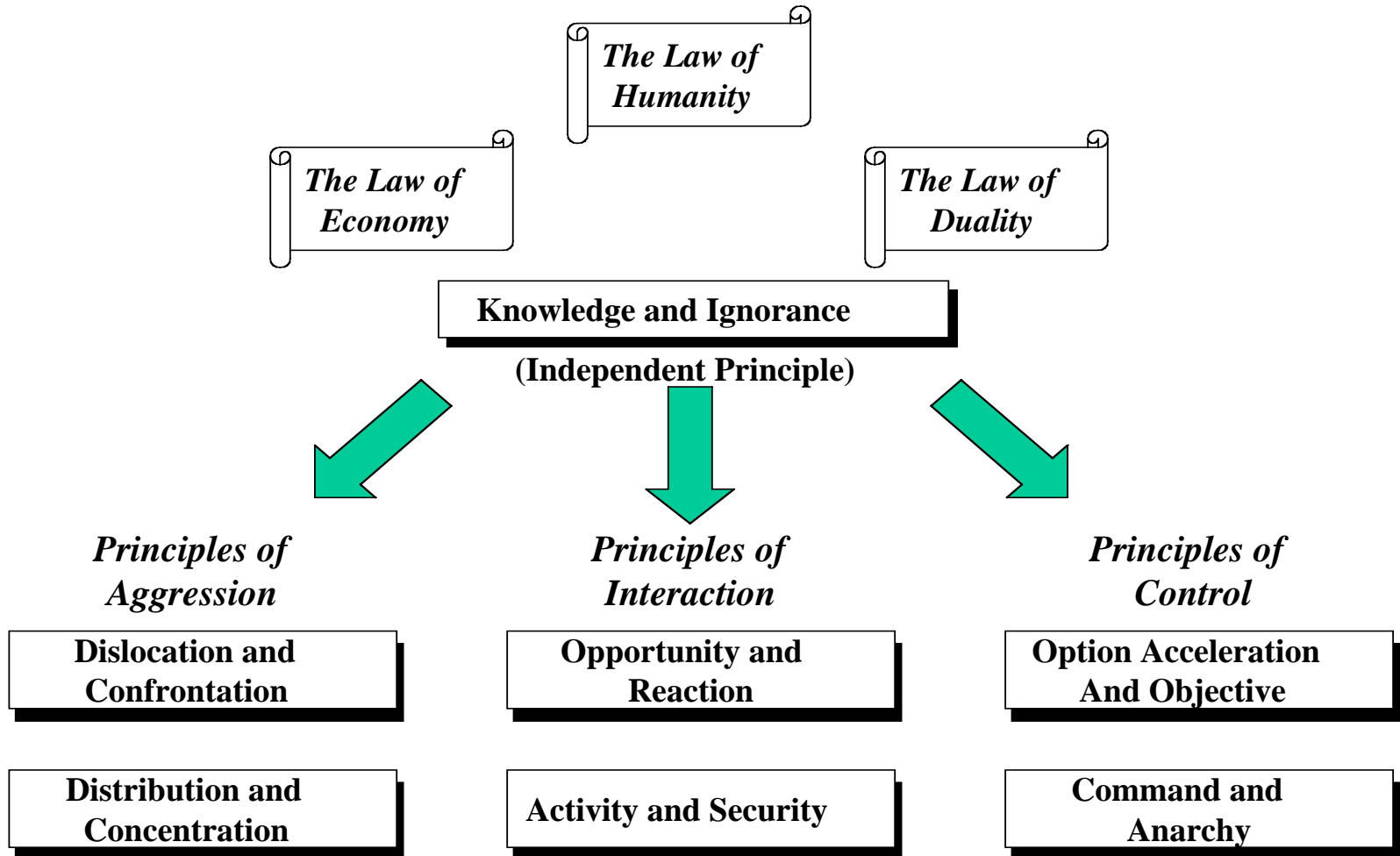
Presentation Outline

- Principals of Warfare for Net Space
- Mapping IO to Network Battlespace
- A Main Defensive Battle in Net Space

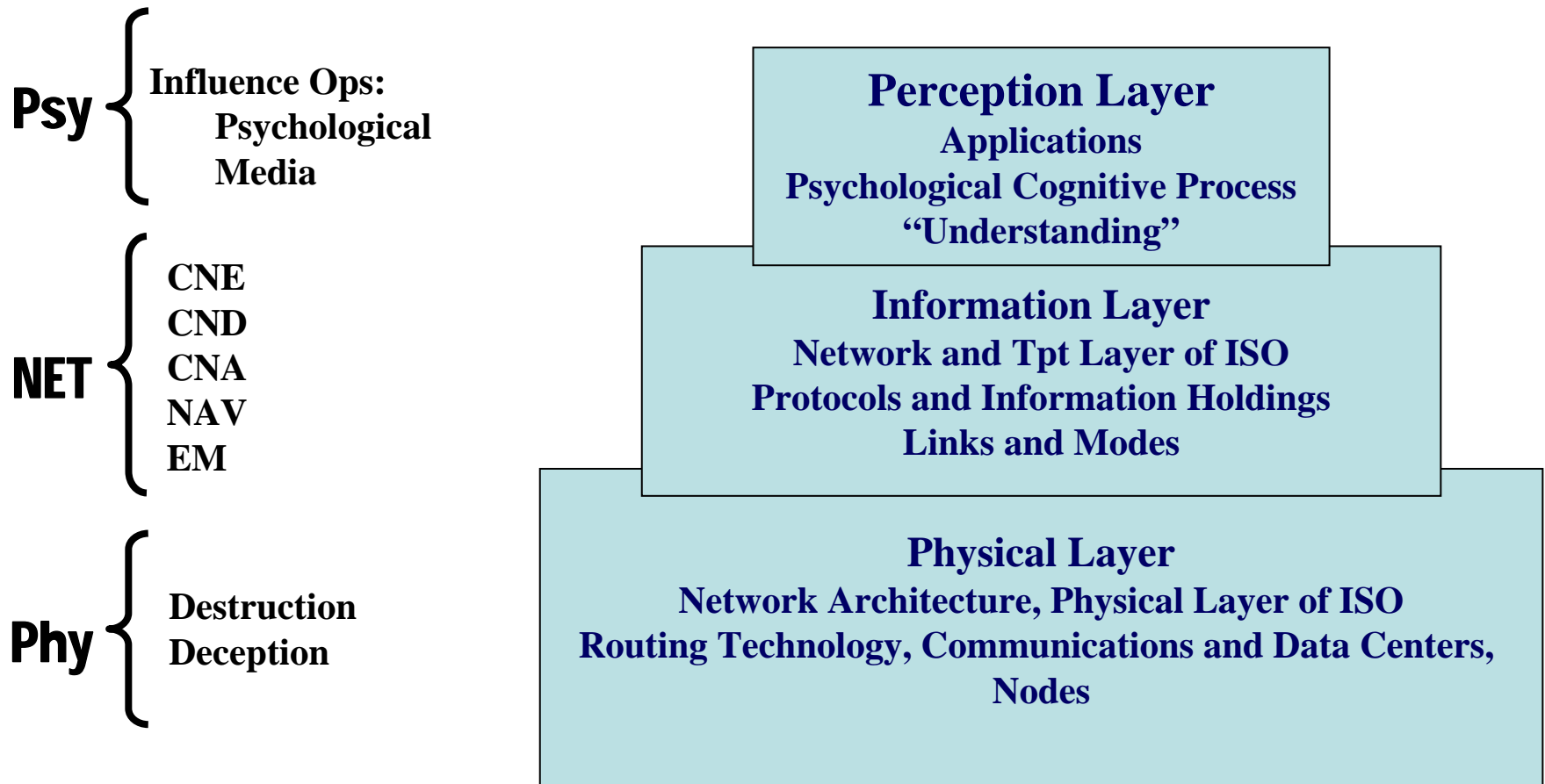
- A Vision for Computer Network Operations

- Some useful Analogies?
 - CDD Imagery
 - Air Tasking Order
 - Combat Logistics

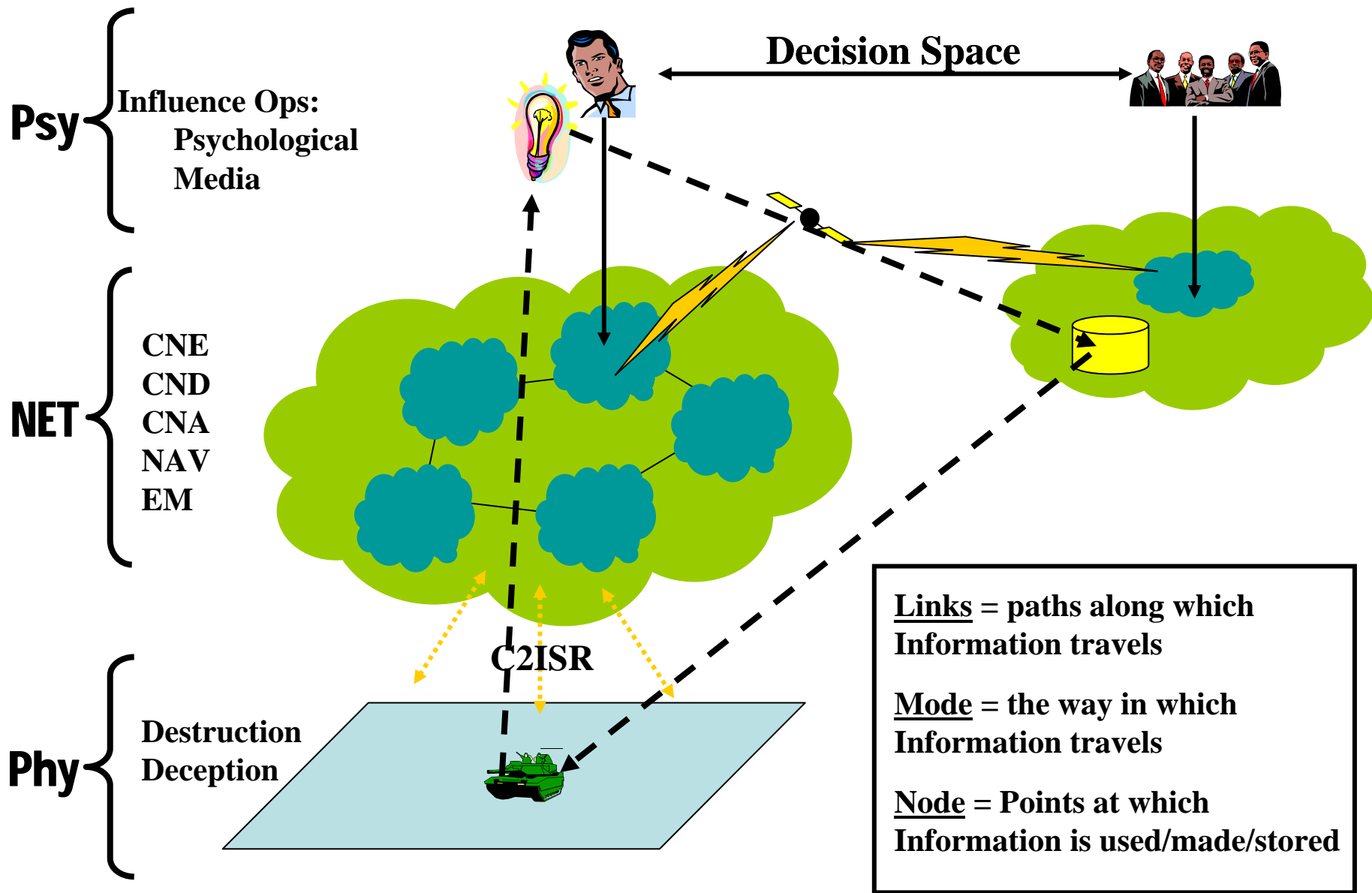
Leonhard's Principles of War for the Information Age



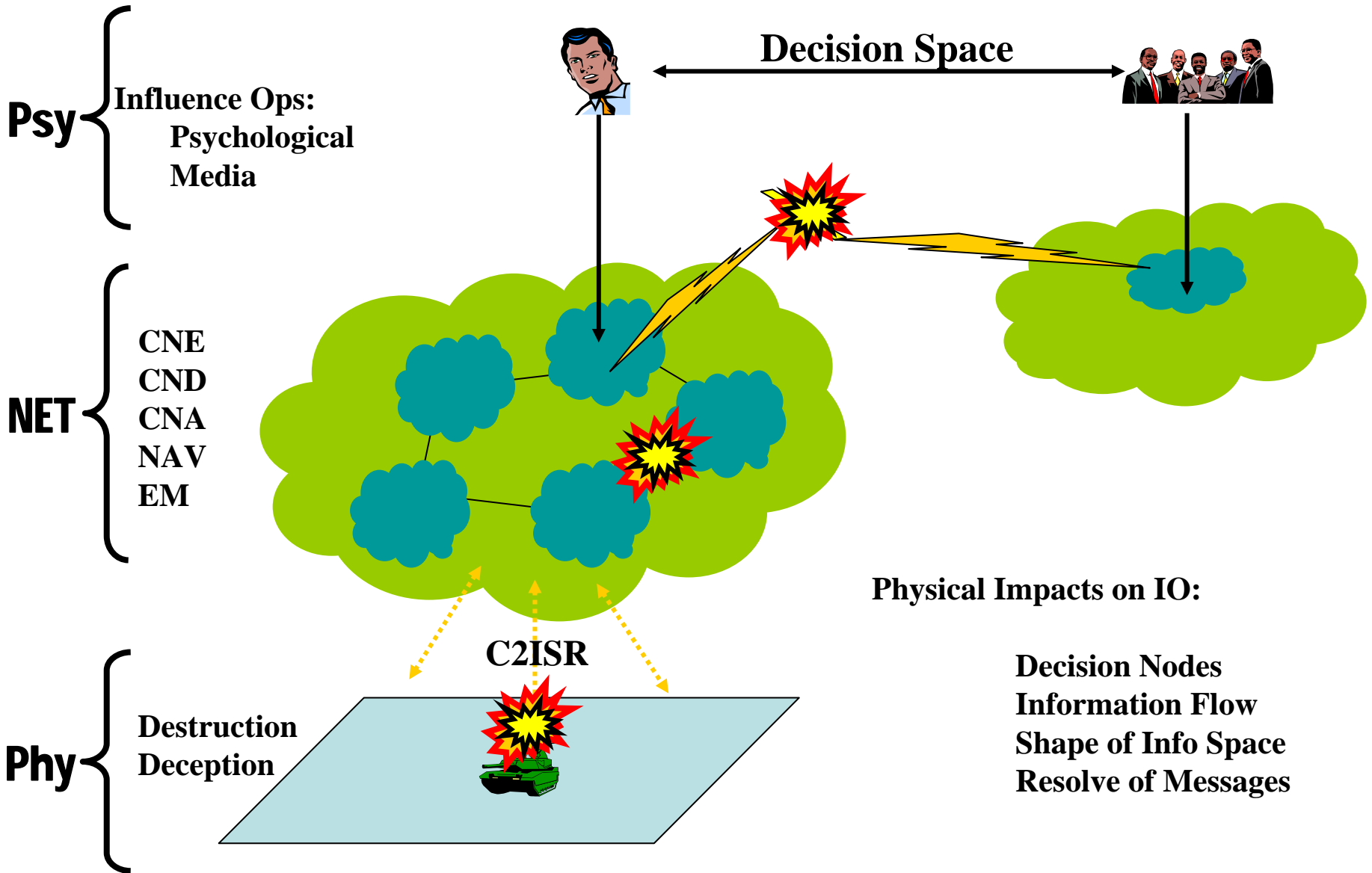
Mapping Knowledge Environment to Information Ops



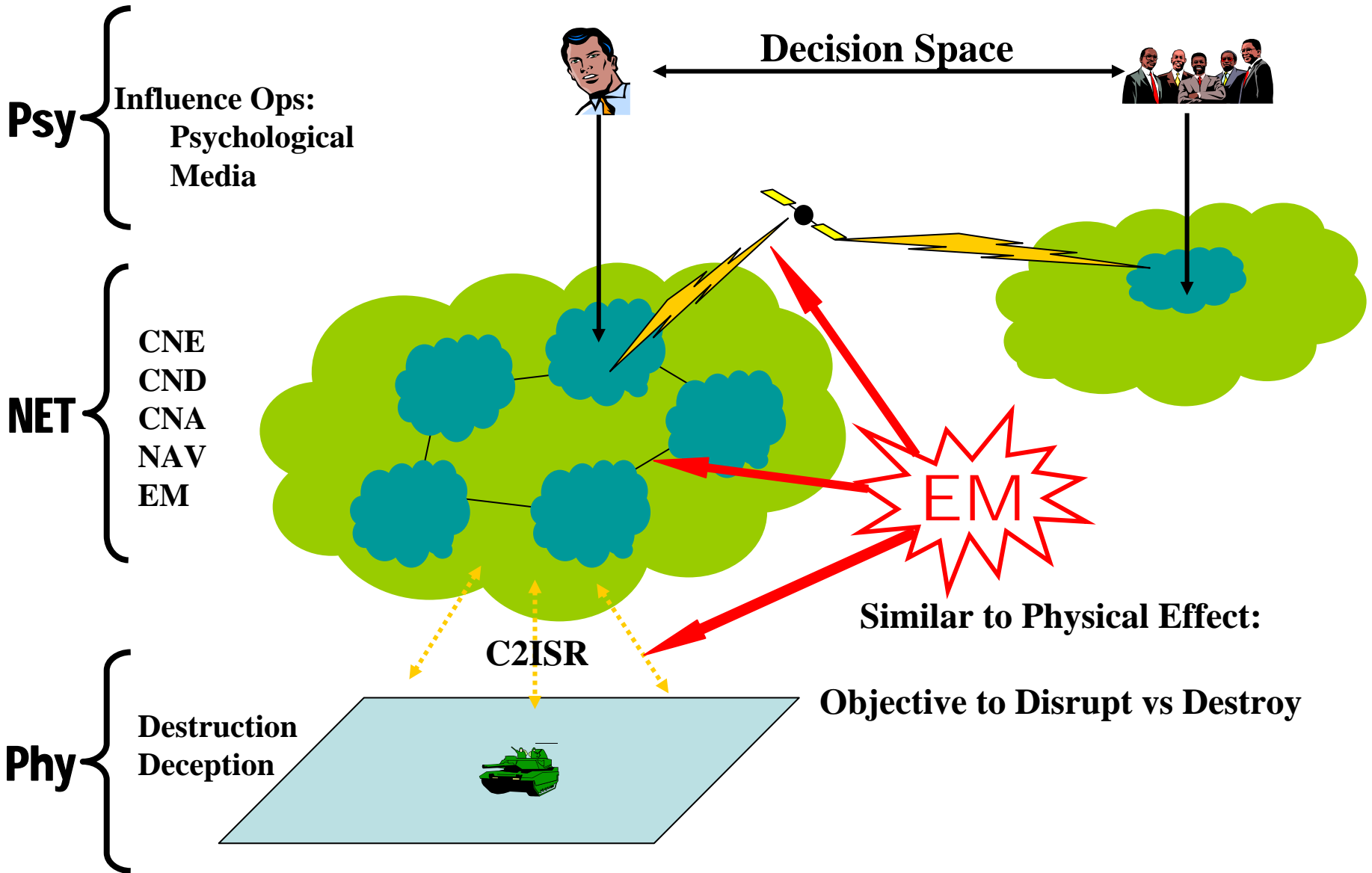
Defining the Information Battle Space:



Physical Dimension:



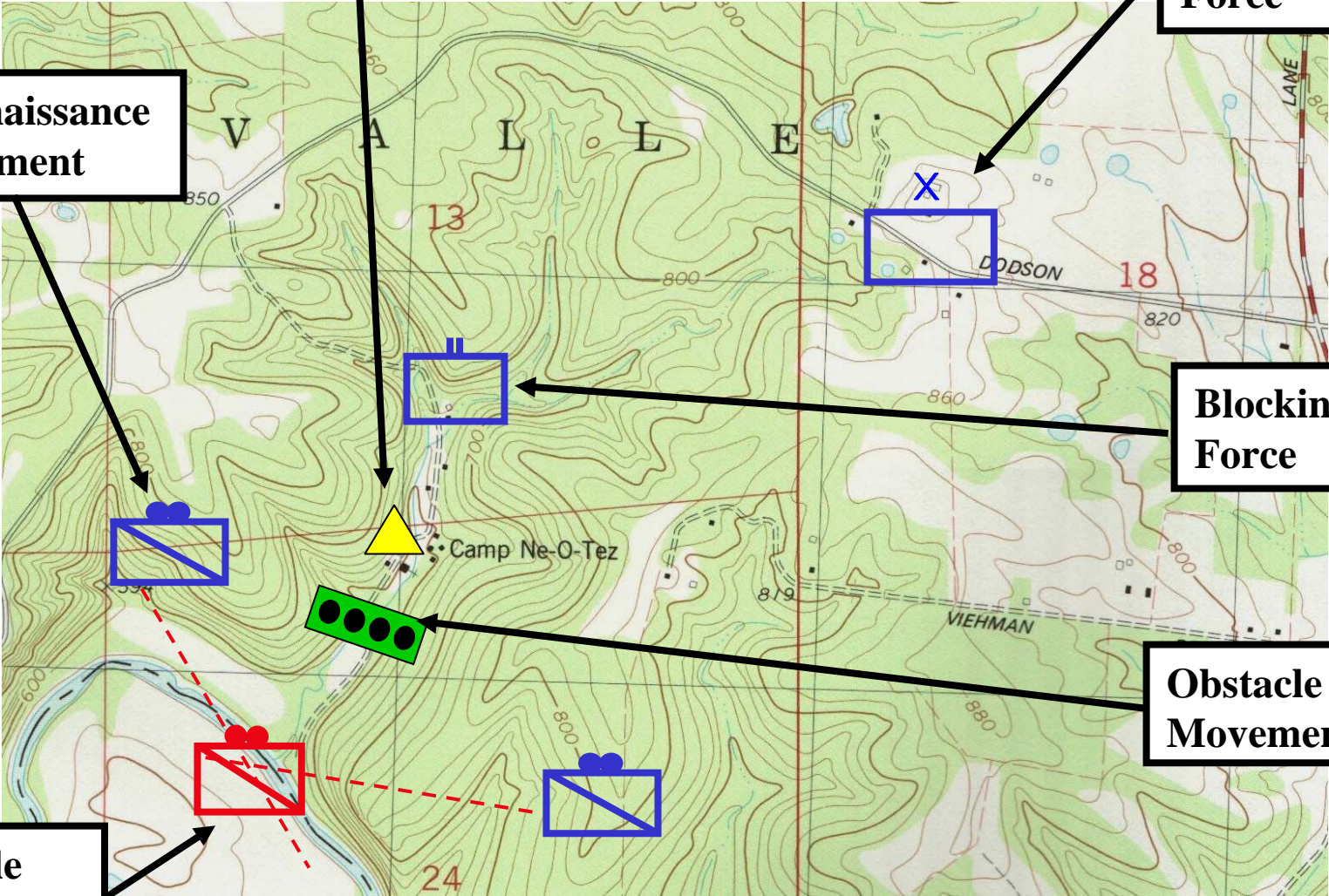
Electromagnetic Battle:



Observation Point

High Value Force

Reconnaissance Detachment

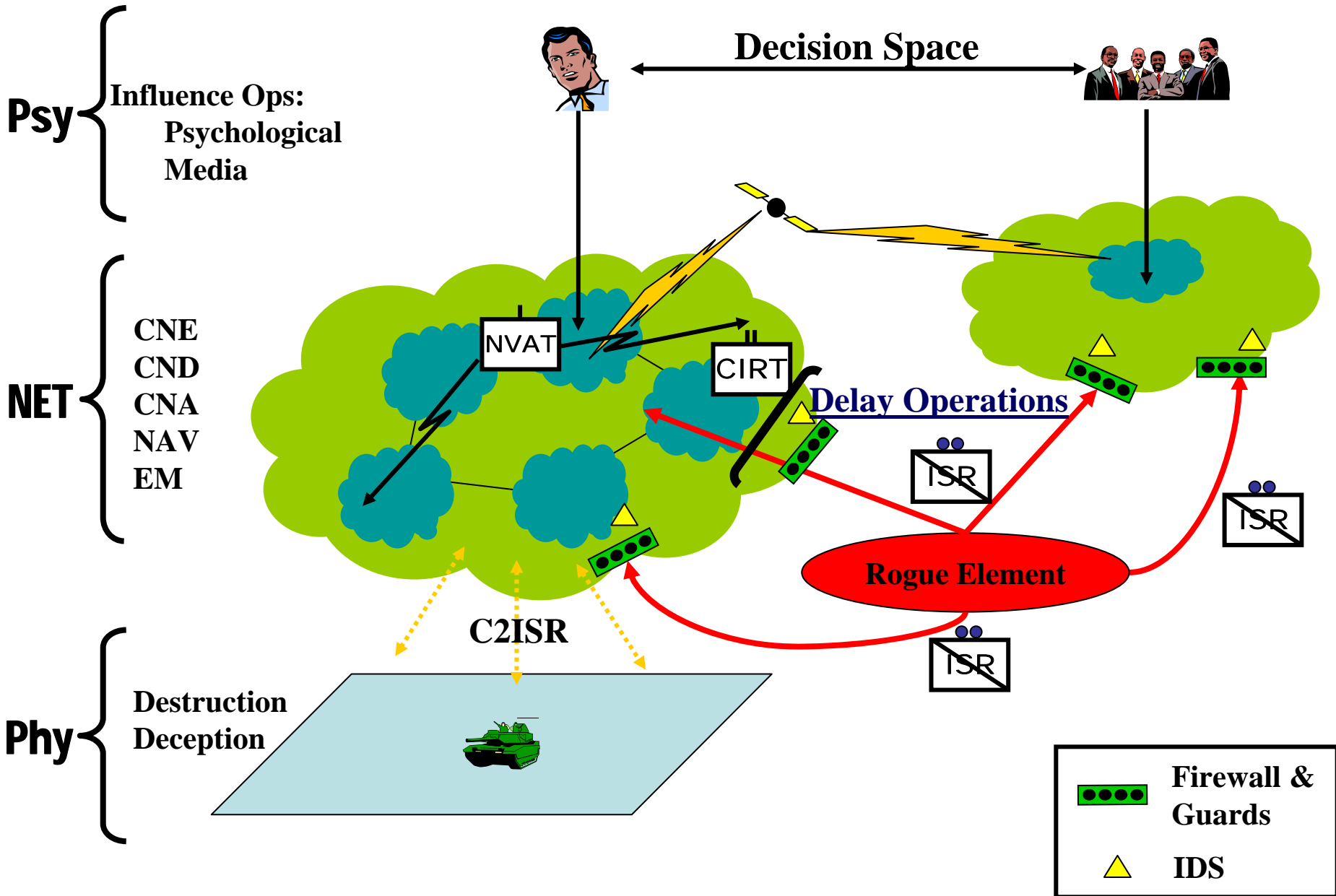


Blocking Force

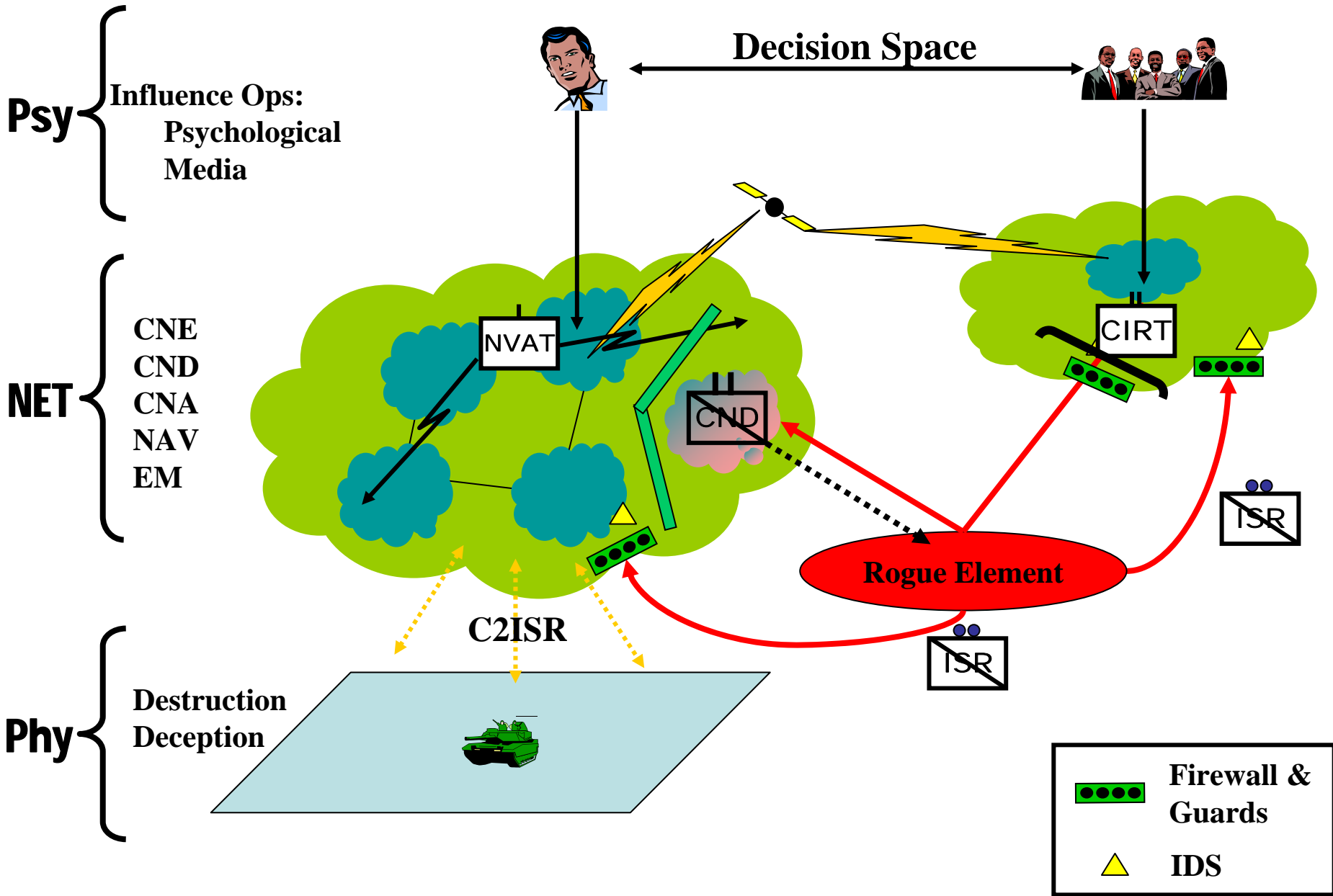
Obstacle to Movement

Hostile Element

Network Operations: Main Defensive Construct

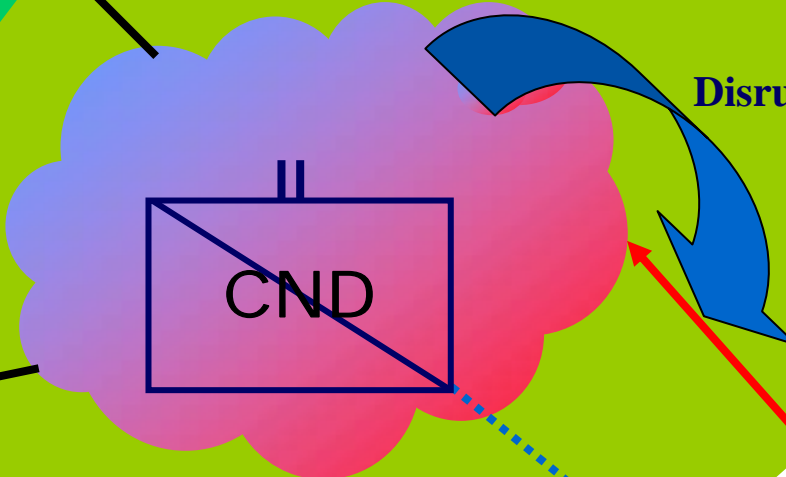
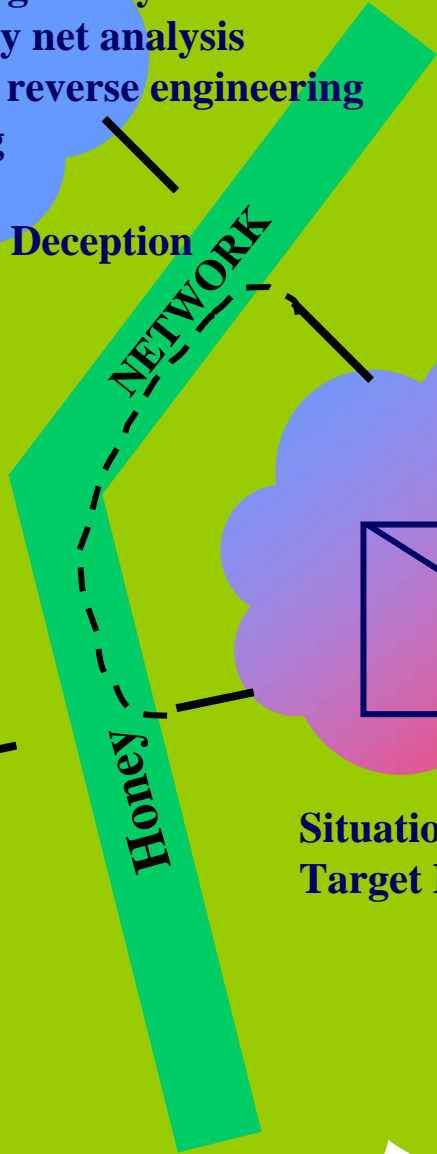


Network Operations: Killing Zone



Killing Zone: Dislocation and Definition of Enemy

Rapidly reconfig Honey Net
Real-time honey net analysis
Real-time code reverse engineering
Covert hacking
Channeling
Disruption and Deception
Techniques



Disruption or Deception Ops

Situational Awareness
Target Development



Rear Area Security

NVAT

CIRT

Architectural Security
&
Vulnerability

INFOCON
Patches and Protocols
SA & Surveillance
Severing Policy

ISSO

ISSO

NOC

Red
Team

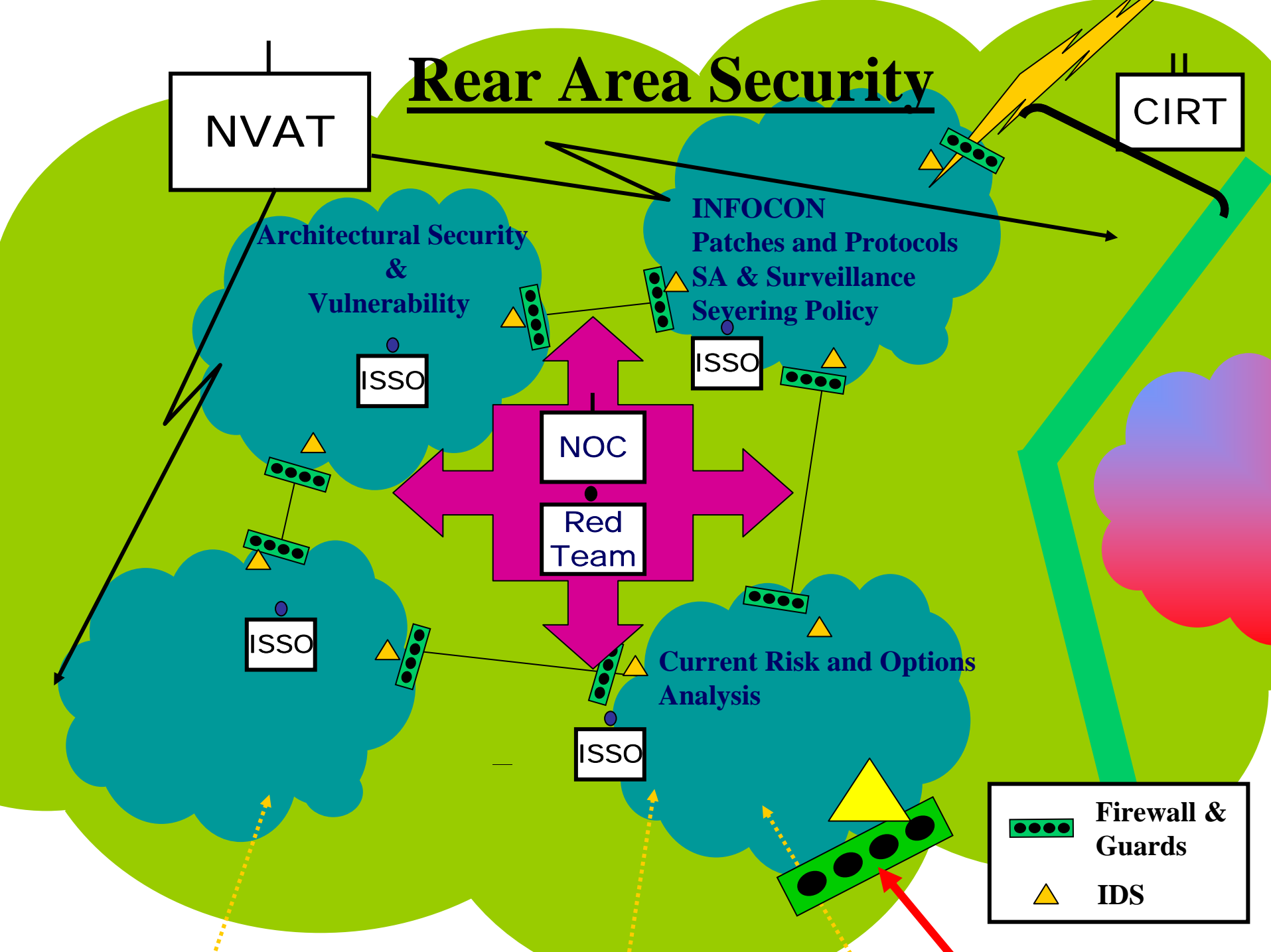
ISSO

ISSO

Current Risk and Options
Analysis

Legend:

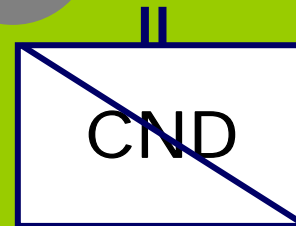
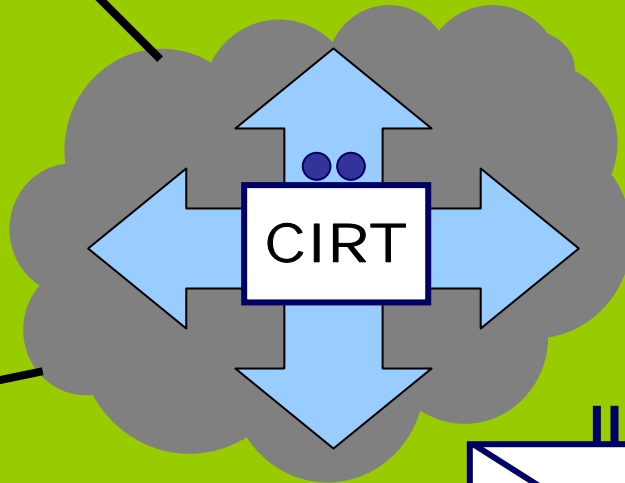
-  Firewall & Guards
-  IDS



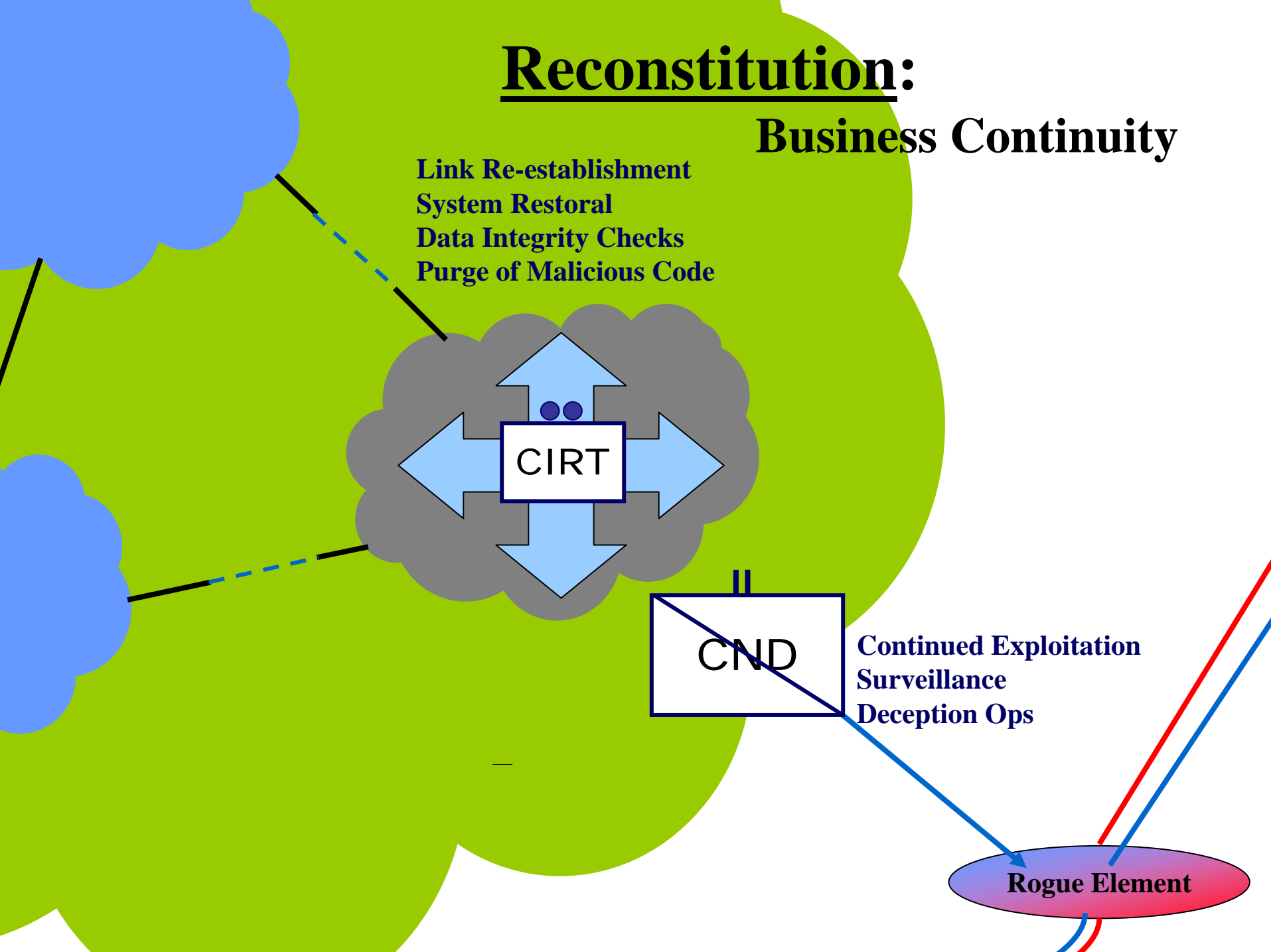
Reconstitution:

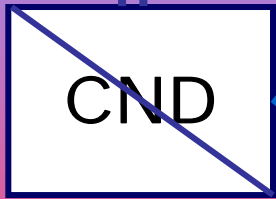
Business Continuity

Link Re-establishment
System Restoral
Data Integrity Checks
Purge of Malicious Code



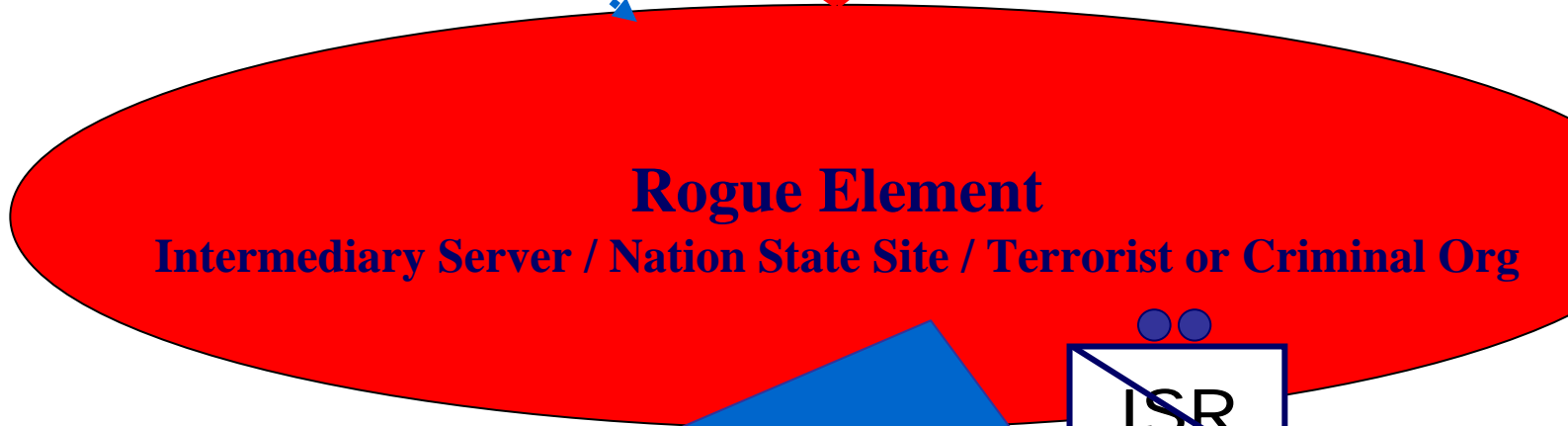
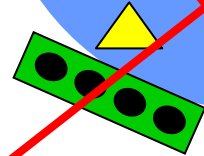
Continued Exploitation
Surveillance
Deception Ops



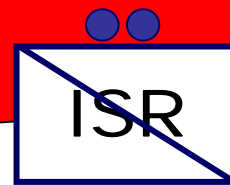


Situational Awareness
Target Development
Disruption or Deception Ops

The Network Attack: Disable or Defeat Enemy



Rogue Element
Intermediary Server / Nation State Site / Terrorist or Criminal Org

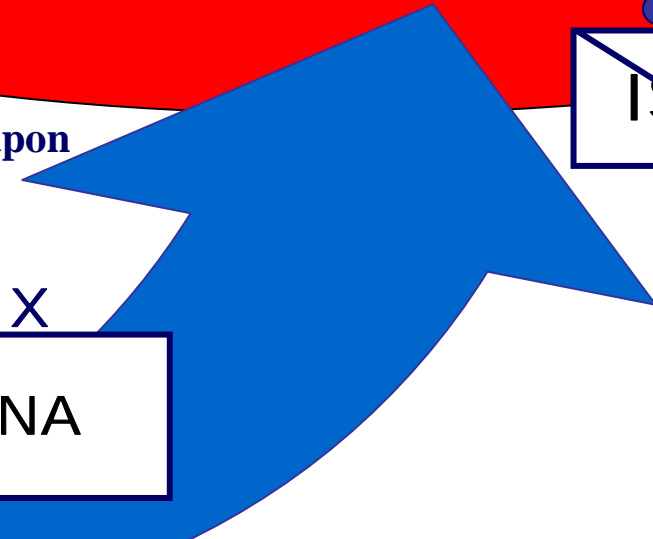


Close Target Recce

Physical Interdiction: Hard Kill - Weapon
Tactical Assault

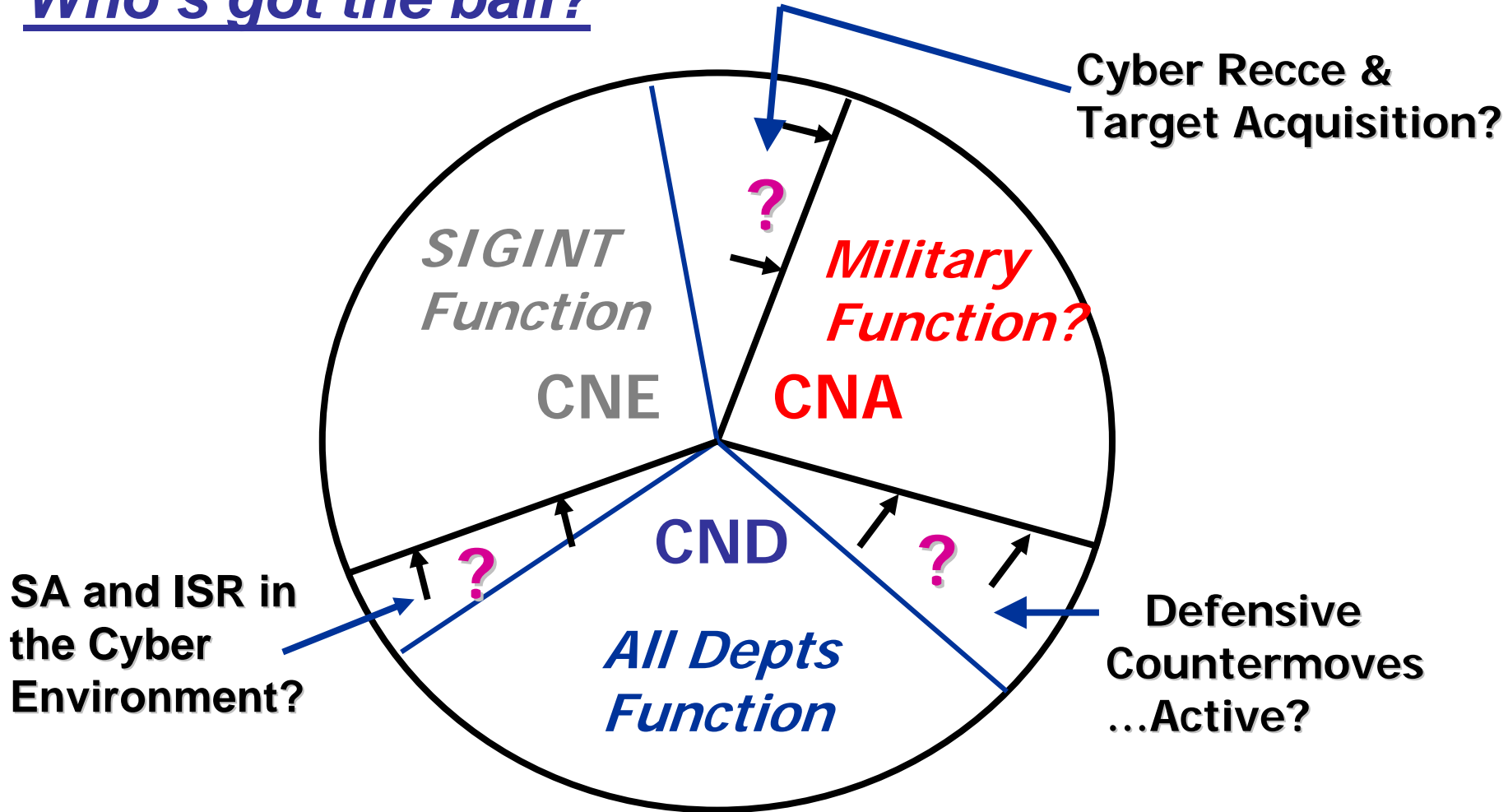
Link Attacks: Jamming
Denial of Service

Network Attacks: Net Weapons
Interdiction
Capture



A Vision of CNO

Who's got the ball?



Further Useful Analogies

CDD Imagery

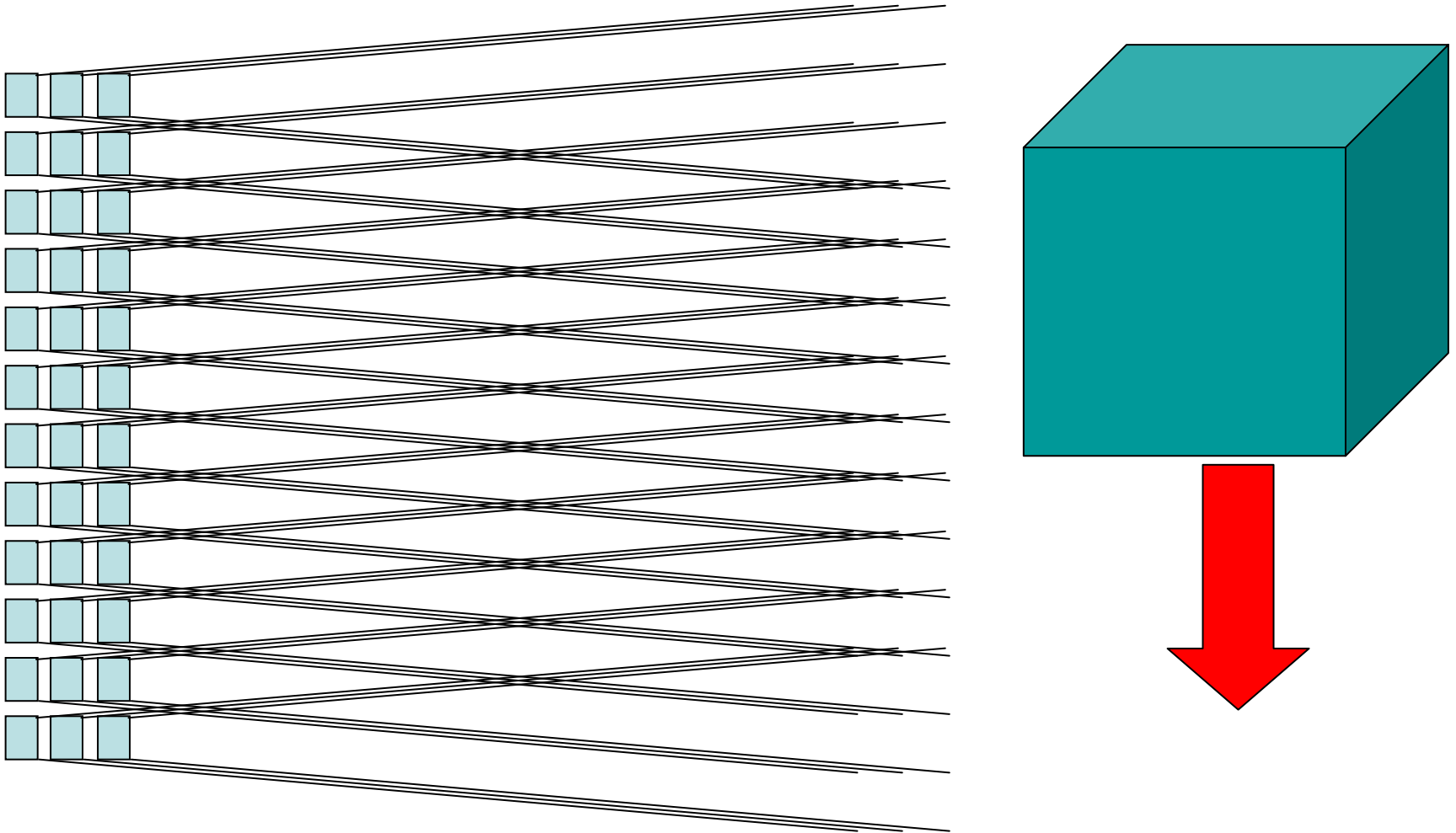
Air Tasking Order Battle Rhythm

Strategic vs Combat Logistics

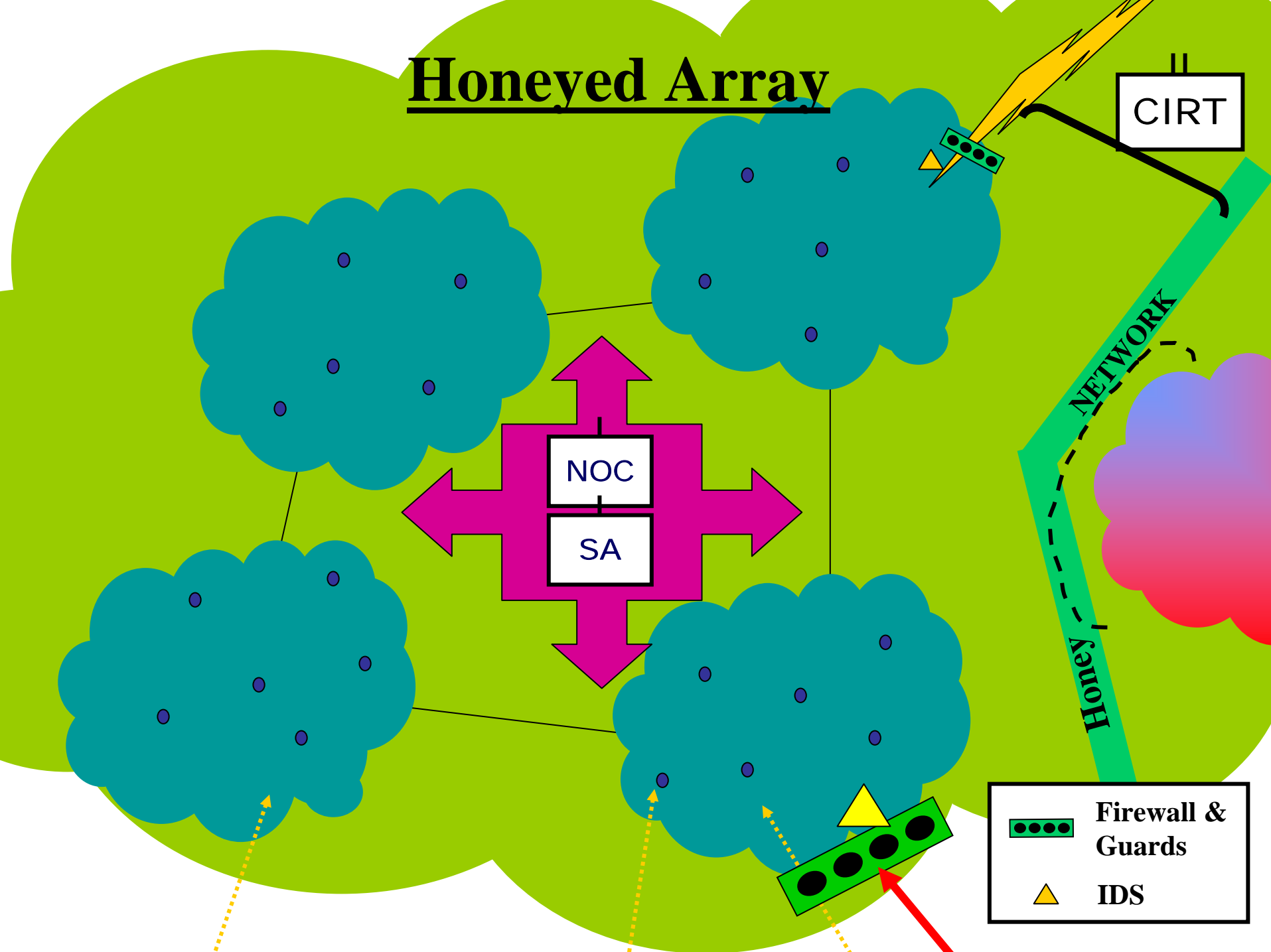
Charge-Coupled Device (CCD)

-is there a photon?

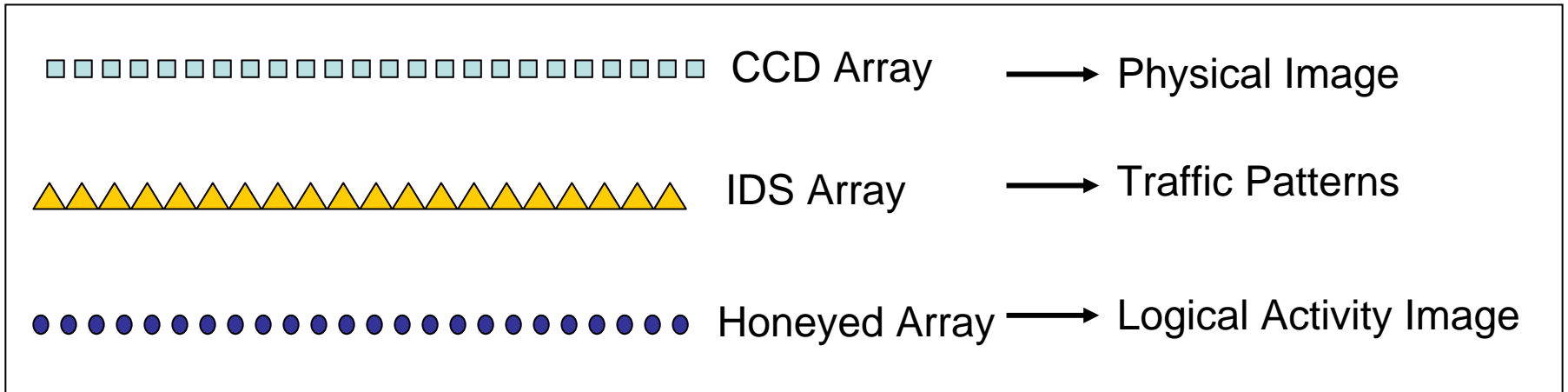
- if yes, then of what energy




Honeyed Array



An Analogy for ISR



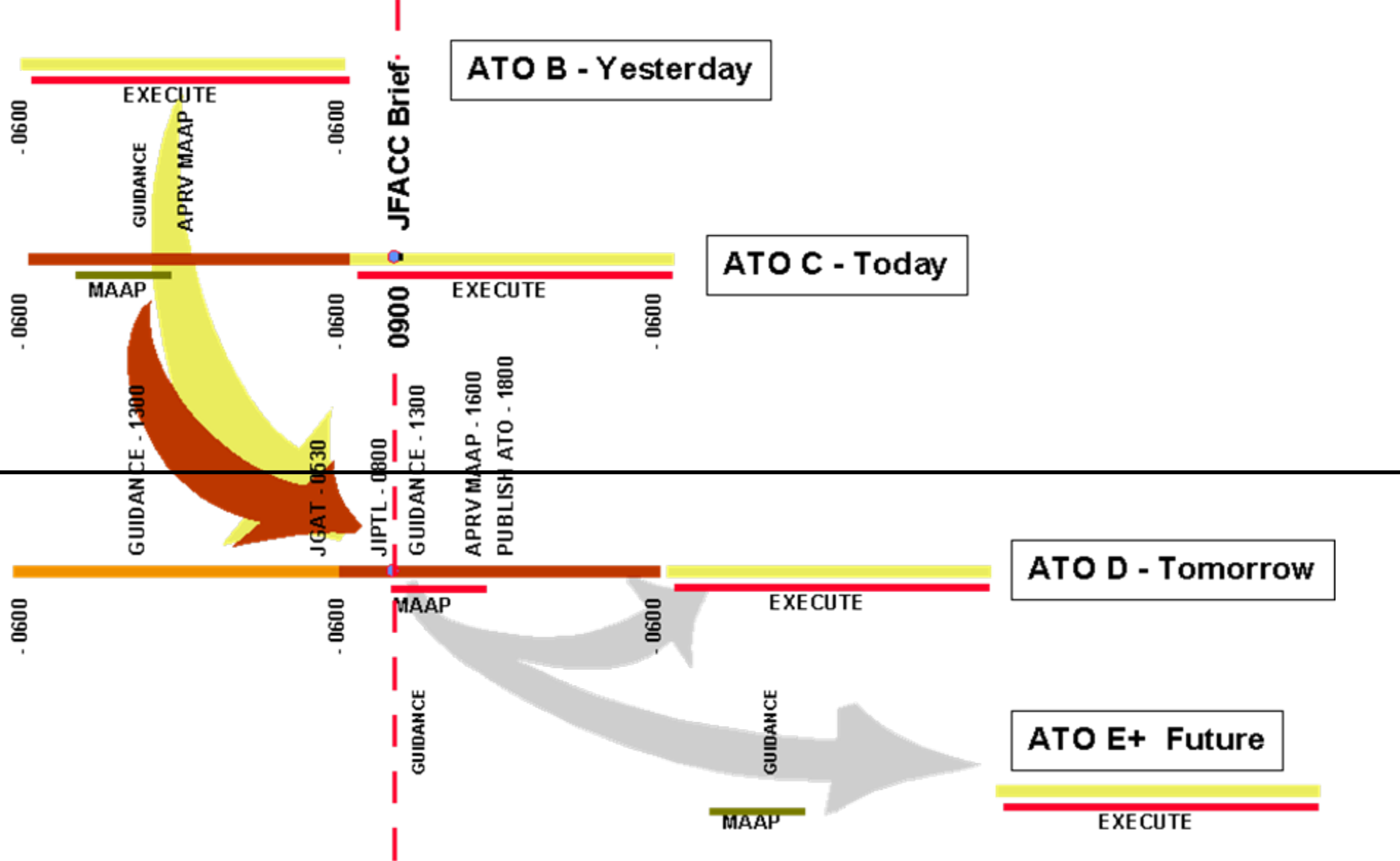
 = Honey Pot

As #   > **Stare time **

As fidelity   > **Stare time **

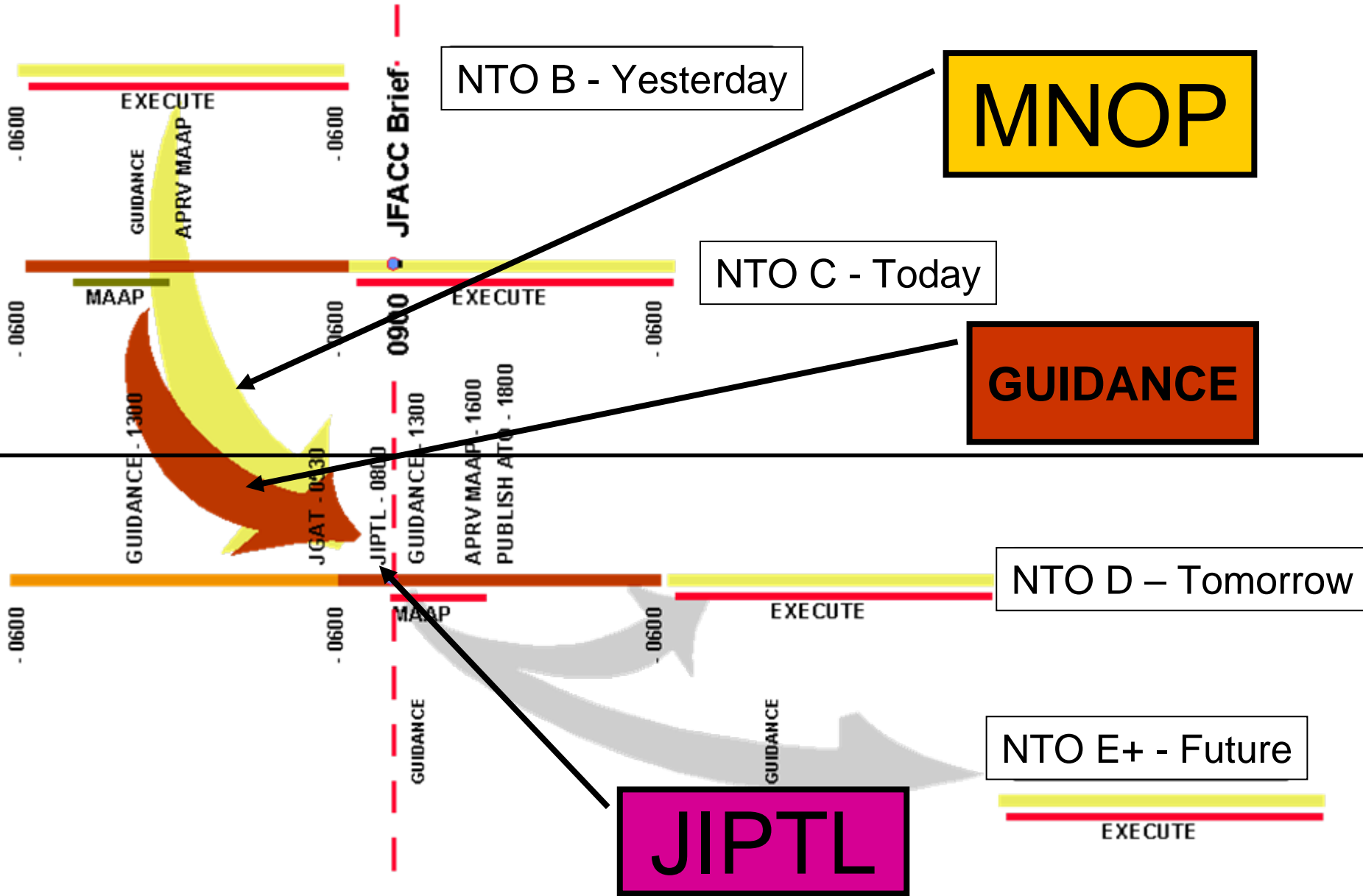
Intelligent Deployment > **Stare time **

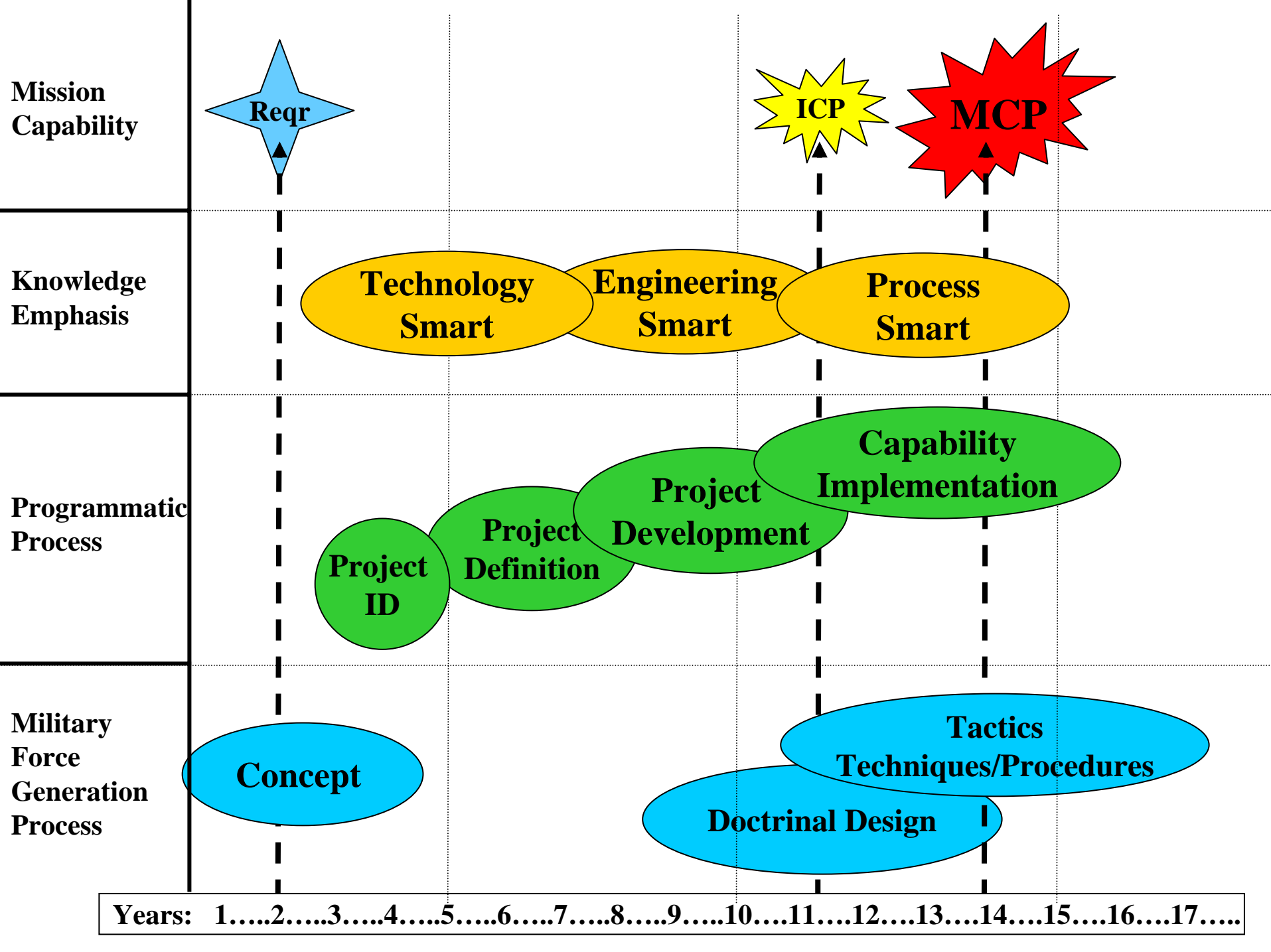
FIGURE 2 - ATO BATTLE RHYTHM/JFACC AIB



Air Operations Center (AOC) Standard Operating Procedure (SOP)
Twelfth Air Force (12AF) Air Force Forces (AFFOR)
ANNEX B TO CHAPTER 3

Network Tasking Order BATTLE RHYTHM

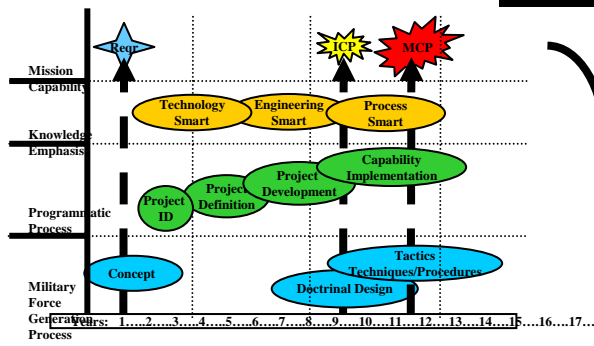




The Problem Space!

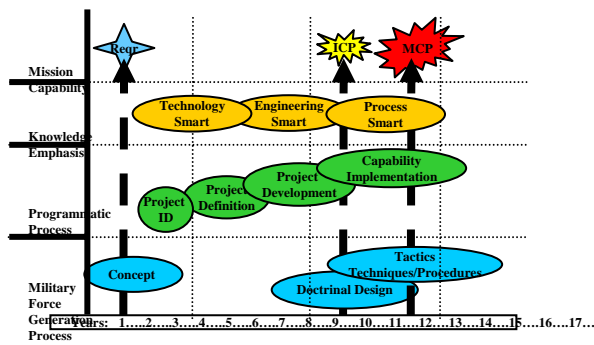
From the synthesis of multiple Global Requirements

- in multiple AORs
- with separate TO&Es and
- with different Environmental leads...

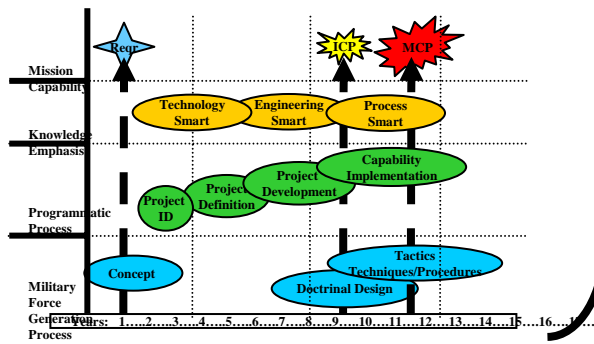


Conventional Military

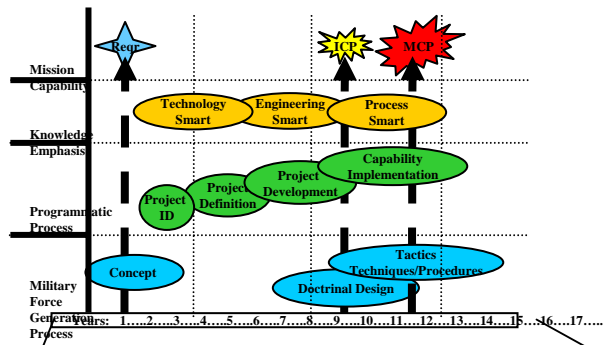
...to a Mission Capability Package in **Weeks!**



Theater / AOR

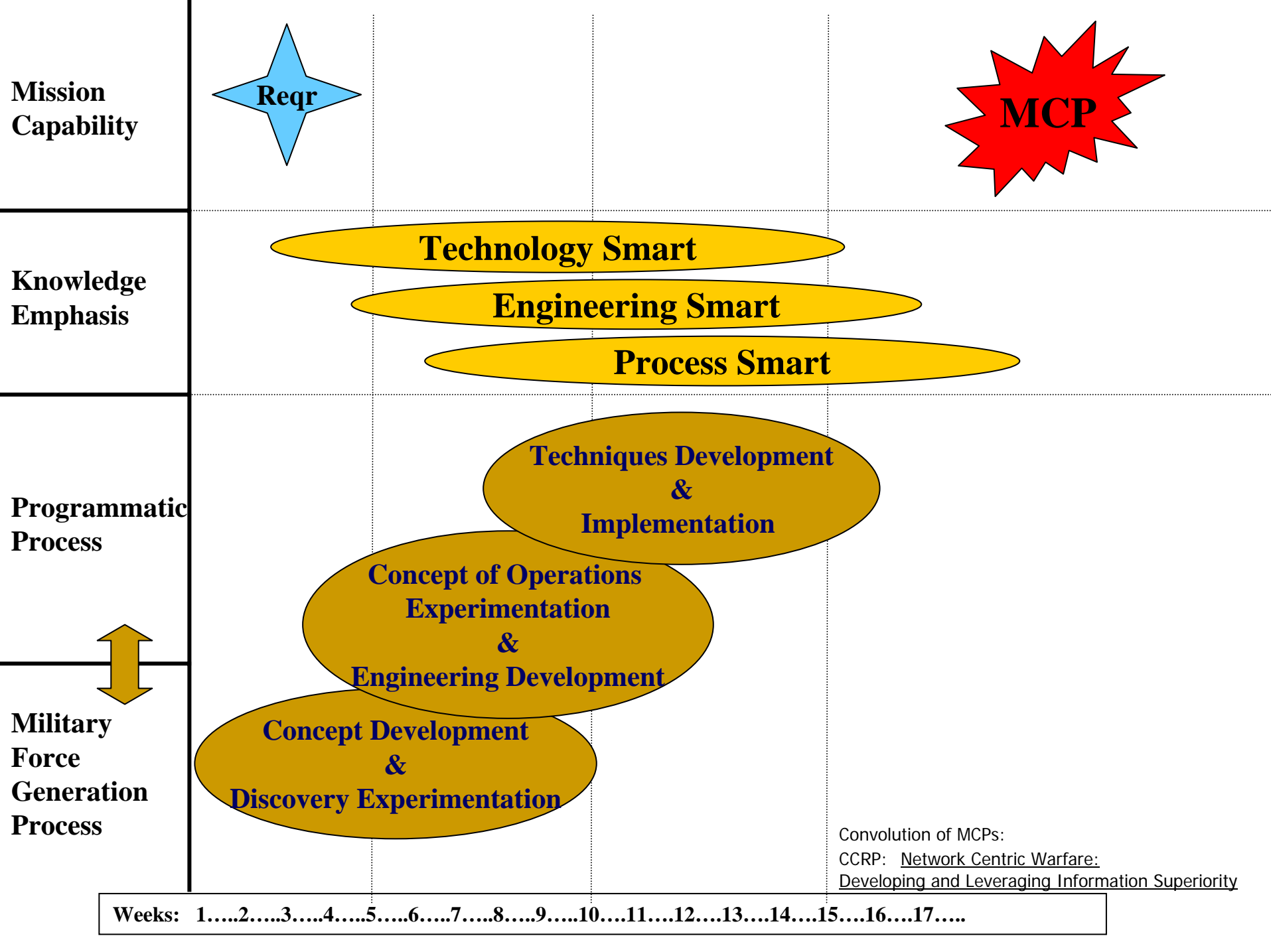


GII / MII / Cyber



...to a Mission Capability Package in **Days?**

Weeks: 1.....2.....3.....4.....5.....6.....7.....8.....9.....10.....11.....12.....13.....14.....15.....



**Mission
Capability**



**Knowledge
Emphasis**

Technology Smart

Engineering Smart

Process Smart

Self Synchronization

Knowledge Workers

Joint Philosophy

- Shared Awareness with Force Generators
- Networked entities
- Clear Purpose
- Knowledge Base of Con Ops and Technologies

- Shared Awareness with J Staff
- Multiple COA development process
- Close coord with War fighter
- Lessons Learned Feed Back

**Robust Programmatic
Process**

- Knowledge Base of Best Practices
- Close Coord with Contract Agents
- Clear Life Cycle and Strategic Capital Business Process

**Program Cost:
(ReCap vs R&O)**

**Lack of
Optimization**

**Loss of
Program
Control**

**Loss of
Program
Control**

**Maint
ILS**

**HR
Training**

What is the Future?

Technology Smart

Engineering Smart

Process Smart

Knowledge Workers



**Network Awareness
&
Joint Strategic Guidance**

