33rd Annual AOC International Electronic Warfare Technical Symposium and Convention

Command and Control Warfare: OODA Loop Countermeasures

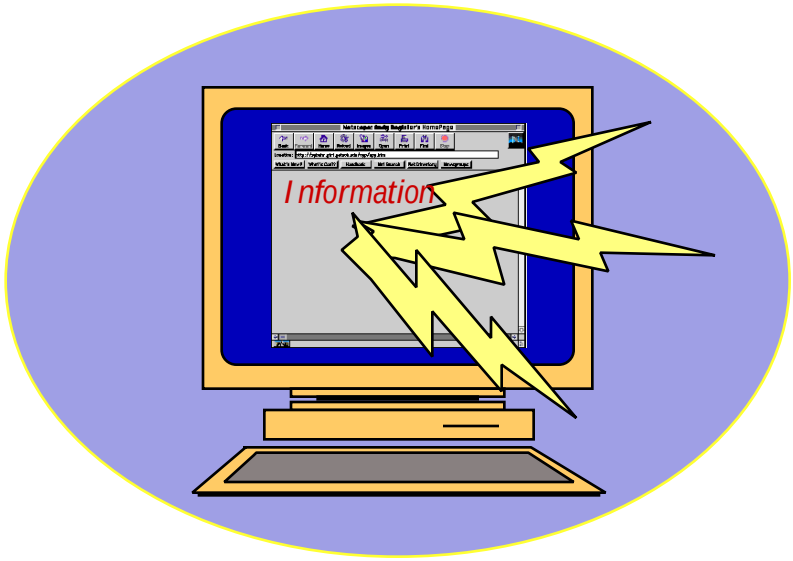
October 2, 1996

Dr. Myron L. Cramer
Georgia Tech Research Institute
400 Tenth Street
Atlanta, Georgia 30332-0840
(404) 894-7292
myron.cramer@gtri.gatech.edu

Georgia Tech

PURPOSE

This presentation:



- » discusses Information Warfare against networked Command and Control (C2) systems
- » proposes a use for C2 conceptual models such as the “OODA Loop”
- » suggests a new role for Electronic Warfare engineering methods

DEFINITION ...

Information Warfare includes:

ways of gaining and maintaining an **information advantage** over competitors or adversaries.

» The term **Dominant Battlespace Knowledge** is currently used to convey the desired result of successful IW practices. Although IW is a general term including a wide variety of different concepts, it is usually connotes a primarily strategic focus. Command and Control Warfare (C2W) is defined as the combat use of IW.

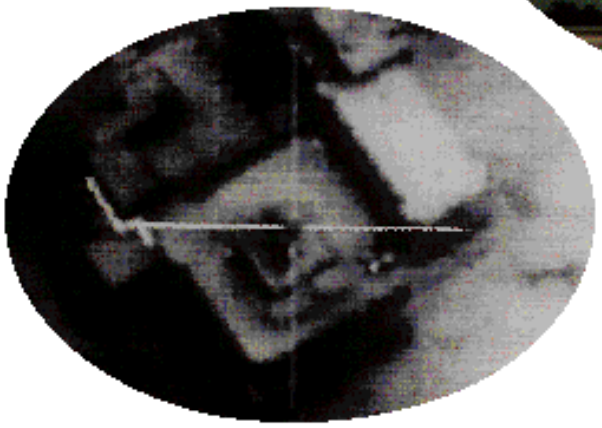
COMMAND & CONTROL WARFARE DEFINED

OPSEC

PSYOP

EW

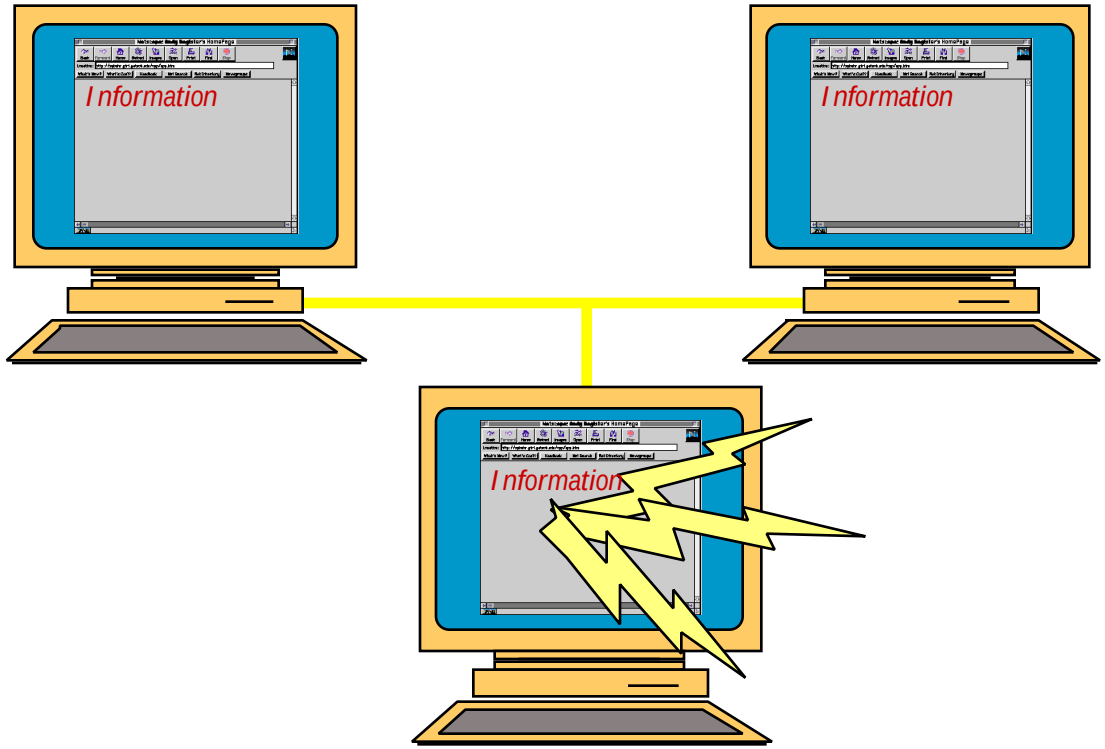
DESTRUCTION



DECEPTION

CYBERWAR

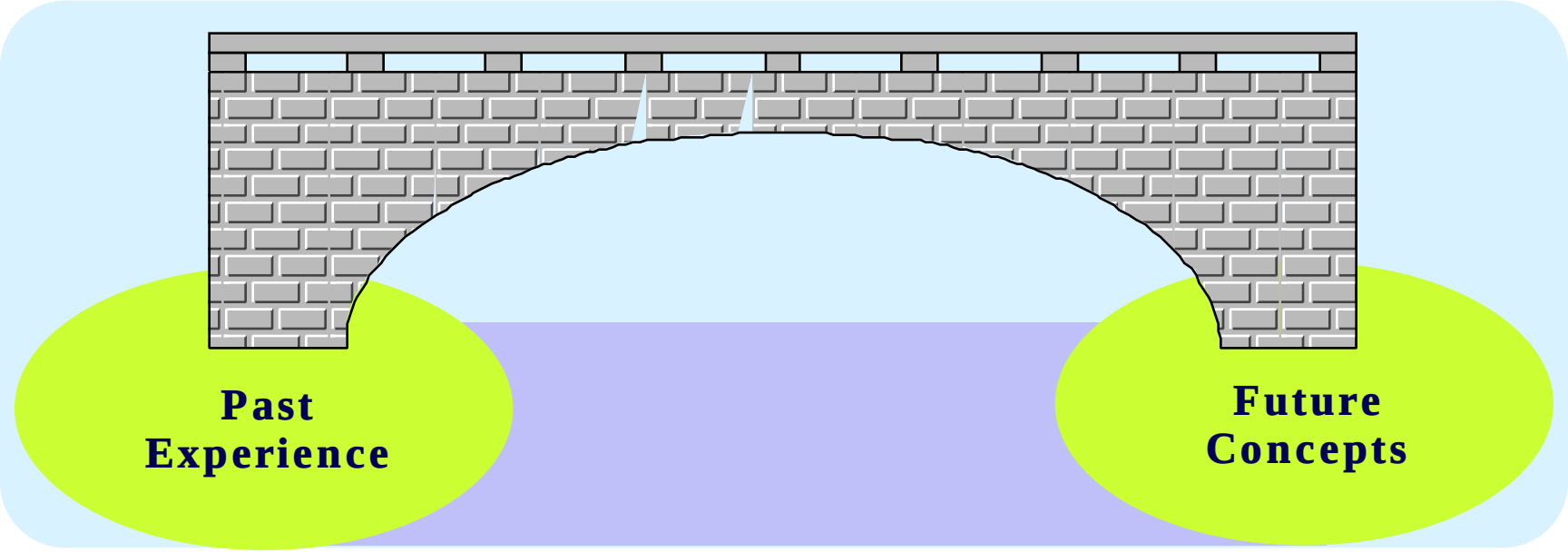
The concepts of CyberWar add a new dimension to C2W.



The implications of these concepts are only beginning to be explored.

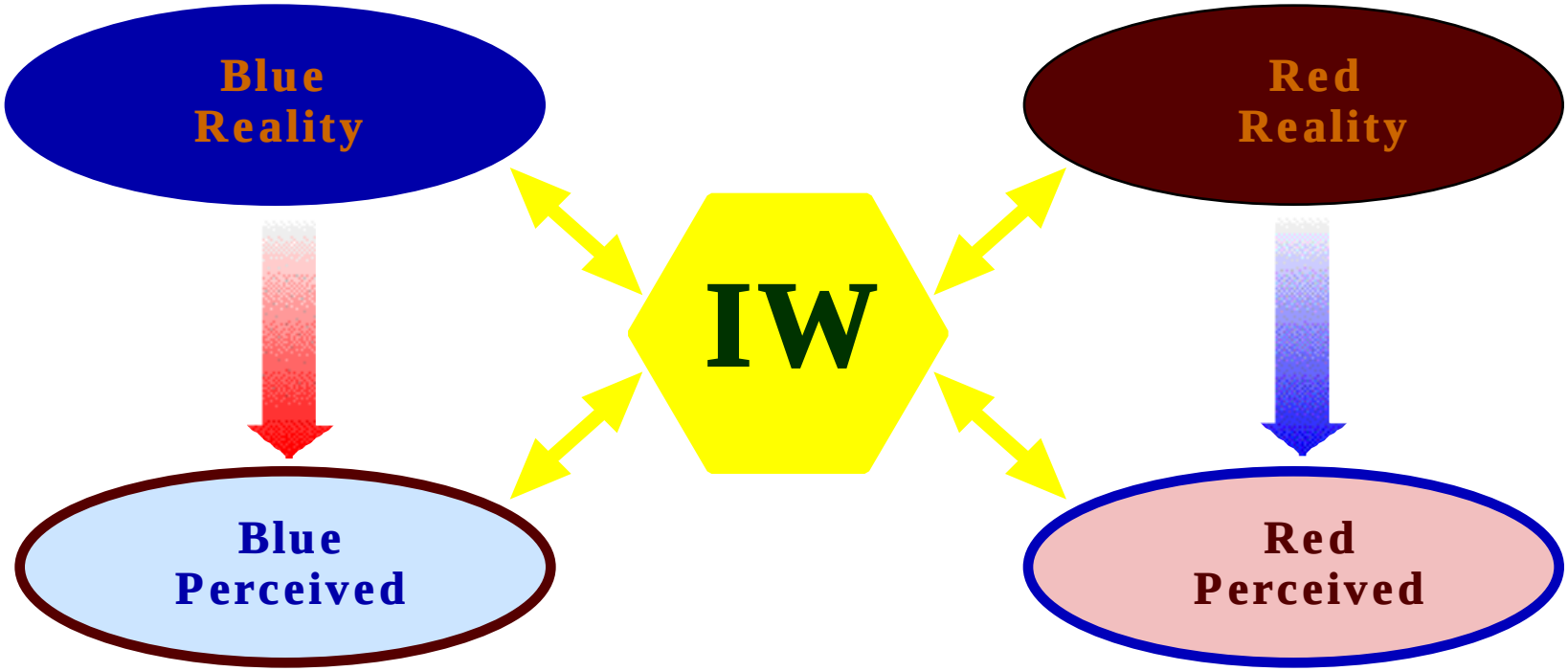
WHAT IS THE ROLE OF EW FOR IW?

Electronic Warfare engineering methods are very applicable to the new problems of Information Warfare.



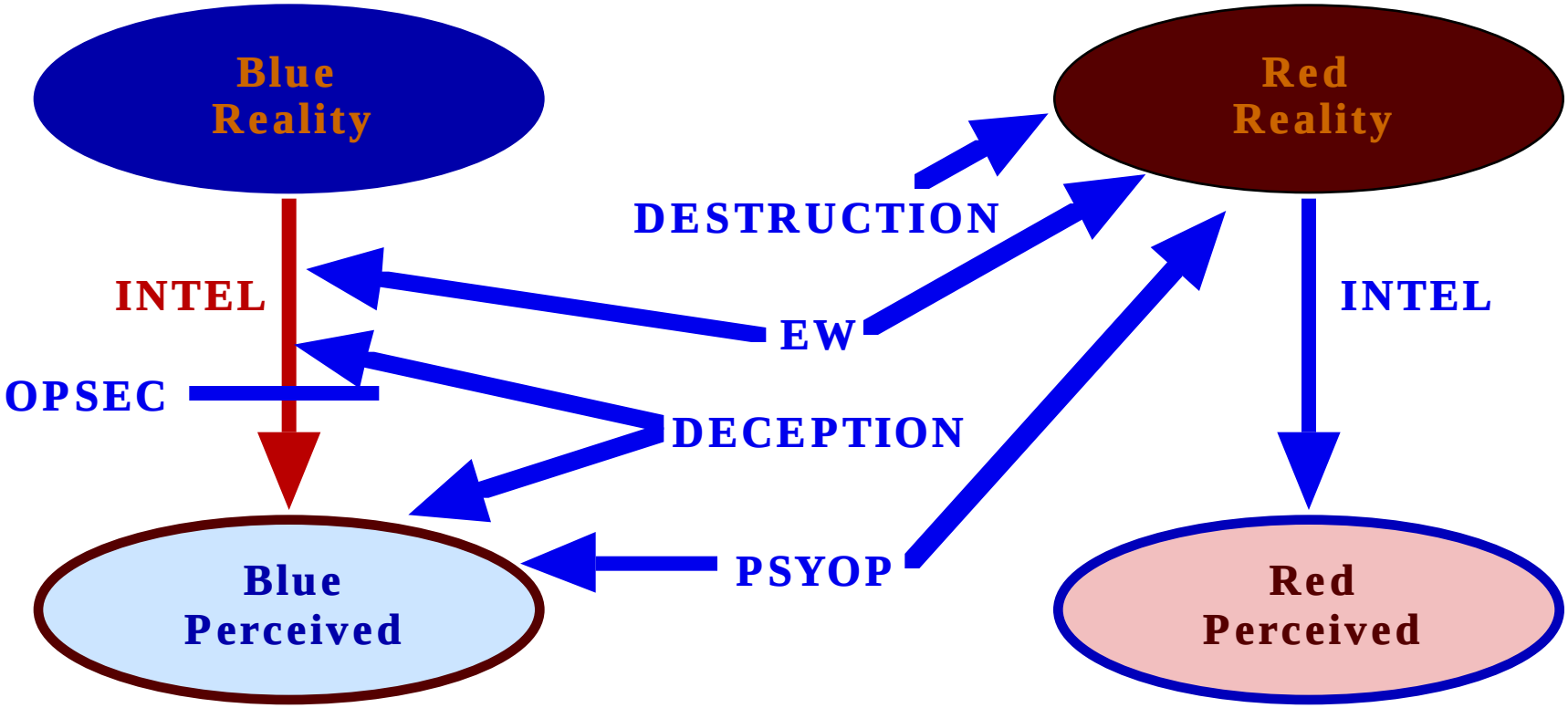
HIGH-LEVEL VIEW OF IW/C2W

Simplest view of IW involves Perceptions vs Reality.



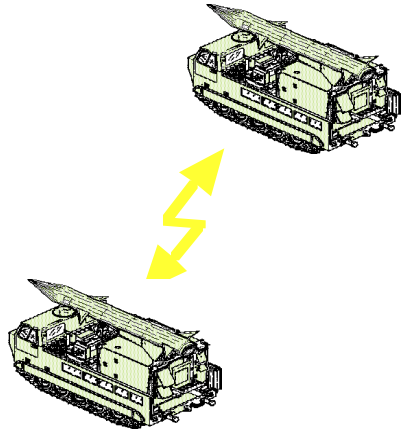
INTEGRATED USE OF IW/C2W

The use of the IW elements is highly interdependent:



C2 EXPLOITATION BENEFITS

The tactical user can benefit from exploiting the enemy's C2:



- reliable identification of threat forces
- location of threat elements
- characterization of current threat system status
- warning of imminent operations before they occur
- opportunity to preempt enemy actions either operationally or with countermeasures

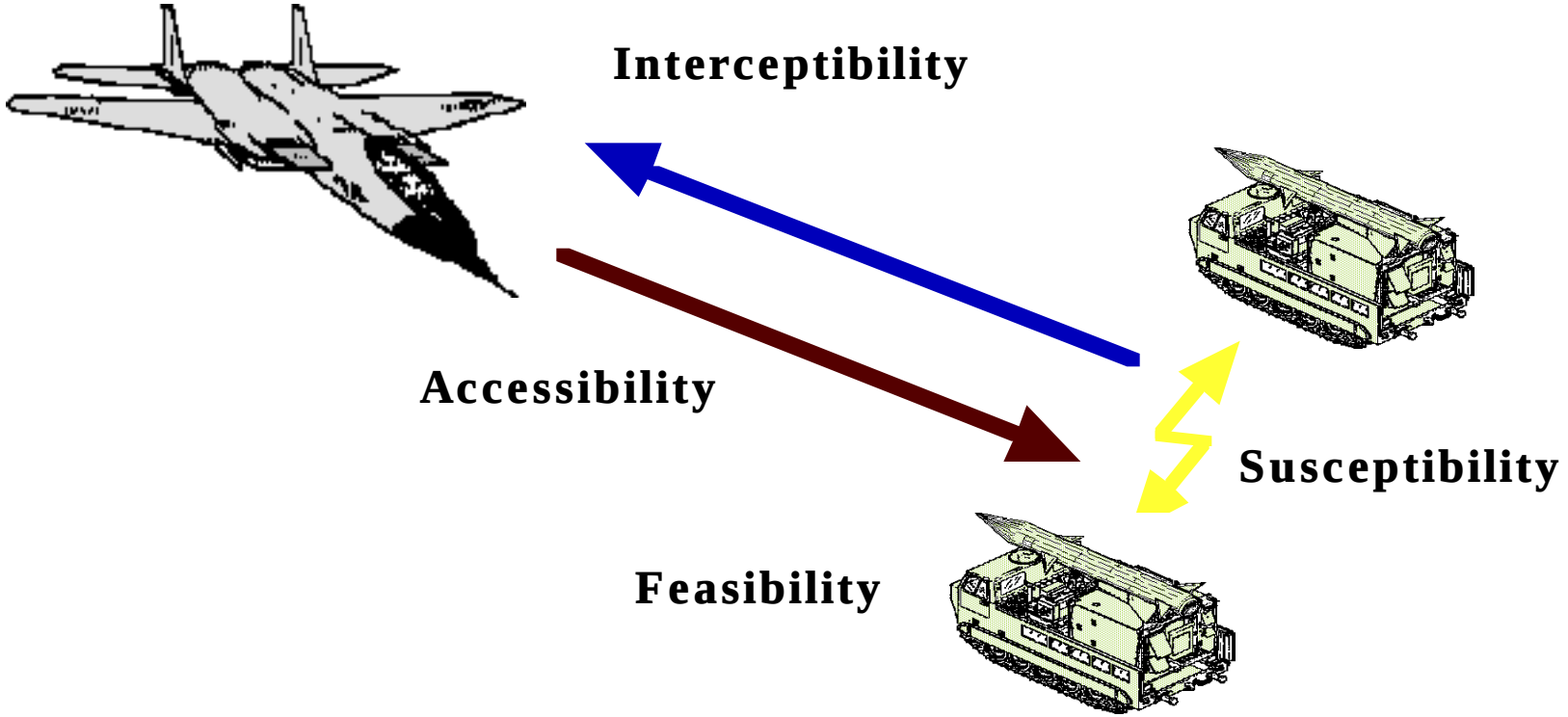
COUNTERMEASURES

Possible results of countermeasures against C2:

- **Delay:** introduces delays by interfering with C2 to impede the transmission of tactical data
- **Disrupt:** introduce periodic breaks in an adversary's use of C2 system
- **Deny:** denies an adversary use of specific parts of C2 systems, forcing alternate modes of C2
- **Deceive:** introduce undetected errors in transmitted information to manipulate the enemy's actions

EW PERSPECTIVE

The Classic EW Vulnerability Analysis includes four elements:

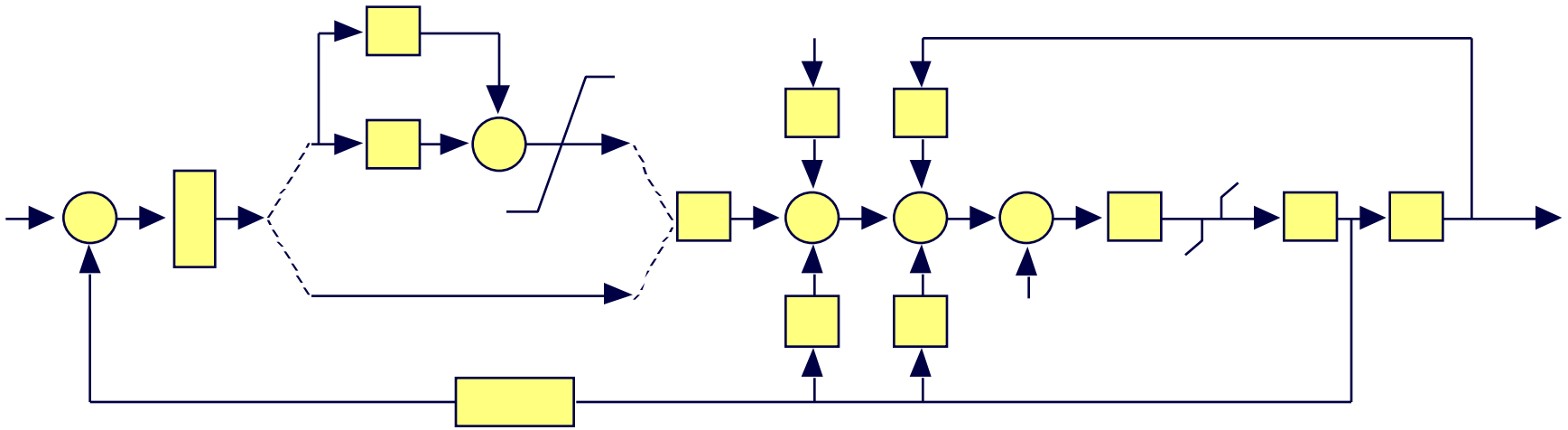


These elements can be applied to analyses of C2W.

ELECTRONIC WARFARE: CONTROL LOOPS

Electronic countermeasures have long been designed to jam threat system control loops.

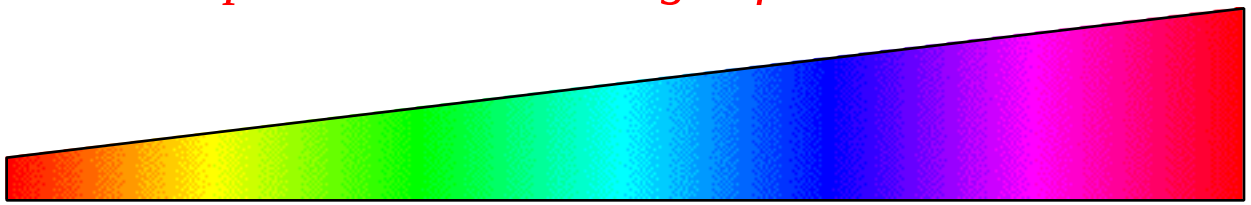
» Functional Block diagram of Seeker illustrating multiple control loops.



Applying these methods to networked C2 systems is a natural extension.

ELECTRONIC WARFARE: COMMUNICATIONS COUNTERMEASURES

Tactical C2 encompasses a wide range of communications.



Tactical Data Links	Combat Net Radio	Unit Comm Facility	Local Comm Switch	Area Tele-comm Switch Center	Wide Band Trunk

Increasing Countermeasure Technique Complexity ⇨

Increasing C2 Bandwidth ⇨

COMMAND & CONTROL SYSTEMS

Command & Control systems have become increasingly sophisticated.

C2 USES

- Dissemination of intelligence
- Control of air and maneuver forces
- Control of direct and indirect fire systems
- Operation of air defense
- Distribution of materiel and support resources

CONCEPT

Command and Control:

- Understanding the *process* of Command and Control provides insights that can be utilized for exploitation
- These fundamental concepts extend through the new networked C2 systems
- New technologies increase not only the complexity of the problem, but also the tools available to solve them

THE PROCESS OF COMMAND AND CONTROL

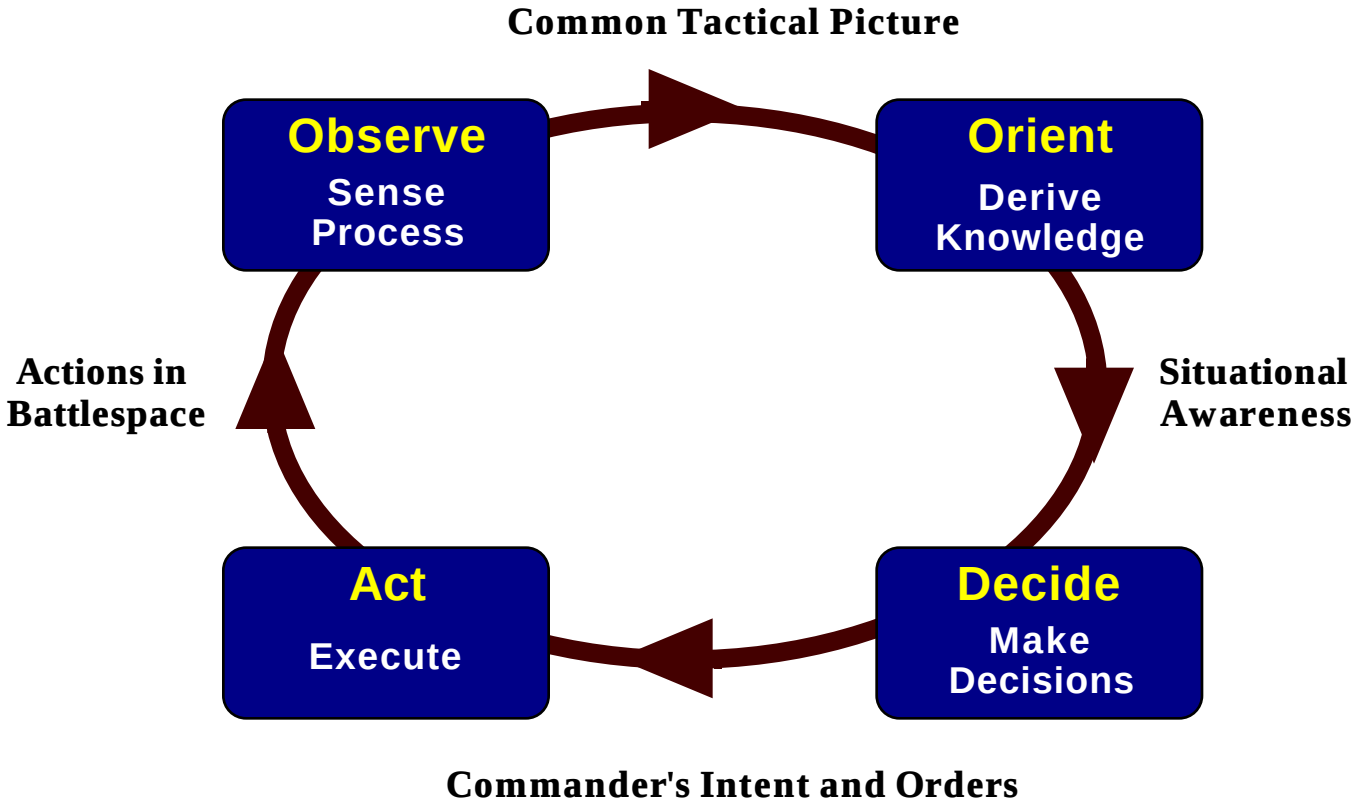
Command and Control is a process to translate ideas into action.

- C2 involves:
  - » information gathering,
  - » strategy formulation,
  - » implementation in decisions, and
  - » controlling subordinates

- C2 is a cyclic, continuous process involving multiple echelons

COMMAND AND CONTROL PROCESS

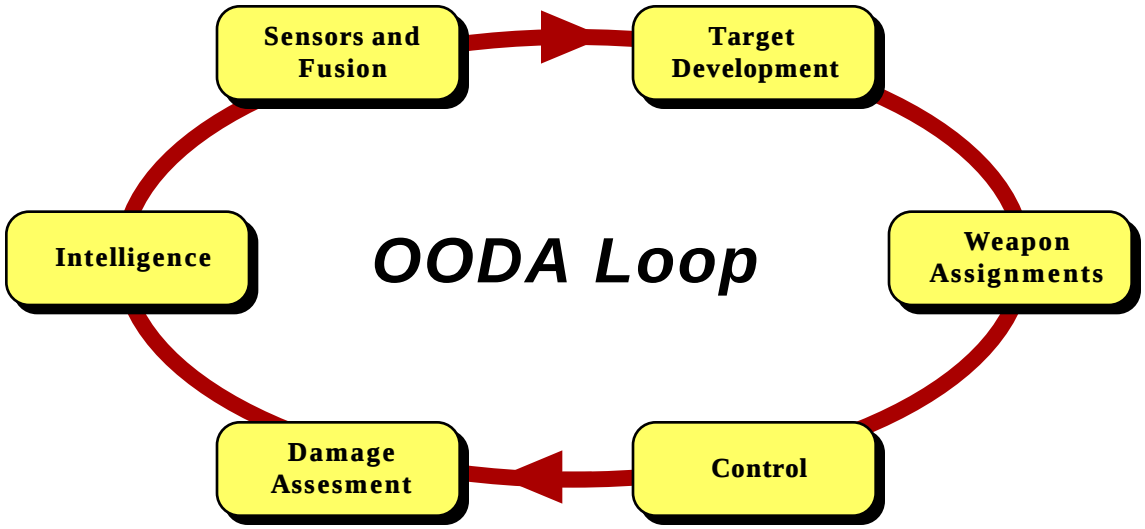
The functional control activities represented in a Command and Control process can be represented by the Observe-Orient-Decide-Act (OODA) Loop. *(Col. John R. Boyd, "A Discourse on Winning and Losing", 1987)*



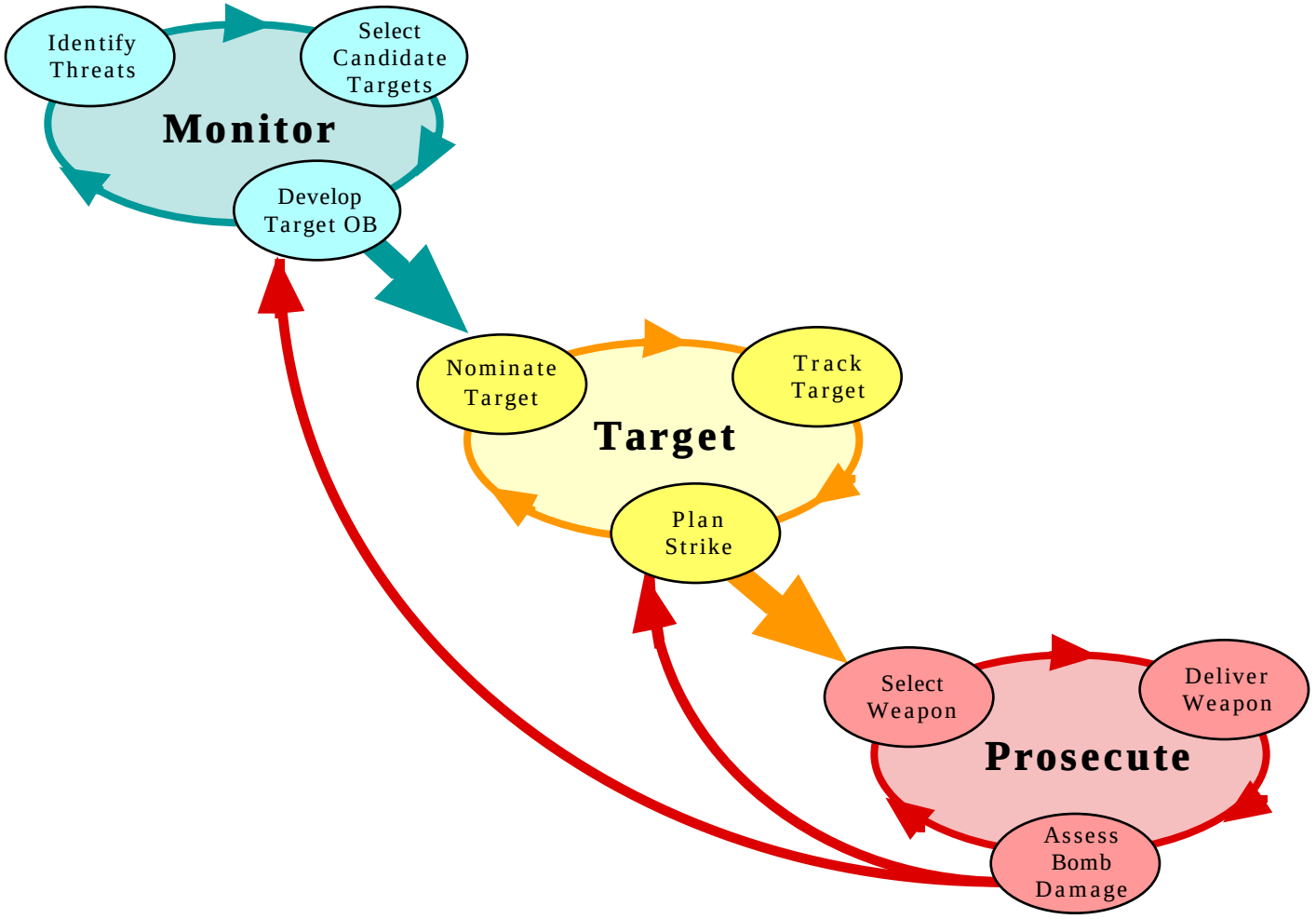
EXAMPLE OF OODA LOOP BEHAVIOR

Command and Control processes are detectable:

» The functional elements in a typical Observe-Orient-Decide-Act (OODA) Loop are implemented in sequences of detectable activities in a networked Command and Control System.

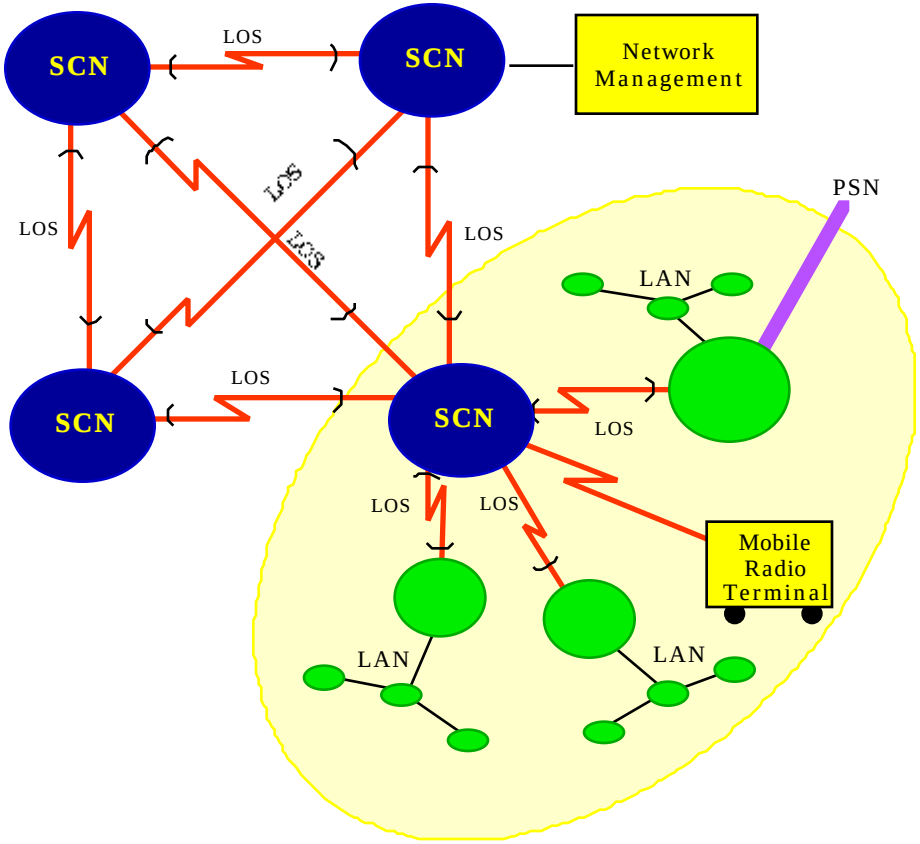


PARALLEL LOOPS

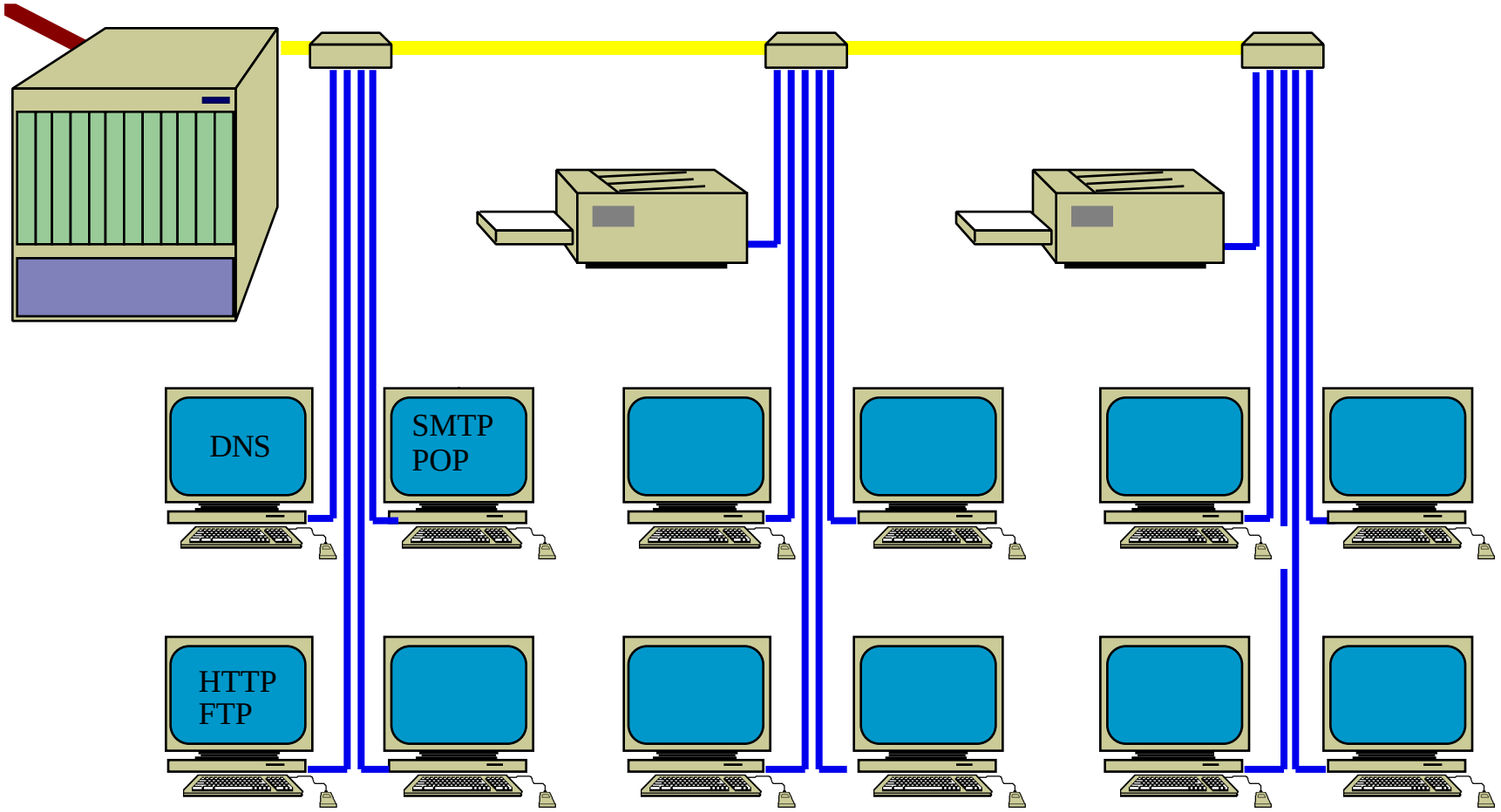


NETWORK TEMPLATES

Network Templates provide Electronic Signatures of Network elements.

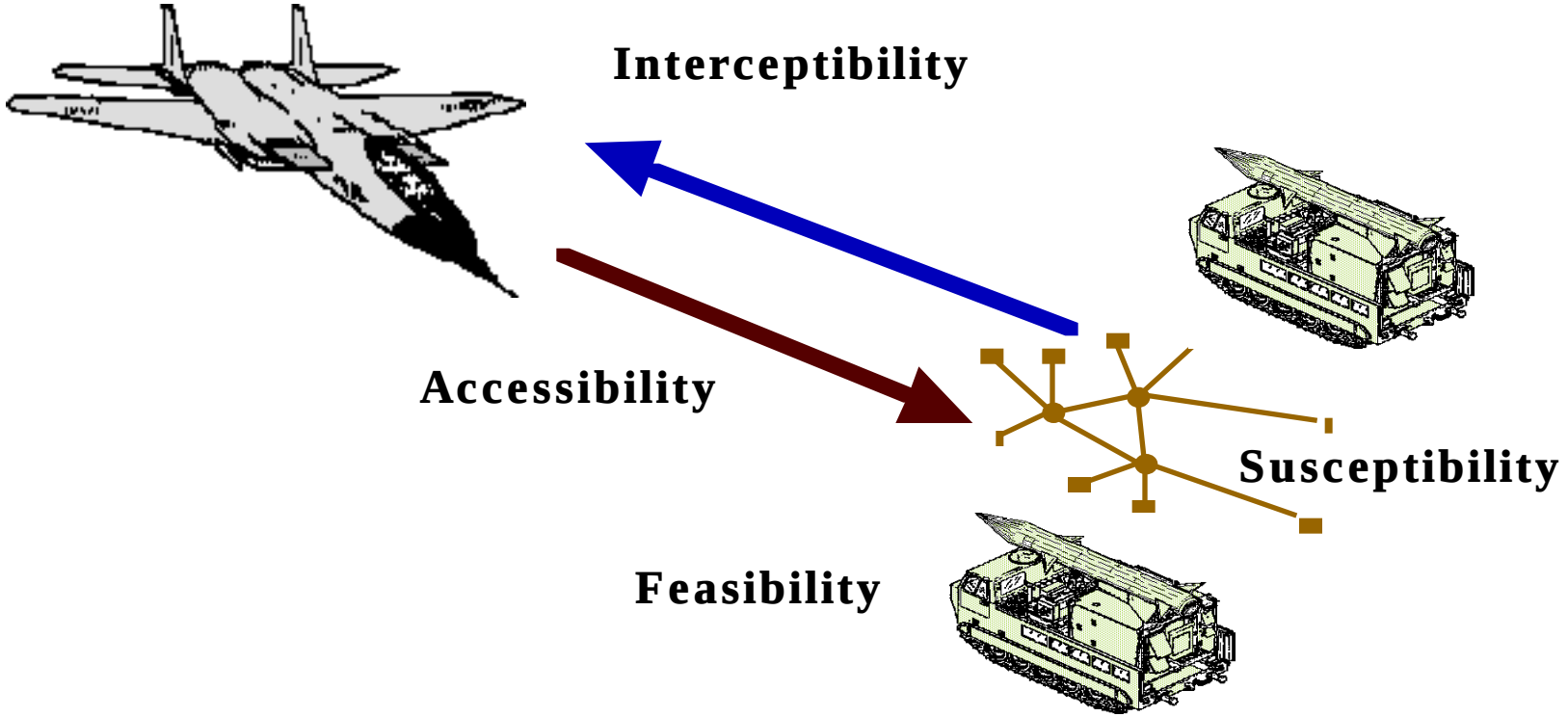


"COMPUTER" ORDER OF BATTLE



EW PERSPECTIVE FOR C2W

The Classic EW Vulnerability Analysis includes four elements:



This approach uses proven engineering disciplines.

INTERCEPTIBILITY

Interceptibility includes factors for technical and operational intelligence.

- Technical intelligence:
  - » How well do we know the system designs and protocols?
- Operational intelligence:
  - » Can we detect, locate, identify, and characterize the key tactical users in the enemy net?

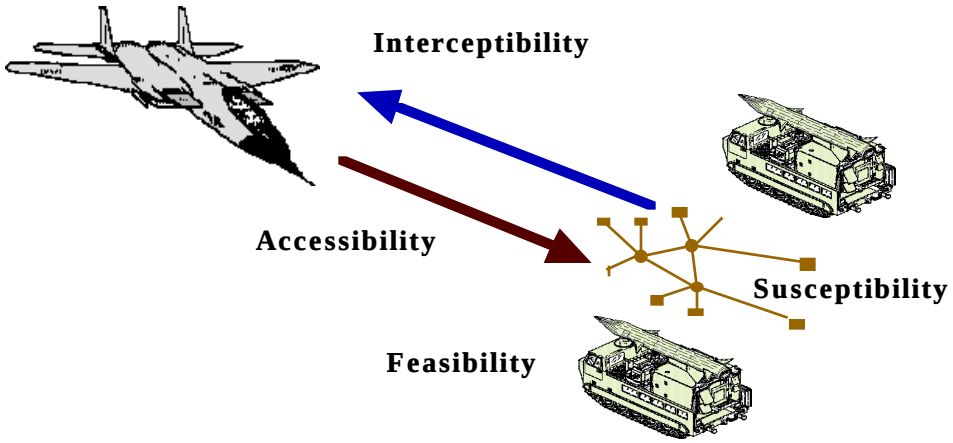
ACCESSIBILITY

Accessibility includes factors for link, transport, and functional penetration.

- Link:
  - » How well can I enter the links?
- Transport:
  - » How well can these links transport my countermeasures?
- Functional:
  - » What functional access is achievable?

COUNTERMEASURE DESIGN

The overall effectiveness of C2W can be assessed using methods adapted from EW.



- Quantifiable by **interceptibility** in conjunction with **accessibility** metrics
- Interceptible Command and Control activities provides a useful way of discriminating interesting activities
- Enemy C2 loops can be efficiently templated and exploited with high potential payoff

C2 ATTACK PLANNING STEPS (FM 100-6)

1. Identify how C2 Attack will support the mission and concept of operations.

   Product: C2W concept of operations

2. Identify enemy C2 systems whose degradation will have a significant effect on his C2.

   Product: Enemy C2 list

3. Analyze enemy C2 systems for critical and vulnerable nodes.

   Product: High value target (HVT) list

4. Prioritize the nodes for degradation.

   Product: Prioritized high payoff target list

5. Determine the desired effect and how the C2W elements will contribute to the overall objective.

   Product: Target list

6. Assign assets to each enemy C2 node.

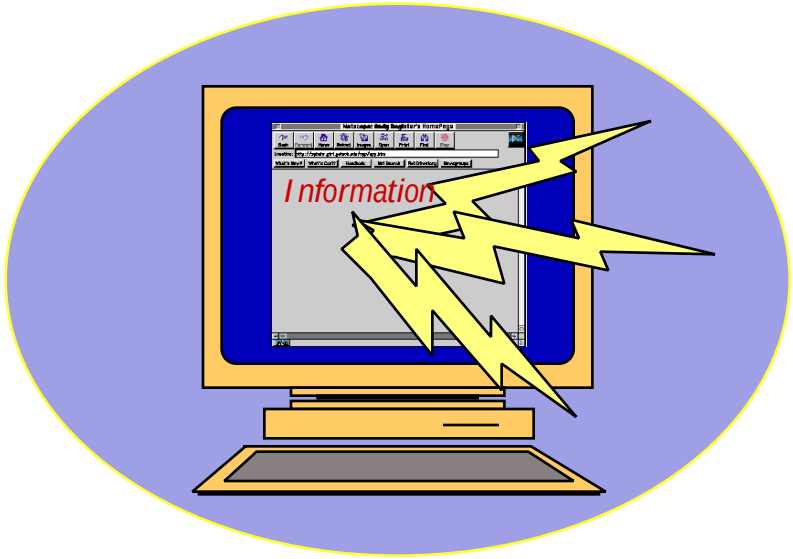
   Product: Subordinate unit tasking

7. Determine the effectiveness of the operation.

   Product: BDA

SUMMARY

This presentation:



- » discussed Information Warfare against networked Command and Control (C2) systems
- » proposed a use for C2 conceptual models such as the “OODA Loop”
- » suggested a new role for Electronic Warfare engineering methods