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
### An Operational Framework for Battle in Network Space

**Title and Subtitle**

**Date Covered**

**Author(s)**

**Performing Organization**

**Performing Organization Report Number**

**Sponsoring/Monitoring Agency**

**Availability Statement**

**Supplementary Notes**

**Abstract**

**Subject Terms**

**Security Classification of:**

<table>
<thead>
<tr>
<th>a. Report</th>
<th>b. Abstract</th>
<th>c. This Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>unclassified</td>
<td>unclassified</td>
<td>unclassified</td>
</tr>
</tbody>
</table>

**Limitation of Abstract**

**Number of Pages**

**Name of Responsible Person**

---

The original document contains color images.
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

The Law of Humanity

The Law of Economy

The Law of Duality

Knowledge and Ignorance

(Independent Principle)

Principles of Aggression
- Dislocation and Confrontation
- Distribution and Concentration

Principles of Interaction
- Opportunity and Reaction
- Activity and Security

Principles of Control
- Option Acceleration And Objective
- Command and Anarchy

Robert R. Leonhard, “The Principles of War for the Information Age
Mapping Knowledge Environment to Information Ops

**Psy**
- Influence Ops: Psychological Media

**Net**
- CNE
- CND
- CNA
- NAV
- EM

**Phy**
- Destruction
- Deception

**Perception Layer**
- Applications
- Psychological Cognitive Process
- “Understanding”

**Information Layer**
- Network and Tpt Layer of ISO
- Protocols and Information Holdings
- Links and Modes

**Physical Layer**
- Network Architecture, Physical Layer of ISO
- Routing Technology, Communications and Data Centers, Nodes

Ed Waltz: “Information Warfare Principles and Operations"
Defining the Information Battle Space:

**Psy**
- Influence Ops: Psychological Media

**NET**
- CNE
- CND
- CNA
- NAV
- EM

**Phy**
- Destruction
- Deception

**Links** = paths along which Information travels

**Mode** = the way in which Information travels

**Node** = Points at which Information is used/made/stored
Influence Ops: Psychological Media

CNE, CND, CNA, NAV, EM

Destruction, Deception

C2ISR

Decision Nodes
Information Flow
Shape of Info Space
Resolve of Messages
Electromagnetic Battle:

**Psy**
- Influence Ops: Psychological Media

**NET**
- CNE
- CND
- CNA
- NAV
- EM

**Phy**
- Destruction
- Deception

Decision Space

Similar to Physical Effect:
Objective to Disrupt vs Destroy
Network Operations: Main Defensive Construct

Psy
- Influence Ops: Psychological Media
  - CNE
  - CND
  - CNA
  - NAV
  - EM

NET
- C2ISR
- Firewall & Guards
- IDS

Phy
- Destruction Deception
- Rogue Element
- Delay Operations
- Decision Space
Network Operations: Killing Zone

Psy
- Influence Ops: Psychological Media
- CNE
- CND
- CNA
- NAV
- EM

NET
- NVAT
- C2ISR
- CIRT
- ISR
- CND
- Firewall & Guards
- IDS

Phy
- Destruction Deception
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

CND

Situational Awareness
Target Development

Disruption or Deception Ops

Rogue Element
Reconstitution: Business Continuity

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

CIRT

CND

- Continued Exploitation
- Surveillance
- Deception Ops

Rogue Element
The Network Attack: Disable or Defeat Enemy

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

- Physical Interdiction: Hard Kill - Weapon
- Tactical Assault
- Link Attacks: Jamming, Denial of Service
- Network Attacks: Net Weapons, Interdiction, Capture

CND (Cytometry and Neuroimmunology Development): Situational Awareness, Target Development, Disruption or Deception Ops

CNA (Cyber Network Analysis): Close Target Recce

ISR (Intelligence, Surveillance, and Reconnaissance)
A Vision of CNO

Who’s got the ball?

Cyber Recce & Target Acquisition?

SIGINT Function

CNE

Military Function?

CNA

SA and ISR in the Cyber Environment?

All Depts Function

CND

Defensive Countermoves ...Active?
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
An Analogy for ISR

CCD Array → Physical Image
IDS Array → Traffic Patterns
Honeyed Array → Logical Activity Image

= Honey Pot

As # ↑ > Stare time ↓
As fidelity ↑ > Stare time ↓
Intelligent Deployment > Stare time ↓
Air Operations Center (AOC) Standard Operating Procedure (SOP)
Twelfth Air Force (12AF) Air Force Forces (AFFOR)
ANNEX B TO CHAPTER 3
From the synthesis of multiple Global Requirements
- in multiple AORs
- with separate TO&Es and
- with different Environmental leads…
…to a Mission Capability Package in Weeks!
…to a Mission Capability Package in Days?

Weeks: 1…2….3….4….5….6….7….8….9….10….11….12….13….14….15….
Convolution of MCPs:
CCRP: Network Centric Warfare:
Developing and Leveraging Information Superiority

Weeks: 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17
MissionCapability

KnowledgeEmphasis

- Reqr

Technology Smart
- Engineering Smart
- Process Smart

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

Knowledge Workers

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

Robust Programmatics 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

What is the Future?