An Operational Framework for Battle in Network Space

“Thus, what is of supreme importance in war is to attack the enemy’s strategy” [i]

LCol Rob Knight
Deputy Commander
Canadian Forces Information Operations Group HQ

Dr. Mark McIntyre
Head, Network Information Operations
Defence R & D Canada - Ottawa

An Operational Model for Information Operations

Psy
- Influence Ops: Psychological Media
- Psychological Cognitive Process
- “Understanding” Plans

CNE
- CND
- CNA
- NAV
- EM

Phy
- Destruction
- Deception
- Physical Presence of Network
- Routing Technology, Communications and Data Centers, Links and Nodes

Perception Layer
- Psychological Cognitive Process
- “Understanding” Plans

Information Layer
- Network and Tpt Layer of ISO Protocols and Data Content
- Links and Modes

Physical Layer
- Physical Presence of Network
- Routing Technology, Communications and Data Centers, Links and Nodes

Defining the Information Battle Space:

Psy
Influence Ops: Psychological Media

NET
CNE
CND
CNA
NAV
EM

C4ISR

Phy
Destruction Deception

Decision Space

Applications
Presentation
Session
Transport
Network
Link
Physical

ISO 7 Layer Model
Defining the Network Battle Space:

NET

CNE  CND  CNA  NAV  EM

Presentation  Session  Transport  Network  Link
Simple Concepts of Physical Battle Space:

- Obstacle to Movement
- Blocking Force
- Hostile Element
- High Value Force
- Observation Point
- Recce Detachment
Simple Concepts of Network Battle Space:

**Psy**
- Influence Ops: Psychological Media

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

**Phy**
- Destruction
- Deception

Decision Space

- C2ISR
- CND
- CIRT
- CNE
- CNISR
- CND
- CNANAVEM
- Destruction
- Deception

Firewall & Guards

IDS
Defining the Network Battle Space:

High Value Network

Blocking Force

CND

Hostile Element

Obstacle to Access

Observation Point

Recce Detachment
Leonhard’s Principles of War for the Information Age [iv]

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

The Law of Humanity

The Law of Duality

Leonhard’s Principles of War for the Information Age [iv]

Knowledge and Ignorance

Aggression
- Dislocation and Confrontation
- Distribution and Concentration

Interaction
- Opportunity and Reaction
- Activity and Security

Control
- Option Acceleration And Objective
- Command and Anarchy
Joint Network Defence and Management System, Julie Lefebvre, Marc Gregoire & Luc Beaudoin, DRDC Ottawa
Leonhard’s Principles of War for the Information Age [iv]

Distribution and Concentration

**Aggression**
- Dislocation and Confrontation
- Distribution and Concentration

**Interaction**
- Opportunity and Reaction
- Activity and Security

**Control**
- Option Acceleration And Objective
- Command and Anarchy

The Law of Humanity
The Law of Duality
The Law of Economy
Knowledge and Ignorance (Independent Principle)
Defence in Depth
Leonhard’s Principles of War for the Information Age

Dislocation and Confrontation

Aggression
- Dislocation and Confrontation
- Distribution and Concentration

Interaction
- Opportunity and Reaction
- Activity and Security

Control
- Option Acceleration And Objective
- Command and Anarchy
Rogue Element

Killing Zone: Dislocation and Definition of Enemy

- Situational Awareness
- Target Development
- Disruption or Deception Ops

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

CND

Rogue Element
Activity and Security

Aggression
- Dislocation and Confrontation
- Distribution and Concentration

Interaction
- Opportunity and Reaction
- Activity and Security

Control
- Option Acceleration And Objective
- Command and Anarchy
Leonhard’s Principles of War for the Information Age [iv]

Opportunity and Reaction

Aggression
- Dislocation and Confrontation
- Distribution and Concentration

Interaction
- Opportunity and Reaction
- Activity and Security

Control
- Option Acceleration And Objective
- Command and Anarchy
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
Situational Awareness
Target Development
Disruption or Deception Ops

CNA

CIRTS
Close Target Recce

CNISR
Knowledge Warriors
- Engineering Smart
  - Knowledge Base of Con Ops and Technologies
  - Just in time resource commitment
  - Clear Strategic Capital & Business Process

Technology Smart
- Self Synchronization
  - Shared Awareness of Functional Environment
  - Network Enabled decision making
  - Clear Purpose / End States
  - Knowledge Base of Con Ops and Technologies

Process Smart
- Joint Philosophy
  - Shared Strategic Awareness
  - Multiple COA development process - End State Development
  - Close coord with Operations
  - Rapid Lessons Learned & Feed Back

Knowledge-based Command Structure
Leonhard’s Principles of War for the Information Age [iv]

Command and Anarchy

Aggression
- Dislocation and Confrontation
- Distribution and Concentration

Interaction
- Opportunity and Reaction
- Activity and Security

Control
- Option Acceleration And Objective
- Command and Anarchy

The Law of Humanity

The Law of Duality
Elements of CNO

CNE

CNA

CND

Aggressive Exploitation
Cyber Target Acquisition?

Defensive Countermoves
... Active?

SA and ISR in the Cyber Environment?

[i] Col DG Neasmith, Comd CFIOG
Discussion

- Knowledge Base of Best Practices
- Functional Expertise
- Just in time resource commitment
- Clear Strategic Capital & Business Process

Self Synchronization

- Technology Smart
- Engineering Smart
- Process Smart

Precision

- Knowledge Warriors

Joint Philosophy

- Shared Awareness of Functional Environment
- Network Enabled decision making
- Clear Purpose / End States
- Knowledge Base of Con Ops and Technologies

- Shared Strategic Awareness
- Multiple COA development process - End State Development
- Close coord with Operations
- Rapid Lessons Learned & Feed Back

- SA and ISR in the Cyber Environment?
- Cyber Target Acquisition?
- Defensive Countermoves ...Active?

Decision Space

- Rogue Element

- C2ISR
- NVAT
- CNE
- CNA
- CND