

Some thoughts on the applications of military theory to Information Operations and Network Centric Warfare

June 20-22 2006

Dr. Roland Heickerö
roland.heickero@foi.se

Outline

- **Introduction**
- **Mega trends**
- **Definitions of centres of gravity, COG and critical vulnerabilities, CV**
- **The logic of networks**
- **COGs and CVs in different types of networks**
- **Conclusions**
- **Discussions**

Objective

Purpose: to discuss development of InfoOps methodology from a network logic perspective and theories based on CoGs and CVs

Theses

Thes1: We are in the age of network and information that change prerequisites for war faring (RMA). To understand information domain is becoming more important

Thes2: all types of networks have their own strengths and vulnerabilities respectively due to their structure

Thes3: knowledge and understanding of your own and others COGs and CVs gives an advantage (DBA)

Thes4: it is possible to develop methods for InfoOps by using theories for network centric logics as well as theories on CoGs and CVs

Mega trends

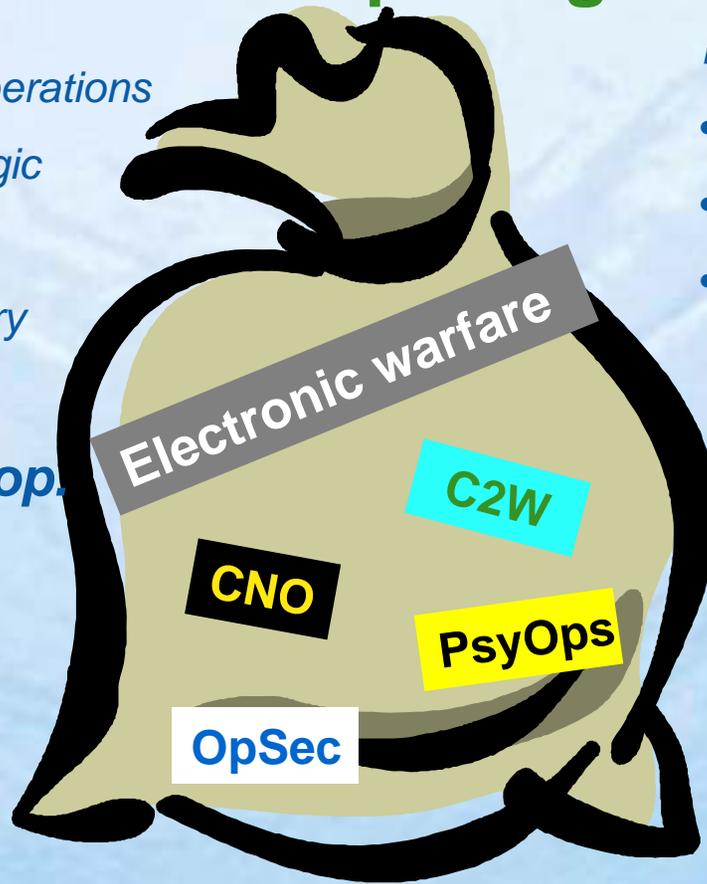
New doctrines

- Expeditionary & Mobile operations
- NBD – network centric logic
- Threats from terrorism
- Cooperation civilian-military

Technological developments

- CTI – digitalization & convergence
- New material, low energy focus
- Automated systems & sensors

”InfoOps-bag”



New vulnerabilities

- Asymmetric warfare
- COTS - products
- Critical infrastructure

New actors

- Religious & political groups
- Criminals
- Individuals

New behaviors

- Network organized – virtual
- Ad-hoc structures

COGs and critical vulnerabilities

Definitions

- Clausewitz (1832): a COG is some kind of central point of force and speed for a state that everything should be related to
- Strange (2001): CoG is related to the force of an enemy, it could be either physical or moral and may exist on strategic, operative and tactical level
- NATO GOP (2003): a capability or place where a nation, alliance, a military force etc. sets their standard for freedom of action, physical strength and willingness to fight

COGs and critical vulnerabilities (cont.)

Definitions

- Echevarria (2003): a CoG is not a strength or a quality but a centripetal force that glues an enemy's different systems together
- Warden (2004): an enemy should be studied as a system that is built up from a number of interrelated parts. The basic components is energy of different kinds both physical and psychological. If it is possible to influence the flow of energy in a specific direction by hitting certain parts, the whole system will be affected. There is only a small number of nodes and links that are critical for the system as whole

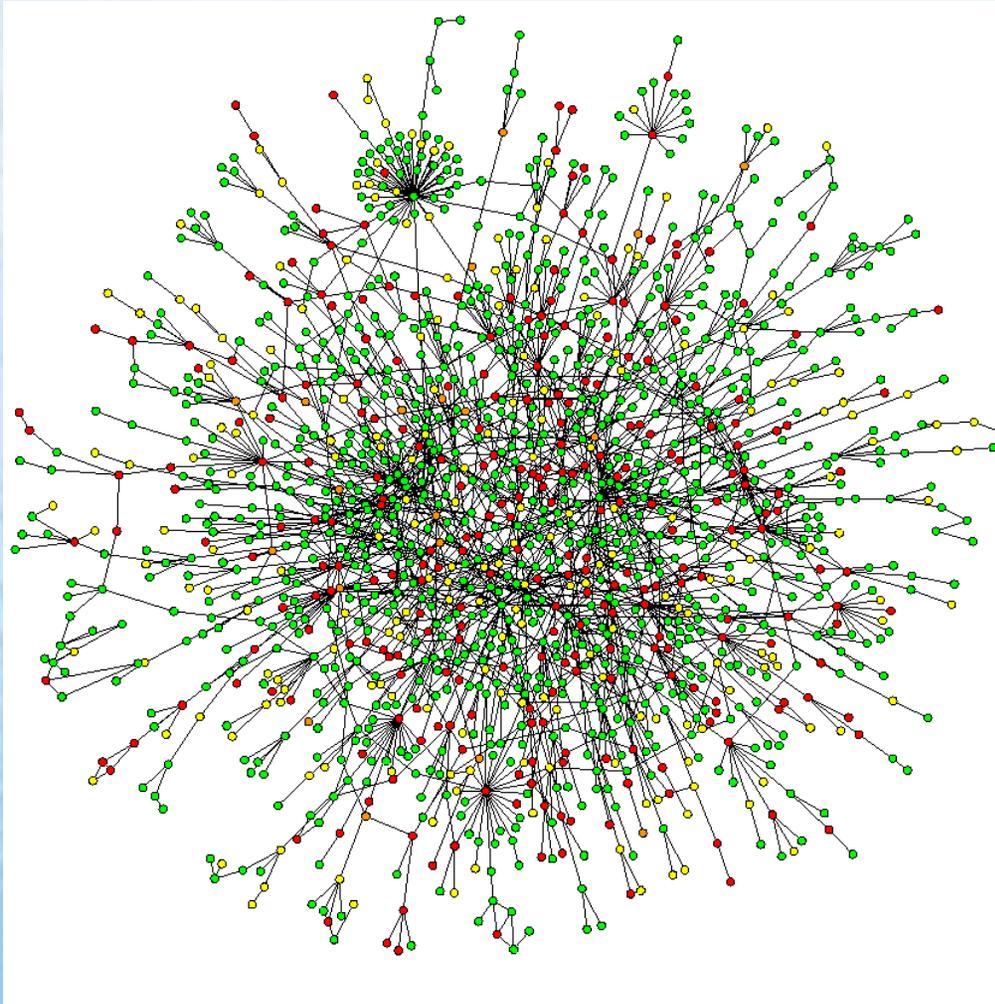
There could be several CoGs within a system. The nodes with most links are probably CoGs. Greatest effect will be achieved by combining attacks on several nodes at same time

The logic of networks

Characteristics of networks?

- **purpose:** to combine functions, platforms, nodes and links to a system of system
- **value:** ability to coordinate activities, mustering of resources, transmit/receive information, people and products etc.
- **types:** biological, social, organizational communication networks etc.
- **architecture:** actual nodes and links
- **topology:** information flow

Example of a biological network



Cell metabolism

Al-Qaida Sep 11 2001

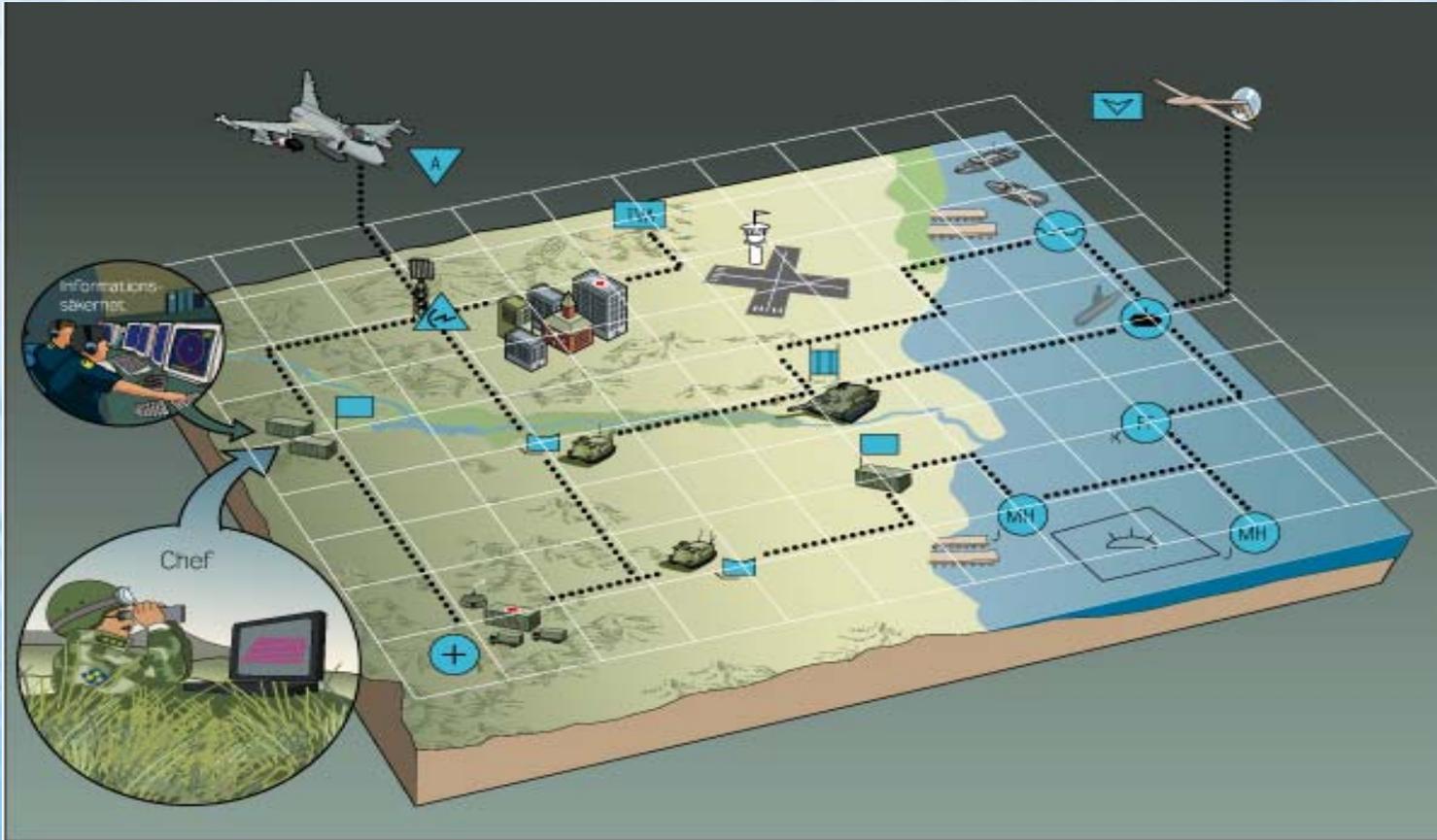
Communication links between hijackers and others suspects

Source: Krebs 2002,

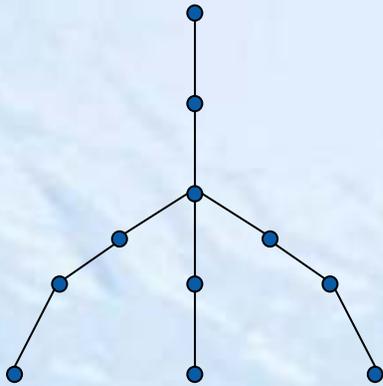


Network Based Defense: NBD

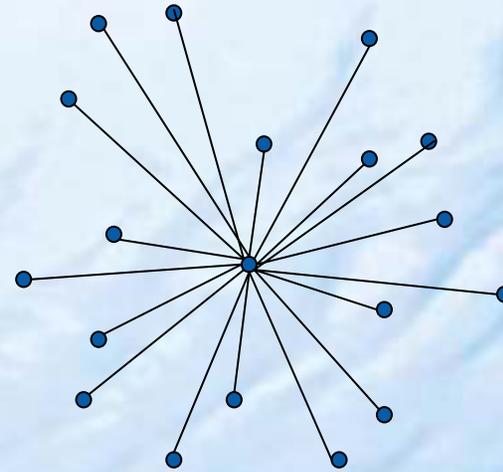
Command & Control, sensors, weapon systems and platforms connected into a network



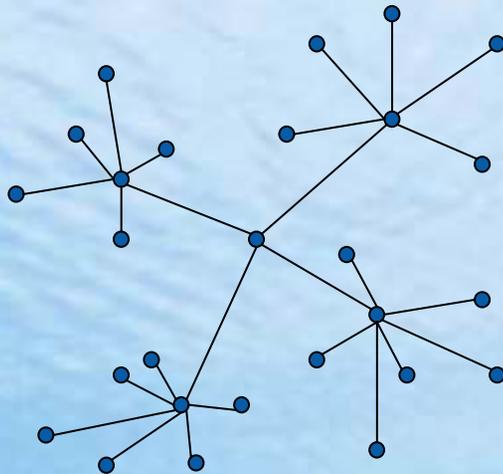
Different kinds of networks



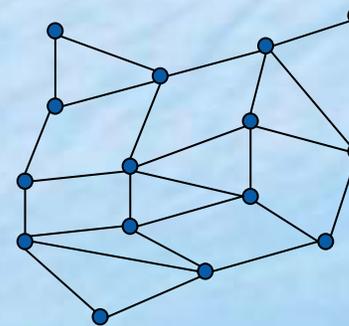
Hierarchical



Centralized

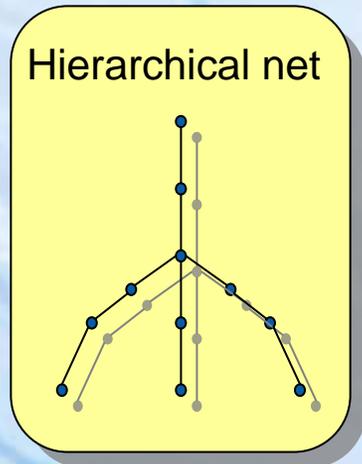


Decentralized



Distributed

COGs and critical vulnerabilities (1)

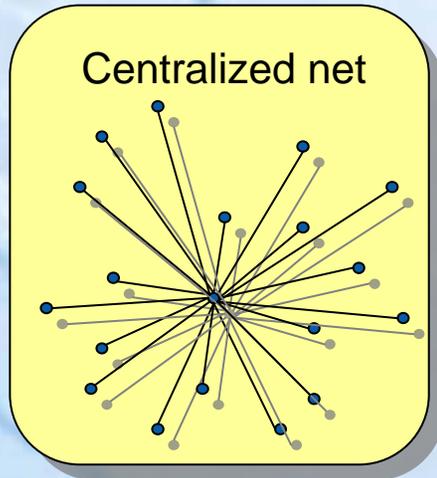


Description: Structured command & control, clear chain of command

CoG: Lacks flexibility, possible to attack top-down (traditional C2W). Time critical, vulnerable for manipulation/deception on sensor level; the nodes on end of the chain

Robustness: Robust against internal "fuzzes" such as mutiny at lower levels . Possible to separate different levels from each other and through this control them

COGs and critical vulnerabilities (2)



Description: All sub nodes are under command of the central node which simplifies C2 activities

CoG: Not very flexible, central node is sensible for attacks, acts as bottle neck. Vulnerable to saturation and "information overflow"

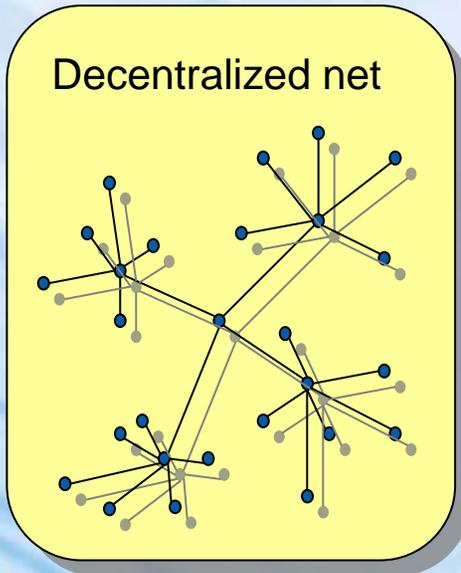
Robustness: Should be attacked in a similar way to hierarchical structures

COGs and critical vulnerabilities (3)

Description: Consist of a number of interconnected centralized sub-networks

CoG: Both main node and sub-networks central nodes are vulnerable to attacks

Robustness: Greater power to the edge, the sub-networks, robust against saturation attacks, if central node is eliminated it is possible to self organize

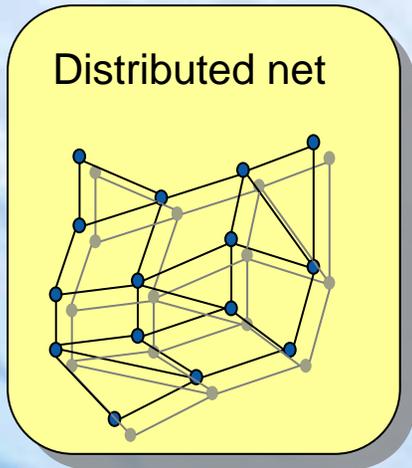


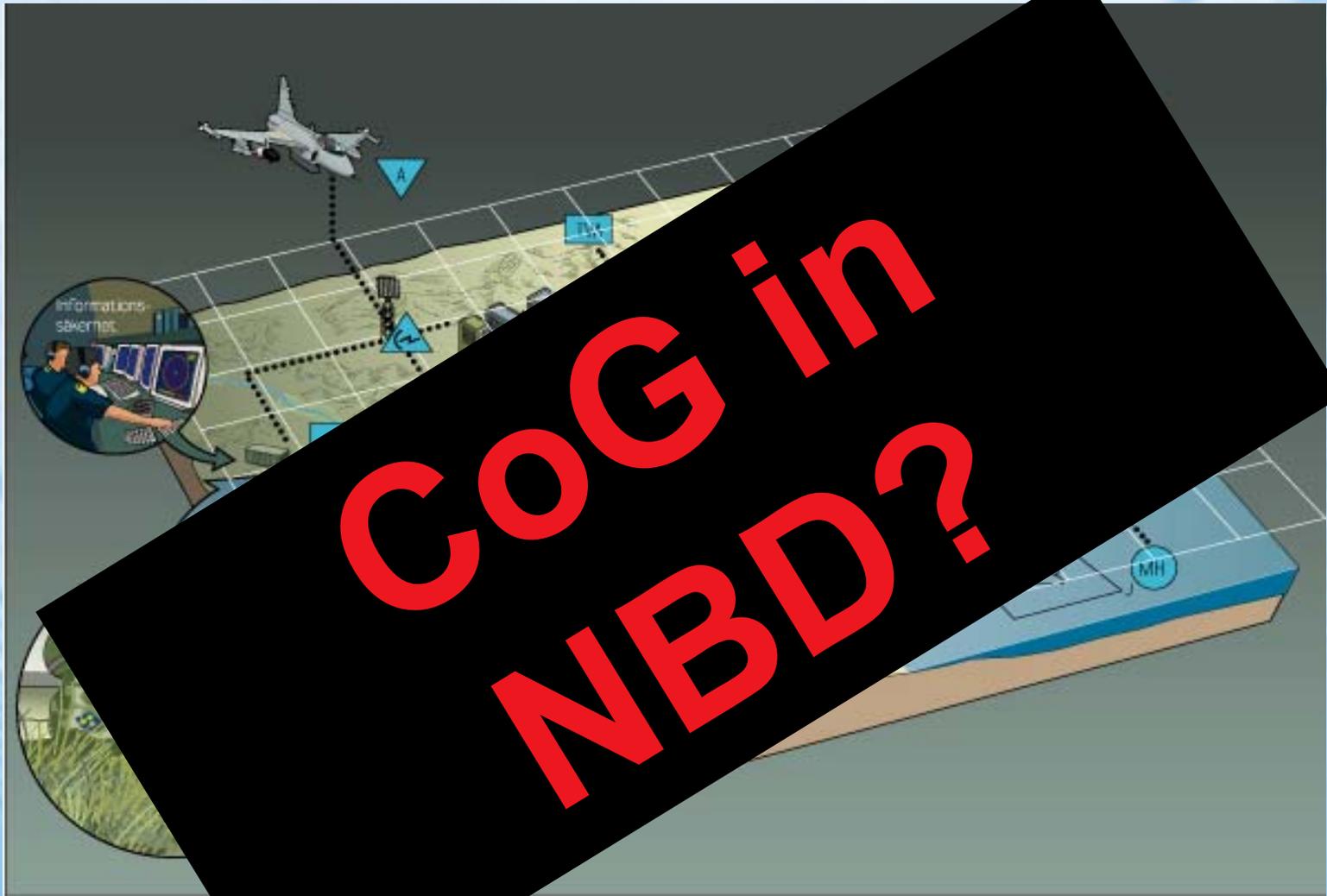
COGs and critical vulnerabilities (4)

Description: Lacks hierarchy, all information should be received all nodes, through coordination gives possibilities to use network as a common resource

CoG: Unclear C2. Sensitive to rumors and misleading but also secure due to possibility to get a "second opinion". Need for coordination that may leads to a large amount of signaling with risk for saturation

Robustness Possible to short-circuit stressed parts, very good ability for combined attacks and protection, inbuilt redundancy





Conclusions

- The development of methods for InfoOps ought to be related to ongoing mega change
- Network centric logic and theories of CoG could be useful tools/parts of the method
- All networks have it owns pros & cons, strengths and vulnerabilities and by knowing your enemy's as well as your own you can obtain advantages that may be decisive in an eventual conflict

More to read ...

IO Sphere: The Professional Journal of Joint Operations. Autumn 2005

Värdering av telekrig i NBF. FOI - Underlagsrapport. December 2005

Questions?