2006 CCRTS

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

Information Operations/Assurance

Roland Heickerö, PhD
Adjunct Professor
Deputy Research Director

Swedish Defence Research Agency, FOI
Division of Defence Analysis
Gullfossgatan 6, Kista
SE-164 90 Stockholm
Sweden
Phone: +46 8 5550 38 25
Mobile: +46 (0)70 208 06 86
E-mail: roland.heickero@foi.se

Abstract

The transformation into a world based on communication and information, leads to Information Operations (IO) becoming more important than ever. Thus, there is a need to develop new methodologies for successful IO, taking account of the change towards network enabling warfare capabilities.

In a network centric warfare approach it is important to understand the opponents' network structure and communication system and how they use these resources. Equally important is to understand your own network structure in terms of strengths and weaknesses. Every type of network has it own vulnerabilities in the form of vital nodes, links and platforms, regardless of whether it is a communications, organizational or biological network. If you understand your own structure as well as your opponents, the chances of effective IO increase greatly. A fruitful way forward is to use theories based on centre of gravity (CoG) and critical vulnerabilities (CV).

The paper first discusses the logic of networks in general terms and then considers different types of networks and their respective abilities to resist attacks of different kinds due to centre of gravity and critical vulnerabilities.

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	2. REPORT TYPE	3. DATES COVERED
2006		**00-00-2006 to 00-00-2006**

4. TITLE AND SUBTITLE	5a. CONTRACT NUMBER
Some thoughts on the application of military theory to Information Operations and Network Centric Warfare	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) **Swedish Defence Research Agency, FOI,Division of Defence Analysis,Gullfossgatan 6, Kista,SE-164 90 Stockholm Sweden, ,**	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	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT	b. ABSTRACT	c. THIS PAGE			
unclassified	**unclassified**	**unclassified**		**26**	

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

Introduction

The move to a warfare concept based on network enabling capabilities is a truly revolutionary step. It will affect military development in many areas for many years to come. One important part of the new era is the ability to conduct Information Operations (IO). In general terms these are operations related to information in order to influence the decision process of an adversary. The overall goal is to persuade the adversary to act in a manner that best suits your own objectives and purposes. Other important parts of IO are to gain and retain control of your opponents' communication systems and networks whilst protecting and retaining control of your own systems.

IO includes five capabilities[1]: electronic warfare (EW), psychological operations (PSYOPS), operation security (OPSEC), military deception and computer network operations (CNO). In order to conduct a successful operation all these capabilities should be used together in an attack or defense situation. The level of success depends on the coordination of all available resources in time and space. In a network centric warfare approach it is important to understand the opponents' network structure and communication system and how they use these resources. Equally important is to understand your own network structure in terms of strengths and weaknesses. Every type of network has it own vulnerabilities in the form of vital nodes, links and platforms, regardless of whether it is a communications, organizational or biological network. If you understand your own structure as well as your opponents, the chances of effective IO increase greatly.

Hence, a fruitful way to develop a methodology for IO in a network centric warfare context is to use theories based on centers of gravity (COG) and critical vulnerabilities (CV). The paper first discusses the logic of networks in general terms and then considers different types of networks and their respective abilities to resist attacks of different kinds before drawing some conclusions.

The logic of networks

The basis of all modern warfare concepts is the network. The network concept is built on the idea that it is possible to interconnect and cluster minor parts into subsystems and whole structures into a net of networks. It comprises not only platforms, nodes and links in a technical sense but could also include social interactions between individuals, groups of people and organisations. The term is used in a wide range of disciplines. Humans have always acted in a networked manner but owing to the IT revolution people have access to various kinds of information from the "ether" and may through this gain information superiority over an opponent. The net may also create more possibilities to act locally with global consequences.

The growth of the network depends on the number of links and nodes within it. The number of combinations could be more or less infinite. The advantage of the network is the ability to co-ordinate and muster strength against a target. The total effect should be higher than using single, unconnected nodes. For instance, it is not a coincidence that the terror

[1] Lamb, C (2005) *Information Operation as a core competence*. JFQ-article: issue thirty six

organisation al-Qaida organises itself in a loose network of networks. Within the network structure it is possible to reroute information, services, people and equipment depending on the situation.

There are four different categories of networks[2]; *hierarchical, centralised* and *decentralised* as well as *distributed*. All of them have their own advantages, strengths and weaknesses in relation to the needs of co-ordination, security and function and these are further discussed in Table 1.

Centre of gravity and critical vulnerability in different types of networks

Centre of gravity (COG) is a basic term used in military theory. For many years a number of theorists have put a lot of effort into understand the concept and its consequences. Clausewitz was the first person to discuss the concept. His theory is that a COG is some kind of a central point of force and speed for a state that everything should be related to[3]. Strange et al[4] on the other hand, say that a central point is related to the force of an enemy. The characteristic of that type of force is either physical or moral and may exist at a strategic, operative and tactical level. In NATO doctrine[5] COG is defined as a capability or place where a nation, an alliance, a military force or other type of grouping set their standards for freedom of action, physical strength and willingness to fight. Echevarria[6] uses a somewhat different definition. He proposes that a COG is not strength as Strange et al propose or a quality as in the NATO definition but a centripetal force that glues an enemy's different systems together. By taking a holistic approach in order to study the factors that bind the parts together it is possible to find the centre of gravity of the enemy.

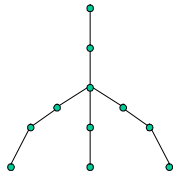
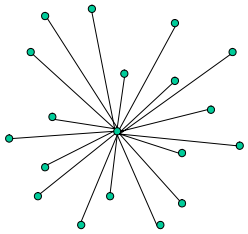
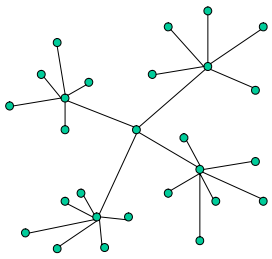
Warden[7] takes a similar approach. He argues that an enemy should be studied as a system that is built up from a number of interrelated parts. The basic component of the system is energy of different kinds: physical energies (people, buildings, communications and weapons) as well as psychological energies (will power, capability and capacity). If it is possible to influence the flow of energy in a specific direction by hitting certain parts, the whole system will be affected. He also points out that within a system that is built up of a number of nodes and links (e.g. relations between units in a network), there should be only a small number of nodes and links that are critical for the system as whole.

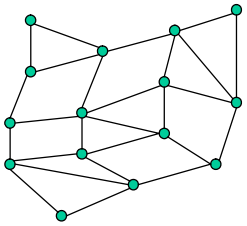
In theory, if it is possible to identify the nodes with most links you have also identified the critical points. Some military theorists argue that there is not one single COG in a system but many that can exist simultaneously. Hence, the understanding that there are a number of critical points is also the first step to carry out an effective operation against them[8]. If several COGs are attacked at same time in parallel, the best effect should be achieved. By using all resources together, the possibility of achieving a system change should increase dramatically

[2] Baran, P. (1964). On distributed communications. Introduction to distributed communications networks. Santa Monica, USA: RAND Memorandum RM 3420-PR
[3] Clausewitz, C-V (1832). *On War*. Swedish translation by Mårtensson, Böhme och Johansson (1991). Stockholm, Sweden: Bonnier Fakta Bokförlag
[4] Strange, J, Iron R. (2001). *Understanding Centres of Gravity and Critical Vulnerabilities*. Research paper. http://www.au.af.mil/au/awc/awcgate/usmc/cog2.pdf
[5] NATO (2003). Gudelines for operational planning
[6] Echevarria A, J. (2003). Clausewitz's center of gravity it's not what we thought. Naval War College Review. Vol. LVI, No1.
[7] Warden, J (2004). Centers of gravity in military operations. Preliminary draft. Royal Swedish Defence College
[8] In Wardens argument there is a clear connection to manoeuvre warfare theory: to get inside the adversaries decision cycles (OODA- loop) and through this to achieve a system collapse

and in the longer term it may lead to a total collapse of the enemy structure. Times, co-ordination of resources and good preparatory work are consequently vital factors that determine if the operation will succeed or not. Warden also points out the importance of not mixing the term COG with critical vulnerabilities (CV). The first exist because they are essential to the existence of the whole system, the latter are interesting first when planning to attack centres of gravity. In this paper the both terms are used in combination and related to different type of network as shown in table 1.

Table 1: COG, Vulnerabilities and robustness in different network structures

Type of network	General description	Vulnerabilities and COG	Robustness
Hierarchical 	Well defined command & control structure. Clear chain of command with good ability to execute orders at a rapid pace.	The structure lacks flexibility. Hierarchical networks could be attacked using a top-down approach, e.g. using traditional C2 warfare. Similarly such networks are also time critical in the sense that it is possible to cause strategic consequences by disrupting levels of command and/or the central node. It is also possible to achieve tactical advantages through influencing sensors in the chain. The information flow could also be manipulated at sensor level.	Generally hierarchical networks are quite robust against internal fuzzes such as "mutiny" at lower levels. Due to their structure, it is possible to separate different levels from each other and through this control them.
Centralised 	In a centralised network all sub nodes are under command of the central node which simplifies C2 activities.	A centralised type of network is not very flexible but with delegation some agility can be achieved. The central node is vulnerable. If it is choked or saturated it will affect the total network. It acts as a bottle neck through which all information has to pass. There is always some restriction in the information flow because all the information has to be approved by the main node.	Centralised structures should be attacked in a similar way to hierarchical structures, e.g. try to hit the central node as well as to deceive the sensors at the extreme points of the network.
Decentralised 	Decentralised networks consist of a number of interconnected centralised sub-networks. All local nodes/sub networks are independent of the others and the central node.	In this type of network both the main node and the sub-networks central nodes are vulnerable to attacks.	A distributed control mechanism gives greater power to the edge, in this case the sub-networks. The structure it is relatively robust against saturation attacks on a tactical level. Through delegation the analysing/executing capacity could be carried out in lower levels of command. If the capacity of the central node is reduced the network could reorganize itself and every sub-network could continue their respective

			activities.
Distributed 	A distributed network lacks hierarchy in a traditional sense. Hence, all information should be received all nodes in the network. In a distributed network information could be rerouted between nodes. If some part of the network is knocked out other parts could execute the tasks. An advantage is that it is possible to use the whole network as a common resource for a combined and co-ordinated attack.	A possible vulnerability is related to an unclear command and control function. A distributed network is also sensitive to rumours and misleading information due to the fact that all nodes are interconnected to each others. In the same way it is also robust. It is always possible to get a "second opinion" in order to verify the truth of the information. A problem is that information should be given all nodes more or less in real time, which opens the network to saturation attacks. The amount of signalling that is required in order to co-ordinate all parts of the network can be very significant.	It is possible to short-circuit those parts of network that are under attack and retain the ability to act. Because all nodes are more or less interconnected the prerequisite for combined attacks and protection is good. Effective and fast routing of information gives an advantage. Due to its structure the network has in-built redundancy. This is the most robust network against physical attack but may be the most vulnerable to deception or saturation attacks.

When discussing different kinds of structures it is important to point out that a mega network could contain both distributed and decentralised networks as well as centralised and decentralised ones. In some cases the growth of a network is uncontrolled or "organic" and the form it ends up in the long term is not necessary predictable. The best example of this is the Internet.

Furthermore, ad-hoc network structures are used for networks that are constantly reconfigured according to situation and needs. They can have all of the above mentioned structures. If an activity requires a certain type of structure the ad-hoc network "wakes up" and in similar way closes down when the tasks are fulfilled. This will of course affect the overall robustness and vulnerability of the network. In general terms the two most secure types of networks are the decentralised and distributed ones. But as shown they also have their critical points that may form the target for an information operation.

Conclusion

The transformation into a world based on communication and information, leads to IO becoming more important than ever. Thus, there is a need to develop new methodologies for successful IO, taking account of the change towards network enabling warfare capabilities. A fruitful way forward is to use theories based on centre of gravity and critical vulnerabilities. Regardless of structure all networks have their own weakness and strength and by knowing your enemy's as well as your own you can obtain advantages that may be decisive in an eventual conflict.

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

FOI

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

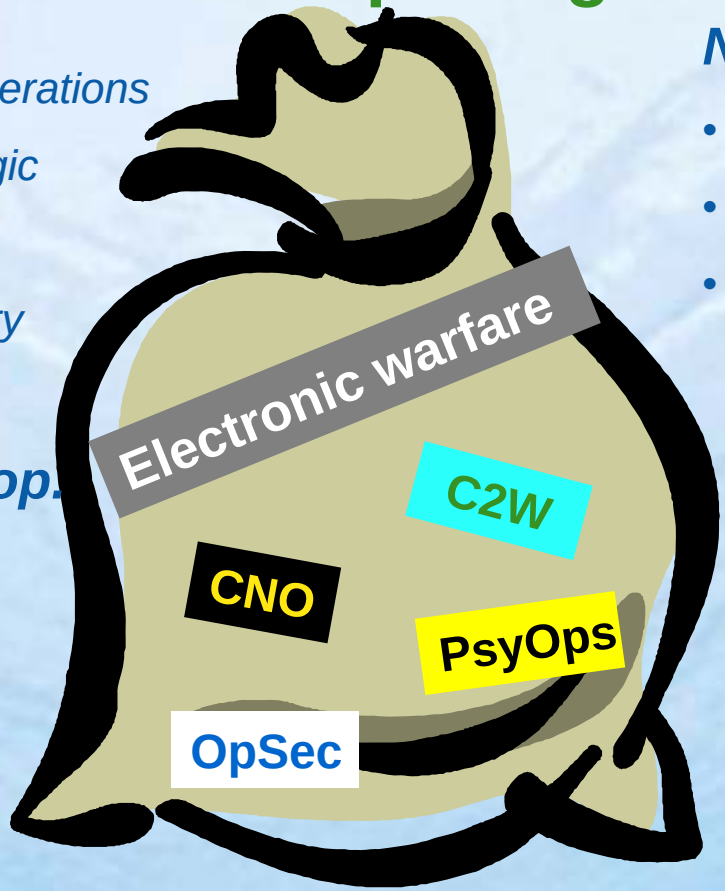
Thes2: all types of networks have their own strengths and vulnerabilities respectively due to their structure

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

”InfoOps-bag”



New doctrines

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

New vulnerabilities

- *Asymmetric warfare*
- *COTS - products*
- *Critical infrastructure*

Technological develop.

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

New actors

- *Religious & political groups*
- *Criminals*
- *Individuals*

New behaviors

- *Network organized – virtual*
- *Ad-hoc structures*

FOI

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**

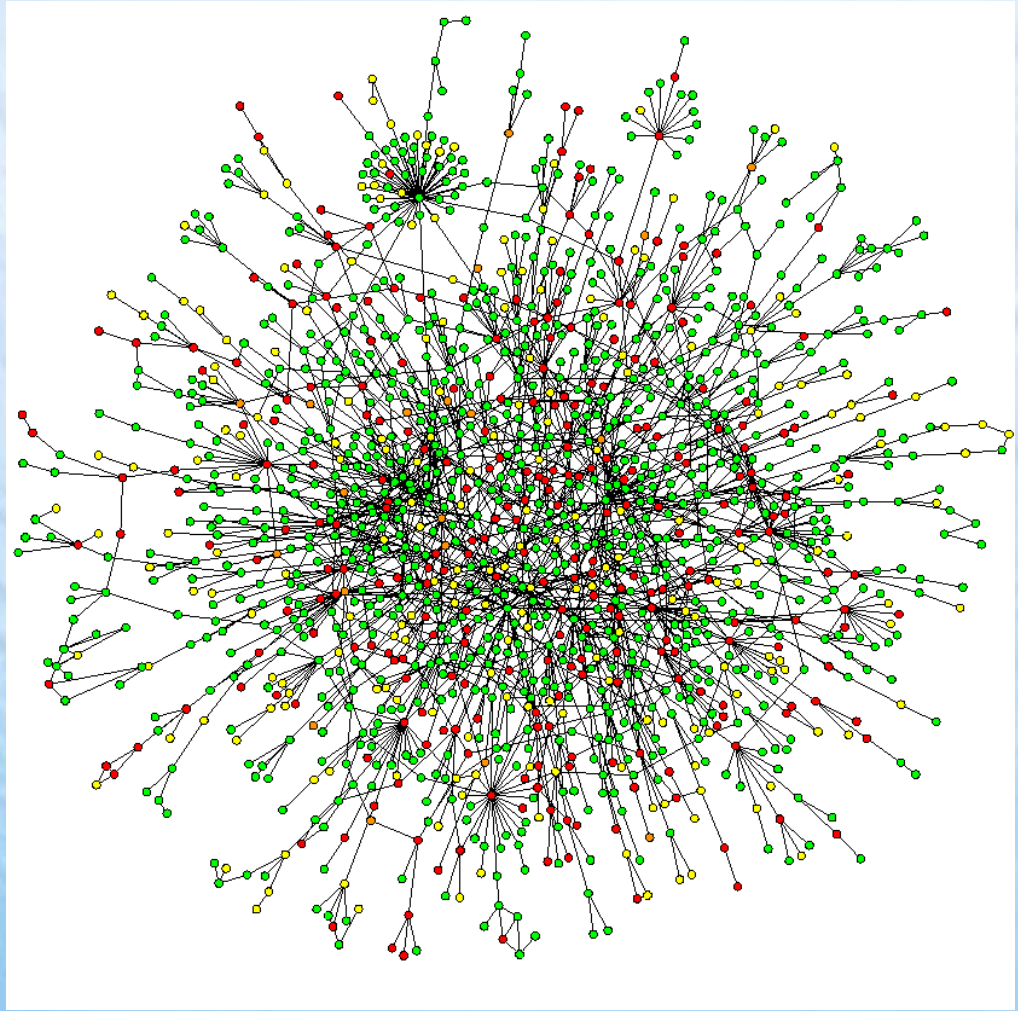
- **value: ability to coordinate activities, mustering of resources, transmit/receive information, people and products etc.**

- **types: biological, social, organizational communication networks etc.**

- **architecture: actual nodes and links**

- **topology: information flow**

Example of a biological network

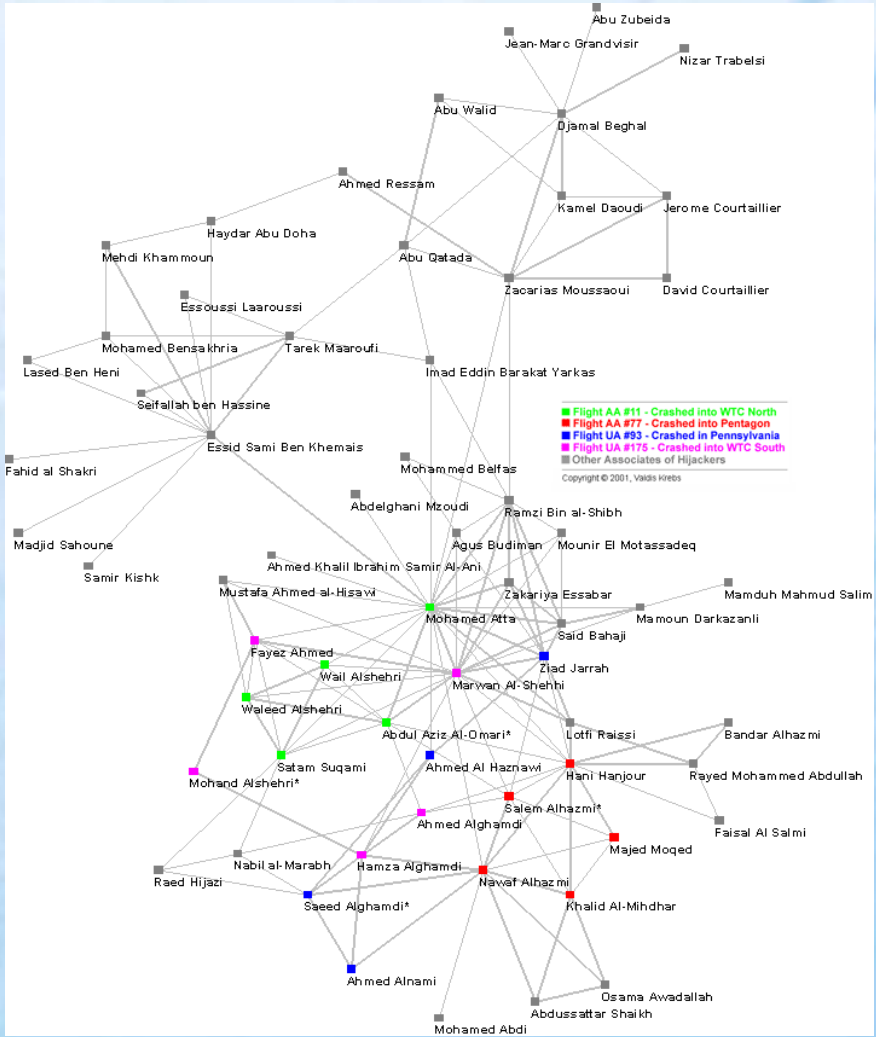


Cell metabolism

Al-Qaida Sep 11 2001

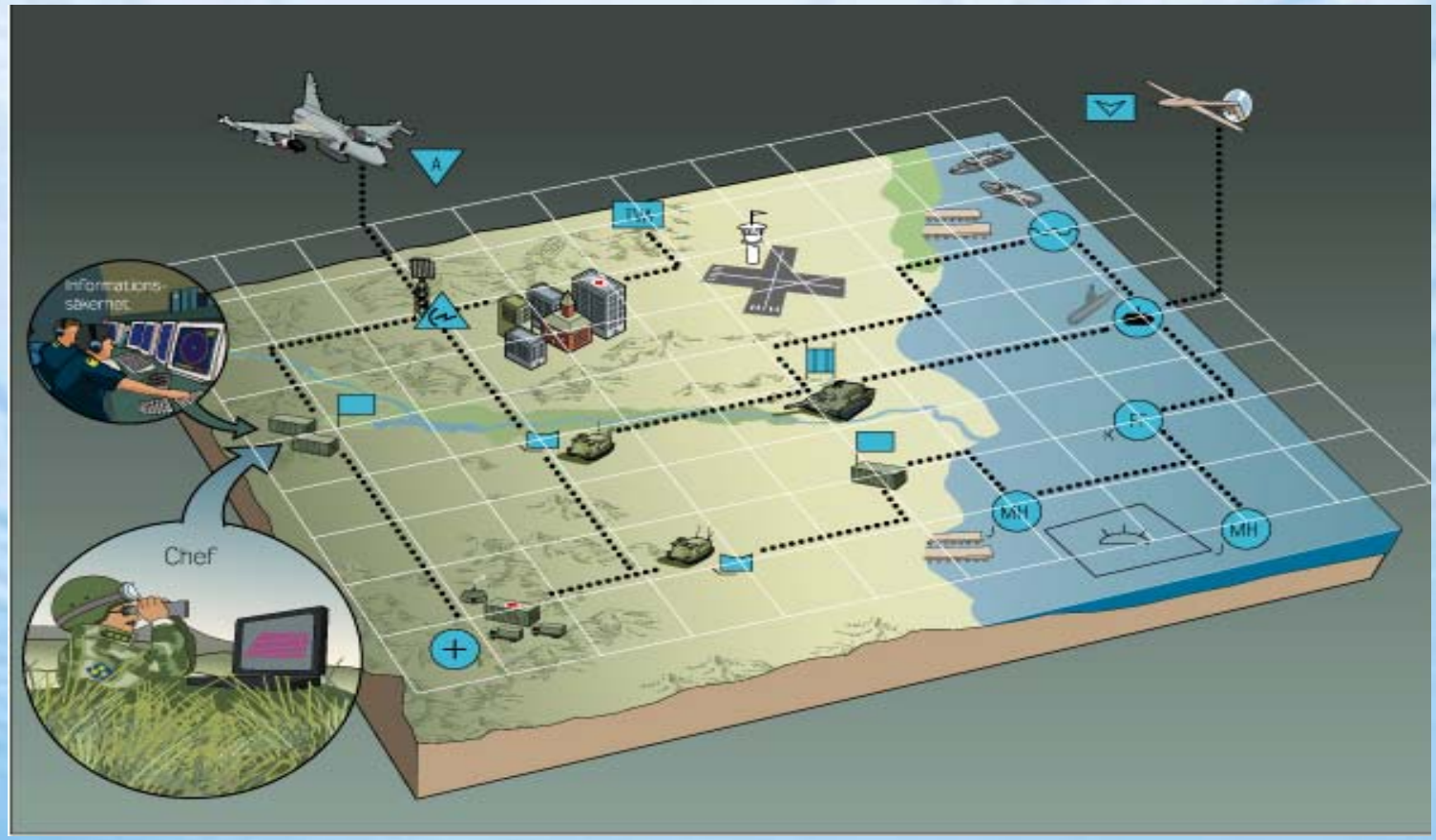
Communication links between hijackers and others suspects

Source: Krebs 2002,

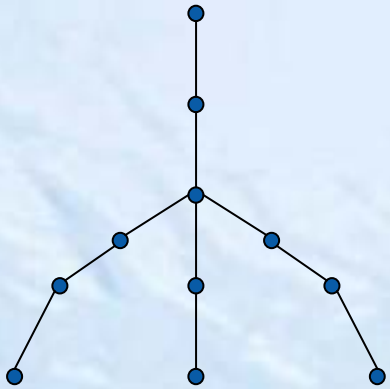


Network Based Defense: NBD

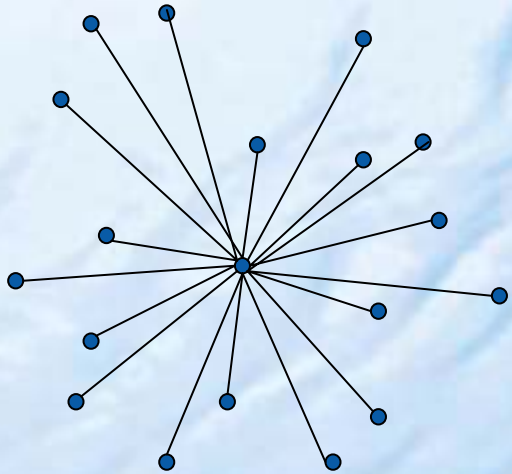
Command & Control, sensors, weapon systems and platforms connected into a network



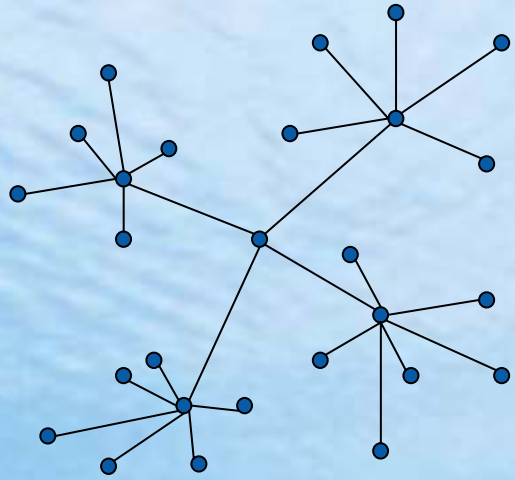
Different kinds of networks



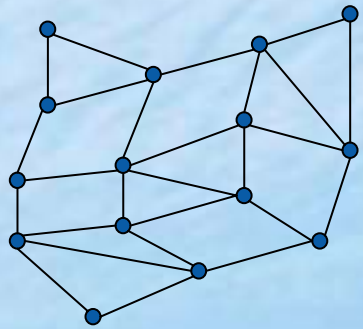
Hierarchical



Centralized



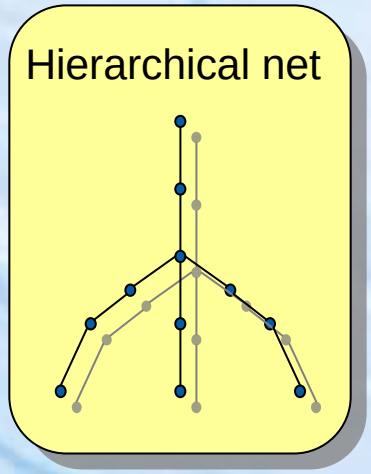
Decentralized



Distributed

FOI

COGs and critical vulnerabilities (1)

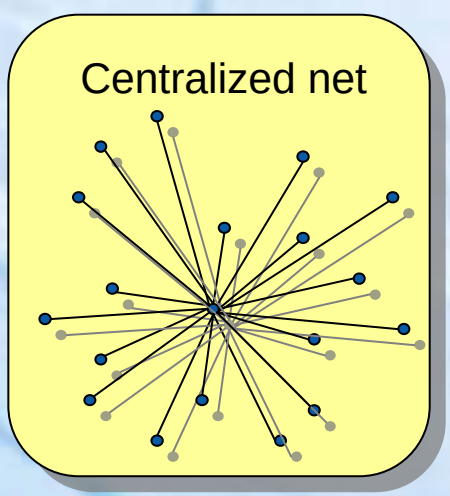


Description: Structured command & control, clear chain of command

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)

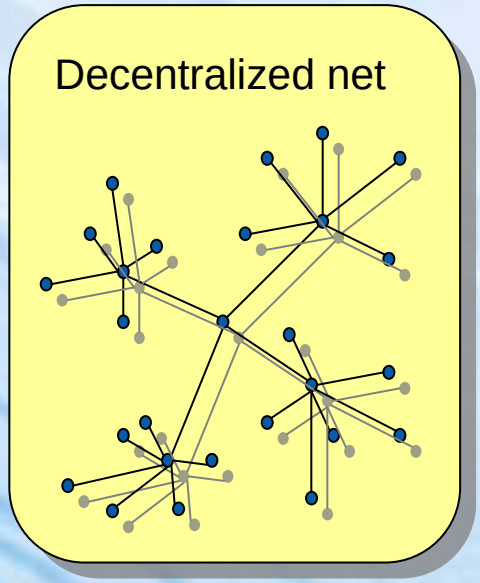


Description: All sub nodes are under command of the central node which simplifies C2 activities

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)

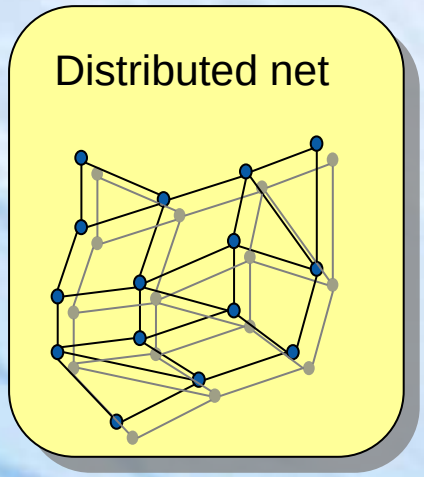


Description: Consist of a number of interconnected centralized sub-networks

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

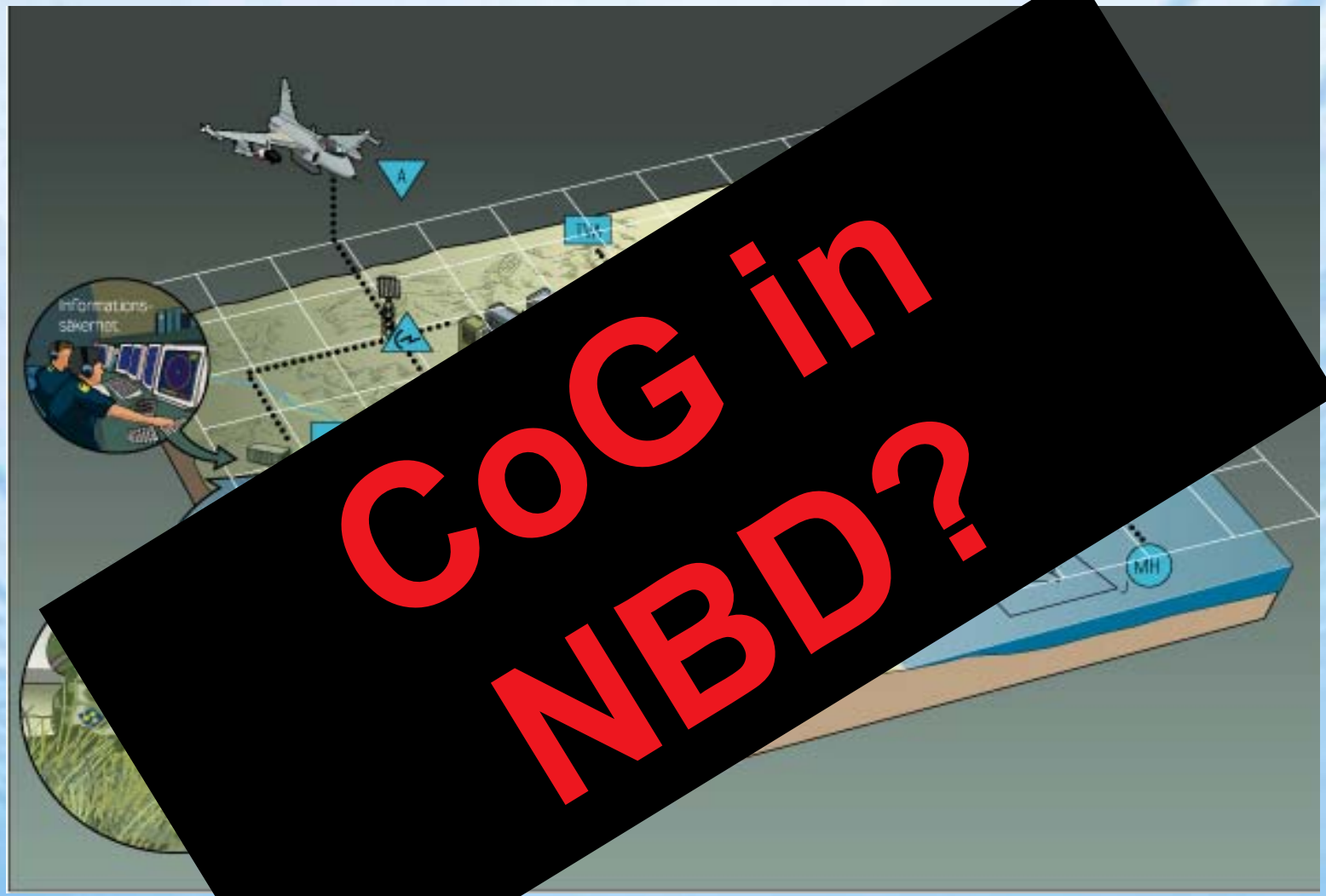
COGs and critical vulnerabilities (4)



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



CoG in NBD?

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?