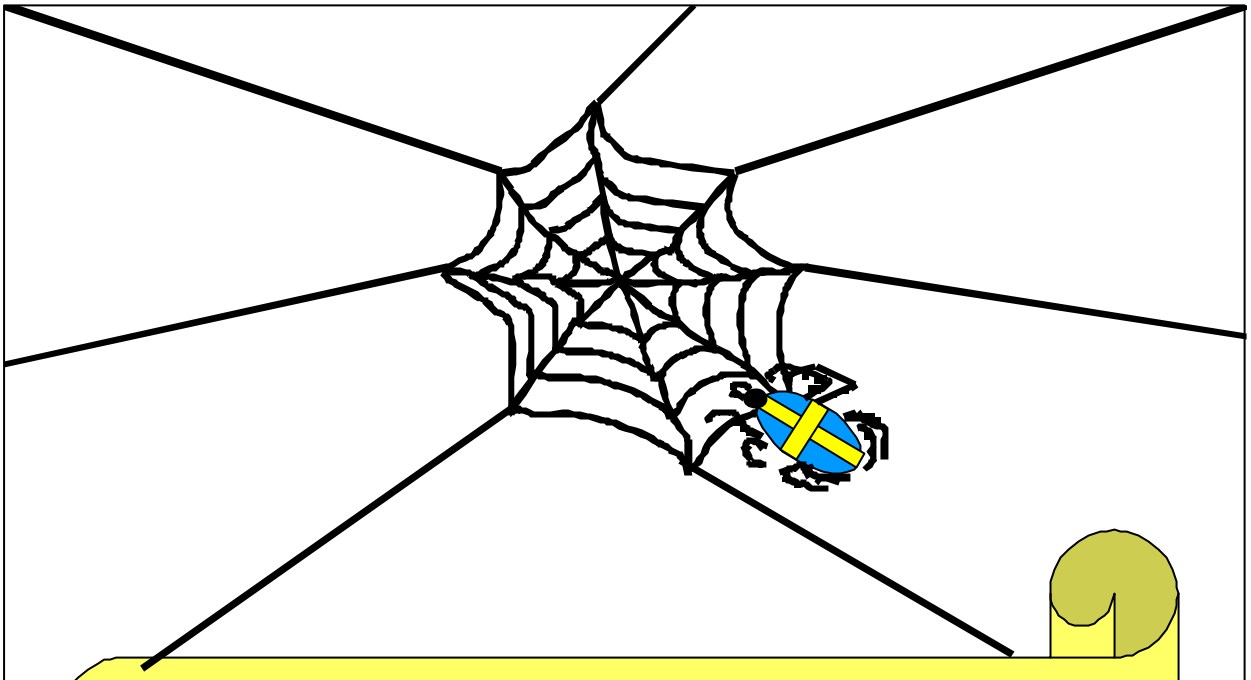


Network-Based Defence for Sweden - Latest Fashion or a Strategic Step Into the Future?

Manuel W. Wik

Defence Materiel Administration, FMV
SE 115 88 Stockholm
Sweden

FMV

NETWORK-BASED DEFENCE FOR SWEDEN – LATEST FASHION OR A STRATEGIC STEP INTO THE FUTURE?

By Strategic Specialist Manuel W. Wik
Defence Materiel Administration, FMV
SE 115 88 Stockholm
manuel.wik@fmv.se

Lieutenant General Johan Kihl, The Swedish Armed Forces:

Network-Based Defence –
The beginning of the most fundamental change of the defence in modern times
Making information the lifeline linking forces
Making information Ground Zero as target.

Disclaimer

All material in this document is primarily based on the authors' perspectives. The preparation of the document neither confirms nor denies that the material to its full extent is consistent with official Governmental views.

Abstract

Network-Based Defence is Sweden's version of Network Centric Warfare. The article describes changes compared to the present defence. The meaning of *network* and *defence* are discussed, questions are raised and some answered. One important objective is to inspire discussions about issues in connection with today's development. Apart from the author's ideas some of the material resembles the US Joint Vision 2010, visions from the Swedish Armed Forces, and thoughts from NATO countries.

An important perspective is man himself in this new context, where the simultaneous actions on the physical, information and cognitive arenas must be taken into consideration. An extension of Clausewitz theories is discussed in connection with defence capabilities constituted by the four parameters doctrine, organisation, personnel and technology.

Implementation challenges, requisites, and evaluation of the degree of networking are mentioned. One question deals with the grey zone between peace and war and the possible addition of a Network-Based Civil Defence adopting ideas of network instead of stove-piped organisations.

Finally the basic question of latest fashion or a strategic step into the future is answered. There is no way of return. There are signs on the road ahead but there is no final destination in the future.

Possibilities for fundamental change

Based on Government bill 2001/02:10, "Continued Renewal of the Total Defence"[1], the Swedish Parliament has taken a step towards a Network-Based Defence. That has initiated the

[1] *Fortsatt förnyelse av totalförsvaret*, Regeringens proposition 2001/02:10. (*Continued Renewal of the Total Defence*, Government Bill 2001/02:10)

greatest change of the Swedish national defence in modern times. It is considered that the development in communications and information technology has opened up possibilities for a radical change of how military forces can be shaped and act. While many people assert that this is no less than a revolution, other people think that the changes are less intense. In any case, in a period of *time out* after the Cold War, Sweden has decided to take a strategic risk.

The Swedish national defence has been relieved of its heavy traditional dress from the days of the Cold War and has instead started to try out a new fashion, better suited to a changing world. The tailor is in place, and the new fashion is scheduled to be on show in a few years time allowing financial scope for the new investments. If this new fashion keeps its promise, a new and stronger defence is being built than if one keeps on patching up and mending the old costume. A tough decision because the defence is a huge organisation, and the decision has serious implications for so many people. Several high-ranking officers have raised their voices in warning against the development when they have noticed the consequences of reduction of training and education. Nevertheless – a necessary decision and an important step to take, because so much has been changed round the world since the days of the Cold War.

The strategic step

But what kind of step is this, and what does one actually mean by Network-Based Defence? Answers are somewhat different depending on who is being asked, and some answers are rather vague. "We have to experiment and see what comes out. Everything is not clear." Does this mean that one has taken a decision in Parliament about a step without knowing where to tread? Is it a giant step or many small steps? Don't let us be afraid that the question does not lead to an established definition. It is more important to disseminate the fundamental ideas and theories about network centric operations than to force people to accept a specific term.

It is inevitable that different groups will have their own opinions about Network-Based Defence. One interpretation might be network-supported defence. Why should the term "*Network-Based Defence*" already be a wholly accepted one in Sweden when the term "*Network Centric Warfare*" isn't universally accepted or well understood in the American world of defence?[2] Several other terms are also discussed, such as "*Network Enabled Defence*", "*Network Centric Operations*". Still, as has already been said, a change of the defence is inevitable after the Cold War. A couple of citations might be in place: *"The only thing more difficult than to accept a new idea is to get rid of an old one." " We can decide to lead developments or become their victim."*

Fundamental thoughts about Network-Based Defence

<u>Developments in the information era</u>

The fundamental thoughts emanate like much else from the USA in relation with "*Revolution in Military Affairs*" (RMA). In Sweden, attention was first paid to RMA in 1996 in conjunction with the Jubilee Symposium of the Royal Academy of War Sciences, when Admiral William Owens became something of a revivalist.[3] This started a process in Sweden looking for an action component of Sweden's Revolution in Military Affairs[4]. The term Network Centric Warfare originates from USA and became better known in 1998 with the

[2] Money, Arthur L: *Report on Network Centric Warfare. Sense of the Report*, March 2001.
[3] Owens, William A: *Revolution in Military Affairs*, The Royal Swedish Academy of War Sciences Proceedings and Journal No. 6, 1996.
[4] Kihl, Johan: *Dynamic Engagement. The Action Component of Sweden's Revolution in Military Affairs*, SAIC Contract Number 56244-LB124576

article *"Network Centric Warfare: Its Origin and Future"*[5]. The approach shifted *from platform-centric warfare to network-centric warfare*, a change that was considered revolutionary. Platforms can deliver firepower but are stove-piped and isolated, while networks tie together grids of sensors, command and control, and shooters. Sensors on one platform can then be used for command and control on another platform commanding a shooter on a third platform. The authors compared the defence with developments in civil business just like Alvin and Heidi Toffler[6] previously had done. The basic thesis was that war could be fought the same way wealth is created. Network centric warfare was considered the military equivalence to Internet E-business. The business world depends on the instantaneous exchange of digital information. The civil world has its revolution, its change and its virtual organisations[7]. Interesting comparisons concerning the network society can also be made with "The watchful organisation"[8].

Comparison of previous and future defence

Future Network Centric Warfare is different compared to First and Second World Warfare. Some profound changes are:

- Massing effects instead of massing forces
- Less number of forces and platforms
- Much more information
- Higher speed of operations
- Just in time action
- Importance of Soft War (e.g. IO/IW[9])
- Sophisticated supporting technologies
- Precision targeting
- Powerful media role
- Grey zone conflicts
- Additional non-nation actors, asymmetries
- Soft civil targets
- Global consequences of local events
- Need for more world-wide co-operation

What is a network?

What is a network? It can be a group of humans linked together so that they can disseminate and receive the same information, if desired. The grid can be designed to link a number of smaller grids, each one with different services. Different media can be used for the network, e.g. computer networks, telephone, radio, television, newspapers. The network must be:

- Well structured and organised
- Fundamentally stable when upper layers are changed
- Transparent for efficiency and speed
- Adaptable with safe and secure links and nodes

[5] Cebrowski, Arthur K; Garstka, John J: *Network Centric Warfare: Its Origin and Future.* Naval Institute Proceedings, January 1998.
[6] Toffler, Alvin and Heidi: *War and Anti-War*, Warner Books, ISBN 07515 0938 8, London 1994.
[7] Hamel, Gary: *Leading the Revolution*, Harvard Business School Press, ISBN 1-57851-189-6, Boston 2000; *Harvard Business Review on Change*, Harvard Business School Press, ISBN 0-87584-884-2, Boston 1992; Siebel, Thomas M.; House, Pat: *Cyber Rules. Strategies for Excelling at E-Business*, Doubleday, ISBN 0-385-49412-2, New York 1999.
[8] Hamrefors, Sven: *Den uppmärksamma organisationen. Från Business Intelligence till Intelligent Business*, Studentlitteratur, ISBN 91-44-01633-6, Lund 2002
[9] Information Operations (IO), Information Warfare (IW)

Characteristics of NBD, NCW and NCO

The Swedish national defence has chosen to use the term *Network-Based Defence, NBD,* instead of *Network Centric Warfare, NCW.* Since no definition exists either of the Swedish or the American term it is not possible to compare them either. With respect to internationalising the defence and the need for understanding among nations, it is important that no major differences exist. The American term is described in a number of reports and books[10], which have been utilized below.

It is not very easy to summarize Network-Based Defence in a few words. Network-Based Defence takes as its model the development of information technology in order to attain higher pace in decision-making processes and better synchronization of military units from all the defence forces[11]. This is accomplished by establishing computer network connections between sensors, decision-makers and weapon systems and disseminating a common situational picture in near real time to all geographically dispersed units, systems and decision-makers who need it. The network is made up of components with well-defined open interfaces. This forms the foundation for interoperability[12] and continuous, gradual development. The network makes it possible to summarize valuable characteristics (e.g. situational pictures, ranges or fire power), and the sum leads to more powerful capabilities.

Cebrowski and Garstka explain "Network-Centric Warfare" in the following way (ref. footnote 5): "*Network-Centric Warfare* derives its powers from the strong networking of a well-informed but geographically dispersed force. The enabling elements are high-performance information grid, access to all appropriate information sources, weapons reach and maneuver with precision and speed of response, value-adding command-and-control (C2) processes – to include high-speed automated assignment of resources to need – and integrated sensor grids closely coupled in time to shooters and C2 processes. Network-centric warfare is applicable to all levels of warfare and contributes to the coalescence of strategy, operations, and tactics. It is transparent to mission, force size and composition, and geography."

The information flow is non-hierarchical and can support the command and control organisation most suitable for the task. This forms a flexible battle system, which in theory adapts to the forever-changing situation in moving information instead of units. Moreover, the transfer takes place travelling at the speed of light. Automatic decision support functions in the network facilitate speedy decisions and command and control from the most suitable level prevailing at the time. Information makes it possible to form virtual organisations, which in a flexible way are established and cease to function when the desired result is obtained and the task fulfilled (self-synchronization[13]). Fewer units will thus be needed, since existing

[10] *Network Centric Warfare*, US Department of Defence Report to Congress 27 July 2001; Alberts, David S; Garstka, John J; Hayes, Richard E; Signori, David A: *Understanding Information Age Warfare*, CCRP, ISBN 1-893723-04-6, August 2001; Alberts, David S; Garstka, John J; Stein, Frederick P: *Network Centric Warfare. Developing and Leveraging Information Superiority*, CCRP, ISBN 1-57906-019-6, 1999

[11] Lie, L K; Krogh, L H; Hjulgaard, L: *Network-centric Warfare*, Forsvarsakademiet VUT II/L-STK 2001/2002, Köpenhamn 2002

[12] Interoperability between systems implies that the systems have the capability to co-operate in order to solve tasks. (From ref. 11.)

[13] Self-synchronization is a method for a well-informed unit to organise and synchronise complex activities on the battlefield bottom-up. The principles for the organisation are unity of effort, clear intention from the leader and accepted solid Rules of Engagement. Self-synchronisation is applicable when the level of knowledge is high about friendly forces, enemy forces and other conditions affecting the operation. Self-synchronisation makes it possible for the units to operate without the traditional hierarchical mechanisms in the command and control system. (From footnote 11.) Cebrowski and Garstka explain the following (ref. footnote 5): "*Self-*

resources can then be used more efficiently. In return this requires a higher technical level, both from a materiel and personnel point of view. This makes the units easier to deploy and more flexible in solving their tasks.

Good situational awareness and powerful command and control make arms capabilities and effects more efficient, more precise and better suited at the right moment. All in all, synergies are created in the Network-Based Defence. More efficient control of resources provides a capacity for continuously adapted logistic measures in order to keep up combat capability and power of endurance. The network also creates possibilities for active and passive multi-dimensional protection of personnel, weapon systems, information, and command and control systems.

Network Centric Operations, NCO, are applicable at all military levels from strategic to operational and tactical. At the operational level the command will have the capability to carry out precision engagements at an unrivalled pace in order to quickly prevent enemy engagements. It has been said that network centric operations can be like releasing the genie from the bottle, when at long last the rifts between the armed forces no longer exist. However, this will only happen if they have all adopted it and practiced it equally. Network centric operations are also considered to involve new ways of operating not yet thought of and new technologies not yet invented.

One characteristic of a network is that different areas are connected, information is exchanged, and the areas become more mutually dependent on each other[14]. It is not possible to benefit from networks and at the same time keep hierarchies and rigid limits. Military organisations are known for their rigid hierarchical structure. Likewise, the division of strategic, operational and tactical areas is practically sacred. At the end of the day, this can result in rigid sequential activities. However, introducing network defence involves something interesting, which breaks down the artificial division between the three areas.

Mutuality and feedback break the sequential order; create parallel processes and open up new ways of action. As a consequence, pace – the Americans say "*op tempo*" - increases and the time to get results is shorter. Keen perception, adaptation to rapid changes, improvisations and self-synchronisation are in stark contrast to rigid plans, traditional linear working procedures, and always obeying command. This implies the necessity to think about how command and control and other systems should be developed in Network-Based Defence. It is all about being able to perceive, decide upon a course of action and to take an active enough part in the constantly changing processes, which all together form a comprehensive picture.

In today's private business intermediate organisational levels are commonly eliminated resulting in *flat hierarchy*. The military command structure in Sweden is *mission command* ("*uppdragstaktik*"), which supersedes previous *direct command*. In the Network-Based Defence combining pyramidal power structure, hierarchical command structure and flat information structure must be analysed and tested.

---

synchronization is the ability of a well-informed force to organize and synchronize complex warfare activities from the bottom up. The organizing principles are unity of effort, clearly articulated commander's intent, and carefully crafted rules of engagement. Self-synchronization is enabled by a high level of knowledge of one's own forces, enemy forces, and all appropriate elements of the operating environment. It overcomes the loss of combat power inherent in top-down command directed synchronization characteristic of more conventional doctrine and converts combat from a step function to a high-speed continuum."

[14] Hamrefors, op cit.

How much of "control" can be replaced by "creativity"? It is quite clear that information technology changes our way of working. This has an impact on demands for competence, staffing and organisation. Such changes are hard enough in the civil network society where changes may be tested to full scale. In military defence – seldom or never in confrontation with war – such changes are considerably more difficult to evaluate.

Self-synchronisation is mentioned as a value added characteristic of Network-Based Defence. So far, this is mostly theory. What will happen in practise? And what does the situation look like when the network doesn't function in all respects? In high tempo situations it might be hard for people to wait for command, when necessary information seems to be at hand.

The new defence network will become what one designs it to be. If one wishes to have a rigid hierarchical and sequential order, this is quite possible. The idea of networking is partly eliminated if one introduces classification restrictions preventing exchange of information where actually needed. The design will be about the art of finding a balance between all kinds or restrictions and the free flow of information.

The network engine

Defence capabilities, systems and arenas[15]
Military defence can be characterised by six all-embracing *capabilities* (or powers):

- Information (resources, environment, operations, infrastructure)
- Command and control (operational levels, tasks)
- Mobility and manoeuvre (transportation capabilities and platforms for land, sea, underwater, air, and space)
- Arms in all dimensions (fire power for land, sea, underwater, air, and space)
- Safety and security in all dimensions (physical, information, cognitive)
- Logistics (for land, sea, underwater, air, and space)

Each one of these six capabilities depends on four *systems (parameters)*:

- Doctrine (doctrines and rules of engagement for physical, information, and cognitive attack and defence)
- Organisation (physical units and materiel, plans of organisation, network organisation culture)
- Personnel (competence requirements, services, education, training)
- Technology (technical support services, hardware, software, adaptation to human needs)

The six major defence capabilities, each one consisting of the four systems, must be used in combination in order to form the military defence as a whole. A certain amount of each capability will always be needed. As an example the same applies for a human being. Man needs a combination of head, heart, body, arms, and legs in order to function in all respects. The metaphor is useful when describing a number of defence functions and missions.

[15] Latin word meaning *sanded area for combats, sand*, (sand used by Romans to absorb blood from gladiators)

The Six Major Defence Capabilities

INFORMATION	COMMAND & CONTROL	MOBILITY & MANEUVER	ARMS	SAFETY & SECURITY	LOGISTICS
RESOURCES *ENVIRONMENT* *OPERATIONS* *INFRASTRUCTURE*	*STRATEGIC, OPERATIONAL, TACTICAL LEVELS* *ALERT LEVELS* *LAND, SEA, AIR, JOINT, COMBINED LEVELS* *TASKS*	*TRANSPOR-TATION CAPABILITY FOR LAND, SEA, UNDERWATER, AIR, SPACE* *PLATFORMS*	*FIREPOWER FOR LAND, SEA, UNDERWATER, AIR, SPACE* *PLATFORMS*	*PHYSICAL, INFORMATION, COGNITIVE*	*FOR LAND, SEA, UNDERWATER, AIR, SPACE*

Information network Infrastsructure:
Partly unique for the defence, and largely shared with the private sector. The computer and telecom infrastructure is extensively civil. International standards fulfill many different needs.

Examples from the civil world:
Companies' management and command and control. Non-standard, changes in a changing world

→ *The Information Network Infrastructure must be designed for different needs in a changing world.*

The Defence: Capabilities and Systems

Formed by combining the six major defence capabilities, each one consisting of four systems (6x4).
{These activities appear on three arenas simultaneously (3x6x4).}

SYSTEMS	DEFENCE CAPABILITIES					
	INFOR-MATION	COMMAND & CONTROL	MOBILITY & MANEUVER	ARMS	SAFETY & SECURITY	LOGISTICS
DOCTRINE ROE						
ORGANI-SATION						
PERSONNEL						
TECHNOLOGY						

 manuel.wik@fmv.se

All six capabilities, characterised by their four systems, appear simultaneously on three *arenas* (battlefields, domains):

- The physical arena (land, sea, underwater, air, space)
- The information arena (electromagnetic space, cyberspace, and all other spaces where information can appear)
- The cognitive arena (perception, decision, knowledge, and wisdom space)

Examples of System Contents on the Three Arenas

The interplay between doctrine, organisation, personnel and technology is fundamental when developing Network-Based Defence capabilities.

	PHYSICAL ARENA	**INFORMATION ARENA**	**COGNITIVE ARENA**
DOCTRINE	*PHYSICAL ATTACK AND DEFENCE*	*INFORMATION ATTACK AND DEFENCE*	*COGNITIVE ATTACK AND DEFENCE*
ORGANISATION	*PHYSICAL UNITS, MATERIEL*	*PLANS OF ORGANISATION*	*NETWORK ORGANISATION CULTURE*
PERSONNEL	*COMPETENCE REQUIREMENTS*	*SERVICES*	*EDUCATION, TRAINING*
TECHNOLOGY	*HARDWARE* *TECHNICAL SUPPORT SERVICES*	*SOFTWARE* *TECHNICAL SUPPORT SERVICES*	*ADAPTATION TO HUMAN NEEDS* *TECHNICAL SUPPORT SERVICES*

Comments on the arenas

Some comments are needed concerning the arenas. All three of them have actually always existed, but more or less visualised. Until recently in modern-time thinking, focus and resources have, to the greatest extent, been on the physical arena. The information age brought about some more thinking about the information arena[16]. However, it took some time for the military world to understand about information warfare and information operations and to start organising special information forces. In the beginning – and still to some extent – people working in the traditional organisations, fearing it would decrease their own budgets, looked upon this with scepticism. In 1995 it was forecasted[17] that the network era with data fusion, communications and multimedia would last from about the year 2000 – 2020. The knowledge era would then take over, characterised more profoundly by internationalism and co-operation. Thus, it will still take some time before the military world will understand and

[16] Wik, Manuel W: *Mobilization for a New Era*. Royal Danish Defence College, November 16, 1998, http://www.fhs.mil.se/institut/kvi/cios/doc/vorb156k.doc

[17] Wik, Manuel W: *Spekulationer kring informationsteknologi och krigskonst*. The Royal Swedish Academy of War Sciences Proceedings and Journal No. 1, 1995.

acknowledge the cognitive arena[18] in such a way as to build suitable organisations in co-operation with the civil world. It is astonishing that the cognitive arena – the key and solution to conflicts – is neglected or overlooked in the minds of many people with important decisions to make.

- The cognitive arena – the key and solution to most conflicts

Comments on the Information capability

Some comments are justified concerning Information capability. Resources, Environment, Operations and Infrastructure may characterize it. For clarity it is good to separate *information management* (management of information of all kinds, not always directly used for command and control) and *command and control management* (management of missions and tasks; leadership including command and control messages). *Information capability resources* are Information, Computers, Communications and Sensors, Information Network Infrastructure, and Electronic Warfare Resources. *Information capability environment* covers Electromagnetic spectrum, Cyberspace, Mass media, Paper, air and all other spaces where information appears. *Information capability operations* are Information and Network Management, Information Operations, Electronic Warfare, Intelligence, Surveillance, and Reconnaissance.

The cognitive arena is supported by Information Operations on the information arena. It has been said[19] that Information Operations (IO):
"…can make an important contribution to defusing crises; reducing periods of confrontation and enhancing the impact of informational, diplomatic, economic, and military efforts; and forestalling or eliminating the need to employ forces in a combat situation"
"…may have their greatest impact as a deterrent in peace and during the initial stages of crises"
"…capitalize on the growing sophistication, connectivity, and reliance on information technology"
"…target information or information systems in order to affect the information-based process, whether human or automated"

There are different apprehensions of the meaning of Information Operations, and definitions vary somewhat. However depending on the situation, it may be necessary to be aware of and consider the whole picture, including Information Operations and all related activities. They are two-sided. Both Attack and Protect/Defend exist:

Information Operations and related activities engaging the physical arena:
Physical Attack/Destruction of information values, Physical Security/Protection of information values

Information Operations and related activities engaging mostly the information arena:
Information Attack, Information Security
Communications Attack, Communications Security
Computer Attack, Computer Security

[18] Jones, Andy; Kovacich, Gerald L; Luzwick, Perry G: *Global Information Warfare.* Auerbach Publications, Washington D.C. 2002, ISBN 0-8493-1114-4, Appendix D: Wik, Manuel W: *Revolution in Information Affairs: Tactical and Strategic Implications of Information Warfare and Information Operations.* (First published at Data Security Nordic '99, October 14, 1999)
[19] Joint Doctrine for Information Operations, Joint Pub 3-13, 9 October 1998, USA

Network Management, Attack and Protection
Communication Network Attack, Communication Network Protection
Computer Network Attack, Computer Network Protection
Information Operations Attack, Information Operations Security
Information Warfare
Command and Control Warfare
Electronic Warfare (Electronic Attack, Electronic Protect, Electronic Support Measures)
Other Signals Warfare
Civil Affairs
Public Affairs

Information Operations and related activities engaging mostly the cognitive arena:
Surveillance, Counter Surveillance
Reconnaissance, Counter Reconnaissance
Intelligence, Counter Intelligence
Deception, Counter Deception
Propaganda, Counter-Propaganda
Psychological Operations, Counter Psychological Operations

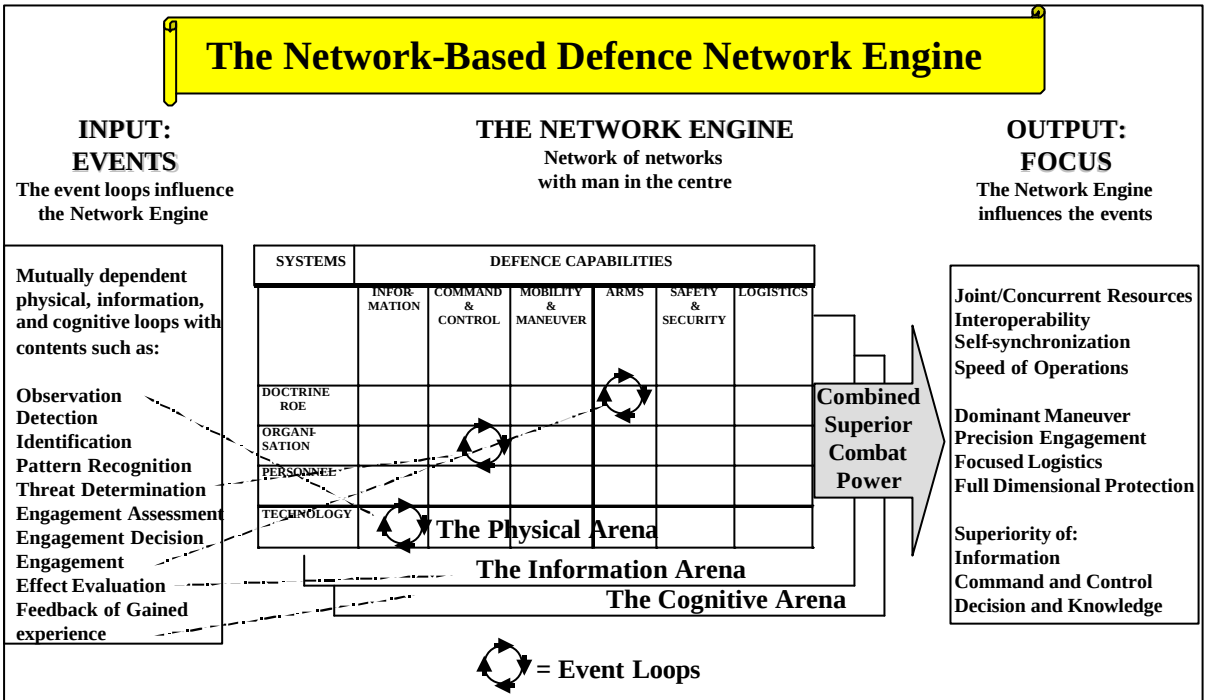
The network engine's input and output

Putting capabilities, systems and arenas together constitute a network – or you might say a network of networks. Each arena consists of 24 major areas of concern formed by the combination of capabilities and systems. Together the three arenas form 72 major areas to be considered in the network. Some of them are more important than the others, but all of them together form the overall picture. The function of the network as an engine can be illustrated using its parts together with course of events, routines, services and roles. The course of events can start event cycles within each system of the capabilities appearing on the three arenas. The event cycles interact with one another in ways depending on the situation. The output of the network engine comes from *combinations of the three arenas* as well as from each one of the three arenas. The major output from the physical arena is physical superiority, and from the information arena information superiority. The major output from the cognitive arena is decision and knowledge superiority. The superior combination of the three arenas at every instant is the most important total output from the engine. Major outputs from combinations of the arenas are focus and sharpened calls for concurrent resources, interoperability, command and control superiority, self-synchronisation, speed of operations, dominant manoeuvre, precision engagement, focused logistics, and full dimensional protection. The engine operates according to pre-programmed and pre-tested routines, which gradually are developed further and adapted in accordance with existing conditions. The network can resemble an optical lens focusing defence capabilities on current tasks[20]. Time is a vital parameter for each part of the network, driving combined capabilities into the superior time slots. The output is speed of operations and a proportionate response at the right time and in the right place.

The course of events engages a combination of capabilities and system parts at the same time on the three arenas. This makes it important to develop the Network-Based Defence in harmony on the three arenas. A course of events starting the network engine can comprise observation, detection, identification, pattern recognition, threat determination, engagement

[20] Recognizing the RMA focus on: *Dominant Manoeuvre, Precision Engagement, Focused Logistics, Full Dimensional Protection*. Originally from US *Joint Vision 2010*, John M. Shalkashvili, Chairman of the Joint Chiefs of Staff, http://www.dtic.mil/jv2010/jv2010.pdf

assessment, engagement decision, engagement, effect evaluation, and feedback of gained experience. The course of events engages the network in a tailor-made fashion considering the situation and focuses on control, composition and network-centric resources. One part of the course of events is the decision loop (OODA-loop[21]). Mission-composed task forces, or (as in the United States) *Mission Capability Packages* (MCP)[22], are resources that basically follow a number of modes of action or *Rules of Engagement* (ROE).



The input ("fuel") to the network engine are the event loops (see the examples). Tasks and roles are determined and services produced. The six defence capabilities (Information; Command and Control; Mobility and Maneuver; Arms; Safety and Security; Logistics) consisting of four systems (Doctrine and Rules of Engagement, ROE; Organisation; Personnel; Technology) appear simultaneously on three arenas (Physical; Information; Cognitive). Engagement awareness is generated, leveraging combat power. Mission Capability Packages, MCP, and Task Forces, TF, are formed. The output of the network engine is combined superior combat power, focus on all joint/concurrent capabilities, superior engagement and speed of operations ("op tempo").

Services and users

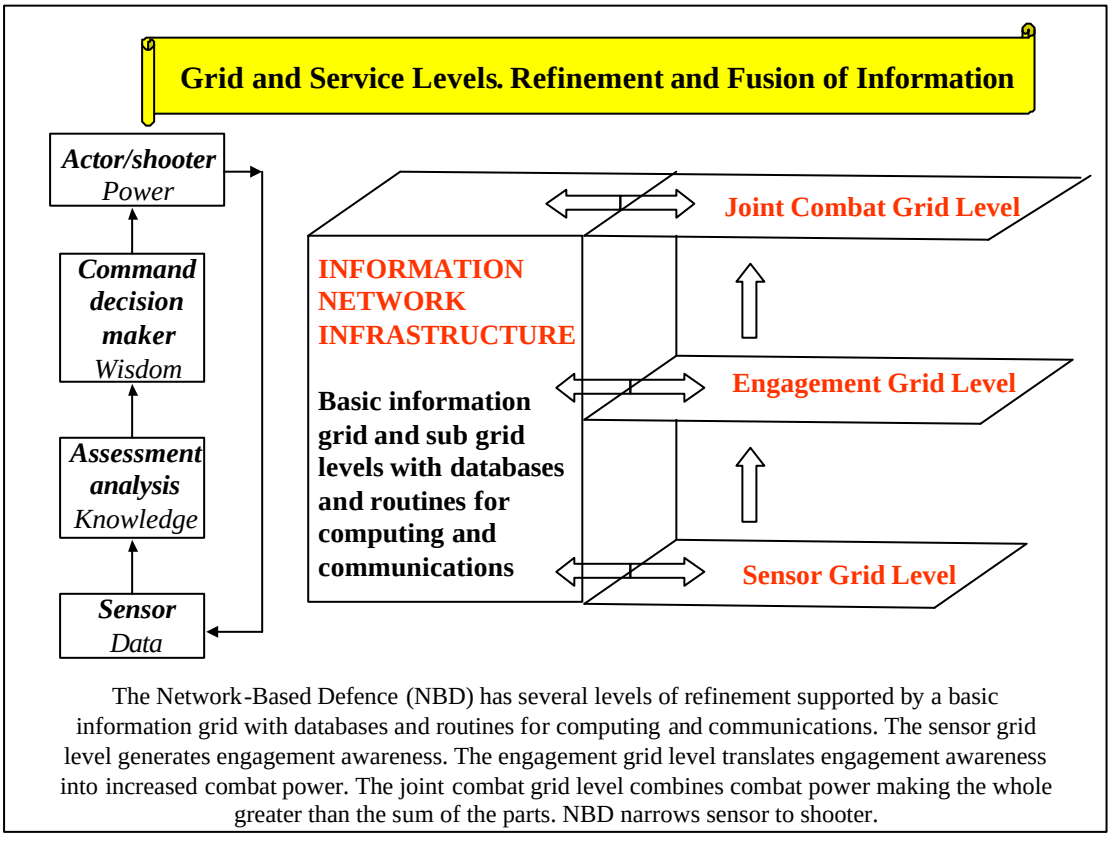
Each single component of any type, which is part of any of the systems and is interoperable, meaning it can communicate with other units and exchange or share information, is also part of the network. As an example it could be a special sensor on a weapons platform able to provide sensor information not only to the platform itself but also to other parts of the network. However, no single part is by itself to be the heart of the network if the network is to be robust. A number of special nodes in the network are designed to automatically collect and process information and act as service centres providing an overview within various areas, for example weather conditions in a geographical region and weapons capability close to the region. In such a way, a number of services are created for each of the six capabilities and can be assigned to people having specific roles. In order to add information value further, services can be combined to form multi-services and to focus on tasks, such as command of operations. Authorization to acquire services depends on what kind of role one has. There is a

[21] The OODA decision loop stands for Observe, Orient, Decide, and Act.
[22] Sometimes described as *Doctrine, Organization, Training, Materiel, Leadership & Education, Personnel, and Facilities (DOTMLPF).*

striking resemblance to the E-business on the Intra- and the Internet within the civil community.

Users with specific roles will be authorized to access data of concern to them. The users will not be able to access data, which is non-relevant to their specific task[23]. This will limit the dissemination of information concerning e.g. for a specific task non-relevant units' positions and performance. This limits dissemination of secret information on the network, but also limits overloading the users with lots of information. However, it places high demands on the network information management to search for and handle all possible synergies. Such synergies are one of the main purposes of the network.

A network, or rather network of networks, must be *transparent to its users* so that they themselves are not caught somewhere in the network grid without finding their way around. The service part of the network resembles a multi-storeyed house where the rebar grid at each floor corresponds to a network layer for a specific service. The nodes in such a service grid can refer to sensors, in another service grid refer to fire power, transport capability, logistics or command. At each floor level focus can be directed at the task in hand. In between the different floor levels of the service networks connections are made dependent on the situation. Each service should have such an interface that it can be added to other services in order to jointly form multi-services on an open standardised network[24]. Refinement of information (data and information fusion) takes place on many levels from *data (sensor)* to *knowledge (assessment analysis)*, to wisdom *(command decision maker)*, and to *power (actor/shooter)*.



The Network-Based Defence (NBD) has several levels of refinement supported by a basic information grid with databases and routines for computing and communications. The sensor grid level generates engagement awareness. The engagement grid level translates engagement awareness into increased combat power. The joint combat grid level combines combat power making the whole greater than the sum of the parts. NBD narrows sensor to shooter.

[23] Nilsson, Per: *From Brute Force to Brainpower*, Swedish Journal of Military Technology No.3, 2000.
[24] Bergh, Svante: *From Platform to Network Centric Defence*, The Royal Swedish Academy of War Sciences Proceedings and Journal No. 4, 2001. Bergh, Svante; Lans, Håkan; Lidström, Christer: *Network Centric Warfare – A Wizard's New Command and Control Toolbox*, The Royal Swedish Academy of War Sciences Proceedings and Journal No. 6, 2001.

 manuel.wik@fmv.se

Man is at the centre of the network. All activities must be dictated as originating from human conditions. Thus, one can talk about a human centric network, making one think of *Human Centric Warfare*.

The network has several levels of information refinement supported by a basic information grid level with databases and routines for computing and communications. One Network-Based Defence design possibility is with three major action grid levels (network of networks):

- Sensor grid level
- Engagement grid level
- Joint combat grid level

The sensor grid level generates engagement awareness. The engagement grid level translates engagement awareness into increased combat power. The joint combat grid level combines combat power making the whole greater than the sum of its parts[25]. Information refinement is transferred from the sensor grid level to the engagement grid level and to the joint combat grid level. The number of users at the grid levels is reduced at the higher levels of refinement.

Comparison with a well-known small network
A football team can be compared to a network where the physical arena (football ground and other things), information arena (sight and hearing) and the cognitive arena (football players situational awareness) co-operate. Co-operation between the arenas can be described as follows:

- The information arena: A robustly networked football team improves the capability to share information about the immediate situation guided by the five human senses and by communication.

- The cognitive arena: Information sharing enhances the football players´ shared situational awareness.

- The physical arena: Shared situational awareness facilitates physical collaboration and, based on football rules and individually acquired roles, it gives players the chance to synchronise their engagements with the other players, and to increase their staying power and speed.

- All in all, this increases the football team's chance to win the game.

Let us assume the following. Pull the football players apart geographically so that they now no longer can make eye contact with one another. Technology now has to be used to compensate for the large distances between the players. They need assistance from computers and communications, technical sensors, command and control systems, perhaps robots to transport the football and so on. The game can then go on supported by a network of players where their physical arena works with their information and cognitive arenas. Let us now assume that we exchange the players for military personnel with technical sensors, weapons, computer and communication systems and so on and that we let the personnel work together in a network in a way similar to the football players.

[25] Ref. to footnote No. 5

Applied to a Network-Based Defence, the fundamental tenets are (citation[26]):

- "A robustly networked force improves information sharing
- Information sharing enhances the quality or information and shared situational awareness
- Shared situational awareness enables collaboration and self-synchronization, and enhances sustainability and speed of command
- These, in turn, dramatically increase mission effectiveness"

The co-operation between the systems for doctrine, organisation, personnel and technology

Football games need rules, organisation, team leadership, trained people, and technical means. The Network-Based Defence operation needs this as well. In both cases the physical arena, the information arena and the cognitive arena are united. The co-operation between the arenas is nothing new. The new thing is that technical means make an inter-connection between the arenas possible so that efficiency and pace can be dramatically increased in Network-Based Defence. Networks are nothing new either. The new thing is information technology and the Internet, which dramatically increases the opportunity for more and more people to build networks.

New technical possibilities create new human needs not previously thought of. Interoperability has increasingly come to the fore lately, but would no doubt have been applied from time immemorial had the technical means existed. Likewise, today many people consider they need mobile phones since these phones offer them considerable latitude, both as regards their whereabouts and their ability to synchronize their activities with others.

Clausewitz has explained the connection between doctrine, organisation and technology. If one of the three parameters is changed, it is necessary to adjust the others. The theory may be applied with the addition of the parameter personnel. It is the most unpredictable parameter since it concerns man himself.

- **All four parameters: doctrine, organisation, personnel and technology interact with one another mutually when developing Network-Based Defence capabilities.**

From the mass armies of the two World Wars and the Cold War developments have been moving towards a considerable slimming down of organisations with personnel requiring a considerable amount of education and training for advanced tasks. New possibilities emerge with network technology and they influence the development of doctrine, organisation and personnel. In turn this creates new conditions where all four parameters interact. A development with interaction between the four parameters requires a new network-dependent method of working where each person senses and understands other factors than those within his own special field. The influence of technology within the defence arena increases considerably with Network-Based Defence, and this technology could easily dominate. Such conditions must never hide the golden rule:

[26] *Network Centric Warfare*, US Department of Defence Report to Congress 27 July 2001

- **Technology must comply with human behaviour, never the other way round. Man is central and common sense must prevail.**

The four systems operate on the three arenas, which implies twelve combinations. An analysis of Network-Based Defence, structured in this way, covers all essential areas and does not risk missing out on essential parts. All twelve areas require a lot of new thinking and talent to break new untested ground. One speaks of *sustaining innovation* and *disruptive innovation*. The latter implies that one breaks up traditional trains of thought and that advantages can crop up not thought to be possible earlier. Previously the unconditionally largest part of all work was about the physical arena, that is the development of doctrine, organisation, personnel and technology for land, sea, air, underwater and space. For the information and cognitive arenas, a high degree of new thinking is now required.

The physical arena
The physical arena comprises the traditional operational activities within the army, navy, and air force and has been concentrated around the platforms. Platforms can have functions for communication, sensors, electronic warfare, command and control, weapons, transport, logistics, protection, etc. The Network-Based Defence now calls for new requirements. The platform is no longer one solid unity around which all activities are centred. The platform now shares its functions with other platforms and its functions in the network. The platform can share any one function, and the function or functions can be part of, or controlled from, some other place in the network, which momentarily happens to be the centre of activity.

It can for example mean that an aircraft shares its target information with an armoured vehicle. Via the aircraft it receives an order to fire. Another example is when an armoured vehicle receives information from an aircraft and shares it with a special task force, which, using other functions in the network, guides a logistic transport to a Coast Artillery Centre. People in Afghanistan were given satellite phones to report information to US aircraft pilots circulating over the country about the location of enemies. The aircraft then blew up the targets. The fact that each individual function can be added to other functions in the network also leads to synergies.

Looking at more separate conditions this is no new defence method as there has always been an endeavour to seek co-operation with various other units and between platforms. The new thing is that, taking advantage of considerably larger resources for joint communication and information, we can have a sum total or cumulative effect consisting of results from a large number of systems – *mass effects, not forces*. In principle, each single unit in the network is then given a situational picture far more powerful than the single unit can achieve in itself. Each unit then knows as well exactly where all other units are at each moment. All friendly units know the whereabouts of detected targets. Transport resources, firepower, protection and logistics can, depending on the situation, be added, commanded and deployed and also focus in such a way that the best effect is achieved. Counter-measures can make engagement more difficult, for example such as is caused by positioning and navigation warfare.

<u>The physical arena doctrine</u>
Current doctrine of the physical arena for land-, sea- and air forces will have to be changed and supplemented in a number of respects. An important change concerns command and control functions. The development implies more flexible, efficient and speedy utilization of various levels of command depending on the situation. The development in the direction of Network-Based Defence involves network functions both within each force, between forces

and in multi-national co-operation. An adaptation to NATO co-operation becomes more necessary with time. Rules of Engagement (ROE) need to be prepared for situations that can be anticipated. Such a menu of standard procedures facilitates delegating and the execution of tasks. The network enables centralised control of even very low-level tactical operations. Is that a good thing? If not, how do you avoid falling into that trap? In an operational concept, flow charts can be put up, showing dissemination of information, how this leads to rapid decision processes and self-synchronisation, and, as a logical consequence of this, how a virtual Task Force (TF) can be organised supported by a menu of standard procedures.

The personnel and its organisation in the physical arena

The organisation within the physical arena is directed towards a rapid reaction defence consisting of task forces. There is every reason to experiment with new types of deployable forces and Mission Capability Packages (MCP), and to learn from experience gained and developments in other countries. Doctrine, organisation, personnel, leadership, materiel and other means need to be woven together in various patterns assisted by education and training. New forms of collaboration between forces need to be tested. It is thought that changes can turn out to be more profound for current land forces because within sea- and air forces there is already a higher degree of interoperability.

The physical arena technology

The technology of the physical arena implies large challenges. The units building the network must be able to communicate with one another by fixed and mobile transmission networks. New generations of sensors, electronic warfare materiel, signal processing and surveillance systems are going to be developed. Means for information, command and control are going to be constructed and adapted to platforms and networks. Physical and logical interfaces must be standardised. All kinds of materiel must be mutually compatible in the network and all future development proceeds accordingly.

It is not enough that units like aircraft, ships and armoured vehicles can move at high speed for a long time and with good weaponry. The units must also carry information, being equipped with sensors, communication systems, and having interoperability, electronic warfare means, stealth characteristics and command and control. These requirements easily result in higher costs than if the platform itself served only as a means of transporting weaponry.

The information arena

The information arena is central in Network-Based Defence. It is the arena where information is born, lives, is processed and shared and where it is disseminated, collected and protected and where quality can increase by correlation, fusion and analysis. Information is now more than ever the prerequisite of all activities, good or bad. Your own information must be protected, whereas your adversary's must be disrupted and attacked in various ways. In extreme cases, a conflict goes no further than Information Operations and Information Warfare. *The network itself is the primary target.* Without it nothing functions. In the battle of information superiority, the information arena is *Ground Zero*. This makes heavy demands on the four parameters.

It must be understood that there are many actors on the information arena. Apart from military friends and enemies, important actors are politicians, media, and civil societies. In the age of mass media possibilities exist of immediate global distribution of pictures from events. Without healthy relationship with media one of the most powerful elements of Information

Operations is ignored. Media is independent in the free world but depends on its masters in the rest of the world. How do the military act in a media powerful world and what does the medias' OODA-loop then look like?

The information arena doctrine

Information operations require doctrines for attack and defence and involve all-important societal functions[27]. The Network-Based Defence also needs regulations concerning the information arena where factors like services, roles, and authorization can be defined and controlled. It must, in addition, be possible to have regulations rapidly changed in order to adapt to new situations. All regulations will be strongly dependent on Mission Capability Packages and Rules of Engagement. In both cases, a purposeful co-development is needed of doctrine, organisation, personnel, leadership, education and training, materiel and other means.

Examples of services in the network are positioning and navigation services, transport services, command and control services, fire-power services, intelligence services, protection services, logistic services, weather services, safety and security services, integrated services (multi-services), services for air, sea and ground situation.

Accessible services depend on what role one has and during what time it is valid. Access can be delegated from one player to another. Registers of roles with duration of time must be developed for the network and demands for faultless management must be made.

Information must be divided into different classes depending on value, urgency, secrecy, generality, and major alert. Such classifications make it easier to plan authorization with respect to roles. It is important to be able to rapidly communicate vital information to all parties concerned, but likewise not to drown operators with less important information ("noise").

The personnel and its organisation in the information arena

The organisation needs personnel responsible for the network telecommunication transmission and distribution functions, for service-based nodes, for the quality, safety and security of information, for authorization distribution, for functions concerning control and supervision of information, processing and storing, positioning, navigation, recognition, identification, high-level pattern recognition, decision support, and many other functions. Electromagnetic expertise and electronic warfare units are needed to supervise the electromagnetic spectrum, to avoid electromagnetic conflicts within friendly units, and to protect and attack within positioning, navigation, and electronic warfare.

Information warfare expertise and IT defence forces are needed to protect and attack in cyber space. Special expertise is needed for information security and information technology security, and to assess the degree of security needed in a given situation. In many situations the use of a security time lock must be considered. One must be fully aware that *there is no such thing as a hundred percent security guarantee anywhere*. It is necessary to estimate the usefulness of communication in comparison with the risk of being exposed.

When looking at the organisation it appears that new forms of education and training are going to be an absolute necessity for the qualified personnel responsible for the information

[27] See footnote No. 18

arena. “Information Operation Cells” can be organised. Up to now, far too little effort has been devoted to this central arena, which obviously already ought to have a given place in the Swedish operational command.

The information arena technology

There will be heavy demands on qualified technology in the information arena.[28]. Technical developments must be aligned intimately with doctrine (regulations), organisation and personnel. High-performing information networks will refine information, thus facilitating the human undertakings of the OODA-loop, for instance by data-fusion from integrated sensor grids, signal processing, pattern recognition, signal- and scenario libraries, and decision support by high-speed automated assignment of resources. Information stored from events having taken place builds learning and can be used as advice and support on later occasions.

Information is transmitted in physically insecure but logically secure virtual task-specific networks where time restrictions control assignment of roles and the supply of resources in the network. Among security mechanisms are priority and load control of networks, self-healing and alternative network functions, individual encryption assigned and adapted according to protection time slots, intrusion detection, and two-way authentication and authorization.

An important task is mapping, collecting and composing different parts of the information arena by technical means. Belonging to this task, in addition to cyber space and IT warfare, is the electromagnetic spectrum and electronic warfare. The network defence is dependent upon easy and secure identification of friendly and enemy resources. There must be a determined effort to make this technology secure.

The network defence will never be finished and come to an end. Technology will continuously be developed further and the supporting means be changed. Comparison can be made with the civil development of constantly new versions of software, and also of hardware such as data processors and memories. At all times while the network puzzle is being laid, interfaces between old and new must fit together.

The cognitive arena

On the cognitive arena the battle of brains is being fought. Many battles are finally decided by brainpower and not by muscle power. The battle is extended to the highest strategical and political level and its struggle for “*influence*”. The arena is difficult to apprehend, because its characteristics are abstract. It is about factors like leadership, morals, trust, perception and psychological influence, ability to apply experience and knowledge. Sun Tzu’s advice: *“Know your enemy*” is easy to say but difficult to follow.

Decision superiority is a competitive advantage in the cognitive arena and builds on information superiority from the information arena. Decision superiority refers to situations when the right information is available collectively resulting, as it does, in both better and speedier decisions than those of your enemy, thereby giving you the upper hand. What it is all about, really, is thinking fast and right, basing your decisions on past experience and training.

The cognitive arena is an area hardly ever mentioned when developing Network-Based Defence, but it is of equally great importance. The relation and simultaneous interplay

[28] See footnote No. 24

between all activities on the three arenas must be understood in order to be able to synchronize activities. Understanding this makes network-based warfare *transparent* concerning task, size and composition of forces, other pieces of information, and geography. Speed of command and control superiority is achieved when information superiority can be exchanged for a competitive advantage. *Self-synchronization* is the ability of a well-informed force to organize and synchronize complex warfare activities from the bottom up.

The sum of all participating operators´ knowledge can be added up in the network. In the cognitive arena, opportunities for shared knowledge and an understanding of the management's intention and existing situation and how to handle it are given. This provides an opportunity to synchronize one's own actions with the other players in the network.

Disruptive innovation is here clearly applicable in a field known at least since Sun Tzu's days but which becomes of even greater importance with the emerging Network-Based Defence. What help is there if weapon systems and network and information technology is in perfect condition but man himself fails? Still, the cognitive arena makes special demands. You must get to know your enemy, and not just be able to launch an air assault on the physical arena. You must also *invade your enemy´s brain*, and in so doing make use of power from the two other arenas. It is felt that the cognitive arena is far from being enough understood and developed. With all due deference to information superiority, it must still be said that a higher goal is cognitive superiority.

The road to cognitive superiority has many traps. There are many ways of presenting and understanding messages. Information can be corrupted and in addition to human means modern technology offers additional ways of corruption. Delivering a message, and the receiving and the perception of it can be described with compatibility between the sender and the receiver. A message can be delivered on the physical arena (e.g. a punch on the nose), or on the information arena, or on both in combination. The following examples are limited to delivery on the information arena.

Information can be studied on the transmitting and on the receiving side. Apart from the information itself it must be known who is the sender and who is the receiver. Several conditions are possible on the transmission side. Information can be true, partly true, true said to be false, false said to be true, true or false, false, or without any content at all.

The information can undergo changes on its way to the receiver. It might not at all be received. If it arrives, it will have to pass the cognitive filter of the person who is receiving it. The largest degree of compatibility exists when the content and meaning of the information is the same on both the true sender and the true receiver side, and no changes have been made on the way between the sender and receiver. Time is also important and the information can be delayed, which can make it useless. The information can be disturbed or misunderstood. There is language, technical, classification and other barriers. In international co-operation there are complex organizational and national cultural barriers.

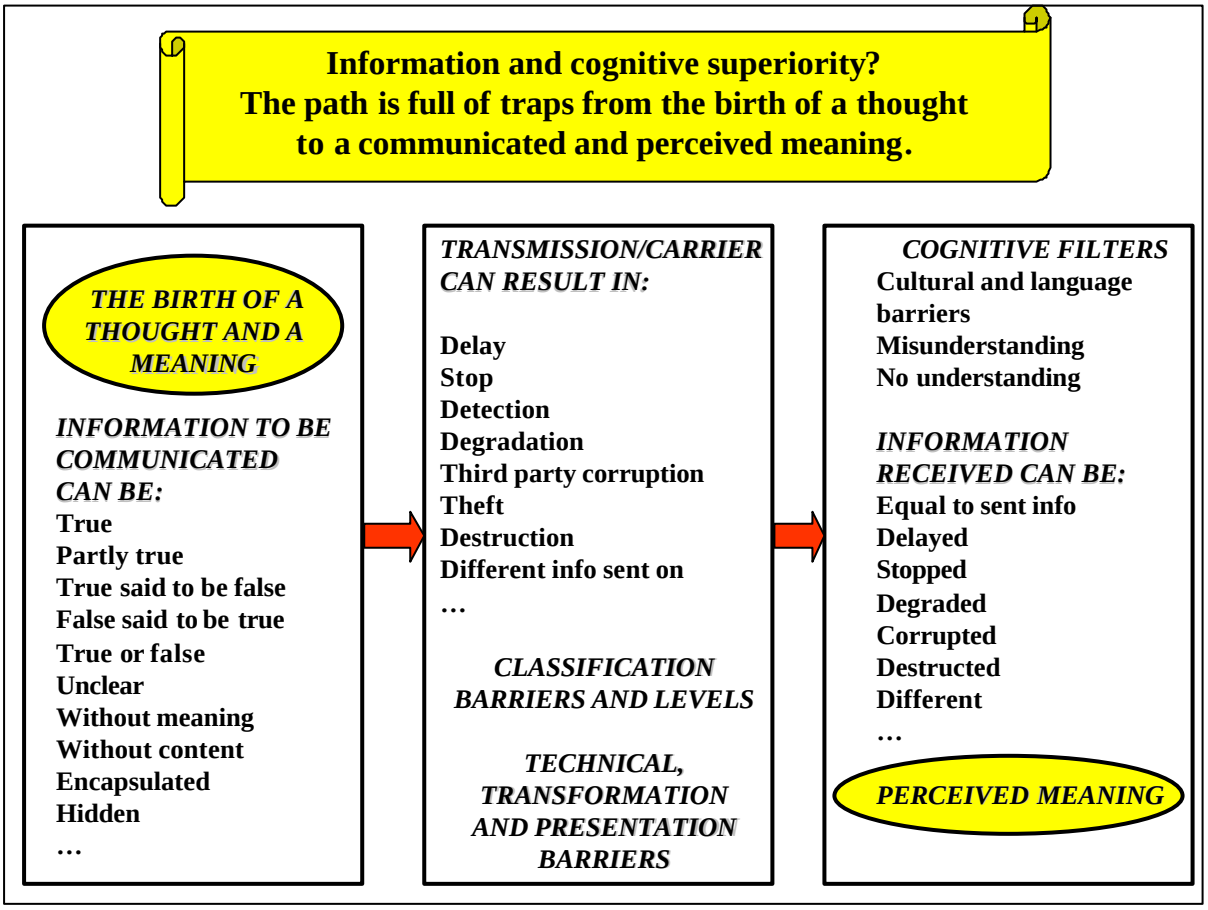
<u>The cognitive arena doctrine</u>

The interplay between military, political and media representatives can lead to unexpected and dramatic results. What kind of rules and responsibility can and should be in force in the cognitive arena, both for protection of and attack on perception? What kind of questions can be so sensitive that one would like to avoid bringing them up? Psychological warfare will be developed using the four parameters. When designed in the right way, it can become

extremely cost efficient for those who understand to put it into practice. The mass media will, at any rate, play a central role in conflicts, and *the power of the media* has many times proved to be stronger than everything else. A mass media presentation reeking of blood can have a high degree of leverage in the information society.

The cognitive arena organisation

The network society may be high fashion and on everybody's lips today. However, the transfer from a hierarchical limiting to a cross-sectoral releasing culture might not always happen as smoothly and easily as might be desired. Asymmetrical information providing information superiority and competitive advantage on a small or large scale is something to be generally safeguarded, just like scarce resources. It can become especially delicate when things begin in earnest. A true network culture builds upon responsibility, trust, delegating, happiness when sharing things with other people, and much more. The organisation must quickly be able to switch between hierarchical and cross-sectoral structures depending on the situation. Will everybody understand their roles and play as well together as they have to? Handing over a task, delegating and making one's leadership easier can be quite tough for those who are filled with the sweetness of their own power.



The cognitive arena personnel

The cognitive arena has its own high standards. Each individual has his or her own world of imagination, uniquely acquired throughout the years. We perceive things in different ways. Thus each individual has his or her own *unique perception or cognitive filter* through which all information passes. This implies that even if the network conveys a shared situational picture it can be perceived in different ways. When leadership responsibility can be distributed based on mission oriented command and control, and the stress is severe due to

high pace and demand to be ahead in the OODA-loop, it is easy to act in a wrong way. The risk is largest except in previously well-rehearsed situations where relevant Rules of Engagement have already been established.

The ability to make quick use of an upcoming Window of Opportunity (Opportunity Space) is therefore crucial. A football match is a metaphor on a small scale. It is a matter of being the most speedy and intelligent player in order to win in the network society. To come in a close second just does not count. It is not just a matter of achieving information superiority but also of achieving cognitive superiority. In the future Network-Based Defence, a great number of those involved will be responsible or jointly responsible for decisions. Heavy demands are made on knowledge and capability to rapidly grasp courses of events in a complex overall picture. The elements of the OODA-loop are more and more melting together and disappearing when the network defence becomes more efficient and the pace increases. This also closes the gap between "Sensor and Shooter".

In theory "the same situational picture" leads to "the same situational perception and interpretation". In practice peoples' different cognitive filters can screw things up. "The same situational picture" can lead to "different situational perceptions and interpretations" and thus to different reactions.

In practice it is also difficult to achieve "the same absolute clear situational picture", especially in high tempo. Such difficulties and differences are actually the foundation of human acting on markets, for example the trading of shares. Trade exists when perspectives are different: someone thinks it is good to buy and someone else thinks the opposite – it is good to sell. Without different perspectives there would be no such trading.

The cognitive arena technology

On the cognitive arena questions concerning technology are about adaptation of technology to human needs, conditions and behaviour. Technology must be easily workable, and conflicts between users and systems must be as low as possible. Information should be presented in as clear and comprehensible a way as possible. Time-critical and other prioritised information must be clear. Underlying computer programs must be easy to handle. Sophisticated automatic means for situation recognition and for decision support will be needed, but there must be a balance between what man and what machine can do and does.

Challenges

A gigantic task

Network-Based Defence is easy to say but difficult to achieve. It is a huge task not easily realized. So far the Network-Based Defence builds almost entirely on abstract concepts, and it will take a long time to implement the ideas more fully. A period of several decades will probably not be enough, as there are going to be economic, technical, personnel and other limitations, and an inheritance within each of the four parameters to work on. The main problem might not be technical but rather financial and especially human as the transformation involves a change of culture.

There will be two major principles: working top down, and working bottom up. The top-down perspective or the view from above starts with an overview of the whole defence and the new landscape and architecture. From an overall strategy a number of directions towards more detailed compositions will be tried. The bottom-up or grass-root perspective starts with the

individual components of the defence such as soldiers and platforms. Questions will be asked how these could be interconnected in a smart way and what the individual interfaces should look like. Both perspectives are valid and need working procedures and will generate practical cases how to build the network.

In the future the Swedish Network-Based Defence network is thought to be able to operate in three ways:

- Swedish military Network-Based Defence stand-alone
- Swedish military Network-Based Defence together with other nations' military networks
- Swedish military Network-Based Defence together with civil networks

In order to be able to make valuable extensions of the network it is important to look for appropriate physical and logical interoperability and interconnections with other networks. This must be considered continuously throughout the development.

The "Crisis Power"

The network should act as a driving force for the four fundamental tasks of the Swedish Armed Forces[29]:

- To defend against armed attack
- To monitor and assert territorial integrity in peacetime and war
- To make resources available for international peace-support and humanitarian missions
- To support the community continually in times of severe strains on society in peace-time

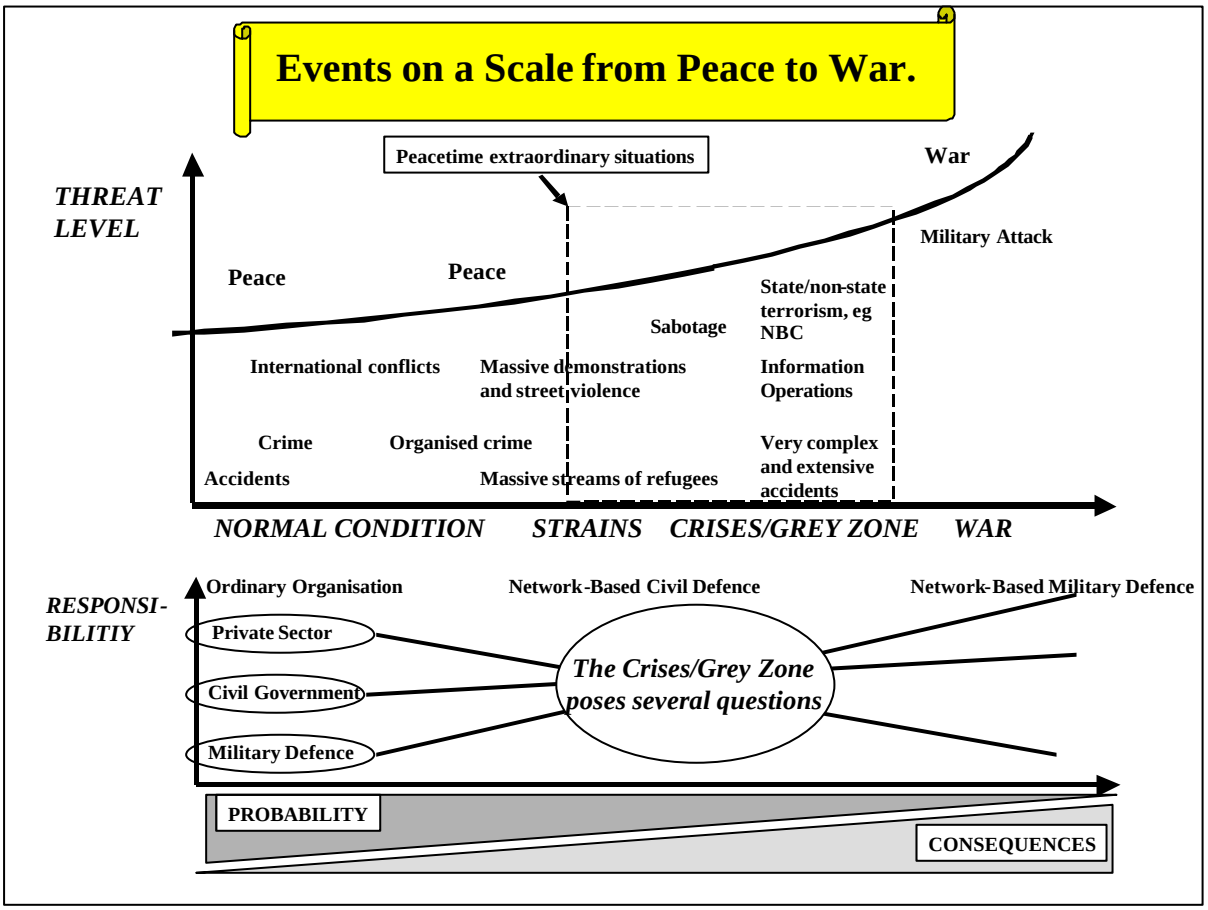
Thus the force engine must also attain interoperability and joint action between Swedish and other countries' forces and systems working within the commitments within the *European Union*, NATO's *Partnership for Peace* and a future multinational network defence. Co-operation between the defence and the civil authorities during grey-zone conditions in between peace and war must also be accomplished. For that reason – but not only for that reason – the civil authorities must also develop a network between themselves – a *Network-Based Civil Defence* for crisis management. In times of war we used to talk about *The Military Power*. In times of crisis we need to add *The Crisis Power*. It can serve as the operational part of the *Swedish Emergency Management Agency*[30] and be organised by forces from the "blue-light authorities" (police, fire brigades, ambulance, rescue brigades, etc), Home Guard personnel, the security police and intelligence units, special resources and expertise within *Swedish Armed Forces* and *The Swedish Defence Research Agency*, and possibly others, all of them under civil leadership.

A special task for the Crisis Power concerns the emerging terrorism all over the world. In particular the kind of terrorism that is aimed at weak civil targets, such as vital parts of the technical infrastructure (electric power and energy systems, computer and telecommunication systems, transportation systems and similar vital technical systems) and which completely defies our military defence effort. It is the most serious threat today, and it appears at the

[29] *Facts and Figures, Swedish Defence 2001-2002 on the Internet*, http://www.mil.se/article.php?id=1672
[30] English translation of *Krisberedskapsmyndigheten, KBM*

intersection of advanced criminality and war. If we are not capable of counterchecking it, it can increase in the future. We must now develop a preparedness to counter the five big terrorist threats:

- Attack with explosives and bombs transported by vehicles, ships, aircraft (conventional weapons)
- Cyber attack on the technical infrastructure; that is against electric power, computer and telecommunication systems and how this can intensify its effects on the other four (weapons of mass disruption)
- Attack with chemical agents (weapons of mass destruction)
- Attack with biological agents (weapons of mass destruction)
- Attack with radioactive bombs and improvised or stolen nuclear weapons (weapons of mass destruction)



Overall requisites and questions to solve

Some of the overall requisites and potential problems that can be foreseen will be mentioned below. The reason is that already from the beginning it is important to identify them and to establish strategies and action plans how to deal with them if and when they appear. In such a way the defence can more rapidly be guided on to the road towards the Network-Based Defence and can avoid ending up in difficulties at later stages.

The working climate must be able to encourage innovations breaking up traditional thinking. However, there is a risk that developments continue too much in centralised traditional

patterns and channels without making use of the wide working network that ought to shape progress.

On the one hand we will certainly benefit from failures on the road towards the Network-Based Defence. The reason is that such failures will teach us a lot, show us limitations and guide us further. On the other hand, if we keep on working too much in a traditional stove-pipe fashion, failures will involve a risk that in the future one will talk about a bursting defence bubble in the same way as one talked about the burst of the IT- and telecom bubble.

Some overall requisites are as follows:

- The significance to create a new culture, breaking traditional isolation and making cross-section bonds between land, naval and air power and in between different fields of activities. Creating new forms of jointness, including Government and perhaps even some parts of the private sector (e.g. NGO, humanitarian relief). Jointness is imperative in a complex world.

- The significance of constantly developing, testing and training the defence further, nationally and internationally, supported by the network.

- The need for an understanding of disruptive innovation - breaking traditional work, for instance new organisational roles and responsibilities.

- The need for an understanding and knowledge concerning development of Network-Based Defence on the information and cognitive arenas in harmony with the physical arena. Necessity to create an *understanding of the interplay between the three arenas* and different fields of knowledge. One important method to achieve this is *job rotation* between jobs on the three arenas.

- The need for understanding that the battle on the information arena (information operations and information warfare) and the battle on the cognitive arena are crucial for the outcome of the battle on the physical arena. Thus there is a need for an understanding of new creative thoughts that must be added.

- Management of co-operation between Swedish and other countries' forces and systems.

- Management of grey-zone situations involving the five big terrorist threats.

- The significance of having an overall picture throughout the development.

- The need for mutual trust and understanding between different actors who jointly are building the new defence (buyers and customers, technicians and military personnel, innovators and managers, government and enterprise etc).

- The need for an understanding of the fundamental significance of human behaviour.

- In the network defence, pace will be stepped up, leading to higher risk of failure, which must be manageable.

Problems concerning vulnerability and security:

- The need to create *trustworthiness*
- In the Network-Based Defence information is *Ground Zero*
- Vulnerability of the network of networks and key nodes
- The significance of secure and robust communication and interoperability
- The threat picture of the Network-Based Defence needs to be treated
- The dependence on the vulnerable civil technical infrastructure and its impact on military/defence capability
- Limited supply of private telecommunication networks, risk of overload and problems to get priority, limited space of frequencies, telecommunication conflicts
- Fear of disseminating sensitive information in computer networks having possible "life-and-death" implications
- Risk of falling into the hands of insiders

Risk of wrong planning causing additional time, cost, and reduced defence capability:

- Risk of basic misguided ventures requiring starting all over again. Basic deficiencies in security work, badly arranged displays making it more difficult to use the network.
- Risk of over-confidence in technology.
- Risk of over-confidence that developments will lead to rapid introduction of the Network-Based Defence.
- The planned increase of defence capabilities can be inhibited by lack of network-based technology investments.
- The cost of being at the forefront of developments must be weighed against the benefit of gaining experience from others.

Measuring the degree of Network-Based Defence

When is the Network-Based Defence ready to be tested? An essential question is thus how the degree of the Network-Based Defence can be measured. It will be necessary to develop methods in order to analyse and evaluate network-based capabilities. If one does not develop measurement instruments, the conception of the whole defence business will be suspended. Some essential factors, which ought to be measured, are:

- Each unit’s degree of interoperability

- The number of nodes within each kind of network service and connections to other service nodes
- Multi-services and display of information fusion
- The degree of self-synchronization among the task forces
- The network robustness and power to resist threats
- The speed of the OODA-loop
- The speed of the whole network engine

Network interoperability applies in every sense (namely the four parameters and the three arenas) to a battle component (which can be a platform, force unit, sensor, fire power etc). There is a tradition measuring the value of a battle force on the physical arena. It will be much harder – but necessary – to measure it on the information and cognitive arenas.

One factor to measure is the number of acceptable interoperable battle units in comparison with the total number of units. Communication is one of the requirements for interoperability. A characteristic of Network-Based Defence must be the value of the additional contribution of a certain property achievable from available components. One example of adding information is sensors, each one contributing to a clearer and better picture of a situation.

The general public learnt about the Internet when a certain critical number of users the world over was reached. Since then the value of the Internet has increased exponentially. The development of the Network-Based Defence might follow a similar pattern in the future. It is possible that when the critical number is reached, not only in our country but also in a large part of our surrounding world, international defence co-operation can accelerate in a revolutionary way. Within our country societal support in grey-zone situations can become far more efficient when the interoperable network reaches out over civil cross-sectoral functions. Internationally there is a need for grey zones for the Red Cross and UNHCR. A dream in the long run is a global observation and intelligence network under UN auspices with the ability to detect disturbance and conflict with the help of high fidelity. Detection should take place at the earliest possible moment so that by using peaceful measures we could prevent matters from developing into more serious situations.

Concluding words

Network-Based Defence – latest fashion or a strategic step into the future? This article concludes that the answer is that the strategic step into the future has been taken. There is no turning back. Major General Svante Bergh puts it this way:

"*The Network-Based Defence is a consequence of the information technology development in society and cannot be excluded by option. It builds to a great extent on the development of civil telecommunications. As this is a strong Swedish sector, we should take the lead and contribute to the superiority of the free world.*"

The purpose of this article is to interpret and convey parts of today's thinking, to add some thoughts of my own, to contribute with a structure, and to stimulate debate and further development. It will be needed. The task ahead is a giant one and involves a preparation for a

new culture. The world is changing and the defence likewise. There is a need for mobilization for a new era[31]. The challenges are here to be met. The Network-Based Defence must be built with knowledge at a reasonable pace. Opinions about the steps to be taken may vary along the way. That will provide vitality, because if everybody thinks in the same way, there will be no progress.

Sooner or later we will have a Network-Based Defence in co-operation with the civil sector and with the democratic nations of the world. My hope is that this will mitigate and limit conflicts in the world and thus lead to a more peaceful development in the future. This is our great goal.

Acknowledgements
I wish to thank Dr. Daniel T. Kuehl, National Defense University, Washington DC, for his valuable comments and review of my article and Mr. Bo Grawe for his valuable language review. My sincere thanks also go to my wife Margareta Wik von Bornstedt for her kind support and encouragement.

ooOoo

[31] See footnote No. 16