Backgrounds and Principles of Network-Centric Warfare

Lt.Col (G.S.) Sakari Ahvenainen (Ret., Finnish Army)

National Defence College November 2003
Course of Network-Centric Warfare for Post-Graduate Students

Table of Content

Backgrounds and Principles of Network-Centric Warfare

1. Introduction: What is NCW?

This paper analyses some backgrounds and main principles of Network-Centric Warfare (NCW) mostly as a United States of America (USA) military notion as in the end of 2003.

Warfare takes on the characteristics of its Age. NCW continues this trend - it is the military response to both the challenges and the opportunities created by the Information Age.[1]

NCW is a operational concept that makes information superiority possible, it creates increased combat power by networking sensors, leaders and shooters to get shared situational awareness, increased decision making speed, increased tempo, increased lethality, increased survivability and increased self-synchronisation. It is also essential to separate sensors and shooters.

NCW is warfare. To understand what is different in NCW and to be able to understand the increased combat power that is associated with it, one has to concentrate on three, four levels and on their interactions. These three levels are information level, cognitive level and physical level. The fourth level is the social level.

The Physical Domain[2]
The physical domain is the place where the situation the military seeks to influence exists. It is the domain where strike, protect, and manoeuver take place across the environments of ground, sea, air, and space. It is the domain where physical platforms and the communications networks that connect them reside. Comparatively, the elements of domain are, the easiest to measure, and consequently, combat power has traditionally been measured primarily in this domain. In our analyses and models, the physical domain is characterized as reality, or ground truth. Important metrics for measuring combat power in this domain include lethality and survivability.

This domain is concrete, touchable. We can move communication systems, units, fire power etc. This is the newest, most changed area of the warfare. The physical domain is one for all. Its elements are our own troops and systems, enemy troops and its systems, their common environment (terrain, weather, time, electromagnetic spectrum...), third parties, neutrals, world public opinion etc. In NCW the core of the physical domain is to network the force robust and seamless.

The Information Domain
The information domain is where information is created, manipulated, and shared. It the domain that facilitates the communication of information among war fighters. It is the domain where the command and control of modern military forces is communicated, with commander's intent is conveyed. There is for instance the transmitted information of the communication systems, data fusion and computer data and program. Without ones own sensory perception, all information is transmitted to the leaders through information domain. This domain is already somewhat unconcrete. What is information? One can still see it, for instance in the computer screen. Information is partly movable (data and information) and partly impossible to move, it is the knowledge, understanding and wisdom in a human brains. This domain is partly old (human information processing) and partly new (technological information processing). Information domain can be multiple. We can have different information on the same situation: company, battalion, brigade, division, corps and theater information on a specific event. In NCW the core of information domain is to collect information, process information, distribute information and to store information.

The Cognitive Domain
The cognitive domain is in the minds of the participants. This is the place where perceptions, awareness, understanding, beliefs, and values reside and where, as a result sense making, decisions are made. This is the domain where many battles and wars are actually won and lost. This is the domain of intangibles: leadership, morale, unit cohesion, level of training and experience, situational awareness, and public opinion. This is the domain where an understanding of a commander's intent, doctrine, tactics, techniques, a procedures reside. We can not move wisdom, leadership, moral or cohesion. This is the most traditional area of warfare. The cognitive domain is fully personal, private. At the same situations, at the same information, different persons can have quite different perceptions. Even same words have different meaning for different persons. This is because their interpreting information, their brains (history, education, mood...) is always different at some decree. In NCW the core of cognitive domain is to develop and distribute superior situational awareness, common understanding of the commanders intent and to synchronise operations and activities.

The fourth domain is the social domain. Here we have the cooperations of organizations, even coalition partners, different cultures and religions, the world public opinion. This is very, very hard domain to change. It takes many decades, a century, maybe more. This is the base of human acting. Like the cognitive domain, this is dispersed. In NCW the core of social domain is cooperation of organizations and cultures.

The fundamental characteristics of NCW can be described with a set of integrated linkage hypotheses that can be organized into three classes:
- Hypotheses of the first class deal with relationships among degree of networking, information sharing, improved awareness, improved information quality and shared situational awareness
- Hypotheses of the second class include those that involve the relationships between shared situational awareness and syncronization
- The third class of hypotheses involves the link between syncronization and mission effectiveness.[3]

2. Backgrounds of NCW

2.1. Information and information technology

Information context of warfare has increased. There are three historical levels of information use in warfare.[4] First was the time of mass. Basic question was: Where is the main body of the armed forces of the adversary?. Lots of resources and some information was needed. This is an indirect way of influence. Very elementary information technology is needed: Maps to navigate, messengers to delivery messages, spies to uncover secrets, leaders to make decisions.

The second phase was or is the time of precision. The adversary is investigated as a system. What are the parts of the adversary and what kind of connection the parts have? Which parts have the most influence on the enemy as a system? Resources and information are needed about on the equal base. This is still an indirect way of influence. This is the time on precision weapons and the time of information warfare. Sophisticated information technology is needed: Navigation systems to geolocate elements of warfare, communication systems (radios, telecommunication systems), sophisticated intelligence and surveillance systems and computers to aid decision making.

The third phase is or will be the time of the decision maker. The basic questions are who is the decision maker, what kind of network he/she has, what does he/she want, what are his/her values, education, history, preferences and when does the decision maker consider the war lost. Lots of information is needed, but only limited amount of other resources. This is a direct way of influence and the time of network based warfare. Networks are needed to get all the information that one has to have to be able to influence on the decision maker. Networks of intelligence systems, networks of decision makers and their computers, networks of people, networks of geolocating satellites, so networks of networks.

So NCW means increased information influence in warfare (ref. Information Superiority). Refer also the Sun Tzu's possibilities and some 2000 year later Napoleon's or Clausewitz's possibilities to collect, process and distribute information and the possibilities now, 200 years after Clausewitz. And how we see, that these possibilities will develop during the next 20 years.

2.2. Changes in Technology, in Societies and in Warfare

NCW and networks are important in warfare for multiple of reasons. First new information technology (IT) changed the societies in the west in the 1980's and 1990's. IT brought new systems to the military technology: computer based intelligence-, surveillance-, command and control (C2) and communications systems and precision guided weapons, where the computer and the information is a central part of the weapon.

Secondly international third sector organizations and their networks e.g. environmental movement, shape the international politics, economy and even warfare. One example of the latest is the anti land mine movement.

Thirdly it is harder and harder to imagine any activity without taking into consideration the global Internet and its smaller notions, computer networks inside firms (intranet) and between them (extranet). Internet is also important in warfare, e.g. tactical internet and strategic use of civilian internet.

Fourthly single computer are more and more networked and smart weapons actually embedded computers. Advanced mines communicate with each other and with their sensors and optimize their

actions comprehensively. So they are intelligent, communicating, precision effecting and networked.

Fifth, if something becomes important in warfare, it become target of attack and object of defence. This has happened for information and is happening for networks.

Sixthly, there has been new interpretations concerning networks theory, even a new paradigm, fundamental new description of networks. It means scale free networks. Internet is its principal application. One principle of scale free networks is "Winner takes all". Can there be more significant application in the economy of in the warfare? Ref. Microsoft, Google and Nokia.[5]

2.3. Hierarchy and fully connected network

There are different kinds of network shapes: tree or pyramid (hierarchy, H), chain, loop, star and fully connected network (FCN). Lets look at the differences of hierarchy and the most networked net, the fully connected network. This comparisons gives one an idea what happens when hierarchy is moving towards more networked organizations. Both the hierarchy (H) and FCN are at the opposite end of organisational systems, which seldom exists as a stand alone application.

Both consists of hubs and connections between the hubs. These two network modes have not other resemblance.

Differences are numerous:
(1) FCN has less command and control levels, only one. So it is self organizing. This means potentially higher command and control tempo.
(2) The values of the connections are different. Higher connections in H influence on many connections. So the higher connections in H are targeted more probably. In FCN every connections has the same value, it is more robust. This is an important counteraction in C2W.
(3) The amount of connections are different. H manages with less connections. So the use of FCN is a resource and communication technology issue.
(4) FCN has more capacity to transmit information, or the information can be versatile or the same information can be transmitted quicker.
(5) Less connections per hub to hub information transfer is needed in FCN. So the transmission is quicker. This is especially important if there is a need to use the whole information potential of the network. This means, that FCN is better in a complex situation, where one needs more information.
(6) The power and the control is greater in H. In FCN there is no control at all, so it is very "democratic". In H one need always ones superior, one or more, to communicate with ones neighbour.
(7) The order is more structural in H. Actually, FCN is a chaos. So leadership and power is more problematic in FCN. So to move towards FCN besides communication and information problems one has more leadership and authority problems.
(8) As a organizational structure FCN is flexible. It is easy to add and to remove a component from FCN. In H one usually has to restructure many parts and connections of the system to reorganize it.

2.4. When is Network better?

So according to the previous chapter, more networked networks are less vulnerable, they can use more easily the whole information in the network, they are more democratic (more equal, harder target in war), they are quicker, they can manage more complex information, it is more complex situations, and they are as an organizational model more adjustable. But they are more demanding

in areas of leadership (people), rule of complexity, power and authority and communication and information technology.

So, when is network better than hierarchy? When information technology and command and control has reached a certain, networked level, or there is a need for a quicker and/or many-sided information or good survivability. Network is better in complex, dynamic situations and in open systems. Thus hierarchy is better in simple, static situations and in closed systems. Warfare is none of those. So if one gets networks to function (people, technology, tactics, etc.), they are "natural" organizations of warfare. Moving from hierarchy towards FCNs is a holistic and a big change.

2.5. Some special features of networks

Networks makes it possible (a) to increase tempo, when the levels of command and control are decreasing and information is quicker to reach (b) to distribute any activity to the whole area of network, because in the net one can get any place that is in the net, (c) to use information more efficiently when information is distributed to all in the net who need it and the whole information in the network is for everybody to use and (d) together with the information superiority to get results with less resources because information replaces other resources.

Network and net based activity optimizes specialised organization in dynamic and complex organizations. Cheaper and more efficient information technology makes it possible to co-ordinate complex, dynamic and specialised organization and its parts with reasonable costs.[6] So the starting points to use networks are specialised organization and their increased efficience and cheaper information technology to co-ordinate specialised organizations and their parts.

The responsibility to co-ordinate is moving from the managers to the subordinates. It is possible for every member of the organization to get information that was previously only in the hands of the managers. Managers are not any more the first information source. The structure of the power is transforming through distributed information. This means that the base of leadership is transforming.

Call for specialization and to concentrate on ones key knowledge or skills will bring up precision craftsmanship and networking. Those activities that are not the key knowledge or skills will be outsourced and they will network outside the original organization and also they will network the original organization outside networks. So specialization and outsourcing are starting points for networking.

Networks are light dynamic organization. One can easily add new, valuable structures into networks without changing the whole structure and one can also easily cancel or get rid of what is not functioning in a network.[7] This is very important when one speaks about agility and organizations. Hierarchy is a burden in a change.

The power is moving over to the networks. There will be a virtual, interdependent and abstract highest power structure that is above the political, economical, media and financial power and that is not controlled by any single entity.[8] This is the democratic dimension of the networks. It is more complicated to use the power in the era of networks. There will be new type of coalitions that will be born and break suddenly. To respond to this kinds of coalition the hierarchy is not at its best.

"Genuine" communication is interaction and interaction is network based.[9] So there is a essential connection between network, interaction and communication.

Only in networks can the majority of multiple components survive whole.[10] The hierarchy unites the thinking in a negative way during a transformation when there is a need for innovations. Diversity is a central feature of innovation and innovation is a central feature for sucsess in the future, in a dynamic environment. So the network has an essential connection to the innovation and to the sucsess in a dynamic environment. Network based activity is also ensurance against bad decisions when one gets vertisale knowledge outside superiors and subordinates.

The core of network activity is cooperation, the horizontal level. There will be an important horizontal level beside the traditional military vertical level. At he highest level it means cooperation between the army, navy, air force etc. and for instance in the army the importance of the department of army in respect to the branch of services. The core of the horizontal level are the structures and standards that enable the cooperation, the sharing of information in the areas of communication, command and control, intelligence and data processing.

With the horizontal level arises the importance of united process control, information and its flow, the add on value of different actors in the net, commitment of the actors to the network, parallelism of the goals of the actors (win- win situations), learning, forums that are used for developing strategies, trust and distribution of work and responsibilities.[11]

The power of the network is in its ability to process information and knowledge and that it lacks the valuable point targets that are important for command and control warfare. It weakness is in its need for continuous and broad ability to communicate[12] and in its need for common information, for common data bases.

2.6. Conclusions

NCW is first the use of new communication and information technological possibilities, secondly new doctrine, the new idea to make war, and thirdly new organizations, that use the most of the possibilities of the new technology and the new doctrine. Also the increased complexity of the world and its need for more information and knowledge emphasizes the use of networks.

More networked organizations decrease also the number of organizational levels and create direct connections to the source of information and increase so the tempo of the operations. The tempo (time) again is a central key for victory, especially if the organization has a competitor in business or in sport or an adversary in war.

On the technological side of the NCW communication systems and information systems that use communication systems are the key factors. Their robustness, flexibility and interoperability are the technological key factors of the NCW.

More networked organizations are more adapted to the complex and dynamic situations of the modern warfare. New technology is making it possible to use more networked organization in the lower levels of warfare. Still: The full use of networked activity is possible only by a holistic and demanding transformation.

NCW is a permanent change like its predecessor the information warfare. NCW is in a way also just a better and broader version of IW.

3. Main Principles of NCW

3.1. Logic of NCW

The logic of NCW is as follows: The base is new information technology that makes it possible to share information. This means networked sensors, leaders and shooters, it is robustly networked force. Shared information makes it possible to have better shared information, to have shared situational awareness and to be able to collaborate. They can be transformed to self-synchronization, boldness, tempo and speed of manoeuver. At the end this means precision application of force, precision effects and mission effectiveness.[13]

3.2. A List of main principles

Main principles of NCW are according to previous chapter:
- Quality of organic information and individual situational awareness
- Robustly networked forces: Swarming, distributed and networked force
- Robustly networked forces: Communication networks
- Information sharing: The secret of the force of warfare
- Information sharing: Metcalf's Law
- Quality of shared information: Information Superiority
- Quality of shared information: More with less
- Shared situational awareness
- Collaboration and self-synchronization
- Tempo and speed of maneuver
- Precision application of force and effects and
- Mission effectiveness.

Next these principles are dealt with in more detail below.

3.3. Quality of organic information and individual situational awareness

Quality of organic information can have three views:
1. Quality inside all areas of information
2. Quality in relationship to the enemy and ones tactical needs of information
3. Quality in relationship to ones organization and
4. Quality in relationship to the information itself.

First there is four kinds of information, that has to have quality. John Boyd defines the OODA- loop as a command and control structure: loops of observing, orientation, decision and action[14]. When the OODA- loop in expanded from command and control to information based universal object-oriented acting, it has following parts (in brackets OODA- loop parts)

1. Input- or new information (Observation);
2. System- information, information that interprets the input- information. This section is extensive: genetic system information, language and cultural information, other learned information (profession, mission, up-to date, metadata about ones network), ones inner mental models and values, computer programs. (Orientation)
3. Output- information (Decision);

4. Ability, know-how to put the decision in to actions: skill and information how to do it (Action) and resources: time, energy, raw materials, tools, other people (ones organization and authority, outside networks).
5. Will to do the decided action.
6. Courage to do the decided action.
7. Endurance to do the decided action.

Thus, four kinds of information is needed to act: First input information: information about own troops, about the enemy and about the common environment. Secondly one needs system information to interpret input information. Thirdly one needs good decision, output information and lastly one needs know-how information, how to do the decided action.

Secondly, in the quality of organic information, one needs better quality information than the enemy. And this also in respect to ones own need of information. To have better quality information in respect to the enemy there is the information itself, attack against enemy's information and defence of ones information against the enemy's attack of ones information.

Thirdly, best quality information one has if the information one gets is the best ones organization can provide. For this one needs communication resources to the best source of ones organization's information. One needs a network, that is best in every action, at every information.

Fourthly, quality of information (inside itself) is measured by:[15]
- completeness (is it all there?)
- correctness (is the information according to what they are supposed to present?)
- currency (??)
- accuracy (is the precision of the information as the user suppose?)
- consistency (is the information same everywhere?)
- relevance (has the information meaning for the situation?)
- timeliness (is the information fresh enough according to ones needs?) and
- information assurance (is the information reliable?)

3.4. Robustly networked forces: Swarming, distributed and networked force

Swarming is one of four type of doctrine to use military force. The others are chaotic melee, brute force massing and nimble manoeuver.[16] Swarming can be realized by force or by fire.[17]

Swarming has two fundamental requirements. First large number of small units of manoeuver that are tightly internetted. Secondly there have to be sensory organization for top sight view. [18] Both of these two are connected to NCW.

Swarming can be a way for relative small, mobile, internetted forces, operating with superior top sight, to optimize military effectiveness, even when the balance of forces runs against the swarmers.[19]

There were dramatic consequences when US military armed its special forces in a simulation exercises during 1994. 7th Special Force Group was defending Saudi-Arabia with XVIII Airborne Corps. First the special force was used exclusively for reconnaissance as in Desert Storm 1991. Then the commander of the special force asked if his small, dispersed troops could be used for strike designation tasks as well. The results were both immediate and astonishing. Heavily armoured invaders were routinely defeated and XVIII casualties dropped over 80 percent.[20]

This experience led to new use of special forces in Kosovo and Afghanistan, although not so intensively in Irak 2003!

The hierarchical system works mainly from up to bottom. The superior tells and the subordinate obeys. NCW works from bottom up. In swarmed, small and mobile units information comes from bottom and from neighbours and neighbours self-synchronize themselves to this information. This principle need a special kind of information technology and communication tactics to work. One has to be able to recognize one's neighbours and to be able to communicate with them. This can be a problem when multiple military services cooperate on the same tactical area or when civil-military cooperation is needed.

3.5. Robustly networked forces: Communication system

NCW is first based on robustly networked, dispersed and distributed forces. So it is not beatable at any one place, at the centre of gravity. This principle is evident in the internet as a distributed communication network, that is capable to survive a nuclear war.

The shared situational picture makes its impossible to defeat a distributed force by one piece at the time. Cooperation forms also a concentrated effect out of the distributed force. First principle, distributed force is already introduced by the guerilla war. The second principle, real time cooperation of the distributed force, has been possible only after communication, information and command and control technology, that makes it possible to share information quickly over distances and across organizations.

So, at the focus of NCW there is integrated communication, information, intelligence and command and control systems, that makes distributed actions possible. These elements, that are connected to the information, are the very centre of NCW. Distribution means distribution of command and control, sensors, shooters and effects over the whole network and the integrated use of these distributed resources.

Better communication and information technology of the information age will enable continuous command and control instead of cyclical command and control of the Industrial age.[21] This means that instead of sending only fully processed order or other product of command and control, one can send pre-orders and change them continuously in the process. This means that command and control processes at different levels can be compressed and merged. This means higher tempo and more agile command and control. It means also continuous and intensive communication.

3.6. Information sharing: The secret of the Force of warfare:

The ability to share information is key to being able to develop a state of shared awareness, as well as being able to collaborate and/or synchronize.[22]

It is the heart of NCW . For it first a horizontal level is needed beside the hierarchical vertical level to share information across different organization and secondly new information technology is needed. At the base one has robustly networked military power. In Finland YVI I and II, message terminal switch system (Kesla), OPJO/JOTI- command and control system and integrated G3 systems work at this level.

What will happen when we share information? An example: If Finnish Hornets (F-18) had a system to share information with each other, it is the targets it sees with its radar, its armament status etc.,

this could happen: If a Hornet locks its radar to target, other Hornet in air and anti aircraft artillery and missile systems on the grounds get this information, so they do not shoot the same targets. This is an important precondition of Lancaster Square Law (LSL). It requires among other things that no unit shoots the same target and if a target is destroyed, no one shoots it anymore [23].

So to use Lancaster Square Law one have to share information. At the tactical level the one who can use LSL has a decisive advantage.[24] This understanding of the meaning of quantity in warfare at the tactical level is one of the principal scientific facts of warfare.

What more is possible? One can see behind one's radar coverage (further or the tail section) and one can see the air situation without the use of one's radar or radio.

To share information and knowledge means it at every level of warfare: the global actors, counties inside a coalition, one's own security actors in a one's country, the services inside one's armed forces, branch of military service in one's military service, different tactical actors at the battlefield and so on. Common processes and standards become important, holistic interoperability. At the highest level only one standard is possible, the global: Intel, Microsoft, internet... Network theory at its best: The winner takes it all[25].

Sharing information can also mean connecting the information of many platforms or sensors. For instance RC-135 aircraft has been traditionally used as a single unit. This means that to intercept a signal takes time and it is situation dependent. If the signal is on just a short time, its geolocating is especially difficult. But when one combines other signal intelligence sources or other RC-135 platforms one gets following benefits:
(a) even a short signal is enough for geolocating when there are multiple concurrent directions. With one platform the area of a short signal is pencil- like form for instance 200 kilometres long and 10 kilometres wide. With two platforms the area can be 10 * 10 square kilometres, 20 times less.
(b) the intercept probability increases when there is multiple intercept at different locations, which means that many intercepts that had been disregarded as unreliable or that had not been heard at all by one platform, are now reliable and are used as information.
(c) if there is more than one platform there is reserve for trouble etc. situations.

NCW means increased information reach (global) and increased information richness (more bandwidth).[26]

Shared information means sharing the status and especially position of ones own forces. This shared information is one base for cooperation and self-synchronization.

Sharing knowledge is important when humans work together in a large organizations. Training and doctrine have been employed througout history to develop a high degree of shared knowledge among troops so that they will understand and react to situations in a predictable way.[27]

3.7. Information sharing: Metcalf's Law

The power of distribution of information in the previous chapter is based partly on the Metcalfe's Law. According to it the expenses of the networks increase linearly but the benefits of the network exponentially. Expenses are the hubs of the networks (N) and benefits the connections of the network ($N*(N-1) = N^2 - N$). The problem is of cause how to really take advantage of the increased connections. Refer for instance internet. Its huge information content is of no use, if there is no way to find the information, that one needs particularly in a problem at hand. Here the search engines

are the first cure, but one still needs a more sophisticated methods of information search. One needs precision information.

The value of the connections of the network is dependant on the content of the information exchange that the net makes possible, their quality and timeliness, on the add-on values of the users and on the add-on value that the logic that the network makes possible.[28]

3.8. Quality of shared information: Information Superiority

The new rule of NCW is first to fight for information superiority.[29]

What is information superiority? It is a relative advantage that consist of ones information systems and of the enemy's information systems. On both side these information systems include use of information and information systems, attack against the other side's information systems and defence on one's information systems against the other side's information attack.[30]

Information superiority means also better information in respect to ones information needs in regard to ones tactics etc.[31] Information needs are very much tactic- dependant, ref. dispersed guerilla war or high intensive maneuver war. This is an application of the fact, that warfare should be a holistic enterprise in which for instance ones tactics, technology, people and information needs support each other.

Information superiority in NCW means, that the advantage in information is created by the new information technology and especially by networking the elements of warfare: sensors, shooters and leaders. First the new information technology makes it possible to transmit information longer distances, even globally and secondly to transmit more wide-band information.

Longer distances mean satellites, long distance optical cable, information systems in air crafts and in UAVs and new automatic areal communication systems (MSE, YVI I and II). Longer distances mean also networking tactical and theater elements of warfare and even tactical and national (global) elements of warfare.

More wide-band information means fast internet connections, video conferencing, data transmit, fax, transmitting UAV's video and signal information, controlling UAVs and UCAV's and ??

Information as an information superiority transforms in NCW to the superiority in the battlefields (see chapter The logic of NCW ??). New information age technology make it possible to move information instead of people, to conduct distributed operations and substitute information for mass[32].

Then one has to have effective information attack systems (computer network attack, electronic warfare) and effective information defence systems against the enemy's information attack. ??

3.9. Quality of shared information: More with less

Information warfare has introduced the principle "more with less". For instance anti tank warfare with artillery. It is a fact that it is not wise to shoot tanks with conventional indirect fire. It is because (a) one need a direct hit to have an effect on a tank, (b) a tank is a small target (about 20 square metres) and a artillery shell is spread over 10.000 square metres at ranges of 10 - 15 kilometres. If there is 1 to 3 tanks in a target area of one artillery piece, the expected value to hit a

tank is 0,006 - 0,002. To get one hit one need on the average 166 - 500 rounds of ammunition. But with a smart precision guided ammunition with a search radius of more that 50 metres, the probability of hit is 1,000. So with more information on a weapon, one needs less weapons.

In the Battle of Atlantic Allied hit a small percentage of German submarines to collapse the effects of the total submarine fleet. The targets were the supply submarines, that transported the torpedos and the diesel for the attacking submarines.

More generally it is here the question about the increasing information content of the warfare. The phases have been:
(1) Mass. One needs only little information, actually just where the main body of the adversary's armed forces is. But one need very much of other resources to have an effect on the enemy forces, to cause it 20 - 50 percent of losses.
(2) Precision. One needs lots of information and lots of other resources to have an effect on the enemy forces. Information is needed on the systemic structure on the enemy forces and on the importance of main pieces of the enemy forces on the whole system. But now the enemy may suffer just 1 - 10 percent of losses but collapse as a system.
(3) Leaders. One needs very much of information of the leader of enemy forces and only little other resources to have an effect on the enemy forces (through its leaders). Basically the central question here is, under what circumstances the enemy leader considers the battle or the war lost. To dig this information out of the enemy leader's head and to distribute him/her the corresponding information, are the main information questions. Here the enemy may not suffer any losses at all. One example of this type of increased information effect is the surrender of the most powerful Nordic naval fortress, The Viaborg in Helsinki 8th of May 1808.

In Irak 2003 its integrated air defence and air force was destroyed this way by using all available means, concentrating on the key points of the system and so letting it numerically very much untouched, but as a system destroying it totally.[33]

NCW emphasises the principle of "More with less". The first dynamic to get it done is the distribution of information and to get the LSL in effect (see Lancaster above). The second dynamic is to have a unified effect through distributed forces.

3.10. Shared situation awareness

Situational awareness can be shared by:[34]
1. sensing the same physical object or event (see, hear, smell...)
2. sensing the same physical object or event by the same sensor (e.g. UAV picture)
3. distributing the information or knowledge of the object or event
4. sharing the fused information of multiple sensors (combining the above)
5. discussing the situation in combination with the above or without them. This enrich the shared understanding of the situation and discussing parties can collaborate on the base of the same understanding. This last case is the most effective one, but also the most demanding for networked communication systems.

Networked power, it is networked communication, command and control and intelligence systems make it possible to share information and knowledge and it makes possible to cooperate and share situation awareness.

An example: Own troops have been targeted by enemy artillery. Engineer's terrain analyse reveal where the artillery observation post (AOB) can have been. This information is combined with

signal corps communication intelligence. This smaller area is ordered to UAV to look for and the detected AOB is destroyed by a counter intelligence unit.

To do this at tactical level in near real time fully network communication and information systems are needed.

During second world war the allied counter submarine force made four times more submarine sinks after they combined HF- radio direction finding with patrolling radar aircraft intelligence. It was possible to cover whole Atlantic ocean with HF- radio direction finding but with poor accuracy and only small part of Atlantic ocean with patrolling radar anti submarine air crafts but with good precision. By combining them one got a perfect system to hunt down German submarines.

Shared situational picture is a revolution. The traditional situational picture is different for every military unit. It is made up by its level's intelligence units and its subordinate's and neighbour's situation messages. In NCW the picture is shared through a common distributed data base and now everyone has the same information, so an integrated base for the situational picture. Shared situational picture means also better quality of information and knowledge. The information of a stand-alone sensor is buried into the mass of information or is not reliable without more data. When a single data is correlated to other data, it can highlight a new and important phenomenon in the battlefield. So data fusion is a important feature of NCW, of information sharing.

If the changing situation is shared by multiple levels of command and in advance (warning orders), planing can be done simultaneously in multiple levels of command and so time can be suppressed.[35] This is a communication intensive approach, it is a network age approach.

Information sharing with other sensors: For instance stealth aircraft is not invisible to the radar, it is just hard to see by the radar. A stand-alone radar can pick up a stealth aircraft from a certain distance and from a certain angle. This separate intercept is not processed by a standard radar system. But when multiple stand alone intercept are fused together, one gets information out of data, in this case an approximate route of a stealth aircraft.

3.11. Boldness

Individual situational awareness and shared situational awareness result into boldness. One knows where the bad gays are and where the nearest own troops are. It is easy to act when one has the information one needs to act. When this information is a quality product, one can trust it. When there is no need for hesitation a speed of maneuver will emerge.

Ref. also chapter 3.3. where the preconditions of an act have been discussed. One of those preconditions was the courage to do the decided act.

3.12. Speed of maneuver and tempo

Speed and tempo are important in war. In NCW speed and tempo is achieved (1) by decreasing levels of command, (2) by interleaving command and control precesses (3) by creating direct contacts between sources of information and knowledge, (4) by concentrating effects (shock and awe) to have the effect quicker and so with a greater psychological effect and (5) by separating sensor, shooters and leaders, so that a shooter can act, if necessary, without the guidance or the decision making process of the leader.

Speed means also increasing the ability to acquire material and especially commercial information technology material.

USA experience show that it is possible by using networked activity to increase the operational tempo at the divisional level six fold from 72 hours to 12 hours, decrease speed of calls of fire six-fold from 3 minutes to 0,5 minutes and to cut planing time at the company level half, from 40 minutes to 20 minutes.[36]

There are still some ways to have real time effects. One is to increase the presence of shooters in the battlefield. One new application that had dramatic effects was to arm the special forces, reconnaissance troops and UAVs (see footnote ??).

Second way to increase real time effects on the battlefield was heavy use of bombers in a waiting position above the battlefield. With precision weapons (JDAM) a bomber could have 16 separate weapons to hit 16 separate targets with precision and annihilating effect.

3.13. Collaboration and self-synchronization

Collaboration is an active process unlike information sharing. Collaboration always implies working together towards a common purpose.[37]

In a traditional war the leader tells what is to be done and the subordinate thinks how to best realize it. NCW is based on a different hypotheses, it is on self-synchronization, acting without leaders. This sounds at least a bit dubious. This is one of the most important changes in NCW. So, what is self-synchronization? It is achieving the goals of the organisation without or with less leaders than in a hierarchical organizations.

Self-synchronization is based on pre-information before the situation occur, for instance on war games and their conclusions and on knowledge of the neighbouring leaders. At war every leader act as his/her own and synchronize his/her actions on previous information and information transmitted from bottom up. So there is lots of pre- information that is not needed to transmit during the battle. It means to make information and knowledge for the future. Information and knowledge is always the base of purposeful acting and they have to made at some point. If one has to do them in war without any previous knowledge, it takes time and is called surprise. If the battle goes on according to earlier made knowledge, it is generally called winning.

It is very difficult to crush this kind of command and control system. The needed information is pre- made in the heads of every leader. It seems that it is not possible to have meaningful actions in a war without some kind of pre- made information and knowledge[38]. The parts of the systems have to have some kind of model in their heads to self-synchronize their actions meaningful. It is also possible to have one leader pointing out the general desired direction for a lots of subordinates.

The second need for self-synchronizing military units is a shared situational awareness that builds up its picture of the battlefield from bottom up.

Collaboration means horizontally shared information. First it means information sharing across different countries in a coalition or global organizations, then inside the security and information organisation of one country, then different military services in an armed forces of a country, then inside the branch of a military service inside a military service and basically and at last across every collaborating unit in a small tactical part of a battlefield.

One of the key benefits of a network-centric environment is the ability to share information and collaborate over distance[39]. USA saw that its JOINT- level collaboration was at an unbelievable level in Irak 2003[40].

3.14. Precise application of force and effect: Mission effectiveness

When a unit of military force has quality organic information, quality shared information and is aware of the situation it can use its force with a precision and as a consequence it has precise effect on the enemy. When precise effects are combined with speed of maneuver the result is mission effectiveness.

So by understanding (cognitive domain) the quality information (information domain) one has by sharing it with ones neighbours, one get ultimately physical effects (physical domain), mission effectiveness.

3.15. New concepts and TTPs

Warfare is a complex undertaking. In a functional level of warfare there are eight domains, that form a entity in the warfare. These domains are (1) technology, (2) doctrine, (3) organization, (4) logistics, (5) humans, (6) information and knowledge, (7) time and (8) energy[41]. To react to the changes of the flow of information in the networked age requires changes in the other domains as well[42].

TTP (tactics, techniques and procedures) are one element to consider to change when one has new technology in use.

1. “Network Centric Warfare” p. 3-1, Department of Defense Report to Congress 27. July 2001 www.dodccrp.org

2. (a) Network-Centric Warfare, NCW Department of Defense Report to Congress 27. July 2001 3-8 - 3-11) and
(b) D S Alberts, J J Gartska, R E Hayes & D A Signori:”Understanding Information Warfare Age Warfare” CCRP Publication Series USA 2001 p. 10 - 14 and 57 - 59

3. “Network Centric Warfare” p. 3-11, Department of Defense Report to Congress 27. July 2001 www.dodccrp.org

4. John Boyd:"Pattern of Conflict" 1986 (http://www.d-n-i.net/boyd/pdf/poc.pdf 9.3.2003). Boyd speaks about attrition warfare, maneuver warfare and about moral warfare. The ability of the Information Age is the precision, to be able to influence on the precise part of the system. The real end target of warfare is always the enemy decision maker. To do this, the direct means have been historically scarce and that is why one have been forced to use indirect means, the warfare. To influence to the people is in democracy to influence to the decision maker, hence the importance of the psychological warfare.

5. This new paradigm is described in: Albert-Laszlo Barabasi:”Linked; The New Science of Network” Persus Publishing USA 2002

6. In the book: M Metsä (ed.):”Tuleva tuhat” Tilastokeskus, Gummerus 1999 P Lillrank:”Globaali verkostotalous” p. 142 --> (In English:”The next millennium” and the article “Global net economy”)

7. M Castells:”The Contours of Information Age” In FUTU’s seminar “Life Beyond the Information Society” 16.- 17.8.1999 Turku, Finland

8. M Castells’s interview Finnish TV 1 A-Studio 7.1.2000 21.00 - 21.30

9. A Keskinen:”Tieto ja valta verkoissa” Presentation in Paikkatietomarkkinat, Finland 17.9.1996 p. 1 - 2 (In English:”Information and power in networks”)

10. Kevin Kelly:”Out of Control; The Rise of Neo-biologial Civilization” Menlo Park; Kalifornia Addison -Wesley 1995 p. 25 - 7

11. Professor Markku Sotarauta, E-mail to the author 6.2.2000

12. John Arquilla & David Ronfield:”The Advent of Netwar” RAND 1996 p. 15

13. John J. Gartska:”Defence Transformation and Network Centric Warfare” Slide 61, National Security 2003 Conference, Tieturi Oy, Helsinki 24.10.2003

14. G T Hammond:”The Mind of War. John Boyd and American Security” Smithsonian Institution Press, USA 2001, p. 190

15. D S Alberts, J J Gartska, R E Hayes & D A Signori:”Understanding Information Warfare Age Warfare” CCRP Publication Series USA 2001 p. 84 and 97

16. J Arquilla & D Ronfeldt:”Swarming & The Future of Conflict” RAND 2000 p. vii

17. J Arquilla & D Ronfeldt:"Swarming & The Future of Conflict" RAND 2000 p. 37

18. J Arquilla & D Ronfeldt:"Swarming & The Future of Conflict" RAND 2000 p. 22

19. J Arquilla & D Ronfeldt:"Swarming & The Future of Conflict" RAND 2000 p. 41

20. J Arquilla & D Ronfeldt:"Swarming & The Future of Conflict" RAND 2000 p. 82

21. "Network Centric Warfare" s. 2-2, Department of Defense Raport to Congress 27. July 2001 www.dodccrp.org

22. D S Alberts, J J Gartska, R E Hayes & D A Signori:"Understanding Information Warfare Age Warfare" CCRP Publication Series USA 2001 p. 24

23. Preconditions of Lancaster's Square Law (LSL) are:
(a) Blue and Red forces are homogenous
(b) All units take part to the combat
(c) Every unit is inside effective range of weapons
(d) Destroyed targets are not targeted any more
(e) Losses do not affect to the rate of fire
(f) The fire is optimally distributed
(Source: Mika Hyytiäinen:"Taistelumallit" Report of Finnish Defence College, Tactical Department, Research Group 19.12.2001 p. 15 (In English:"Combat models")

24. Lancaster Square Law says that ones losses are inverse proportional to the square of ones numeric superiority. An example: If we have one to three numerical superiority over the enemy (1:3), our losses are one ninth of the losses of our enemy (3*3:1 = 9:1).

25. Albert-Laszlo Barabasi:"Linked; The New Science of Network" Persus Publishing USA 2002, p. 102

26. "Network Centric Warfare" p. 2-4, Department of Defense Raport to Congress 27. July 2001 www.dodccrp.org

27. D S Alberts, J J Gartska, R E Hayes & D A Signori:"Understanding Information Warfare Age Warfare" CCRP Publication Series USA 2001 p. 25

28. D S Albert & J J Garstka & F P Stein:"Network Centric Warfare; Developing and Leveraging Information Superiority" CCPR 1999 p. 265

29. John J. Gartska:"Defence Transformation and Network Centric Warfare" Slide 22, National Security 2003 Conference, Tieturi Oy, Helsinki 24.10.2003

30. S Ahvenainen:"Acquiring Information Superiority by Time-Divergent Communication" 2nd European Conference on Information Warfare and Security, University of Reading 30.6. - 1.7.2003. England, together with Tuija Helokunnas and Rauno Kuusisto, p. 3

31. D S Alberts, J J Gartska, R E Hayes & D A Signori:"Understanding Information Warfare Age Warfare" CCRP Publication Series USA 2001 p. 54

32. D S Alberts, J J Gartska, R E Hayes & D A Signori:"Understanding Information Warfare Age Warfare" CCRP Publication Series USA 2001 p. 55

33. H S Kenyon:"Unconventional Information Operations Shorten Wars" Signal August 2003 p. 34

34. D S Alberts, J J Gartska, R E Hayes & D A Signori:"Understanding Information Warfare Age Warfare" CCRP Publication Series USA 2001 p. 127

35. D S Alberts, J J Gartska, R E Hayes & D A Signori:"Understanding Information Warfare Age Warfare" CCRP Publication Series USA 2001 p. 150

36. "Network Centric Warfare" p. 8-21, Department of Defense Raport to Congress 27. July 2001 www.dodccrp.org

37. D S Alberts, J J Gartska, R E Hayes & D A Signori:"Understanding Information Warfare Age Warfare" CCRP Publication Series USA 2001 p. 27

38. C C Chen:"Anatomy of Network-Centric Warfare" Signal August 2003 p. 48

39. D S Alberts, J J Gartska, R E Hayes & D A Signori:"Understanding Information Warfare Age Warfare" CCRP Publication Series USA 2001 p. 28

40. R Ackerman:"Iraq War Operations Validate Hotly Debated Theories" Signal July 2003 p. 31

41. S Ahvenainen:"Acquiring Information Superiority by Time-Divergent Communication" 2nd European Conference on Information Warfare and Security, University of Reading 30.6. - 1.7.2003. England, together with Tuija Helokunnas and Rauno Kuusisto, p. 3 - 4

42. D S Alberts, J J Gartska, R E Hayes & D A Signori:"Understanding Information Warfare Age Warfare" CCRP Publication Series USA 2001 p. 50