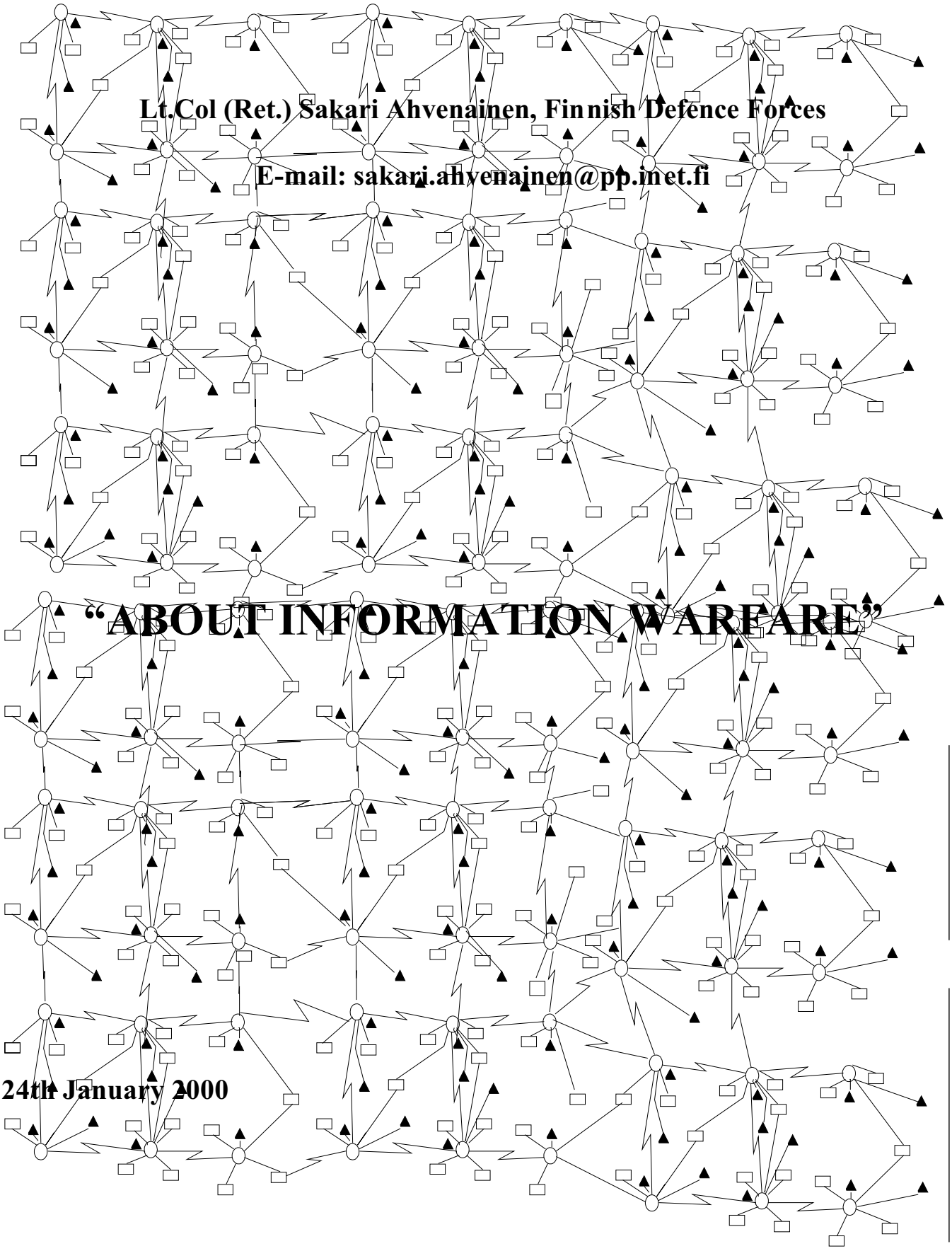
Lt.Col (Ret.) Sakari Ahvenainen, Finnish Defence Forces

E-mail: sakari.ahvenainen@pp.inet.fi



"ABOUT INFORMATION WARFARE"

24th January 2000

TABLE OF CONTENT

ABOUT INFORMATION WARFARE

Motto 1: Information warfare is a hostile influence of which an effect of over 50% is caused by direct information means. It can be aided by other means of influence, for instance physical and electromagnetic.[1]

Motto 2: There is just few means of influence but their combinations are incalculable.[2]

Motto 3: Those peoples and individuals that rule the complexity, will be the super power of the future in industrial, political and cultural areas.[3]
Physicist Heinz Pagels
And military. Lt.Col S Ahvenainen.

Motto 4: "When the core of warfare in the 20th century has been the tank, in the 21st century it will be the computer".[4]
General Sullivan, USA.

Motto 5: If a system can be modelled --- it can be made to collapse. [5]
Major K B Smith, USA.

0. Introduction

0.1. Some definitions

Definition 1: Information Warfare is actions taken to achieve information superiority by affecting adversary information, information-based processes, information systems and computer-based network while defending one's information, information-based processes, information systems and computer-based networks.[6]

Definition 2: Information warfare is the hostile influence, of which effect over 50 percent is caused by direct information measures.[7]

0.2. Structure and basic thesis of this essay

What is the worst mistake in the war ? It is to prepare to the wrong war. Refer to the French and to the Maginot line 1918 - 1940. This presentation deals with the possible changes in the warfare and with the question:"What is warfare in the time of a rapid change, in the time of information dominance?"

This essay presents some views to the background of information warfare. Parts of this essay

are (1) some general elements of warfare, which have perspectives to the information warfare, (2) warfare as a part of society's evolution, (3) some backgrounds associated to warfare, (4) information and information technology's relationships with warfare and (4) the seven elements of information warfare.

Basic thesis of this essay are:
(1) We live in the middle of a big change. This change is about means of might and influence. First from the military to the economy and then from the economy to the information. The categories of influence will not increase, but their rank will change and there will be some new means inside old categories of influence.
(2) The principal change is caused by global and commercial[8] technology and science, especially information technology. They will lead societies to information society and warfare to the information warfare. Globalization, transnational corporations and networked systems are short term central consequences of this development. Long term consequence is the start of the synthetic evolution and artilects, beginning of technical singularity[9].
(3) Computers, computer networks, communication networks and information as programs, data, algorithms, artificial intelligence, modelling, simulation and visualization in them will be the central elements of efficiency and power everywhere; in society, in military, in economy, in crime, in transportation, in energy, ... They will merge together, as a basic infrastructure of a information society and information warfare. As a consequence of these new tools we will have beside the reality also the virtual reality and real virtuality[10].
(4) The evolution of technology, especially microprocessor and artificial intelligence will lead in the physical world to the supremacy of technology, especially technical intelligence everywhere, including warfare (ref. Point 2 above).
(5) Basically the big change in warfare is also change **inside** different ways of influence. This change will mean increased importance of informational, economical and psychological influence and decreased importance of physical (=conventional warfare) and political influence. This means stepwise movement from pure warfare to hostile influence and first supremacy of economy and then information dominance.
(6) Nothing old will disappear, some new elements will emerge and this will lead to increased complexity in societies and in warfare.

1. About warfare

There are some basic factors in warfare, which are general to any type of warfare and so important also in the information warfare. These factors give also some basic perspective for information warfare. Those factors in this essay are: (1) Warfare as a means of influence, (2) relative advantage as an central feature of warfare and (3) increased complexity due to advance of technology, especially information technology.

(1) **Warfare as a means of influence** (ref chapter 3.1. "Warfare as a way of influence" Basically warfare is about influence to chance the will, decisions and actions of the enemy (leader). Traditionally the basic means to influence in warfare is through physical violence. Other kinds of influence besides physical are informational, legal, psychological, electromagnetic, political[11], economical, chemical, and biological influence.

So information warfare's view to the influence is first the fact, that information is a old means of influence. Secondly, that through information's technology's advance, there are more ways to influence through information and the effect of information is bigger and it concerns to more systems than before. Basically this means information's dominance and birth of information warfare.

(2) **Relative advantage as an central feature of warfare** Warfare is an enlarged duel, so

some absolute level of efficiency is not important in warfare. It is important to be enough more efficient than the enemy, to have a relative difference or relative advantage. So there is in warfare three things in every action in the military: (A) The action itself, (B) enemy's attack against the action and (C) our defence for the action against enemy's attack.

These same three activity are on our and the enemy's side. The enemy's action, our attack against the enemy's action and the enemy's defence against our attack. And our action, the enemy's attack against our action and our defence against the enemy's attack This makes six variables and has as a final result the difference in efficiency in the area of action involved. The relative difference.

Because the attack or the defence is just a action , which has defence or attack against them, this process will give birth to endlessly deep series of action and counteractions. This process give birth to the increased complexity of the warfare. Refer to the Motto 3:"Those peoples and individuals, that rule the complexity, will be the super power of the future in industrial, political and cultural areas".

So information warfare's view to relative difference is, that three things are important and have to considered all together: (1) Information itself, (2) attack against information and (3) defence of one's information. And both apply to our side and to the enemy's side.[12] The attack and the defence have endlessly deep series of actions and counter actions.

(3) **Increased complexity due to advance of technology** Central feature in the last 150 years's history of warfare is the increased complexity of warfare.[13] The cause of complexity is advance of technology and lately especially advance of information technology. The big picture in here is, that warfare's dimensions have increased. First new dimension after thousands of years of warfare in surface, in time and on will, was air (1918 - 1939), then electromagnetic spectrum (1968 - 1982), then informational and physical space (1991 -). See chapter 2.6. "New dimensions to control, new means of victory".

So information warfare's view to increased complexity is, that information is the next essential source of complexity after air dimension and electromagnetic spectrum. Information is a complex thing. (Cf. Chapter 6.1. - 6.2.)

2. The cultural backgrounds: Three waves of society

2.1. The concept

We are living in the middle of tree, four big changes: End of the Communist Era (1914 - 1989), End of the Era of Nations (1789 - 1989) and end of The Colombian Era (1492 - 1992).[14] Forth: End of the State Warfare (1648 - 1989).

Warfare is in many ways connected to society for example to it's culture, technology, values, infrastructure, organisation and educational level.[15] Warfare is a organised social activity between men.[16] Other aspect in the relationship between society and armed forces is society's's economical resources to support them, general relationship between society and armed forces, task given to armed forces and society's threat scenario. That's why it's important to have an idea of changes and backgrounds of societies.

The Tofflers[17] have spoken about the big change in the society for a long time, since early 70's. They see three big waves in the evolution of societies: The (gatherer-hunter phase, the) agricultural phase, the industrial phase and the information phase.[18]

It's important to notice, that nothing disappears in the change.[19] A good and basic example of this phenomenon is that in the information society, beside information, there will be eating, agriculture, and lots of goods, industry. As a consequence, complexity and means of welfare will increase.

The basis in the information society is "intuition", which is also the next paradigm from reasoning.[20] Intuition as understood in this essay has two sides: (1) The technological side: networked computers and (2) the human side: Networked and educated brains.

Scientific revolution occur because an existing paradigm cannot accommodate new discoveries or theories. "Intuition" is information, which due to the complexity of the entity can be made in many[21] cases only by computers. It has been impossible for some time now to describe by conventional science exactly any entities. Only pieces and part of them. This is the technological side of the "intuition", the paradigm of thinking, knowledge.

The change in the information society is very fast. To understand any significant complex, you have to use computers, modelling, simulation, visualization and new principles of science (e.g. complexity theory, chaos theory). You need informationalization of your systems and technical intelligence in the form of computers and artificial intelligence to handle the mass of information from your systems or from the source of information. These all are important new power tools of the information age.

By using these tools time after time, one will at the end have an intuition of the entity you are working with. And for this work you need lots of data, which you process to knowledge, understanding and wisdom. In the processing the more and more valuable tool is the computer, computer networks, programs and artificial intelligence. This is the computer side of the intuition.
Human side of the intuition in here is not the lack of information, it's enlarged and preinformation, anticipation, information of the subconscious mind, networked with other similar brains.

Conceptualism is great in the information society. Food and artifacts are very concrete. Information is not. Land and gold are concrete, paper money is not so concrete and electronic money is just some bits in a computer memory. Conceptualism on warfare is also great at higher, essential levels. This means risk and will.[22] Previously the climate of warfare was made up by danger, exertion, uncertainty and change[23], not very concrete things. Now the warfare is increasingly dependent on information in computers and threat libraries, also not very concrete things.

To estimate a nation's military might without concern to it's information systems and the use of information, is already a waste of time, and will be increasingly that in the future.[24] There is a change happening from hardware towards ideas and perception[25].

In the information society and warfare everything depends on computers, computer networks and their programs. Power is in the men enlarged by intelligent, information and network based systems.

This will create a situation, in which the presence and influence of organisations will be bigger than ever. There is over thousand surveillance cameras watching over Helsinki City. Your work done by computers is guided by your organisation's programs and flow of work and you will leave many electronic footprints in your work and leisure time. We live in a electronic surveillance society[26].

And the change is very fast. In an information age five years is eternity[27]. The ability of a man and his organisation to change is the greatest obstacle. Thus, the important factors to the change are organizations and people.

It has been estimated, that the fulfilment of the change to the information society will require still a couple of decades. It will probably also include a long period of social unrest, even wars[28].

Because of the accelerating change and complexity and because of the evolution, where nothing old would not disappear, we will se "nasty" problems.[29] They are connected to the open[30] systems, which are not easy to define. Open systems have many connections to other open systems. If one can solve a problem, the system or its connection has changed. So one needs a new solution. "Nasty" problems in open systems can not be solved. One have to process them constantly.

Opens systems, for instance a modern state or firma is vulnerable to netwar.[31]

2.2. First and second wave

The first phase of warfare in the Tofflerian model was "man and tools"- war. Machine and information exist, but man enlarged by tools dominates.

In order to have an influence on the other systems, nations or states, one has to move his units on surface and first attack on the military of the other side. The warfare was serial, beginning with battles on the border, then inland and finally on decisive points. It took time and battles were fought on the surface, on one, small piece of land or sea. And in time and on will.

The second phase of warfare was or is man and machine- war. It included man and tools plus machine and systems. Machine such as aircraft and tanks. Systems like railroads. Man, tools and information exist, but man enlarged by machine dominates. Fighting was happening on a larger area. Battles of mass armies were unified to operations. The military gravity moved from tactics to operations.

The key word in this phase is mass. Mass army, mass education, mass production, mass media, mass information, mass death, mass destruction.

The second phase's end created air force and electronic mass media, radio, new means to influence. They largely bypassed traditional military might and lower dimensions of warfare, the surface, the lines and the points. One consequence was the decreased importance of the geographical borders of nations and the birth of new borders.

The air force and use of E.M. spectrum (radio, radar) also facilitated to strike many points at once, the whole depth of the enemy territory. This was possible with much decreased complexity and with much increased speed in respect to the surface. It also made it possible for the first time to strike whatever points in the enemy territory within you air force's range and other capabilities. The air force made one free of the limitation of the surface. The parallelism, complexity and speed of warfare began to move on. New dimensions, air (height) and E.M. spectrum were included in the warfare.

The use of air created:
(1) the troops of use of the air (e.g. transport planes, surveillance planes, bombers, fighter bombers, air to surface missiles (ASM), cruise missiles)

(2) the troops of attack against the air (e.g. interceptor, air superiority fighters, air to air missiles (AAM)) (Air Countermeasure, ACM)
(3) the troops of defence against the air attack (e.g. anti-air artillery, surface to air missiles, (SAM), air defence fighters, escort fighters) (=Air Counter Counter Measures, ACCM)

Because Air Counter Counter Measures is just measures, which have countermeasures this process creates ever increased deep action - counteraction chains.[32] This means increased complexity and new means of victory and defeat.

2.3. Third wave: The network society

Advanced nations live more and more in a network society. A new mode of connected, more and more virtual, dynamic, ever changing society with many connections inside and outside the society or state.

In a broader historical perspective, the network society presents a qualitative change in the human experience. If we refer to an old sociological tradition according to which social action at the most fundamental level can be understood as the changing pattern of relationship between Nature and Culture The first model was for millennia by the domination of the Nature over Culture. The second model beginning at the origin of Modern Age was domination of Nature by Culture. We are just entering a new sage in which Culture refers to Culture, having superseded Nature to the point that Nature is artificially revived ("preserved") as a cultural form. ... This is why information is the key ingredient of our social organisation and why flows of messages and images between networks constitute the basic thread of our social structure.[33]

A new world is taking shape in this end of millennium. It originated in the historical coincidence, around late 1960's and mid- 1970's, of three independent processes; the information technology revolution; the economic crises of both capitalism and statism, and their subsequent restructuring; and the blooming of cultural social movements such as libertarianism, human rights, feminism, and environmentalism.[34]

Power... is no longer concentrated in institutions (the state), organizations (capitalist firms), or symbolic controllers (corporate media, churches). It is diffused in global network of wealth, power, information, and images, which circulate and transmute in a system of variable geometry and dematerialized geography. Yet, it does not disappear. *Power still rules society; it still shapes, and dominates, us*. Not only because apparatuses of different kinds can still discipline bodies and silence minds. This form of power is, at the same time, eternal, and fading away. It is eternal because humans are, and will be, predators. But, in its current form of existence, it is fading away; the exercise of this kind of power is increasingly ineffective for the interest that it is supposed to serve. States can shoot, but because of profiles of their enemies, and the whereabouts of their challengers, are increasingly unclear, they tend to shoot randomly, with the probability that they may shoot themselves in the process.[35]

Alongside the public and private sector a "third global sector", a social sector is well under away. The key is for governmental and non- governmental actors to learn to cooperate better. This will strengthen the state.[36]

In USA big corporations have started a well planed and broad-based counter-attack against environmental movements. In their counter- attack the corporations have used first the cover - organisations that they have created and which represent themselves as environmental organisations and secondly conservative research organisations. On the other hand the

environmental movement is also networking. A civil organisation that resist poisonous waste has grown to a loose network of 8000 local groups, that has won hundreds of campaigns against chemical industry. A new network of activists, Communities Concerned about Corporation, is watching the actions of corporations.[37]

The main source of meaning in live in the West is based on individual fulfilment. The dynamic that started the evolution of the individual started with the fall of Rome. War has been in the resource based warfare about killing people, but those people were previously just numbers. We felt that it was all right for those numbers to be sacrificed to fix some scarcity.[38] Now in the information based warfare, under the watchful sight of the global media, every death is becoming an individual that is known by the media.

2.4. Third wave:"Man and Information"- war

The third phase of warfare is or will be "man and information"- war. Automation, networking and informationalization are new factors done by computers, their programs and other information technology. They are all a central part of the information warfare. Man, tools and machine exist, but man enlarged by intelligent, information and networked based systems dominates. The key word in this phase will be precision and networks. Precision army, precision education, precision media, precision information, precision death, precision destruction... Social networks, communication networks, computer networks, networks of firms, networks of experts...

Informationalization means to have machine readable information as a central part of all systems of warfare and to use that information for control, learning and for change. Thus, it demands computers in all systems. And to have programs, which integrate, network and automate all these systems. To understand the system you are examining, you need the information that is essential for the processes of the system, for the effectiveness of that system. To find that information, you need modelling.

The Finnish leading newspaper Helsingin Sanomat wrote in May 1996: "The effectiveness of systems (of criminal law) is increasingly dependant on systematic collection of information and on its analyses. By collection of information one can find the change in types and amounts (of the crimes) and the effectiveness (of the police)".[39] Parentheses by Lt.Col Ahvenainen.

In order to have informationalization in organisation demands changes in information, authority and technology. Because of the lack of a wide strategy, no organisation has ever yet been in a situation to totally use its possibilities of informationalization. A will to learn in work is essential.[40] Thus, technology, or any one thing is not important by itself. The Essential Change is bigger than just technology, it is synergic.

The third phase has created or will continue to create still more new means of influence to bypass a state's conventional military might and often also its physical borders. Many of those new means will attack directly on command and control, leadership, will, information, and essential key points of a state's infrastructure.

These new means include more efficient target acquisition and air forces, long range missiles, electronic mass media through satellite-TV and Internet, space forces, directed energy weapons and of course the cyberspace. The traditional warfare will become parallel[41] and the new method will be a strategic strike, parallelism to extremes.

It has been estimated, that operative systems in the year 2000 are capable of transmitting

information from 3500 - 4000 targets to 1200 attack planes in one minute.[42]

If there is going to be traditional warfare at all[43]. Economical and technological dependance between nations is becoming so strong, that temptation to the warfare is decreasing, Nations are increasingly dependant on export/import.[44] Nationstates are too small for the new world.

Strategic strike is the "conventional" warfare of the information age. It means striking only essential key points of essential systems in leadership, will, information, systems, whatever, from long distance, quickly, in a short time and in many dimensions.

The key point of the information age warfare is to avoid conventional warfare, to avoid the breaking of things and the killing of people, by new means of influence, which have usability between conventional warfare and conventional peace. To influence the behaviour of the system, not to break it.[45] Warfare will become a hostile influence, not just organised violence. This will be one of the biggest changes in the warfare's history.

2.5. Essence of the idea, entity

Revolution in military affairs has four elements: technological change, systems development, operational innovation and organizational adaptation[46].

Thus, the technology, a part, is not essential in the warfare by itself. Nor is will, logistics, organisation, neither tactical and operational skills. It is the synergic entity that is essential, but not even it by itself. Only in respect to the enemy, because in the warfare only the final difference is crucial, not some absolute level of efficiency.

The most essential is the new idea of warfare, operational innovation.[47] You have to have background for the new way of warfare. To change all will lead to chaos. And the new way of warfare have to integrate new means of warfare to it and it has to be a synergic whole.

So what is the synergic entity in information warfare, like German Blitzkrieg of World War II in industrial warfare? One is the American doctrine, information warfare's military adaptation, Information Operation and its part, Command and Control Warfare.[48]

It is essential to keep in mind, that there are many elements of victory, so there are many combinations of different kinds of synergic entities, roads to success.[49] Nothing old disappears, but the power is potentially in new systems. Potentially, because you can misuse these new systems and this really isn't anything new in the history of mankind.

2.6. New dimensions to control, new means of victory

> **Motto 1: Those peoples and individuals, that rule the complexity, will be the super power of the future in industrial, political and cultural areas.[50]**
> **Physist Heinz Pagels**
> **And military. Lt.Col S Ahvenainen.**

As a net result, these changes have brought increased complexity to warfare. In the time of Napoleon, there were 11 functions of warfare to be coordinated. Functions like infantry and cavalry. Patton had 20 functions to coordinate during World War II and Schwarzkopf 30 in the Gulf War 1991. [51]

Between Napoleon and Patton air dimension was added to warfare with air forces, anti air troops, airborne troops and intelligence and reconnaissance aircrafts. Between Patton and

Schwarzkopf the electromagnetic spectrum was added to warfare. It includes missiles, electronic intelligence, electronic countermeasures and counter countermeasures.

The next step will add physical and information space to warfare. The latter is also called the Cyberspace. It will include all the world's interconnected computer networks, data, programs and artificial intelligence in them. Computer networks can serve for command and control, its support like modelling, simulation and visualization, for communications, for use of arms, for intelligence, for logistic, for transport, for psychological influence, for everything.

Added complexity brings also new means for victory. In the agrarian warfare the only element of victory was close combat. The industrial warfare brought new elements like artillery, strategic air bombardment, signal intelligence on land and in air, the breaking of the enemy's cipher and electronic warfare.

In the information warfare even more means of victory will emerge. For example computer countermeasures (hardware, software), suppression of enemy air defence, navigation warfare, signal intelligence from space, direct energy weapons, precision strikes by tactical, cruise and ballistic missiles, air mechanised troops and psychological operations through electronic mass media like Direct Broadcast Satellite and Internet.

2.7. Conclusions from culture

Warfare is a organised, social activity. There will be three kind of societies in the future: Agricultural, industrial and informational. So there will be nine kind of warfare in attacker - defender combination.[52] Nothing old will disappear (agricultural, industrial), some new elements will emerge (informational). This means also increased complexity of the warfare and society.

The new paradigm in the chain of faith, reason and intuition is intuition. It will mean things done only or mainly by computers, increased complexity. It means complicated entity, ruling of it or chaos. It will mean increased weight of the technology and networks.

Information society and information warfare means increased complexity, faster change, more conceptual entity, more computers, computer network, artificial intelligence and information dominance. It means also electronic surveillance society, learning as part of your job, networked systems, doing in teams instead of alone, mass replaced by precision, larger entities, new dimensions in warfare, new means and ends of victory and defeat, informationalization of your systems, change in authority, open systems and organisations, virtual reality, new ways to do business or war and "nasty" problems. The change to the information society will take still a couple of decades.

Information society, network society and information warfare means also increased weight of the economy, information, individual, global and strategic, long range effects, systems of systems and decreased weight of the nation state, operational and tactical and of the traditional warfare. They mean controlling instead of killing and destroying. Hostile influence instead of warfare.

In the information and network society and warfare everything depends on computers, computer networks and their programs. Power is in the men enlarged by intelligent, information and networked based systems, organisations and activities.

Most essential is the new synergic idea, operational innovation and to change all dimensions

of you're the activity according to that idea. Innovation. In information warfare the new idea is, that information, information systems, information processes and computers and computer networks have transformed from a support role to the centre of the gravity of the warfare.

3. The backgrounds associated to warfare

3.1. Warfare as a way of influence

"There is just few means of influence but their combinations are incalculable."[53]

3.1.1. The process, ends and means

The end of warfare is to subdue the enemy to do our will, to have a change in the behaviour[54] of the enemy. The traditional mean of warfare is to influence by physical violence, in which violence has no limits. The change is that now there are some new means and ends of influence.

The process to influence, to subdue is:[55]
(1) Information, knowledge, that you have to influence, to subdue (input information)
(2a) System information a: What the input information means? (Modelling, systems understanding)
(2b) System information b: What you should do because of the input information? (Output information)
(3) Will to do the necessary thing.
(4) Ability to do the necessary thing.
(5) Courage to do the necessary thing.
(6) Endurance to do the necessary thing

And maybe the best way to change a person's behaviour is a new idea, new input information. And how to distribute a new idea, basically information? Through information technology. And the Internet is a totally new way to distribute ideas from an individual or an organization or a nation to many individuals. Globally.

And the new thing is global or nation wide information distribution from **an** individual to many individuals. Previously it was possible to distribute information from an organisation to many individuals. By news readers in churches or on market places, in newspapers, in radio, in television.

Thus, war is about influence, ends and means. To get something, from somebody, who has the control of the thing, that we want. In order to get it, we have different options and means to subdue.

Thus, to understand war in the time of rapid change, we have to[56] analyse possible changes:

(1) In those things we want to have or someone wants from us

(2) To whom we have to influence to get it (or is it for free ?) Or who is influencing us to get something and

(3) What kind of options, means of influence we have or the someone has

3.1.2. Ends

Those things we want to have can be: Land, people, gold, money, raw material, markets, industrial capacity, welfare, political support, programs, patents, IPRs, (International Product Rights), trust, education, understanding, information.[57] Are there changes in those things? Yes, The Essential and The Powerful have become more conceptional, like E-money, information, software, trust, legal support, learning and education. But not solely. In our times the price of soil has decreased because the welfare is growing from science and technology instead of soil[58]. Earlier, soil meant more product of agriculture and more people to pay taxes. These, people and soil, were earlier the prime sources of welfare.

To produce the equivalent of 1.000.000.000 dollar of money by corn, automobiles or CD-ROM's, the final package will have weight of 5.000.000 tons, 167.000 tons and 300 tons, respectively[59]. So the need for material is 1:1/30:1/16.600:1. If the product is computer program or other kind of information distributed through Internet, one don't need material at all, just the infrastructure, Internet and tens or hundred of millions of customers in the net.

If you want to get a huge amount of money, you don't invade a country and rob its central bank. More than 90 percent of the money in a modern nation is in electronic form. To rob and to move it out of the country, you don't have to go there. You can do it electronically. By signal, not by men.

Electronics has bypassed oil industry in USA as the biggest industry in the 1980's[60]. World information technology market in the year 2000 will be about 5600.000 million dollars per year. To conquer an oil field is concrete. To conquer raw material equal of 100.000.000 microprocessors (silicon?) is not so concrete. And how to conquer the potential of one million lines of code per year? Or anticipation, innovation, adaptation, trust, education ?

3.1.3. Means

There is some eight different means to have an effect to the individual or smaller or larger group, who has control of the thing we want. These means are physical, chemical, electromagnetic (E.M.), biological, social, informational, economical, political and legal[61] influence.

When you use these means in war, or if you have troops, you call you war type or your troop type by their principal type of influence. So you have biological war if you use germ and viruses as a principal means to get the job done. Or you have electronic warfare troops with different electronic devises although they have jamm-proof radios to communicate, assault rifles or gas mask to defend themselves in different dimensions of warfare.

3.1.4. Effectiveness of the means

Every way of influence has a different level of power of influence. The principal levels are (1) passive preparation for influence, intelligence, (2) active preparation and (3) influence at different levels of effect.

The passive part of every type of influence includes corresponding intelligence, e.g. political, electronic, chemical intelligence. Active preparations for influence includes those actions, which make the actual influence more easy in time of conflict, but are not the influence itself.

Different principal levels of effect include ineffectiveness, fault, accident, crime, terrorism, and war. Each of these principal levels have sub levels at a diverse level of effect. Ineffectiveness can have consequences similar to small war.

For example in the physical influence, the passive preparation for influence, physical intelligence is intelligence by humans. The active preparation is the weakening of the concrete at central fortifications during peace time, the burning or poisoning down the branches before attack and so on. Actual physical influence has different means, which have different power. Stick, lance, rubber bullet, armour piercing bullet, shell, tactical missile with conventional warhead and ballistic missiles with multiple thermonuclear warheads represent different levels of power at physical influence.

3.1.5. Controllers

Who has control of the things we want? Despot, monarch, elected king, self elected president, president elected by people. In what kind of society does he/she rule? Autocratic, theocratic, democratic, infocratic, other? How can we subdue the controlling person? By threatening to kill him? By supporting his enemies? With money, information? By influencing his electors?

Who wants to influence us, states or non-governmental organisations, NGO's? Neighbouring states, international corporations, international crime, other international organisations, terrorists, rogue states, local organisations ?

3.1.6. The increased influence of information

Information itself has new means: One is program as logical information, which is a new, ever increasing and important form of information. Others are Open Source Intelligence (OSINT), modelling, simulation, visualization and artificial intelligence. Basically they mean information dominance in every aspect of our lives. Including warfare.

Information's influence has increased in the means of influence:
(1) on the biological level: The gene manipulation, precision feeding of the rainbow trout[62]
(2) on chemicals: Simulation of reactions and the building of molecules by software,
(3) on physical: Precision guided weapon,
(4) on social: E.M. mass media (Direct Broadcast Television Satellite, Internet),
(5) on economical: electronics's and Information technology's domination,
(6) on E.M. spectrum: Signal intelligence, Threat libraries, Integrated Electronic Self Defence Suites, Direct Energy Weapons (Electromagnetic Pulse, High Power Microwave, laser).

3.1.7. Changes inside means of influence

Physical (warfare) and political influence were important earlier, today economical[63], informational[64] and psychological[65] are more so. When a nation turns it's ambition from politics to the economy, it transfers from warfare the peace.[66]

It will be hard to distinguish crime, terrorism and warfare or accident and attack[67]. Crime can be component of a state's tool for influence.[68] Or state can be crime's tool for influence.[69]

There was as a principal way of influence three types of influence in the three waves of societies: The phases were physical violence in agrarian society, economy in industrial

society and information in information society. In the time of politic's dominance, warfare can be considered as means to make politics by other means. The other means of influence are politics by still other means.

In the time of physical influence warfare can be considered as politics by other means and the rest of means of influence just politics by still other means. In time of the dominance of physical influence (conventional warfare) the main targets were peoples to have more taxpayers or land to have more agriculture products. Agriculture or taxpayers through it is now just few percent of the gross national product of a modern nation. Actually agriculture is a burden to a modern nation.

In the time of economic's dominance warfare can be considered as economics by other means and the rest of means of influence are economics by still other means. In this respect Gulf War 1991 can be categorised as a economical influence (ends: oil) by physical means (means: warfare). World's finance market, trading of shares, currencies and bonds is 3000.000 million dollars[70] per day, twice the annual US budget, ten times the value of trade of material[71].

If the hostile net effect of influence is dominated by physical influence, it is called conventional warfare. If it is dominated by psychological influence, it is called psychological warfare. If the net economical influence is dominated by physical influence it is called conventional economy. If it is dominated by psychological influence it is called psychological economy. If the influence is hostile, it is called warfare (e.g. economical, psychological warfare).

In time of information's dominance economy can be considered as information by other means, meaning all different kinds of information sold in cyberspace. (see chapter "5.3. Computers in 2020's"). Economics are in time of information just information by other means:
first basic information technology: Multimedia computer, their programs, digital manipulation of information,
then cable-TV, mobile and satellite phones, Internet, computer networks,
latter computer and network programs, electronic mass media, electronic games, videos, news, information and
lastly first a big change in the consumer-producer relationship and
then a big change in the lifestyle of people.[72] Warfare and other means of influence are information by still other means. E.g. Information Warfare. Gene manipulation.

3.1.8. Conclusions from means and ends of influence

There is some nine elements of influence and there is a change happening between them. Physical influence (=conventional warfare) is decreasing and economical, informational and psychological are increasing. Now the dominant part of influence is happening through economy and in the future increasingly through information.

The dominant part of the hostile influence determines the type of warfare. According to this model of influence there is nine species of Information Warfare (see chapter 6.4):
(1) Physical Information warfare (precision (quided) weapons)
(2) Psychological Information warfare (PSYOPS)
(3) Economical Information Warfare
(4) Biological Information Warfare
(5) Chemical Information Warfare
(6) Political Information Warfare

(7) Legal Information Warfare
(8) Electromagnetic Information Warfare (Electronic Warfare, Direct Energy Warfare, Navigation Warfare)
(9) Information Information Warfare (Intelligence[73] Information Warfare, Simulation Information Warfare, Hacker Warfare, Software Information Warfare, Netwar/cyberwar)

There is a change happening in the things we want. They will be more conceptual, more information based. Food or artifacts are not a big deal anymore for advanced societies.

When influencing, there is three principal levels in it: (1) passive preparation for influence, intelligence, (2) active preparation and (3) influence at different levels of effect. These levels apply to every form of influence.

In the future there will be increasingly difficult to make a difference in fault, accident, crime, terrorism and war.

Information has more weight inside types of influence through two channels. First, information, processing power and computer are increasingly important inside every type on influence. Secondly, information's own weight has increased through new and important means and ends of influence.

3.2. Change in the functional dimension of warfare

Operational, logistical, social, technological[74] and organizational[75] levels can be categorised as the functional dimensions of warfare. These dimensions differ from each other in being their own kinds of functional entities of warfare.

Operational dimension is the use of military power at a strategic, operational and tactical level. Logistical level is making and sustaining the quantity of physical, artifactial military power, quantity of the physical military power. Social is having feelings, will and motivation in society and in military to the support of warfare, psychological military power. Social dimension includes also learning, which is a very important feature of warfare.[76]

Technological is the sophistication of artifact of warfare, quality of physical military power. Technology (ref to chapter 5."Information technology and warfare") has an effect how to conduct a war, not to it's sources.

Organisational level is relationships, responsibilities, principles of cooperation and order instruction of the military[77] units, the structure of physical military power.

It is possible to lose a war in every functional dimensions. It is important to understand the enemy's situation in different functional dimensions and to avoid strong ones and to strike on weak ones.

It is also important to have an idea on new warfare and then synergy between different functional dimensions. For instance German World War II's blitzkrieg was an idea of a new kind of warfare with synergistic entity on a technological, organisational, social and operational level of warfare.

Information has influence on every functional dimension of warfare:
(1) Operational: manoeuvre warfare, asymmetric warfare, parallel warfare, strategic strike,
(2) logistical: just-on time, updates of programs and threat libraries,
(3) social: electronic mass media (Direct Broadcast Satellite, Internet)),

(4) technological: information technology, Precision Guided Munitions, Direct Energy Weapons,
(5) organizational: net-based activity, new modes of increased organizational complexity: civilian and military co-operation, multinational level of operations, information assurance (IA), co-optition[78] (combination of co-operation and co-competition), Forum for Incident Response and Security Teams (FIRST) and CERT- (Computer Emergency Reporting Team[79]). As a consequence, information will be also means of effect, not just supporting features of warfare, it should be included to the functional dimensions of warfare.

And technology, especially information technology has more influence with respect to other functional dimensions[80]. One of US Army's future goals is technologically empowered army[81].

In information warfare the new idea, synergic entity is Command and Control Warfare. On an organisational level it tries to break the unity of the enemy's organisation and activity. On a social level it tries to break the enemy's and especially his leader's will to resist. On a technical level Command and Control Warfare tries to break the essential key points of the most important systems or to control them. On an operational level it tries to develop the tempo, which the enemy can not respond. On an informational level it tries to develop a decisive difference between command and control systems and their supporting systems like intelligence and communication; in two words: computer networks. And the key is synergy.

Conclusions: Change inside the functional dimensions of warfare: (1) Information dominance and (2) information as a new functional dimension of warfare. Information has <u>added</u> weight in almost every other functional dimension of warfare. (3) Essence of the entity and the idea. (4) Added weight of the technology (and information) inside functional dimensions of warfare.

3.3. Change in the physical dimension of warfare

According to German colonel Rudolf Grabau, there are seven physical dimensions of warfare: Point, line, surface, space, time, information, electromagnetic spectrum and will.[82]

Points are. Line is made by infinite numbers of points, surface by infinite number of lines, space by infinite numbers of surfaces, time by infinite numbers of space (at a different time), information (data) by infinite numbers of space-time snapshots with their potential for information[83], E.M. spectrum by infinite number of information (at a different frequency), and will by infinite number of E.M. spectrum (at a different energy level $E=hv$ or $E=\frac{1}{2}mv^2$). So will is (conscious) energy that have an influence to the environment.

According to Russian admiral Pirumov, in order to facilitate victory in a modern war, one has to achieve first information superiority, then air superiority, then fire superiority[84] and finally superiority on the ground.[85] This is in accordance with colonel Grabau's model, except the highest dimensions, will and E.M. spectrum, which admiral Pirumov did not mention.

"Man and tools"- war was fought on surface, in time and on will. Machine war was fought first on previous dimensions plus later in the air and on E.M. spectrum. Information war will be fought on previous dimensions plus physical and information space. The change in the physical dimensions of warfare is the birth of the dimension of information. The space is called cyberspace, global integrated entity of communications and computer networks, their programs and data in them or passing between various parts of them.

The logic of warfare goes according to these dimensions. For example, in the use of artillery, the following points can be made. First it is essential to take actions against the enemy's counter battery systems, especially counter battery radars, 6th dimensions (ref. to picture 5). Otherwise your artillery will be destroyed what ever it will do. This is ruling the 2½. dimension. When you have freedom of action, you attack the depth of the enemy: command posts, reserves, lines of communications. When the depth of the enemy is in chaos, you will strike the line of contact, break-in area, 1st dimension. Finally you destroy those points, that block your advance, rule the 0. dimension. By acting otherwise or in an other sequence, you endanger your victory.

Conclusions: Added complexity and more dimension to control. Nothing old disappears. New means (dimensions) of victory. Importance of will (people), E.M. spectrum and information.

3.4. Conclusions from warfare

Information warfare is a change inside the order of the means of influence. It is not a new means of influence. Information is or will become the dominant means of influence. Not the only one. Information is a means of influence in peace, in war, outside a nation and inside a nation. For the rich and for the poor. For the individual, for the firms, for the nations and for the international organizations.

Information warfare as a revolution should be a synergic entity with a well balanced levels of operational, logistical, social, technological, organizational and informational entities. Information warfare as a technological change is just a change, maybe an improvement.

Information warfare as a physical dimension in the warfare is a new source of increased complexity inside the warfare.

4. Information in warfare

Military dimension of information on the basis of enlarged duel has three points: (1) Use of information, (2) attack against information and (3) defence of information. These three areas apply to every military actions, for example to infantry, artillery, command and control, intelligence, bridge laying, communications and military electronics.

These three points, action, counter actions and counter counter action, are both on our and on their side. It makes six variables and has as a result: The information difference.[86]

Thus, superior information technology is not essential by itself, if the enemy has effective counter technology or counteraction against it (EMP, HPM, virus, other software and hardware countermeasures, asymmetric doctrine...). And if the information technology has no protection against those countermeasures.

When information was made in humans, stored in humans and mostly transported by humans, there were not very great possibilities to act against information. On a strategic level it was possible and the struggle around information was transformed to struggles between spies and counterspies. Chinese strategist Sun Tzu counted 2500 years ago five different types of spies and instructed how to use them.

Information has always been important in warfare. It may be, that the greatest state ever created, the Mongolian Empire in the 12th century, was established according to very modern principles of operational and command and control warfare.[87]

Information in resource-based warfare was historically a support measure. It was critical, but it's value was casual. Information was hierarchical. Warfare was possible without information. Information was limited and expensive, and information services were not vulnerable. Programs were not important. Every level of command had it's own picture of the situation. Information led to reaction, massive use of fire, to victory by attrition. Learning took place by experience in war. [88]

Conclusions: Information is one functional and physical dimension of warfare, which includes the principled three sides of all military activity: action, counteraction and counter counteraction (and so on). Ruling the complexity (deeper and deeper counteractions).

5. Information technology and warfare

Motto 5: "When the core of warfare in the 20th century has been the tank, in the 21st century it will be the computer".[89] General Sullivan, USA.

The use of technology in the war has four, five phases: The use of tools (- 1500), the use of machines (1500 - 1830), the use of systems (1830 - 1945) and the use of automation, computers.[90] The fifth phase is the use of networks (1969 -), especially computer networks.

There can be seen four phases in use of information technology. Before 1860 practically none[91], after it the use of E.M. spectrum, from 1943 the use of computers and from 1969 the use of computer networks[92] and latter artificial intelligence.

5.1. Use of the E.M. spectrum

Use of the E.M. spectrum (telegraph, telephone, radio, radar, infrared, laser) had as a consequence fast data delivery on global base at speed of light, 300.000 kilometres in a second.

The use of E.M. spectrum created:
(1) the troops using the E.M. spectrum (e.g. signal (communication) and radar troops, radio broadcasting stations),
(2) the troops of attack against the E.M. spectrum (electronic warfare troops, signal intelligence and different category of electronic warfare: Electronic Support Measures, Electronic Counter Measures, Electronic Counter Counter Measures, Radar Warning Receivers, Anti Radar Missiles, ElectroMagnetic Pulse, Directed Energy Weapons) and
(3) the troops and measures of defence of the E.M. spectrum. (Electronic deception, Electronic Counter Counter Measures (ECCM), Low Probability of Intercept (LPI) - type equipment).

Electronic warfare complicated the design and use of new systems that used E.M. spectrum.

Because Electronic Counter Counter Measures are basically just a measure which has countermeasures, this counter, counter counter- process created ever increasingly deep actions and complexity. This means also a new means of influence and victory. It also added complexity.

5.2. Use of the computer

Use of computer, automatic processing of information and synchronization of systems began in World War II. The breaking of German electromechanical ENIGMA- messages was first aided by communication intelligence, cryptography, and then by electronic COLOSSUS-computers. The latter was a new piece of technology and certainly a means of victory.

Increased mobility of targets, the destructive power of arms and more complex threats with shorter and shorter times to react and increased ability to discriminate targets (precision targeting) are the courses for the increase of automatisation.[93]

The computer is hardware and software; new ends to influence: Chipping, back-doors, viruses. The computer meant also the birth of computer-troops in the three categories of military information use: (1) Use, (2) counter- and (3) counter counter-actions.

Capacity to do one million instructions per second (MIPS) (= one computer, 100 kg) cost in 1970 about 400.000 dollars in today's money. Now the same capacity costs about 20 dollars (= one hundredth of a 1 to 10 kg computer) .[94] In the 1970 there were some 40.000 computers, 1995 some 400 million. In 1995 microprocessor industry was worth 300.000 million dollar.

Consequence ?
(1) 1.000.000 **times** more computer power, MIPSs, technical intelligence out there than in the 1970's
(2) 20.000 **times** cheaper technical intelligence, $/MIPS out there than in the 1970's
(3) 10.000 **times** more computers out there than in the 1970's
(4) 1000 **times** more computer power per kilogram than in the 1970's
(5) 50 **times** computer market out there than in the 1970's

What this means ? Cheaper and cheaper technical intelligence and technical intelligence everywhere. Bigger and bigger share of the economy is the information industry and it's part computer industry. The computer beats the human world champion in chess[95]. Revolution. Beginning of the era of technology and artificial intelligence.

5.3. Computers in 2020's

What this means if the computer revolution continue from here to 2020 as it has continued from 1970 to 1995, a linear prediction?

In 2020 there will be:
(1) 1.000.000 times more computer power than today, 40.000 MIPS for **each** of the 10.000.000.000 people on earth (and in space).
(2) one MIPS will cost one thousandth of a dollar
(3) some 4000.000 million "computers", 400 for **each** of the 10.000.000.000 people on earth (and in space).
(4) one MIPS in 0,1 grams
(5) 15.000.000 million dollar in the "computer" market, ten times the US annual budget now.

What this means ? It means information dominance and information society. And Information warfare.

5.4. Super computer and microprocessor

In 1995 the microprocessor industry was a $300.000 million industry, the super computer just $2000 million[96]. The microprocessor, which is a mass product, caught up the supercomputer, which is a national asset, in raw central processing power in 1994. This was done by R8000 microprocessor.[97]

Consequence ? Cheaper and cheaper technical intelligence and super computer power everywhere. The ability to solve bigger and bigger problems, to rule the complexity. Or to simulate bigger entities and to visualize the results. Super computers made by hundreds or thousands microprocessors running parallel. Revolution. Information power for everyone and for everything.

5.5. Software

Software is an other story. It is essential to understand that computers do nothing without software and that they do exactly what the programs tell them to do. And that programs are large, complex and hard to test throughly and they cost in many cases more than hardware. The information view on programs is that they are just logical data. Consequence ? Information dominance through software. Programs are a new type of means of influence, means of new warfare systems and troops, in use, counter measures and counter counter measures[98].

Still some facts about software. It is the central means to update modern civilian and military systems. Software integrates systems to bigger entities. Software is the origin of systems of systems. To buy software to automate your own activity is not easy. It is complex. You need lots of people to define the program. This is a new requirement for organisations, a requirement for a organisational change. It means also added complexity.

Software is a logical data model of the problem, which it is supposed to handle. And the data model is realized through algorithms. So first you have the model, then algorithms, then data model, then the program and in the end a computer system, that does something useful.

5.6. Computer networks

Use of computer networks, which integrate storage, processing and delivery of information. They are used for the (automation), digitalization, informationalization, integration and especially synchronization of systems of systems. The computer network will give birth to computer-network-troops in use, in counter-and counter counter actions. They will also give birth to the global means of influence.

The use of computer networks will create;
- virtual organisations, organisations, which are best in ever9y area of their actions.
- increase of individualization
- new channel for distributing information based products
- infrastructure for information work and business
- a central element for the rule of complexity
- infrastructure for information warfare

Conclusions: Added complexity. New means for victory. New troops. New ends for influence. Technical intelligence computers and programs everywhere. Information dominance.

5.7. Conclusions from information technology

Technology has five phases in the warfare: Tools, machines, systems, automation, and networks. Two last ones are basicly information technology. This means increased weight of the information technology in the warfare.
In the future electronics and computers, computer networks, their data, information, programs and artificial intelligence in them will be dominant part of the society, "warfare" and warfare. Those who role them, role the society.

Technology will dictate the direction of the evolution. As a consequence of the increased power in the information technology, the evolution will turn towards artificial and virtual evolution.

6. Information warfare

6.1. Importance of information

Information warfare is secret in peace time. In the US Army's officer education three areas of military operations are not fully included for international student officers: (1) Information Warfare, (2) Space Operations and (3) Special Force Operations.[99]

Information warfare needs two changes of information before it can be an independent form of warfare. And both of them are happening now. One is that information must become important, decisive for warfare. As mentioned earlier, it was not decisive in resource-based warfare, just a supporting measure. The other is that information must have a practical way to influence anytime and anywhere to many systems,. It must have it's own dimension.

Information warfare is a hostile influence of which an effect of over 50% is caused by information means.. It can be aided by other means of influence, for instance physical and electromagnetic. A definition by Lt.Col Ahvenainen.

Information's importance is increasing through changes in making, handling, storing and distributing of information:

- automatic and integrated navigation (GPS, Glonass)
- automatic and integrated identification of friend and foe (IFF) (NATO Mk XIII Mode 4 or 5, Enhanced Position and Location Reporting System (EPLRS), Joint Tactical Information Distributing System (JTIDS)), integrations of one's communication means (radios; SINCGARS) and navigation systems (GPS- card or chips in radios)
- automatic and integrating areal communication systems (RITA, Ptarmigan, Mobile Subscriber Equipment (MSE) and coming: Civil satellite communication: Inmarsat, Iridium, Globalstar...
- automatic and integrating information systems in command and control (computers, computer network, Artificial Intelligence; Manoeuvre Control Systems, MCS)
- new intelligence and reconnaissance means (e.g. multi sensor, data fusion, digital manipulation of voice and video, Unmanned Areal Vehicles (UAV), civil satellites, Joint Surveillance and Target Systems (JSTARS), wide-band radar, Open source Intelligence (OSINT), integrated Human Intelligence (HUMINT) systems, commercial optical and radar satellites (EarlyBird 1, Ikonos 1) and maybe the most important technical intelligence in the future, Measurements and Signature Intelligence[100] (MASINT)
- new means of electronic warfare (e.g. digital search, Fast Fourier Transformation (FFT), wavelet, precision direction finding, threat warning systems, jamming of all these electronic means of warfare, navigational warfare, electronic destruction (non- nuclear-

Electromagnetic Pulse, high power laser, High Power Microwave (HPM), particle beams), electronic deception through digital manipulation of voice and video and other signals, Digital Radio Frequency Memories (DRFM)...
- computer and computer networks everywhere; (1) as a means to do something, (2) as a means for attack and (3) as a target, as system needing protection: Hardware (chipping, back-door, special signals...) and software (back-door, virus, hacker, cracker, crasher...).
- information technology to support command and control and especially to direct influence: Many of those mentioned above and: Modelling, simulation, visualization, artificial intelligence[101]
- international electronic mass media (e.g. satellite-TV (Direct Broadcast Satellite)) and of course
- The Internet.

6.2. Consequence of increased importance of information

As a consequence of these changes we will see:
- increased area of operations and interest (increased battle space; in physical dimension and in new dimensions)
- long range effect: airborne, space-based, cyberspace-based
- precision guided weapons (e.g. tactical, cruise and ballistic missiles, Laser Guided Bombs, Wide Area Munition (WAM), psychological, cyberspace)
- accelerated speed of operations and actions (air- and heliborne, VerticalTakeOff and Landing (VTOL), electronic/fire-, reconnaissance/strike and reconnaissance/fire- systems, strategic strike, laser, cyberspace)
- dispersion of warfare means and troops (in physical world and in all dimensions of warfare)
- new means of protection (Direct Energy Weapons, Integrated Electro Optical Defence Suites, CERT- (Computer Emergency Reporting Team), firewalls, virus detection
- precision in every form: weapons, planning, logistic, know-how, influence, intelligence, education...)
- decrease of physical influence and increase of electronic, psychological and informational influence
- beginning of informationalization and real change in command and control, authority
- increase of influence before conventional warfare, avoidance of conventional warfare
- increase of net-based activity and organisations (netcentric warfare)
- increased presence of organisation by amount, that we haven't ever seen
- integration of systems and more in the future integration of systems of systems.

These consequences and this evolution will lead to the forming of information troops. They will include:
(1) troops for use of information[102]
(2) troops for information attack and[103]
(3) troops for information defence.[104]

6.3. Enablerers of the information warfare

Enablers of the Information warfare:[105]
1. Distributed computing and communications: Each node offers potential access; Allows long range attacks
2. COTS (Commercial Of The Selves): Makes it easier to attack; harder to defend
3. Growing expertise in Info Tech - InforWar is both old and new; technology is the new part

4. Internet and HTML - Attack scripts, location of our computing resources... all available world-wide
5. Widely available encryption - Provides relative anonymity of attackers; and pretty good protection of information
6. Cheap, widely available resources - Almost anyone can obtain the capability; 1000 commercial satellite by 2010
7. Use of foreign built software - Insertion points for InfoWar; "I'm from Elbonia and I'm here to help you".

Birth of the dimension of information: Cyberspace, the global integrated entity of communications and computer networks, their programs and data in them or passing between various parts of them. The biggest machine in the world, the international telecommunication system, is made by computers. Yesterday computer connected people through telephone- and fax-machines. Now computers are connecting themselves through automatic intelligence, command and control and weapon systems. Human only make the on/off decisions usually aided by computers and programs in them. With increased artificial intelligence and with demand for quicker action and wider coordination, the computer will continue to make more decisions. And still more computers are connected together through Internet.

Information in information or knowledge based warfare is the means of the effect like troops or fire; target and weapons. Information is networked. Uninterrupted flow of information is essential. Without information there is no warfare. Information is cheap and there are lots of it. Information services are vulnerable and all are dependent on programs. Every level of command has the same, united picture of the battlefield. Information leads to action, anticipation, precision influence and quick operational decisions. Learning happens through experience in war and especially thought simulation.[106]

Conclusions: Added complexity. New means of victory. New troops. Dimension of Information. Information dominance.

6.4. Different types of information warfare

6.4.1. The entity

There can be seen seven different species of Information warfare:[107]
1. Command and Control Warfare, C2W
2. Intelligence-Based Warfare, IBW
3. Electronic Warfare, EW
4. Psychological warfare, PSYOP
5. Hacker warfare, HW
6. Economical information warfare, ECOIW and
7. Netwar/Cyberwar.

Different types of information warfare first add the power of conventional warfare, they create new means of victory and defeat.

Secondly, and more important, they make possible to change the entity of warfare in a way that tanks, air planes and HF- radios changed the warfare between the world wars. Today the best guess regarding this aspect of information warfare is the American military doctrine, Information Warfare and its military adaptation, Information Operations.(ref. chapter 6.4. "Different types of information warfare").

This guess is in the above influence model (see chapter 3.1.3.) The Physical Information Warfare. Other types of information warfare include The Economical, The E.M. Spectrum, The Chemical, The Biological, The Political, The Psychological and The Legal Information Warfare. And of course the Information Information Warfare. The decisive difference is the principal means of effect and precision influence.

6.4.2. The types

Command and control warfare (C2W) is an application of IW in military operations and employs various techniques and technologies to attack or protect a specific target set — command and control (C2). C2W is the integrated use of psychological operations (PSYOP), military deception, operations security (OPSEC), electronic warfare (EW), and physical destruction, mutually supported by intelligence, to deny information, to influence, degrade, or destroy adversary C2 capabilities while protecting friendly C2 capabilities against such actions. C2W is applicable throughout the range of military operations.[108]

Command and Control Warfare (C2W) is a strategy, not enabling capability or function, like its predecessor Command, Control and Communication CounterMeassures (C3CM). C2W is military strategy, that implements national Information Warfare with armed forces.[109]

Intelligence-Based Warfare (IBW) is computerizing, automation, new kind of speed and synchronization of warfare. It is more the use of intelligence directly to quiding of operation and weapon systems than to support command and control. Information is input that quids systems. Information Based warfare- systems integrate information to the decision making and the decision making to the action.

Essential elements in the IBW are computer systems which integrate command, control, communication, intelligence and weapon (influence[110]) systems. Building of those systems starts with modelling of the entity. Modelling makes possible to compute, simulate and use the power of technical and artificial intelligence. This means automation and increased speed of action and syncronation. This means also increased parallelism to the warfare.

Electronic Warfare (EW) consist of all those military actions, that use E.M. spectrum or Directed Energy for the dominance of E.M. spectrum or for attack against the enemy. EW is divided to Electronic Support (ES), Electronic Attack (EA) and Electronic Protection (EP). EP is an activity of all those troops or systems, that have systems or equipments that are vulnerable to ES or EA. ES and EA are usually activities of special trained and equipped EW- troops.

EW's fields can be divided to three big areas of use of electromagnetic spectrum, which overlap some. First is command and control, second is sensors and third is electronically supported or electronic weapons systems.

Psychological warfare or Psychological Operations (PSYOP) is associated with information in effect chain: Desired effect - the message to support the effect (action or signal; information) - transmission of the message - reaction - effect of the message - change of the behaviour (to the desired). The transformation from information to behaviour happens in men mainly through subconscious psychological processes.

The areas in psychological warfare are actions against cultures, will of peoples, will of troops and will of commanders.[111]

Psychological warfare is not new by itself. It is as old as warfare. The change is new means to conduct it, especially through electromagnetic means like radio, TV, international computer and TV networks (CNN, DBS), on earth and especially in satellites. It is essential that a man is a visual, seeing creature with a subconsious mind.

Hacker warfare is warfare, or hostile influence, that takes place in the cyberspace, integrated entity of world's computer- and communication networks in different use.

The asocial population in computer networks can be devided into the following groups: (1) Hackers, who break into computer systems motivated by curiosity. (2) Crackers, who insist free usages of computers programs. (3) Crashers, who aim destruction and sabotage in computers systems. (4) Computer criminals, who aim economical benefit through criminal use of computer systems and lastly (5) professionals in intelligence organization or freelance specialists who represent nations or organisations, special forces's special forces, modern mercenaries.[112]

Ends of hacker warfare can be total destruction, closing down the network, wholly or partly, making up random or purposeful data mistakes, stealing information, stealing services, monitoring the system, information collection from countermeasures, and information collections for blackmail.

Means of hacker warfare include for instance back door of hardware or software, bucks in software (accidental or purposeful), virus, logic bomb, Trojan horse, password sniffers, security programs for computer network like SATAN, social engineering, looking over one's shoulder, dumpster diving for written down password and program listings, Back Orifice- type means to control a computer connected to the Cybercpace...

Famous example is the German spy gang in Stoll's book "Cocoo's Egg". Hackers broke in many US computer networks in military and civilian systems and the data was delivered to Soviet KGB.[113]

Economical information warfare is to use information to influence in the economy, first by the economical information blockade and secondly by the information imperialism.

The economical information blockade is based on the thought, that uninterrupted flow of information is as important as the flow of material. In the information barrage one denies a country access to international communications. It makes for instance the international finance impossible. The economical information blockade is a non violent way of influence.

New satellite communication systems like Iridium or Inmarsat make the economical information blockade difficult in the future. The trade of information and expert knowledge in the information networks (Internet) makes the economical information blockade more wounding than today.

The information imperialism is based on the thought that the economy is warfare. The most developed, the fastest growing industry is information intensive. The use of new resources in those areas inside one own country give an considerable advantage as also the research or the military acquisition in those areas. One favour one's own corporations, as a buyer or as a subcontractor. This makes them to develop. Global enterprises make is more difficult to use information imperialism.

An example: Japanese auto manufacturer in USA give the most interesting subcontracts to the Japanese firms. New Japanese information technology is first sold only in Japan for a period of six months.

Netwar is about ideas, and epistemology, what is known and how it is known. Netwar is most likely to be a nation-against-nation strategic level conflict and is new form of psychological warfare. Netwar actors include nations and non-national organisations like Greenpeace, Amnesty International, survivalist militias and Islamic revivalist. Netwar happens largely, but not entirely, in the universe of societies's interneted communications systems. It is precision psychological influence through new medias like computer bulletin boards, cellular phones, video cameras, fax machines, world wide television (DBS) and broadcast news (CNN) and new systems like simulation and voice and video manipulation technologies. As a consequence of these new possibilities, netwar is beginning to enter the zone of illusion, virtual reality. US entertainment industry's impact on other nations is an example of netwar, or a form of cultural imperialism. [114]

Netwar consists of societies view of themselves and world around them. Netwar includes manipulation of this view by diplomacy, propaganda, psychological actions, political and cultural persuasion and by infiltration to the local media and computer networks.

Cyberwar is warfare, hostile influence which is fought in cyberspace. Cyberwar is netwar by the military. It includes hackers, listeners of communications systems, van Elck-radiation[115] listeners and so on. Cyberwar consists of information terrorism, semantic attack, simulation warfare and Gibson warfare. Typically Cyberwar is warfare, or hostile influence between attack- and defence programs in computers, computer networks and communication systems.

6.4.3. Conclusions from modes of information warfare

The types of information warfare in the Libiski's classification are mostly old things. The hacker warfare and the netwar/cyberwar are new types of warfare made possible only after the introduction of modern information technology.

In the other types of information warfare the change is that information handling and distributing has become a central element of the old activity: In the conventional warfare, in the economy, in the psychological influence.

For every major action, there is a counteraction in military history. Information revolution will inevitability form such a counteractions. Different forms for information warfare's counteractions can be: (1) Underground shelters for key installations. (2) Biological substances like biological warfare agents and human performance enchanters. (3) Selective and combinating use of advanced information technology. (4) Lots of simple and cheap intelligence systems. (5) Massive use of cheap, crude, though effective cruise missiles. (6) Use of weapons of mass destruction. (7) Advanced new material in ceramics, steel alloy, polymer composites and thermoplastics. (8) New operational concepts.(9) New discoveries of scientific research.[116]

7. CONCLUSIONS

Information warfare is not a new principle of influence. Information warfare does not mean change in the logic of warfare. Information warfare is not the end of warfare. Information warfare is not warfare through information only.

Information warfare is dominance by information. In time of peace and war. Inside the nations and between the nations. Information warfare is more than ever warfare in peace. Or hostile influence. Information warfare is change **inside** means of influence and new tools inside old means of influence. These changes adds weight to information and information systems. Information warfare is some new things. Information is prestep of influence, necessary but not enough by itself. Except if one controls the enemy's systems. Information is new troops. New means of victory and defeat. Added complexity. New ends to influence. Change from reactions to anticipation. Information warfare is the Change. The Quick and the Big One. It is not difficult to understand the New. It is difficult to give up the Old.

Information society benefits them, who dominate the core of it: microprocessors, computer network, communication networks, their basic and application programs for add on value at different level. Mostly this means now USA and its economy.

Now and in the near future the change in physical influence, in warfare, means it's decreased importance and more emphasis on economical influence and later more information as a principal means of influence. However, warfare and economy will not disappear.

The change in warfare, birth of information warfare, is associated and influenced by:
(1) global technology, especially information technology (microprocessors, programs, computer networks and communication systems) and science,
(2) global means of communications (electronic and physical),
(3) increased importance of economy, especially global (information) economy,
(4) global organisations (coalition warfare, multinational enterprises,),
(5) network organisations and activity...

As a consequence these changes mean decreased importance of nation states, increased importance of virtual reality, network organisations and dominance of economy, information, technical intelligence and USA and other information and network based organizations.

The information age is creating or will create new means of influence and new ends to influence. This process will create new means of victory, new troops and added complexity. It is important, that these new things will add new possibilities between war and peace and it will increase possibilities to act before war and to avoid conventional warfare.

Superior technology is not essential by itself. One can have effective counter technology or counteraction, asymmetric doctrine, against it. And counter-counter technology against counter technology. Consequence: Complexity. The essence of the Entity.

Superior quantity is not essential by itself. Nor superior will, operational or tactical skill. The superior entity in relation to the enemy and operational environment is essential. Consequence: The Synergy. The Complexity. The Entity.

Conventional military is not the correct means to protect all modern nation's essential resources. Security is more complex. In order to protect a nation, one has to protect its borders on land, on and under sea, on air, on E.M. spectrum, on cyberspace and on national will. This protection has to take place in every activity of the society, e.g. in military, in economy, in finance, in transportation, in mass media, in energy and in diplomacy.

What is essential in times of continuos change ? It is the vision of new ways to act in the future, ability to change your acting in steps, which your people and organization can choke down, research-, education- and acquisition system to support the change, people of change,

will to change. Change the entity and change it quicker than the others to rule the complexity and the Entity, to get synergy and to have Intuition. And to give up the Old.

Peace, war and the widening grey area between them. The widening complexity of warfare. The essence of the Entity. New means and ends of victory. New troops. Information dominance. Increased importance of technology. Increased importance of global and networked means (technology, science, communications, economy, organisations...)

We live in an interesting time. There will be the old. And we will see the Change. The Big One.

Post Scriptum 1: Answer to the question at the introduction: What is warfare in the time of a rapid change, in the time of information ?" It is a hostile influence, mainly but not exclusively by information

Post Scriptum 2: More important than the information is E.M. spectrum (Electronic Warfare), a means to acquire and deliver information and even more important than it is the will (Will Warfare), the people, still a principal means to assess and act on complicated information (reality) and hereby to influence, especially other people or systems that they control.

1. A definition by Lt.Col Sakari Ahvenainen.

2. A modified version of Sun Tzu's thought about combinations of ordinary and exraordinary troops, or five tones, five basic colours and five tastes. (Sun Tzu:"Sodankäynnin taito" Love Kirjat Helsinki 1982 p.98 -99) (in finnish) ("Art of warfare").
This is the very core of this essay. There is some (eight) basic means of influence and information is not the new one. Physical influence has losed some of it's effect and economical influence has gained some more. Informational influence will be the next dominant means of influnce. But not the only one.

3.T J Czerwinski:"The Third Wave: What the Tofflers Never Told You" Strategic Forum Number 72 April 1996 (Internet: http://www.ndu.edu/inss/strforum/forum72.htlm); originally physisist Heinz Pagel

4.Computer = hardware (microprosessor) and especially programs (software).

5.Maj K B Smith:"The Crises and Opportunity of Information War" School of Advanced Military Studies, US Army CGSC 1994 p.25

6. Field Manual No 100-6 (FM-100-6) Headquarters, Departement of the Army, Washington DC, p.24

7.Author's definition. (1) One definition of information society is that it is a society, of which products and sevicies over 50 percent is produced, delivered and consumed in the information networks. (Ref. P Järvinen:"Tietoyhteiskunta tulee, mutta mitä se tekee" Helsingin Sanomat Kuukausiliite 3/1998 p.80 (in finnish) ("Information Society is comming, but what does it do ?")
(2) Ref. To chapter 3.1. "Warfare as a way of influence"

8.Each year since 1965, the U.S. commercial sector has invested more of its dollars in research and development than has the Department of Defense (DoD). Note 31 in Lieutenant Colonel William R. Fast:"Knowledge strategies: Balancing ends, ways, and means in the information age" Internet

9.Author Leena Krohn:"Synteettinen evoluutio on alkanut" Helsingin Sanomat 5.7.1998 p.1 (in Finnish) "The syntetic evolution has begun". De Garis (see http:\\www.hip.atr.co.jp.~/degaris/Artilect-phil.htlm) call mashines, that are more intelligent than humans, artilects. Vernor Vinge says, that the civilisations as we know it is going to end. He calls this transformation "technical singularity".

10. Virtual Reality interacting with reality and becoming real. See M Castells:"The Information Age: Economy, Society, And Culture" Volume I "The Rise of The Network Society" Blackwell Publishers Inc. USA 1999 p. 372

11. Political includes in this essay cultural and diplomatic influence.

12.This structure answers also to the question:"Is it possible for a information army to make information warfare towards agricultural or industrial army?" Yes it is, because the information army **uses** its information on their enemy to their advanges (where the enemy is, what means of influence its has and so on). **Attack** is also possible for instance in the psycological level. **Defence** is maybe not so important.

13. S Biddle:"Assessing Theories of Future Warfare" Institute for Defence Analyses. Presented to the 1997 International Studies Assocciation Annual Convention, Toronto, March 19, 1997

14.According to Gwyn Prins in an article by P Tyrell:"Information Warfare - The European Perspective" p.3 HSA's Information Conference, London 13.-14.11.1997

15. Daily Telegraph's defence editor and lecturer in military history J Keegan:"A History of Warfare"Vintage Books, New York 1994, for instance p. xii, 23, 32, 43 and 63

16. M van Creveld:"The Transformation of War" The Free Press 1991 p.157

17.Autors Alvin and Heidi Tofflers:”Future Shock” New York, Bantam 1970

18.Autors Alvin and Heidi Tofflers:”War and Antiwar; Survival at the Dawn of the 21th Century” Warner Books 1993 p.20

19. For instance US Army sees, that in the future there will be following kind of combat forces: (1) Internal security forces, (2) infantry based armies, (3) armour-mechanized- based armies and (4) complex, adaptive armies. Only the last one is a new type of combat force. (US Army, Tradoc Pamphlet 525-5 “Force XXI Operations” 1.August 1994 p. 2-3 - 2-5)

20. See T J Czerwinski:"The Third Wave: What the Tofflers Never Told You" Strategic Forum Number 72 April 1996 (Internet: http://www.ndu.edu/inss/strforum/forum72.htlm)

21. (1) Human brain as a most compicated structure of universe is (still) the prinsipal means of ruling the complexity. Especially in networks with other educated brains. But in many cases, the complexity of the problem or entity is so great, that only computers and computer networks can aid. And the trend is clear: More computers, less brain. This means not incresed stupidity, but increased weight of computers.
(2) There is some examples of this trend of computing beeing superiour to man’s information prossessing. First weather forecast: With the introduction of the super computers in Finland in the 1980's, there was a raise in the succsess to have the short term whether right.
(3) Some of the deduction of neural networks are allready beyond human competence, especially in complex information. (Aaltonen Matti:”Sodan sydänäänet”. Sotilasaikakausilehti 3/96 p.28 - 31 (in finnish) (“War’s heart beats”)
(4) Kasparov, chess and Deep Blue.

22.The British general Simpkin sees in the warfare three levels, which are physical, risk and will levels. (R S Simpkin:”Race to the Swift, thoughts on twenty-first Century Warfare” p. xix - xx)

23.C von Clausewitz:"On war" Princeton University Press 1976 p.103

24. For instance when one compares Israel and Arabic Air Forces one gets next results. First, on the basis of pure quantity Israel is outnumbered 450 to 1408. Secondly, when one counts, how many hard point target can be destroyed per day the Arabs are outnumbered 501 to 3781. (Jane’s Intelligence Review Special Report No 14 p.19). Ability to destroy hard point targets deep in the rear of the enemy means information; Surveillance, target aquisition, communications, presicions quided weapons, computers and programs, EW, SEAD...

25.A D Campen & D H Dearth & R T Goodden (ed.):”Cyberwar; Security, Strategy, and Conflict in the Information Age” AFCEA International Press, USA 1996 p.224 (An article by John L. Petersen)

26.See (1) D Lyon:”The Electronic Eye; The Rise of Surveillance Society” Polity Press, Great Britain, 1994
(2) V I Pajunen:”USA salakuuntelee Euroopassa rikollisia ja kansalaisjärjestöjä” Helsingin Sanomat May 10 1998 p.C1 (“USA eyvesdrops criminals and organization of citizens in Europa”) This article deals with the Encelon, signal intelligence organisation of USA, Great Britain, Australia and New Zeeland.
(3) Social scientist Rob Shields, who says that Finland is ten years behind Great Britain in video camera surveillance and that there is already comprehensive video camera systems in Great Britain in public areas in villages as small as 2000 inhabitants. (J Päivänen:”Matkalla kohti totaallista turvaa” Helsingin Sanomat May 25, 1998 p.B5 (in finnish) (“On the journey towards total security”)
(4) A Karismo:”EU- maiden poliisit kuuntelemaan puheluja rajojen yli” Helsingin Sanomat 25.9.1998 p. C3 (in finnish) (“Polices of EU memderstates will intercept phone calls across bordes”)
(5) P Sadeniemi:”Venäjän turvallisuuspalvelu hakee oikeutta sähköpostien lukemiseen” Helsingin

Sanomat 4.8.1998 p. C 1 (in finnish) (“Russian FSB is seeking right to read e-mail”)
(6) Or Russian Federal Security Service’s (FSB) system called SORM to intercept all Internet traffic direclty from the Internet Service Provider’s in Russia. SORM, In Russian, the letters stand for "System for Facilitating Investigative Searches. (Daily Telegraph 06/08/98 p.3, Independent 11/08/98, p.13)
(7) M Perelman:”Class Warfare in the Information Age” St. Martin’s Press New York 1998 p.2

27.Information expert Bert Mulder in an article by L Lavonius, Helsingin Sanomat, 18th. August 1996 p. A13 (in finnish); for exanple:
(1) In a couple of years, Netscape turned into billion dollar bussines, so also Hotmail and Starwave. (S Waldman:”Lyhyin tie miljonääriksi” Suomen Kuvalehti No 42 1998 p.51 (in finnish) (“The shotest way to become a millionaire”))

28. M Heikka:”Eliitit tulevat” Suomen Kuvalehti No 45 1998 p. (in Finnish) (“The Elite is comming”); Information society is a power shift, which has previously included big and violent struggles in many levels of human activity.

29. In his doctoral thesis: ”Kohti epäselvyyksien hallintaa” Suomen Tulevaisuuden Tutkimuksen Seura, Finnpublisers Gummerus 1996 (“Towards the control of the ambiguity”) Markku Sotarauta introduces the term “nasty” problem, opposite of which is a clear, limited problem which includes a closed systems.

30. A modern state is more and more an open system. It is influenced by neighbouring countries and even pollutions of far-away countries (Chernobyl) and their problems (civil war, refugees). A modern state is tied up with many bonds to international trade and science. The state communication system has many connections with the international communication systems. There is extensive tourism. Broader international division of labor ties up nations to a tighter network. Money is moved in and out of the country literally in a second. All this concerns also firms and individuls. More and more.

31. John Arquilla & David Ronfield:”The Advent of Netwar” RAND 1996 p.46

32. Air Defence (ACCM) (e.g. Anti Air Artillery and Surface to Air Missiles) have as countermeassures Suppression of the Enemy’s Air Defence (SEAD).

33. M Castells:”The Information Age: Economy, Society, And Culture” Volume I ”The Rise of The Network Society” Blackwell Publishers Inc. USA 1999 p. 477

34. M Castells:”The Information Age; Economy, Society and Culture” Volume III “End Of Millennium” p.356 - 360 Blackwell Publishers Inc. USA 1999

35. Manuel Castells:”The Information Age: Economy, Society, And Culture” Volume II”The Power of Indentity” Blackwell Publishers Inc. USA 1999 p. 359

36. John Arquilla & David Ronfield:”The Advent of Netwar” RAND 1996 p. 33 - 34

37. A Vahtera:”Savuverhon suojassa; Peitejärjestöjen ansiosta amerikkalaisyritysten ei tarvitse avoimesti vastustaa ympäristönsuojelua” Helsingin Sanomat 26.7.1998 p. D 4 (in Finnish) (“Behind the smoke screen; Because of the cover organizations, US firms do not need openly resist the environmental control”)

38. A D Campen & D H Dearth & R T Goodden (ed.):”Cyberwar; Security, Strategy, and Conflict in the Information Age” AFCEA International Press, USA 1996: Artikkeli: Elin Whitney-Smith:”War, Information and History: Changing Paradigms” p. 53 - 69

39.T Arolainen:"Britanniassa oikea tieto hillitsi kuolemanrangaistuksen vaatijoita" Helsingin Sanomat 5. May 1995 p. A 11 (in Finnish) (“In Britain the right information restrained those who wanted death penalty”)

40. Professor Shoshana Zuboff:"Viisaan koneen aikakausi" Otava 1990 p.432 (in Finnish). Originally: Shoshana Zuboff:"In the Age of the Smart Mashine; The Future of Work and Power" Basic Books, New York 1988

41. In the Gulf War of 1991 the USA had on the first day as many targets as the Allies had combined in Germany in the years 1942 and 1943. Ref. To Precision Guided Weapons and automatic Command and Control systems.

42. M C FitzGerald:"Russian Views On Information Warfare" Army May 1994 p.60

43. See (1) J Keegan:"A History of Warfare" and
(2) M van Creveld:"The Transformation of War" or
(3) A Rusi:"Sota; väkivalta voidaan rajata ja sen käyttöä valvoa" Suomen Kuvalehti No 20 1998 p.57 (in Finnish) ("War; violence can be restricted and it's use can be controlled") or
(4) Under the microscope of world opinion formed by means of pervasive communication satellites, open warfare is no longer an option for sovereign nations to pursue their national interests. Cable News Network coverage can rapidly trigger a negative international response, as we have seen during the recent wars in Somalia and Bosnia (Lieutenant Colonel William R. Fast:"Knowledge strategies: Balancing ends, ways, and means in the information age" US Army, http://www.ndu.edu/ndu/inss/siws/ch1.html)

44. A Rusi:"Toiveista tehty tulevaisuus" Suomen Kuvalehti No 10/1998 p. 65 - 66. (in Finnish) ("Future made by hopes")

45. A D Campen & D H Dearth & R T Goodden (ed.):"Cyberwar; Security, Strategy, and Conflict in the Information Age" AFCEA International Press, USA 1996 p.224 (An article by John L. Petersen)

46. Andrew F. Krepinevich:"Cavalry to Computers: The Pattern of Military Revolutions" The National Interest Fall 1990 p.30

47. Ref. To German Blitzkrieg or Mongol's 12th century warfare and their operative succsess.

48. US Army Fied Manual 100-6 "Information Operations" p.2-3 - 2-4 6.12.1995

49. The gravity on the enemy can bee seen for instance as the armed forces, the knowledge, the economy, the technology or the public opinion. They will create different strategy and different means and ends.

50. T J Czerwinski:"The Third Wave: What the Tofflers Never Told You" Strategic Forum Number 72 April 1996 (Internet: http://www.ndu.edu/inss/strforum/forum72.htlm); originally physisist Heinz Pagel

51. W E DePuy:"Concepts of Operation..." p. 12 in a book: C E McKnight:"Control of Joint Forces"; AFCEA International Press USA 1989

52. Every attacker - defender combination from three society models: (1) Agra-agra, (2) agra-indu, (3) agra-info, (4) indu-agra, (5) indu-indu, (6) indu-info, (7) info-agra, (8) Info-indu and (9) info-info. It is inuitively clear, that every nine war models are different and one should know just the combination and its characteristic of the warfare type one is preparing. See also A D Campen & D H Dearth & R T Goodden (ed.):"Cyberwar; Security, Strategy, and Conflict in the Information Age" AFCEA International Press, USA 1996, article: Elin Whitney-Smith:"War, Information and History: Changing Paradigms" s. 53 - 60

53. A modified version of Sun Tzu's thought about combinations of ordinary and exraordinary troops, or five tones, five basic colours and five tastes. (Sun Tzu:"Sodankäynnin taito" Love Kirjat Helsinki 1982 p.98 -99) (in Finnish) ("Art of warfare").
This is the very core of this essay. There is some (eight) basic means of influence and information is not the new one. Physical influence has losed some of it's effect and economical influence has gained some more. Informational influence will be the next dominant means of influnce.

54.A D Campen & D H Dearth & R T Goodden (ed.):"Cyberwar; Security, Strategy, and Conflict in the Information Age" AFCEA International Press, USA 1996 p.224 (An article by John L. Petersen)

55. (1) According to doctor of philosophy Terhi Pöyhönen, doing something requires **allways** ability, will, endurance and courage. (T Pöyhönen, lectures in Vierumäki, Finland 10. - 12.4.1998).
(2) According to admiral Cebrowski (US Navy) knowing what to do with the information will be just as important as the information itself. (Cebrowski in an article by B Bender:"Buying into networked warfare" Jane's Defence Review 13 May 1997 p.27)

56. (1) If we dont do it, it may be that we do not undestand the change, we concentrate on old means, ends and ways and the change bybasses us by the new means, ends and ways.
(2) It is common in many countries that in the military, you as a commander have to undestand very well the commanders intent at a one level higher than yours and well also two levels up (two levels up-principle). Well, what is one level higher than the warfare ? Politics or society. What is two levels higher than the warfare ? Influence, evolution. So to understand information warfare, a rapid change, you have to examine politics, societies, influence and evolution.

57. (1) Economist K Arrows says that trust is a necessary and efficient lubricant in the society. It saves money and time, because things get done quickly and easily. (M Heikka:"Länsi hiipuu, Aasia nousee" Suomen Kuvalehti No 31 1998 p.34 (In Finnish) ("The West is fading, Asia is arising")
Ps1. Finns trust the most to other citisens of the own country in the world
Ps2. During the first years of the new millenium, over halv of the age bracket in Finnland will get their education at an institution of higher education as a result of the polytechnic school system.

58. S Peres:"Peres&Jiang; Suurvalta syntyy" Helsingin Sanomat 3.5.1998 p. D 4 (in Finnish)
(Peres&Jiang:" Superpower arising")

59. Corn: 200 dollars per ton, automobiles 6000 dollars per ton and CD- ROM 50 dollars per 15 grams, or 3.300.000 dollars per ton.

60. The New Encyclopedia Britannica 1989, Vol. 18 p.312

61. Legal influence: Local, national, multinational (EU, EMU) and international level (UN, Geneva treaty, new international warcrime tribunal, which was established July 17 1998 in Rome.)

62. P Lapintie:"Kirjolohi oppii käyttämään tietokonetta ruoka-aikana" Helsingin Sanomat 25.11.1998 p.A 5 (In Finnish) ("The rainbow trout learns to use the computer to feed itself"). In this article the writer says that by using computer based feeding systems (a intelligent, information and network based system quided by man), on can lower the food amount from 5 kilos to 1,3 kilos to produce one kilo of fish.

63. (1) It pay off to allogate to the military only so much, that they can support country's economical interesses and to stop direct attack to the country (USA). (Fieldmans in the book "The future of war").
(2) Lt.Col Kuparinen from the Signal School of The Finnish Army has the same conclution in the rapport from MilCom97, California USA (Viestirykmentti, kertomus 9.12.1997 Kuparinen & Kuusisto & Lallo (in Finnish))
(3) According to Finland's president's adviser A Rusi, economical and technological co-dependence between states is becoming so high, that temptation to war is decreasing. (in Finnish) (Suomen Kuvalehti No 10/1998 p.65)
(4) "Our (USA) most vocal critics say the material comfort of America is based upon economic imperialism backed by military forces" (Col P Coakley:"Command and control for war and Peace" NDU)
(5) Security of a nation (in the age of information society) is more influenced by it's knowhow and economy than it's military. (P Järvinen:"Tietoyhteiskunta tulee, mutta mitä se tekee" Helsingin Sanomat Kuukausiliite 3/1998 p.84 (in Finnish) ("Information Society is comming, but what does it do ?").
Comment: "More" is the key word here.

(6) “Economic strength will be more important than military strength. The new world order will be defined by trade ralations, by flow of information, capital, and goods, rather than by armies glaring at each other across borders. “ (Retired Chairman of the Chiefs of Staff General Colin Powell in his book “My American Journey”. This makes an interesting poins for instanse of Finnish baying of F/A-18 Hornet by about 3000 million dollars from USA, with full compensative trade.
(7) J Saatamoinen:”Aarne Nurmio, Näkökulmien avartaja” Suomen Kuvalehti 25-26/1998 p.62 (in Finnish) (“Aarne Nurmio, Expanderer of the point of view”): It seems to the citicens by and by that the real dicisions are made more often in the cabinets of the enterprises instead of the parliament.

64. (1) See chapter 7.1. “Importance of information”
(2) According to US Army’s Field manual 100-6 “Information operations” information, information based prosesses and information systems have become central elements of warfare due to their increased importance. See FM 100-6 definition for IW, chapter 0.1.”Some definitions”

65. Ref. For instance Vietnam and US television or Somalia 1994 and effect of a one video clip, although globally distributed.

66.S Peres:”Peres&Soros; Vieläkö rajoilla on merkitystä?” Helsingin Sanomat March 5, 1998 p. D6 (In Finnish) (“Peres&Soros; Does borders still have significance?”)

67. (1) F Sand & J Ångström:”Mot en ny ording; Hot och säkerhetspolitiska problem bortom sekelskiftet” Kungliga Kriegvetenskapsakademiens handlingar och Tidskrift 2/1997 p.134 (in Swedish) (“Towards a new order; Threath and security political problems after year 2000")
(2) T Ervamaa:”Ganstereiden ja hallituksen yhteistyö kuohuttaa Turkkia” Helsingin Sanomat 24.11.1996 p.C 4 (in Finnish) (“The Co-operation between gangsters and govemment infuriates in Turkey”)

68.Lale Sariibrahimoglu:”The crash that shook Turkish security to the core” Jane’s Intelligence Review April 1998 p.8 - 11

69. (1) Ira Winkler & Stanislav Lunev:”Through the Eyes of the Enemy” Besides of telling the stories of Lunev's life, Through the Eyes of the Enemy tells of GRU tactics, current Chinese and Russian intelligence activities, as well as the infiltration of the Russian Mafia into the Russian Government. The more controversial aspects of the book include details of GRU assassination squads, the possible GRU forward deployment of weapons of mass destruction on US soil, the Russian Mafia purchase of a Kilo class submarine to run drugs, and the Russian Mafia being the major source of tasking for the KGB/SVR and the GRU
(2) In the SMi’s information seminar 26. - 27. March 1998 in London the Swedish lecturer presented three scenarios, which they had used to study the future of the (information) warfare. On scenario was “Russian Cyber Warlords 2010" (Eva Mittermaier:”National and International Security in the Network Age” Presentation at the SMi’s Information Warfare Conference 26. - 27. March 1998)

70.C J Rhodes:”Information Warfare” Military Conference (MilCon97) Proseegings 1997 p.233

71.S Peres:”Peres&Soros; Vieläkö rajoilla on merkitystä?” Helsingin Sanomat March 5, 1998 p. D6 (In Finnish) (“Peres&Soros; Does borders still have significance?”)

72. Doctor J S Kramer in an article by J Ukkola:”Tietotekninen vallankumous” Suomen Kuvalehti No 5 1997 p. 30 - 35 (in Finnish) (“The Revolution in The Information Technology”)

73. This in not the same category as the Inteligence Based Warfare in chapter 6.4.2. in the Libicki’s model, where it means full automatic weapon effect. In here intelligence information warfare means influence, which effect is caused by pure intelligence.

74.M Howard:"The Forgotten Dimensions of Strategy" Foreign Affairs Summer 1979 p.976- 7

75.E A Cohen & J Gooch:"Military Misfortunes: The Anatomy of Failure in War" The Free Press New York 1990 p.231

76. For instance: Miyamoto Musashi:"The book of five rings" p.107 Shambhala Boston & London 1994: "You may have to repeat something once, but it should not be done a third time"

77. The organisational level consearns also economic. Refer to co-optition p.15 Or Helsingin Sanomat July 26 1998 p.D4 (in Finnish) "Because of cover organisations (,which they support economicly), US firmas don't have to oppenly resist inviromental movements" So these cover organisations become part of the supporting firma, part of it's networked organisation. Military or intelligence use of cover organisation is even more common.

78. Eva Mittermaier:"National and International Security in the Network Age" Presentation at the SMi's Information Warfare Conference 26. - 27. March 1998 p.3

79. (1) International Forum for Incident Response and Security Teams (FIRST).
(2) CERT- (Computer Emergency Reporting Team). International, national and local organisation for raporting computer incidents. First was established 1988. (see http://www.cert.org/)

80. Tofflers and Fieldmans scenariorize a war, where technology bybasses everyting else and so a war which is won by the more advansed in tehnology. But according to chapter 3.2. "Change in the functional dimension of warfare", technology is only one functional dimension of warfare, so it is possible to lose a war other way, even if one is superior in technology. Ref to German and Western tanks in technology and in numbers 1940 or Russia and German tansks 1941 (T-34), Vietnam 1973 or Somalia 1994 or RMA II (as a reaction to RMA I)

81.Colonel M Brown, US Army, in the SMi's Information Warfare seminar 26. - 27.3.1998 in London

82.R Grabau:"Sechs Dimension des Krieges; Versuch einer analytischen Betrachtung" Part I: Soldat und Technik 5/1986 p.224 -249, Part II 6/1986 p.328 - 337 and Part III 7/1986 p.392 - 398 (in german)

83. Real world and changes in it can bee converted by observation or/and measuring into information.

84. So beeing between surface (2.dim.) and space (3.dim,) in Pirumov's model, fire can be seen as a 2½. dimensions. A dimension not totally free of surface. As the speed of a projectile goes over 7 km/s, the projectile is free of surface, or gravity of the earth.

85.Amiral Pirumov, Russia, in Bryssel at InfoWarCon96 May 1996

86.Major S Ahvenainen:"On warfare, electronics and EW" Tiede ja Ase No 52 1994 p.103, modified to information (in Finnish)

87.D J H Pittard:"Thirteenth Century Mongol Warfare: Classical Military Strategy on Operational Art ?" School of Advanced Military Studies, US Army CGSC, Kansas 1994

88. (1) Colonel (ret.) A Campen:"Promise and Peril of Information-Based Warfare" InfoWarCon95 Conference Proceedings 1995 p. L7
(2) Ltcol M Koli:"Combat, information and command and control" Presentation in a seminar in Finnish Defence Staff 29.4.1997 (in Finnish)

89.Computer = hardware (microprosessor) and especially programs (software).

90. Martin van Creveld:"Technology and Warfare" The Free Press, New York 1991, table of content.

91.Of course writing, counting and map making were always important for warfare.

92.ARPANET, Internet's predecessor had four computers networked 1969 in USA.

93.Captain (eng.) T Halkola:"Data Fusion - Intergration of Sensors of Diverse Forces" Research work at The Royal Military College of Science, England 1992 p.1

94.C J Rhodes:"Information Warfare" Conferense Proseedings Milcon 97 p.238

95. IBM's Deep Blue- computer defeats Gari Kasparov 3,5 to 2,5, May 1997. His only match defeat ever !

96.Adm. J B Busey:"Microprocessors Threaten Supercomputing's Progress" Signal February 1995 p. 12

97..D Pountain:"The Last Bastion; Feature" Byte September 1994

98.See for instance (1) PROMIS, a program of the 1980's, a tool for intelligence work, but also a tool for spying by it's backdoor capability (Finnish Television A-studio 4.6.1997; http://www.yle.fi/a-studio/promis.html) or
(2) Tieto&Kone:"Suuri sähköpostisäikähdys" Helsingin Sanomat July 7, 1998 p.D3 (in finnish) ("The Great E-mail Scare"). Finnish young data security experts discovered a security hole in new E-mail systems of Microsoft and Netscape. Ref. Also to Swedich researsher in the end note 67 about the difficulty to separate between an accident and a purpouseful attempt of influence or preparation of it. Or
(3) data security (and break-in) programs like SATAN (Security Analysis Tool for Auditing Networks) , SPI, COPS, Internet Security Systems' (ISS') Internet Scanner 5.0 for Winfows NT or PingWare from Bellcore.

99.T Hyötyläinen:"Miten te osallistuitte Afganistanin sotaan" Kylkirauta 2/1997 p.16 (in finnish) ("How did you participate to the war in Afganistan ?" Major T Hyötyläinen was a finnish student in the US Army Command and General Staff Officer Course 1997- 1998.

100.Z Lum:"The Measure of MASINT" Journal of Electronic Defence August 1998 p.44

101. Example of artifical intelligence is US Army's Hawkeye, part of ASAS's (All-Source Analysis System) SIGINT system, its AI- module test bed. It makes from SIGINT's massive data command posts, staffs and troops as part of division and corps. It makes intelligence out of data. (M Hewish:"Workstation-based C3I systems" Defence Electronics & Computing (Supplement to International Defence Review 6/1992 p.82))

102. (1) Intelligence, reconnaissance and surveillance troops.
(2) The Finnish Signal Battailion YVI 2 includes command and control platoon for planing, integration and controlling battailions various communication systems.
(3) Computer Network units in different staff organisations.
(4) All progammers creating, modifing or supporting myriad command and control programs in the military.

103. (1) Electronic Warfare Units
(2) Hacker units (not offically existing anywhere yet)
(3) Deception units (russ. maskirovka)
(4) Offensive Propaganda units

104. (1) Defencive Propaganda units
(2) CERT- type computer network units
(3) Units or individuals using, modifiding and produsing network- and software protection programs and systems

105.Anita D'Amico:"The Roles of Information Warfare and Common Understanding of the Battlespace in the Contest for Information Superiority" p. 27 HSA's Information Conference, London 13.-14.11.1997

Comment: These point ably only to the technical information content of the information warfare. There is for instace sosial psychological content of the information warfare. Or biological information content.

106.(1) Colonel (ret.) A Campen:”Promise and Peril of Information-Based Warfare” InfoWarCon95 Conference Proceedings 1995 p.L7
(2) Ltcol M Koli:”Combat, information and command and control” Presentation in a seminar in Finnish Defence Staff 29.4.1997 (in finnish)

107.M Lubicki:"What is Information Warfare ?" National Defence University ACIS Paper 3 August 1995 Prefase (Internet http://www.ndu/inss/actpubs/act003/a00ch00.hmtl)

108. Joint Doctrine for Command and Control Warfare (C2W) Joint Pub 3-13.1, USA, p. v

109.Lt.Col N B Hutcherson:”Command and Control Warfare; Putting Another Tool in the War-Fighter’s Data Base” Air University Press September 1994 p.8 and 21

110.Weapon systems are just one kind of influence systems. They operate mainly in the physical influence. Other kinds of influence is presented in the chapter 3.1.3.

111.M Libicki:"What Is Information Warfare ?" Chapter 6 p.1 - 4. Internet: http://ndu.edu/inss/actpubs/act003/a003ch06.html

112. W Schwartau:" Information Warfare; Chaos In The Electronic Superhighway" Thunder's Mouth Press 1995 p. 190 - 248

113. See Cliff Stoll:"The Coccoo's Egg" Pocket Book 1989

114.G J Stein:”Information War - Cyberwar - Netwar” Internet

115.van Elck- radiation: In theory and in practise, every device, which has alternating currents (AC) in it, radiates some. This small radiation can be intercepted with a right devise within some tens to some thousand of meters. Principal devises to be intercepted are different kinds of recevers, computers displays, computers in general and ignition systems in vehicles. To cancel this radiation NATO- coutries have a standart called Tempest.

116.Capt (US Navy) James Stavridis:”The Second Revolution” Joint Force Quarterly Spring 1997 p.8 - 13