

Revolution in Information Affairs

Tactical and Strategic Implications of Information Warfare and Information Operations

Manuel W. Wik

Defence Materiel Administration

SE-115 88 Stockholm

+46 8 782 67 32

mawik@fmv.se

Abstract

A new era is born – the information age. Information technology is our means of reinforcing human knowledge and communications and opens up a revolutionary new world to mankind. A revolution in information affairs is envisioned. It is a slow motion revolution, thus not always clearly visible. Information age and information technology creates dependencies, capabilities, and vulnerabilities that have to be understood and managed. A revivalism for this revolutionary new era is needed.

The purposes of this paper are to cast some light on new rising threats and opportunities and to discuss tactical and strategic implications of information warfare and information operations. It is important to increase awareness within private, government and military sectors. A picture of what the future might look like is given. The aspects presented include: the meaning of information operations and information warfare; what is really new; essential drawbacks, driving forces in the development; impact on information infrastructure; and countermeasures. The importance and the necessity to establish a strategy, to introduce processes and to organise resources for national security are explained.¹

1. The New Future

1.1 Power shift

The futurist Alvin Toffler has predicted a revolutionary power struggle to come: “*For we stand at the edge of the deepest powershift in human history*”. He talks about power involving the use of violence or force (which is considered to be the monopoly of military forces), the use of wealth and the use of knowledge. He talks about a shift from the inflexible and low quality power of force and the versatile medium quality of wealth, towards the application of knowledge being the most versatile and high quality power. Actor Sean Connery, in a film set in Cuba during the reign of the dictator Batista, plays a British mercenary. In a memorable scene the tyrant’s military chief says: “*Major, tell me what your favorite weapon is, and I’ll get it for you.*” To which Connery replies: “*Brains.*”

From iron power to brainpower, from hardware to wetware. Is this really something new? Almost 2500 years ago Sun Tzu from China talked about it. Napoleon has said: “*The sword is*

¹ Part of this presentation is based on an address given at the Danish Supreme Commander’s security policy course in 1999. In addition, background material from two major American reports have been used (ref. 1, 2) as well as a report from the European Parliament (ref. 3). Permission has been obtained to use material from these references.

beaten by the mind.“ Winston Churchill has said: “*Empires of the future are the empires of the mind.*“

Are we really standing on the edge of the deepest powershift in human history? We know that knowledge is a force multiplier. By using new means and new technological ideas used in new ways, one does not just make everything a little bit better or more efficient but rather creates new ways of doing things. This multiplier is clearly a tremendous amplifier. *We are not redesigning the past; we are inventing the future.* How is that done?

From time immemorial man has used tools. Tools have been able to strengthen the power of violence and the power of wealth. However, in the past not many tools were invented to strengthen human senses, thoughts, or communications; at least not until the art of printing was invented. Today we experience the beginning of revolutionary changes in this respect – the strengthening of power of information and knowledge - and an historical shift in human development.

Human senses have begun to expand through the technology of a global network of technical sensors with increasing resolution and capability to detect new conditions. *Human thoughts* expand with a global network of computers. The capability to search, navigate, find, examine, understand, assimilate, and refine just the correct information has become a strategic competence. *Human communications* expands with a global communications network carrying speech, text, video, and data. Fibre optic cables, satellites, mobile phones, the Internet, and television media disseminate information globally by the speed of light, far exceeding the speed of our thoughts. Shimon Peres once said: “*The greatest change in our time has not been effected by armies or states or international organisations; it has been driven by the spread of information.*“ Information is a catalyst for our *human actions* and now we can see many means of expanding action far beyond the reach of our hands and to a global level. It changes our life forever, it changes our work and our leisure time, and it changes society, both civil and military. It changes and expands our opportunities. However, it also changes and expands the nature of threats in all conceivable dimensions; and that is also where information warfare occurs. We are only standing at the very beginning of this evolution and are not able to foresee the consequences strategically.

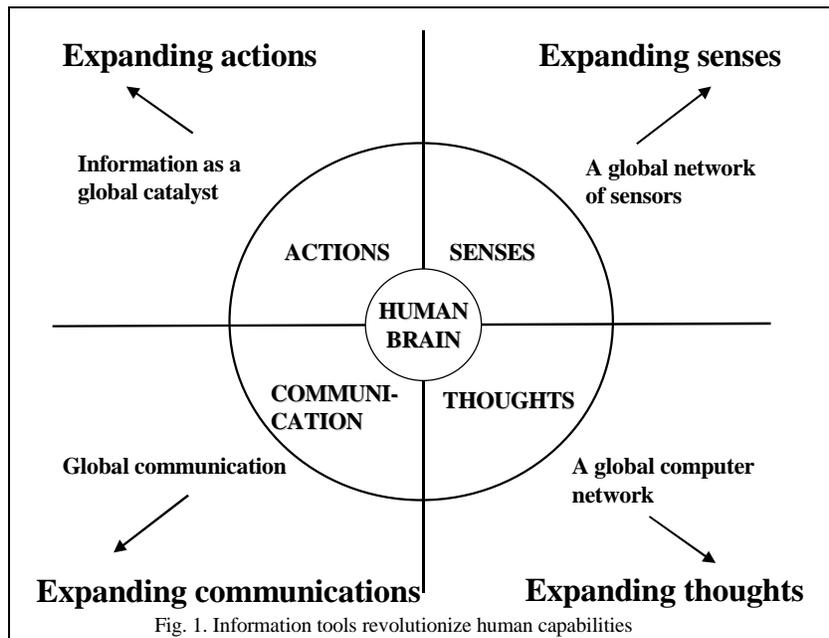
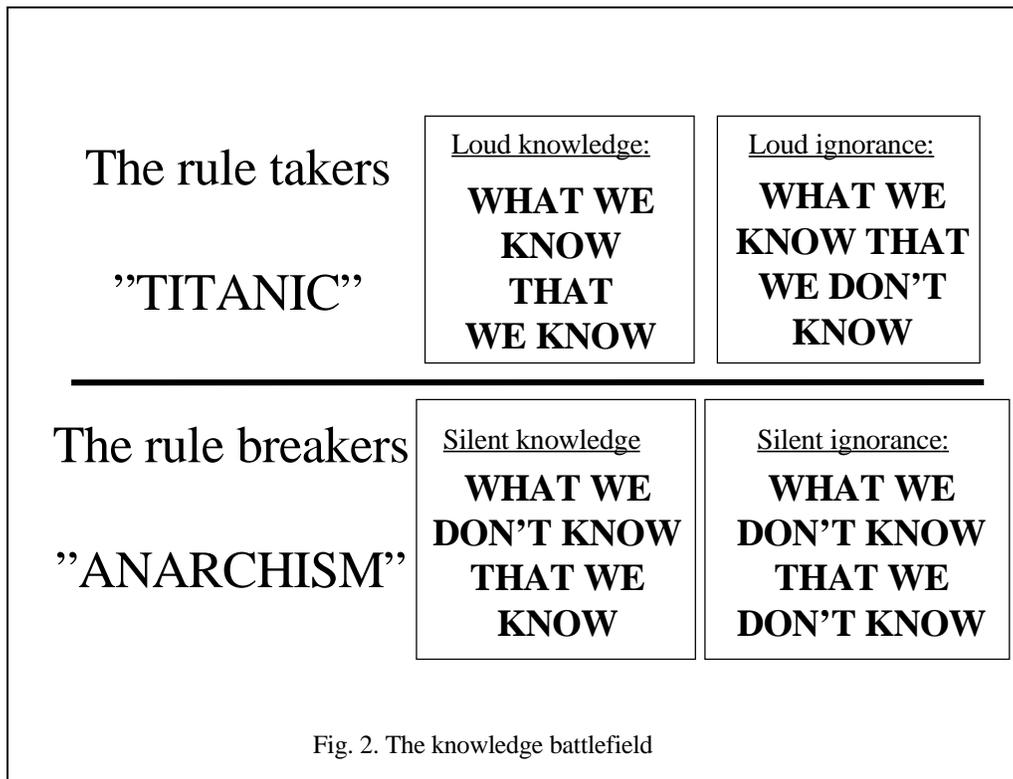


Fig. 1. Information tools revolutionize human capabilities

1.2 The Knowledge Arena

The traditional map we typically use is geographical. We must now supplement it with the logic map, the world map of ideas, and the human biographical map, which deals with how impressions and perceptions influence the human brain. We must enter the knowledge arena, the focal plane of the twenty-first century. The knowledge arena consists of the human consciousness, the subconscious, and the unconscious. The consciousness can be divided into *what you know that you know* and *what you know that you don't know*. They represent the *loud knowledge* and the *loud ignorance*. Together they form the perfect foundation for the planners, the rule takers, those who want to define everything and stick to it. Mark Twain once said, “*for those who only have a hammer as a tool, all problems look like nails*”. Personally, I would name this approach “*Titanic*”, because in the end it will always fail. Sooner or later something unknown comes up; change is the only sure thing in life. “*Those who do not expect the unexpected are not able to find it*” (Herakleitos, Greek philosopher). The more a system is adapted to its purpose, the less it will be able to manage changes. If a competitor in peacetime or an adversary in wartime knows all our rules and we keep to them, we will be lost. It will be as if a chess player has the knowledge of everything the opponent thinks. What you have to do is to do the unexpected and take the opponent by surprise. That is also the essence of war gaming.

We must activate the subconscious, *what you don't know that you know*. This is the *silent knowledge*. Nobody can see the holes where there is no pattern of action. It is hard to animate elusive patterns where many surprises spring up. In order to know how to build a system you must know how it shall be used; but not until you use it, will you know how it should have been built. You learn by mistakes. Not until you are faced with a new situation and you do something, will you find out that you are actually able to handle it.



How well have we actually been able to predict war? General J. Enoch Powell once said: *“The history is full of wars that everyone knew would not come.”* Look at all the negative imaginations of new inventions. In 1943 the chairman of the board of IBM, Thomas Watson, said that there would probably only be a need for five computers in the world in the future. In 1876 after the telephone was invented and introduced, the Western Union Telegraph Company said that the telephone could not seriously be used for communication and was of no value to the company. In 1899 Charles H. Duell, who was a civil servant in a leading position at the American Patent Bureau, motivated a proposal to disband the bureau saying that everything that could be invented had now been invented. When the talking picture was invented, the silent film directors thought it would be ridiculous to listen to the actors. And so on. These examples of delusions and lack of imagination are going to multiply in the future.

In order to find out more about silent knowledge, you need to do mental stretching. Think about those words *“mental stretching”*; when did you last do so? You were probably jogging and did some body stretching, but when did you do the mental one? When you did, you were the rule breaker, the anarchist according to the vocabulary of the rule taker. This is an important kind of knowledge that you should try to experience more in the future. It is needed in the information and knowledge era and is especially useful in conflicts.

Stretching can be accomplished by turning the way of thinking in new directions. George Bernard Shaw gave a good example of mental stretching: *“Most people look at the world as it is and ask them why. I am dreaming of things that never existed and ask myself why not?”* The unexplainable that triggers our thoughts and requires mobilisation of our intellectual capability, which also combines fragmentary knowledge from different parts of our brain in order to form new knowledge, leads the way to mental stretching. Bertrand Russell has said: *“The brain is a remarkable machine that can combine expressions in the most astonishing ways.”* Albert Einstein has expressed it in this way: *“The most beautiful we may experience is the unexplainable. It is the source of all true science.”*

Today and even more tomorrow intangible assets become more important. A trademark or a special design can prove to be far more valuable than a traditional product.

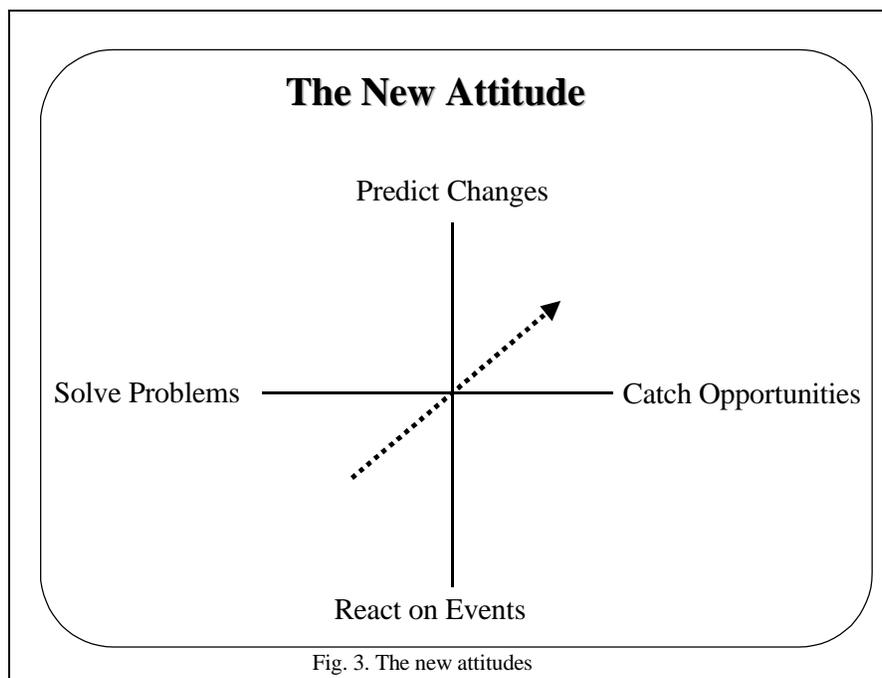


Fig. 3. The new attitudes

Creativity, fantasy, innovation, and flexibility are going to be the most wanted characteristics in the future. The new attitude is to mentally stretch so that one may predict changes and catch opportunities, rather than to react on events and solve problems. In an open architecture rigid constructions become historic buildings. Knowledge wins over strict hierarchical organisations. Organisations must be able to switch in a flexible way between hierarchy and flat networks depending on the tasks. Opaque properties fence in knowledge and counteract the precision of decisions. Hierarchy restrains creativity. Nor can hierarchies react with sufficient speed due to changes as the rate of change increases all the time. *Pace wins over hierarchy*. As human beings we will experience an increasing difficulty to manage this increasing pace, which will change much of our lives. Furthermore in conflicts and war, it will be a matter of life or death.

Last, but not least, the knowledge arena consists of unconsciousness, *what you don't know that you don't know*. I would call it *silent ignorance*. This is a particularly interesting region. We are talking about areas where there is no pattern of action. It is like dropping your keys at night and only searching for them where there is light enabling you to see. Now, if you get in contact with people busy in areas not previously known to you, you will experience new things. This means that you will be able to make cross-cultural excursions into this type of silent ignorance and be able to capture new knowledge. Think about it! Information technology means increased opportunities to transform unconsciousness into consciousness. Thus we learn more.

So, what should you do? Should you be the rule taker or the rule breaker, the passenger on the Titanic or the anarchist? I guess none of them is good forever, and you will have to try to balance between the bright and the dark sides according to the situation and the wisdom that you have.

2. The Rising New Threat

2.1 The Changing World

Information and knowledge have always been – and are now more than ever - part of the economy of a nation, of a corporation, and of a family. In the information society “*knowing*” becomes more important than “*owning*”. As information age evolves, society will be threatened in new ways. Many people take information systems for granted and do not realise the great dependence on them, the significance of their vulnerability, and what would happen in case of malfunction or disruption. Previously all information was hidden that was not open. Today all information is open that is not hidden. Immensely sophisticated information systems have so far been erected on insecure foundations. Networking capability has outpaced the capability of protecting information.

Data traffic is tripling every year and will overtake voice as the dominant type of traffic over the world's telecommunications networks by year 2005. 75 million new customers signed up for cellular phone service in 1998, bringing the worldwide untethered population to roughly 285 million. In 1998 an average of 5 million e-mails were sent every minute. Users can listen to e-mail messages over the phone and then reply to them with voice messages. Or they can have e-mail messages and attachments printed as faxes at a fax machine. Intelligent software agents will sort and filter incoming messages and allow callers to retrieve and manage voice mail using spoken commands rather than a telephone keypad.

Today there are more than 100 million users of the Internet and there is a new Web site added every four seconds. Internet traffic is doubling every 100 days. By the year 2005 there may be 1 billion people using the Internet with an enormous number of Web sites and information to be found and also to be at risk for intrusions. The real assets will be symbols and bytes, not cash money like notes and coins. Time is money, information is money, and filtering high-speed information for special purposes involves a great deal more money. The Internet is changing the way the world economy functions. By the year 2005 sales over the Internet are expected to reach 5 trillion US dollars in the United States and Europe.

It is clear that the information technological revolution and the new global economy of information and knowledge will create a number of new threats that will make the criminals of the past look very pale in comparison. We do not yet know the outcome of the changing circumstances but we will need to rapidly create and mobilise forces of information defence in order to encounter expected cyber crimes. *“Our vulnerability, particularly to cyber attacks, is real and growing.”* (U.S. President Bill Clinton)

Billions in proprietary secrets have been stolen from high-tech corporations. Most corporations have been penetrated electronically by cyber-criminals. In the United States the FBI estimates that electronic crimes cost victims about 10 billion dollars a year. The importance of consumer confidence and shareholder value prevents the reporting of more than a fraction of the actual intrusions to law enforcement agencies. It is also estimated that only a small fraction of all intrusions are known to the owners of the systems under attack.

We have already experienced an arsenal of information warfare weapons: computer viruses, worms, Trojan horses, logic bombs, and software for denial of service. Compromising high-powered scanners and sniffers proliferate and are being used to intercept mobile phone calls, faxes, and satellite and landline communications. A number of new methods are being used and further developed in order to steal information and to camouflage where attacks originate. There is also a large arsenal of tools for destruction of information, and the information infrastructure. For example telephone lines can be overloaded by special software, and traffic control of air, sea and land vehicles can be disrupted or given false information. Financial institutions, emergency services and other government services software can be scrambled. Control of electric power, pipelines, and industrial processes can be altered by remote control and sabotage can be directed against stock exchanges.

“Peace really does not exist in the information age” (Kenneth A. Minihan) and the threat spectrum is constantly changing. Malicious tools are constantly improving and changing. Password-cracking programs are widely available. Programs to detect weak points in the security of a system can now additionally be used to automate attacks against the identified vulnerabilities. Computer chips with malicious code (i.e., trapdoors, backdoors, logic bombs) can be obtained commercially at low cost. Programs to edit home pages on the World Wide Web can be used to attack network servers. Powerful high capacity malicious servers can attack information systems connected to the Internet.

2.2 Computer Threats and Security

2.2.1 Some Threats

There are a number of external and internal threats that must be considered. Most operating systems are shipped with inherent vulnerabilities. Further vulnerabilities are introduced during configuration and usage. Loading files from the Internet can ruin a computer that does not have a very good and recent antivirus program. Exploited information is widely and quickly disseminated.

When it comes to computers connected to neighbouring computers, it must be understood that you depend on the neighbouring computer's security. When you don't know how that computer is connected, you are not protected from running into a cascade of security problems.

To many organised crime groups the Internet is a tool and not a target. There are also many powerful software tools available for hackers on the Internet, and the trend is towards even more powerful tools. Very little skill is needed to make use of hacker tools, as hacking techniques have become automated. Software that anybody can run can crash a computer and shut it down.

As an example Back Orifice (BO) is a back door for Microsoft Windows 95 and 98. It allows a remote unauthorised user to take over your system. The software has higher quality than any commercial product seen so far. People playing on the computer and being beaten by other players developed BO. With the software at hand, they were able to come back and shut down the other player's computer. Capabilities include the execution of commands, listing of files, sharing of directories, uploading and downloading of files, monitoring of keystrokes, opening and closing of the CD ROM door to make people crazy, and the killing of processes.

Programs such as SATAN were originally designed to help computer and network administrators detect weak points in the security of their systems. However, computer intruders who want to rapidly assess the vulnerability of a target can also use it. Coupled with other software programs, it allows a hacker to access an automated reconnaissance and intrusion package without leaving an audit trail. New versions of SATAN also automate attacks against the identified vulnerabilities, and other even more sophisticated software tools can be found.

2.2.2 Security Management

There are several key elements in order to handle intrusion detection:

- Assess implementations of key architectural elements and advise clients on their application
- Make use of analysis and support tools to understand network topologies and information flow between systems
- Execute vulnerability analysis to identify weaknesses
- Mitigate identified vulnerabilities as far as possible

- Employ monitoring and analysis tools to detect exploitation of residual risks
- Repeat the whole process when new capabilities are proposed – i.e., before a new capability is added

Modern tools automate vulnerability detection. Remote servers can be scanned for vulnerability analysis. The web site for Internet Security Systems is <http://www.iss.net>

2.2.3 Security and Vulnerability Tools

There are a number of tools available to study security and vulnerability:

- Network Visualisation, Monitors and Sniffers. Examples are Visio, NetViz, NetPartitioner, NeoTrace, TraceRoute, Ethload, Net Xray, Etherpeak, TCPDump, Snoop, IPWatcher, T-sight, Scott/Tkined
- Vulnerability Analysis. Examples are ISS Internet Scanner, Kane Security Analyst, Trident IP Toolbox / L3 Expert, Security Profile Inspector (SPI), SNI Ballista, SATAN
- Intrusion detection. Examples are RealSecure, NetRanger, Stalker/CyberCop, Intruder Alert, Network Flight Recorder, SHADOW, NIDS
- Exploitation. Examples are NTSecurity, RootShell, Offline NT Password Utility, Lopht Heavy Industries, AntiOnline, Insecure/Fyodor
- Other useful tools are TCPwrappers, Tripwire, COPS, crack, LophtCrack, ScanNT

A network-sniffing device on a communication line acts as a kind of hub. Traffic is usually carried in clear text and the sniffer can pick up usernames, passwords, and E-mail. It allows traffic to be filtered, watched and/or recorded. A sniffer like Net X-Ray provides a traffic map and identifies important points in the network. A tool like IP Watcher is capable of session watching, takeover, and close down.

Defence measures to handle computer security include a number of measures to be implemented concurrently:

- Policy including defence guidance and offensive rules of engagement
- Training and professionalisation
- Assignment of resources, responsibility and authority, including defensive Red Team
- Vulnerability identification and familiarisation
- Countermeasure assessment

It is necessary to apply staff, time, and capital resources to vulnerability analysis and to tool assessment. Effective practical and tolerable procedures must be developed. Open-source

discussions of vulnerabilities, exploitation mechanisms and tools must be followed. One should never buy tools without understanding their capabilities and never rely on a single tool and source. Much of the work requires long days and enthusiasm beyond the norm in order to succeed. It is a big effort to keep up with changing computer environments and new threats.

The financial sector is thought to have the highest degree of computer security, one reason being that it cannot afford a bad reputation. Many military systems are more vulnerable, and personal systems in civil society are among the most vulnerable.

2.2.4 Vulnerability Assessment and Red Teaming

There is a difference between a vulnerability assessment and Red Teaming. Vulnerability assessment includes a review of security posture as part of risk management. The results are reviewed with the security department, and solutions are implemented. This is a regular component of security procedures and a risk management process. Safeguards are evaluated, threats anticipated, and resource allocations are decided upon.

Red Teams act as the enemy to exploit vulnerabilities to the fullest possible extent and to provide perspectives to the threat of an information attack. Vulnerability chains are exploited, and INFOSEC, physical and personnel vulnerabilities are combined. The true implications of known vulnerabilities are thereby demonstrated to management. This supplements a vulnerability assessment as part of risk management, recognises intangible benefits of information security and emphasises dramatic situations. Both vulnerability assessments and red teaming are vital components of information security and critical infrastructure protection. Red Team personnel are selected based on experience and a strong personality.

2.3 Communications Threats and Security: Interception

Communications security and the “Development of surveillance technology and risk of abuse of economic information” has been studied and reported to the Director General for Research of the European Parliament in 1999. The study considers the state of the art in Communications intelligence (Comint) of automated processing for intelligence purposes of intercepted broadband multi-language leased or common carrier systems, and its applicability to Comint targeting and selection, including speech recognition. It includes interception of international communications, the ECHELON and Comint production, law enforcement, economic intelligence, capabilities after year 2000, and policy issues for the European Parliament. The following is a summary from the report:

“Communications intelligence (Comint) involving the covert interception of foreign communications has been practised by almost every advanced nation since international telecommunications became available. Comint is a large-scale industrial activity providing consumers with intelligence on diplomatic, economic and scientific developments. The capabilities of and constraints on Comint activity may usefully be considered in the framework of the “intelligence cycle”.

Globally, about 15-20 billion Euro is expended annually on Comint and related activities. The largest component in this expenditure is incurred by the major English-speaking nations of the UKUSA alliance. The report describes how Comint organisations have for more than 80 years made arrangements for the interception of communications from commercial satellites, of ground communications using satellites,

of undersea cables using submarines, and of the Internet. In excess of 120 satellite systems are currently in simultaneous operation collecting intelligence.

The highly automated UKUSA system for processing Comint, often known as ECHELON, has been widely discussed within Europe following a 1997 Scientific and Technological Options Assessment (STOA) report. That report summarised information from the only two primary sources then available on ECHELON. This report provides original new documentary and other evidence about the ECHELON system and its involvement in the interception of communications satellites.

Comint information derived from the interception of international communications has long been routinely used to obtain sensitive data concerning individuals, governments, trade and international organisations. This report sets out the organisational and reporting framework within which economically sensitive information is collected and disseminated, summarising examples where European commercial organisations have been the subject of surveillance.

This report identifies a previously unknown international organisation – “ILETS” – which has, without parliamentary or public discussion or awareness, put in place contentious plans to require manufacturers and operators of new communications systems to build in monitoring capacity for use by national security or law enforcement organisations.

Comint organisations now perceive that the technical difficulties of collecting communications are increasing, and that future production may be costlier and more limited than at present. The perception of such difficulties may provide a useful basis for policy options aimed at protective measures concerning economic information and effective encryption.

Key findings concerning the state of the art in Comint include:

- Comprehensive systems exist to access, intercept and process every important modern form of communications, with few exceptions
- Contrary to reports in the press, effective “word spotting” search systems automatically to select telephone calls of intelligence interest are not yet available, despite 30 years of research. However, speaker recognition systems – in effect, “voiceprints” – have been developed and are deployed to recognise the speech of targeted individuals making international calls
- Recent diplomatic initiatives by the United States government are seeking European agreement to the “key escrow” system of cryptography masked intelligence collection requirements, and have formed part of a long-term program which has undermined and continues to undermine the communications privacy of non-US nationals, including European governments, companies and citizens
- There is wide-ranging evidence indicating that major governments are routinely utilising communications intelligence to provide commercial advantage to companies and trade”

The United States National Security Agency (NSA) – the signal intelligence agency – directly under the President, has about 20.000 employees and can command another 20.000 people from the defence. NSA has the capability to intercept all wireless and cable communications including voice telephony. Softly encrypted information (perhaps up to 56 bit coding) is decoded in real time. One billion messages are filtered every day and about 0,1 % is analysed manually. There are links between the NSA and the Department of Commerce. One conclusion is that there is no possibility to avoid the risk of fax, telephone, or E-mail messages being intercepted and analysed, even if they are softly encrypted. Thus the only countermeasure is to encrypt all messages thereby saturating the system.

The Swedish Security Service claims that mobile GSM phones can be used for industrial espionage, even when switched off, without putting anything special into the phone, and without the owner knowing that the telephone is being bugged. Other sources deny that this is possible. Until a clear statement is at hand, it is recommended not to bring mobile phones into places where highly secret matters are being discussed.

Information on the location of mobile phones is monitored and there are special computer centres that can handle and record a great number of mobile phone positions. Such information is used by law enforcement agencies.

3. The New Warfare

3.1 What is Information Operations and Information Warfare?

What is information warfare? The meaning of information warfare changes all the time and brings my thoughts to Greek mythology where Hercules was fighting a hydra with many heads that regrew when cut off. Information warfare has also been compared with the story of blind men touching an elephant in order to try to describe what they think it really is. Depending on what they feel, each of them will come up with different ideas. There is no consensus of definitions, and one could even talk about “definition warfare”. Definitions establish conditions, which can prevent looking for new patterns of behaviour and development in a changing environment. In my view there is no end state, all these terms and definitions are only glimpses of road signs on an endless journey towards the future.

INFORMATION OPERATIONS (IO)

Actions taken to affect adversary information and information systems while defending one's own information and information systems.

INFORMATION WARFARE (IW)

Information operations conducted during time of crises or conflict to achieve or promote specific objectives over a specific adversary or adversaries.

ULTIMATE GOAL OF INFORMATION OPERATIONS:

Human decisionmaking.

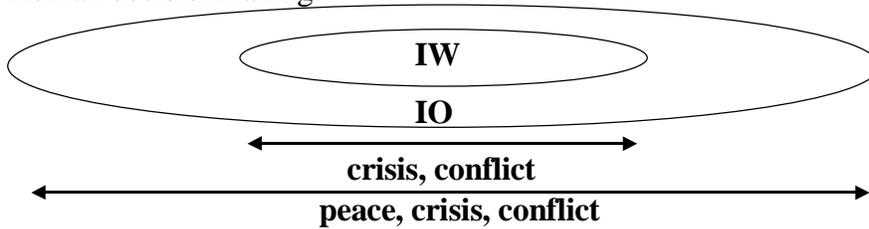


Fig. 4. Information Operations terminology

IW conflicts: Much more than Rubik's cube ...

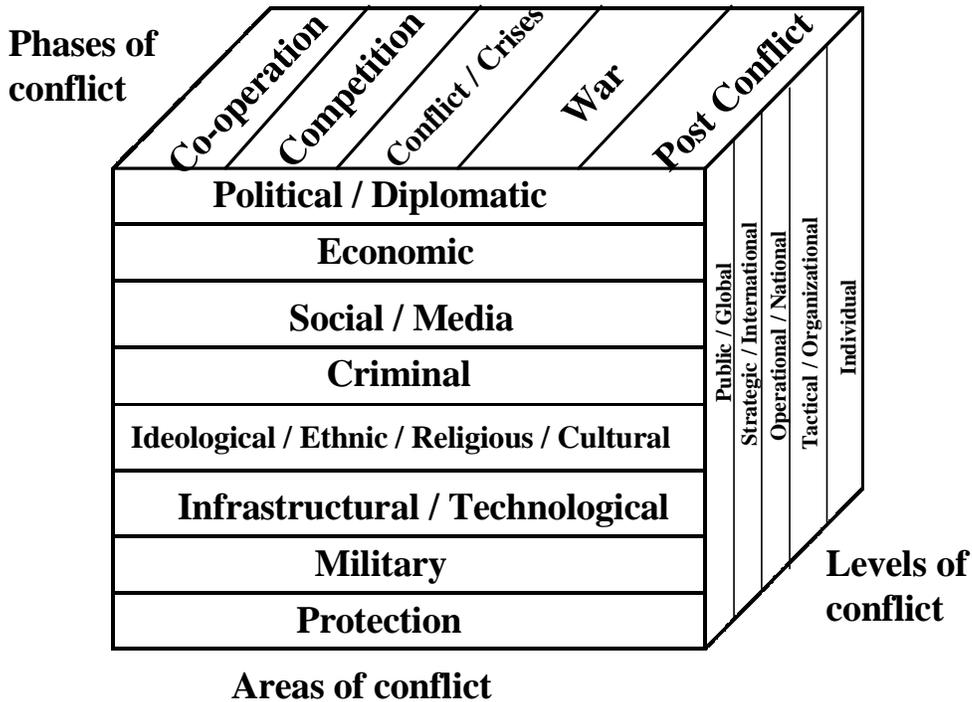


Fig. 5. Information Warfare levels, areas, and phases of conflict

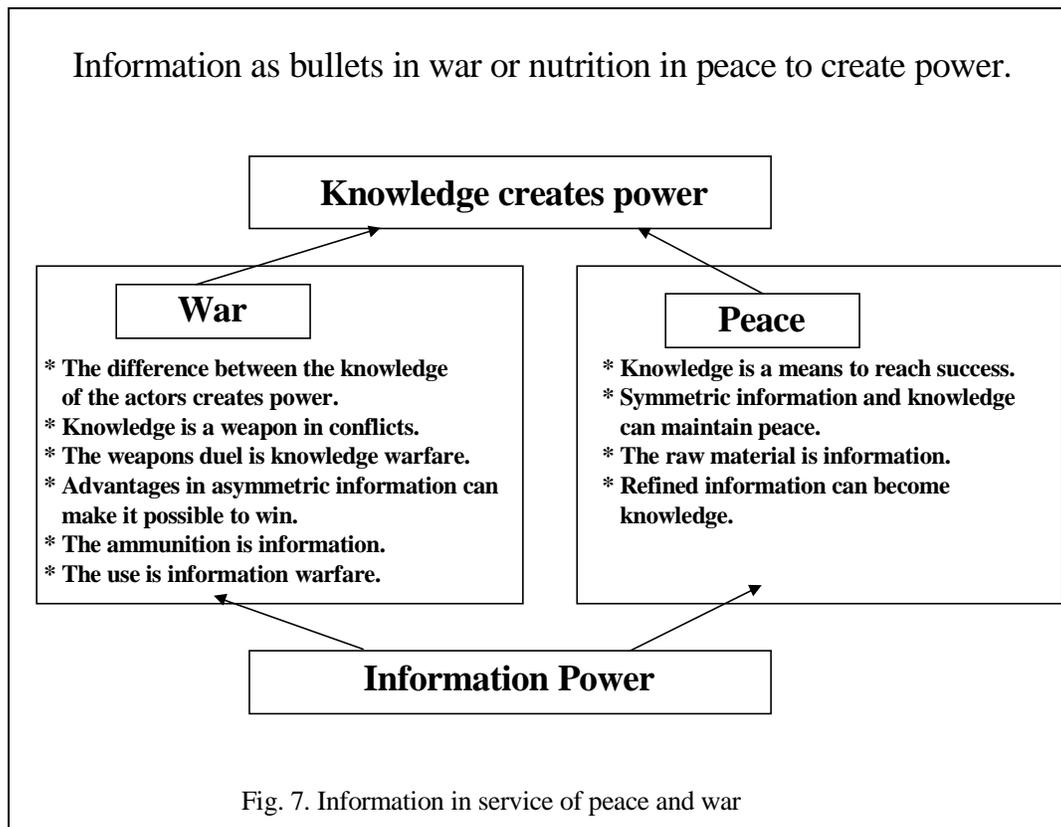
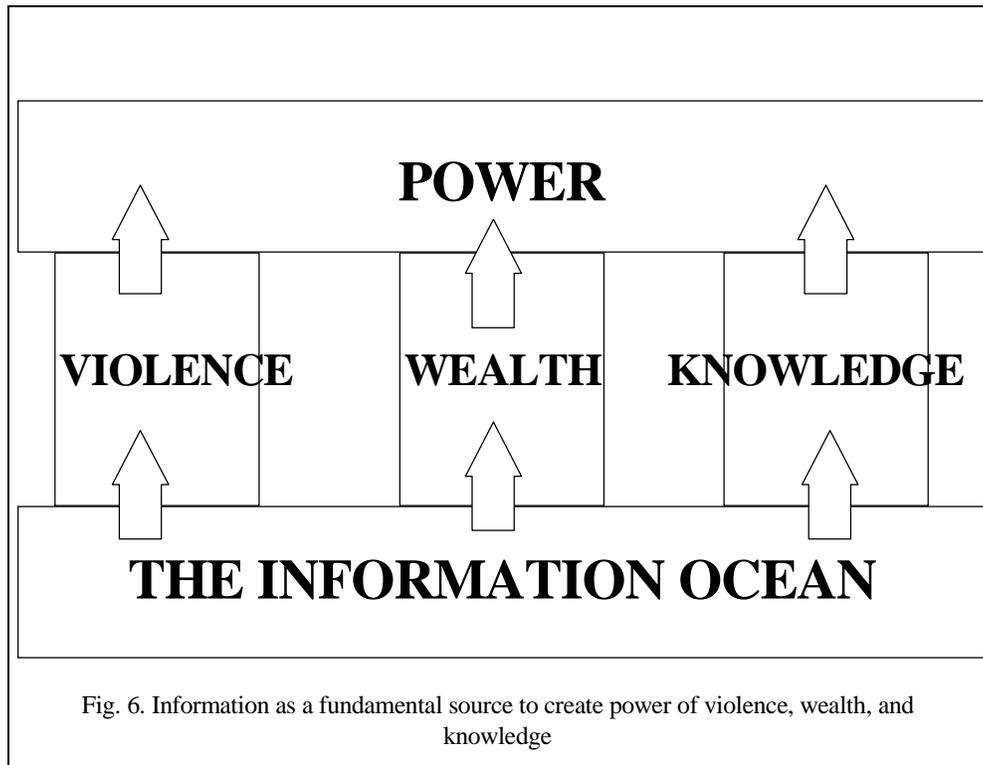
In the United States *Information Operations* is the superior strategic term integrating various capabilities and activities such as information warfare. Information operations are actions taken to affect adversary information and information systems while defending one's own information and information systems. Information warfare is information operations conducted during times of crises or conflicts to achieve or promote specific objectives against a specific adversary or adversaries. The ultimate goal of information operations is to impact the human decisionmaking.

To some people information warfare is a generic term for all forms of struggle for control and superiority concerning information. Ultimately it could be the struggle of minds in order to become the master of a situation. In a very wide view one deals with many levels of interaction, phases of conflict, and arenas. According to one source there are three classes of conflicts: personal, corporate, and global information warfare. Another example is individual, organisational or tactical, national or operative, international or strategic, and global. In a wide sense information warfare appears during all phases of conflict from co-operation, competition, crises, war to post-conflict. The arenas can be military, political, diplomatic, economic, social, infrastructure, criminal, ideological and religious and possibly more. There are several forms or methods of warfare, and a multitude of technologies, goals and targets.

Human power balances on three fundamental pillars: violence, wealth, and knowledge. In the struggle for power, one of the basic sources is information. The struggles are generally speaking information operations and information warfare. They engage the military sector seeking power of violence, the financial sector striving after power of wealth, and humanity aiming at knowledge power. Power can be transformed between violence, wealth, and knowledge; and these transformations also incorporate information operations and information warfare. The model of the Information Ocean from which the three pillars violence, wealth and knowledge rise to carry power is applicable at all levels; state, corporation, family, and personal.

Information can be used for good or evil purposes. Symmetric information and knowledge (refined information) can maintain peace. Advantages in asymmetric information can make it possible to win in a conflict using knowledge as a weapon and information as bullets and ammunition.

Information warfare can begin without a declaration of war and can be fought on a wide front or battlefield - openly or subversively, isolated or widespread. Information operations can stretch over all phases including: peace, crisis, the pursuit of conflict, and actual war. This totality makes the concept complicated and multidimensional and places high demands on the expansion of our field of vision in all directions, to include all the phases of a conflict, at all levels and in all sectors of society. This forms a palette with greater possibilities and threats, with a greater number of targets and wider battlefields than ever before.



CONFLICT PREVENTION PLAN

	Peace/Competition IW action initiatives	Conflict/Crisis IW Plan	War IW annex to war plan	Post-conflict/Peace Sequel to IW plan
POLITICAL	Engage leadership	Discredit leadership Support democratic leader	Isolate leadership Disrupt military C2	Support elections Stabilize government
MILITARY	Access intelligence C2 and logistics	Deter aggression Disrupt aquisition Deceive leadership	Defeat infosystems Disrupt operations Impede reinforcement	Support demobilisation, support arms limitations
ECONOMIC	Access financial systems	Disrupt fund transfers Deny international support	Deny support of military operations	Maintain financial systems
SOCIAL	Premote democracy Deter migration	Support democratic leader. Set expectations	Support democratic leader. Set expectations	Support national reconciliation
INFRA-STRUCTURE	Access transportation, communications, POI and power	Disrupt systems	Deny flow Deny communications	Monitor systems
PROTECTION	Access vulnerabilities Identify adversary IW capabilities	Protect vulnerabilities Manipulate adversary IW	Protect own capabilities. Deny military adversary IW	Monitor adversary IW

Fig. 8. Example of IO/IW to prevent conflicts

The objectives of information warfare can be masking or unmasking of facts, exploitation, deception (such as disinformation), disruption or denial of service, and destruction of information. The activities can be open or concealed, occur in peacetime or in combination with various conflicts and war. Hackers outside the United States have intruded into computers belonging to the American Department of Defense. Media has in one way or another played a significant role in conflicts like the Gulf war, in Yugoslavia, in Somalia, just to mention a few. The Internet has been used to acquire information for news bulletins in order to reveal the Indonesian military actions in East Timor.

Intrusions in computer systems may appear as if they come from one part or country, whereas they actually are launched from quite a different place and country. This can become a significant risk in evaluating who has participated in information warfare.

An example of an American plan for information warfare shows escalation and de-escalation of various activities in each arena such as political, military, etc. It is a good illustration of the totality and the requirements for extensive cooperation between representatives of different responsibilities.

There is also talk of a more restricted application of information warfare. The actors can then be separate organisations, groups or simply individuals instead of being alliances or states. They can achieve their purpose without having to resort to conventional threats or means of pressure. This makes the boundaries unclear between the concepts, competition, rivalry, peace, crisis and war. It has been said that a few clever hackers or insiders could paralyse a high-tech nation within a very short space of time.

The boundaries are also indistinct in conflicts where old military conditions and weapons are used in old ways, together with old military weapons modified and used in new ways, and with new military conditions and weapons used in new ways. Do not regard a combat aircraft as a combat aircraft any more, look upon it as a flying computer centre with a weapons cargo. With less platforms and soldiers and with more information, the development goes *from a platform centric to an information centric defence*. The shift from power of violence to power of knowledge is applicable to military defence as well.

It is not difficult to feel lost in the information warfare environment. The clear grouping national state against national state is gone. The identifiable adversary and uniformed armies are gone. Defined borders and the predictable axis of attack are gone. Mobilisation of a considerable part of the population is gone, and the requirements for a large industrial production are gone. Financing over a considerable part of the state budget is gone. Land, sea and air forces are gone. Declaration of war, Geneva conventions and diplomatic protocols are gone as well as a clear adversary. Information warfare can come sneaking in the shape of a single, only a few, or many actors; they come without reliable identification, without uniform, without borders, without defined front, without large industrial production or large financing, without fire power, without rules of engagement and conventions.

	<u>Conventional war</u>	<u>Information war</u>
Actor	Nation-state versus nation-state	Individual/small group versus nation-state
Adversary	Identifiable Uniformed enemy	No certain identification No uniform
Geography	Fixed frontiers	No frontiers
Axis of attack	Predictable	No definite
Enlistment	Large part of population	Very few individuals
Industrial needs	Large production	No industrial base
Financing	State treasury required	Privately affordable
Military forces	Land-, sea-, air force	No firepower
Mobilization	Required	Not required
Deployment	-”-	-”-
Rules	Declaration of war Geneva conventions Diplomatic protocols	No declaration of war No conventions No diplomatic protocols
Outcome	Clear victor established	Clear loser

Fig. 9. How to get lost in unconventional conflicts

It is often said that the truth is the first victim of war. Normally that refers to conventional war, but information war is no exception. The actors do not necessarily even know that they are participating. International media can play a significant role without knowing it. Weapons of information warfare are deployed at low cost and with good accessibility globally. War can start without notice and propagate at speed of light. The theatre is logical and not physical. A domain can be controlled without physical presence. What does the plan of attack and the defence look like when the map is not a geographical map with marked units and lines of attack but rather the interior of human minds and their knowledge, perceptions and influences?

3.2 What is New?

During conflict or war, information and knowledge have always been key parameters. This is why information warfare is in fact nothing new as a phenomenon.

However, what are new today, are primarily these factors:

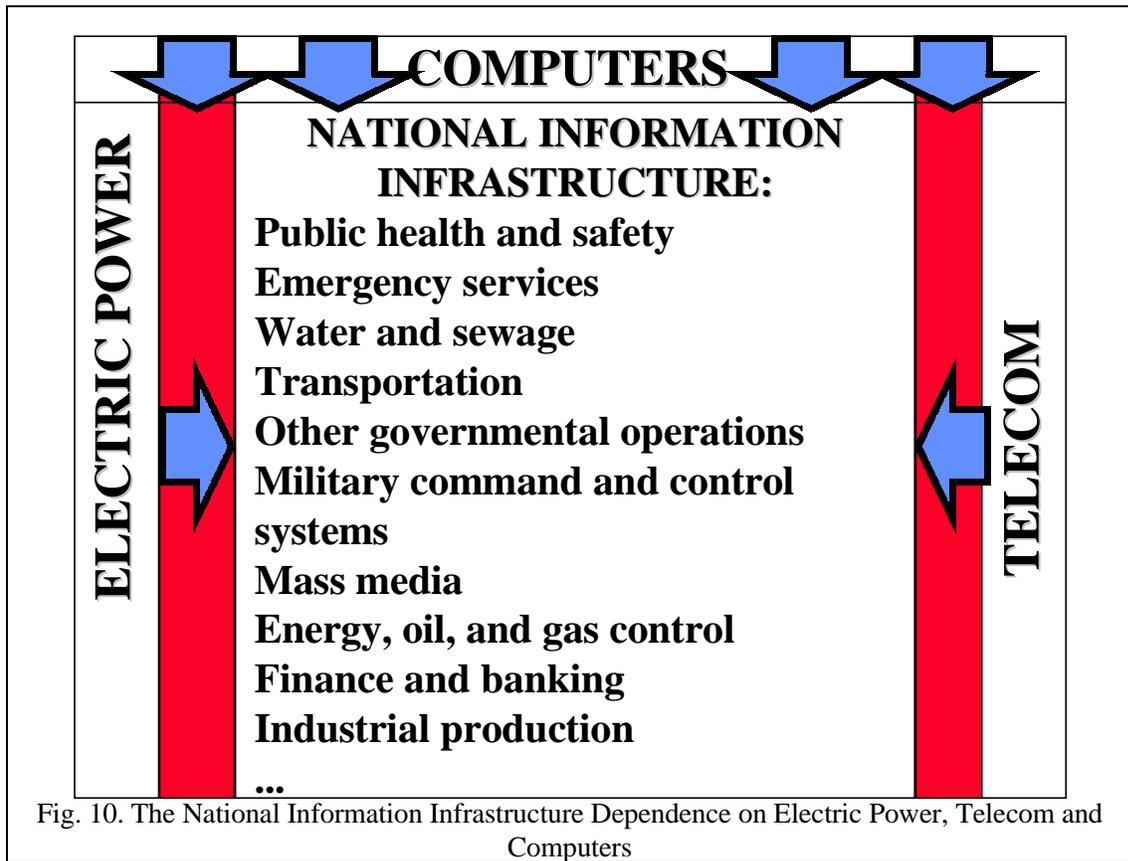
- Widespread expansion of fields of activity and global connections
- Interaction and synchronisation embracing all important areas
- The effects of amplification and intensification through information technology
- The increasingly high tempo in a course of events
- The emphasis (especially in the USA) on reduced casualties

The increasing importance of information makes it a clear, primary target for warfare. This is one reason why modern information warfare is a highly topical subject for debate. The opposite of information warfare is not particularly under debate. One major root of conflicts is lack of confidence. Confidence-building measures are becoming extremely important in solving conflicts. Instead of engaging in information warfare one should develop a number of positive means of using information. For this reason the whole region of producing confidence-building information ought to be studied, developed and used.

3.3 Impact on Infrastructure

Military power and national economy are increasingly reliant upon interdependent critical infrastructures. Advances in information technology and competitive pressure to improve efficiency and productivity have created new vulnerabilities to both physical attacks and information attacks as these infrastructures have become increasingly automated and interlinked. Any interruption or manipulation of these critical functions must be brief, infrequent, manageable, isolated, and minimally detrimental to the well being of a nation.

The national information infrastructure is at the centre of the information warfare. Who is the responsible authority for it and who defends it? The objective of the military defence is armed combat. The police force has its traditional responsibility and needs evidence. Commercial service providers might want to hide their deficiencies. Meanwhile military defence and national assets are increasingly dependent on interdependent critical infrastructures.



The destructive and extensive effect that information warfare can have on an information society is hard to imagine. We need computer support for electrical power supplies, telecommunications, water supplies, sewage, heating, air and rail transport services, daily newspapers, social insurance, taxation and banking procedures, and much more - in fact, for the entire infrastructure. Electric power networks and communication networks are the blood vessels and the nervous systems of society and are controlled by computers – the brain of the society - without which catastrophe is near. When the networks break down, everyone goes down with them. Only when faced with a complete electric power blackout such as in 1983, did Sweden start to understand the chain reactions of electronic systems blackout and further consequences for the infrastructure. If the telecommunications hub and conduits in the World Trade Center in New York City had been damaged during the 1994 attack on the trade center, this would have had a disastrous effect on billions of US dollars propagating throughout the world.

Attacking the command and control systems, telecommunications, and associated infrastructure of a high-tech nation is thought to be an effective way to break down the nation. This can become an even more serious threat in the future. This is possible for a number of reasons:

- The threat increases if an attack of the infrastructure becomes more profitable
- The threat increases if the probability for intrusion, acquisition, and manipulation increases due to more actors with more IT knowledge on a global arena

- The vulnerability increases if the reliability decreases. This can be caused by increased technical complexity and interdependent critical hardware or software dependencies. It can also depend on the susceptibility to deviating environmental conditions (e.g., temperature, electromagnetic radiation)
- The vulnerability increases if installation, operation, and supervision becomes more centralised. Economical and practical reasons often lead to centralisation.
- The vulnerability increases with additional functions depending on electric power if backup power is missing.
- The effects increase if the dependence on technology increases in the society in more and more areas and the consequences of disruptions thus increase.
- Protective measures are insufficient if knowledge of the need for safety is insufficient or if the economical investments are insufficient. Examples of protective measures are redundancy, alternative procedures, and emergency plans.

3.4 Information Warfare Drawbacks

Information warfare has several important drawbacks:

- Trust as one of the most fundamental cornerstones of human civilisation is violated. Involvement in information warfare such that the final outcome is loss of trust can be very expensive indeed.
- An underhanded expansion of information warfare in civilian society blurs the boundaries for everyday competition and is a kind of war fought without declaration of war.
- Information warfare legitimises terrorism. If governments and actors in society, ambitious to be respected by the people, believe it is acceptable for them to engage in information warfare, this will become the final victory for terrorism.
- The effects of information warfare are unpredictable. To achieve the intended effect is virtually impossible. Human behaviour is far less predictable than technical circumstances.

Experimenting with a complex information society is certainly easy with the technical means at our disposal today, but to achieve the intended effect is virtually impossible. Here there are clear parallels with nuclear weapons and biological warfare. The extent of dispersion and long term effects of such operations cannot be predicted nor restricted. Information as a weapon is double-edged and can strike back against the aggressor. It is not unlikely that information warfare activities in the end will have a greater negative effect on the aggressor than on those attacked if the aggressor himself is strongly dependent on information technology and the attacked is a “backward“ nation.

Human behaviour will always be less predictable than technical circumstances. It would be a grave error in judgement to believe that information warfare is so superior, that it will contribute towards solving all military conflicts. This is a real problem but not well recognised by everyone. The will of man depends on human values and cultures and is more

difficult to understand than technological systems. The straightforward military aspects of information warfare are not particularly effective in those cases where the cultural differences of the actors are substantial and where the difference in information technology (IT) dependence is great. There are many examples of homogenous groups, ethnic as well as religious with deeply rooted moral codes, which cannot be defeated by information warfare. On the other hand, their power of mass media is in their favour and thus can reinforce their own opinions.

3.5 Driving Forces of Information Warfare and Information Operations

There are three main reasons why information warfare and information operations have attained interest and have become driving forces.

- One thought is that information warfare can lead to less bloodshedding. There is a dislike of casualties, especially if the motivation to participate in a conflict is low. Media is quick and powerful and can intensify the effects of losses and can influence public opinion. Politically information warfare and information operations may be attractive if trust is not harmed.
- Another thought is that information warfare can lead to less cost than other means of fighting. In some cases there could be a dramatic cost reduction. For example a treacherous chip in a telephone line can cause more harm than a number of bombs, and the restoration cost after the conflict can be minimal.
- Still another thought is that information technology such as computers and communication systems is a phenomenal tool revolutionising the ways we work and thus both a force multiplier and a source for new capabilities.

4. Types of Information Warfare

4.1 Sources. Forms and Objectives

The various forms of information warfare can be described by combining sources of attack, forms of attack and tactical objectives.

There are two *major sources* of attack:

- Outside Defence against the outside can be firewalls, physical isolation, and encryption.
- Inside. Protecting against insiders like disgruntled employees is different and deals with personal security and operating procedures.

There are five *major forms* of attack:

- Data attacks occur when an opponent is inserting data and thus manipulating an information system. Examples are corrupting files, jamming radio transmissions of data, broadcasting deceptive propaganda, and spamming (sending large amounts of input irrelevant data). It must be recognised that information warfare campaigns do not always require sophisticated technology. Disinformation campaigns can be carried out in many unsophisticated ways, and human factors such as decisionmaking are always of main

importance in the operations. The media sector is one major battlefield. Psychological operations can be based on studies of public opinion and analyses as a basis for tailor-made messages. Databased picture and sound manipulation (morphing) can make the observer believe that the person he sees and hears in reality also does and says what is shown.

- Software attacks intend to carry out functions that cause the system to fail, like computer viruses, Trojan horses, logic bombs, and trap doors that allow a hostile party continuing access to a system. Back doors in software can be aimed at attacking built-in safety and security mechanisms. Microchips can have weaknesses that have been programmed beforehand or have hidden added functions that can be used by an adversary in a conflict (chipping).
- Hacking (or cracking which is the criminal aspect) is unauthorised entry into an information system in order to interact with its function to cause deception, theft, fraud, destruction, and other types of harm. One can detect or create tempest radiation – the electromagnetic emanations from computers, monitors, encryption devices, and keyboards. Software can be employed covertly to generate intentional emanations that bypass conventional security mechanisms. This can be used for commercial and national espionage, or even for software compliance.
- Denial of service which is loss of accessibility. This kind of attack is simple to perform and difficult to protect against. Recent distributed attacks on the Internet have shown that this can impact complete systems.
- Physical attacks are attempts to destroy a system physically. Examples are methods for causing fires; using bombs; producing various harmful environments such as electromagnetic pulse, high power microwave and other directed energy environments; or creating electromagnetic terrorism. High Power Microwave (HPM) weapons can emanate high power repetitive pulses in a narrow frequency band concentrated at a frequency between a few hundred MHz and several GHz. The duration is short (typically a hundred nanoseconds). Such normally high-tech weapons can cause “front door damage” to equipment. High power impulse ultra wideband (UWB) weapons can emanate very short repetitive pulses (typically a pulse width of hundreds of picoseconds) spreading power over a very broad spectrum. Weapons can be low-tech, cheap, and are likely to cause “back door disruption”. Continuous jammers are commercially available that can disrupt Global Positioning System (GPS), or mobile phone services; there are other types of Radio Frequency (RF) and Electromagnetic Pulse (EMP) weapons as well.

The *main objectives* of information warfare attacks are:

- Exploitation - to make use of the opponent’s information for ones own purposes.
- Deception - to manipulate the opponent's information and to keep him operating.
- Disruption or denial of service - to put the system out of operation for some time or to make it unreliable.
- Destruction - to harm the system in such a way that it cannot operate any more.

Information warfare embraces a wide range of *threat magnitudes*:

- *Natural hazards and unintended threats.* Natural hazards, errors, and unintended consequences represent the low end of threats. Examples are natural disasters, year 2000 problems (Y2K), human operator accidents, design and manufacturing errors, and acts of God.
- *Hacker type threats.* Unorganised or loosely coordinated information warfare threats form the next category of threats. Examples are hackers, pranksters, gangs, individual criminals, organised crime, and disgruntled employees.
- *Tactical threats.* Tactical information warfare is the next higher threat magnitude and can be sophisticated in its technology and planning. Examples are operational deception, electronic warfare (EW), electronic countermeasures (ECM), stealth in military operations, arms control camouflage, concealment, and deception, industrial espionage, organised crime, limited strikes to demonstrate, resolve or deter would-be opponents.
- *Strategic threats.* Strategic information warfare is the top of the line. It has not received as much attention as the three previous categories although it is thought to become the most important in years to come. Examples are extended terrorist campaigns, organised crime, industrial espionage, and organised strategically targeted IT operations.

4.2 *Comparison between Electronic Warfare and Information Warfare*

There is a similarity between the structure of electronic warfare and information warfare. In both cases there is a never-ending duel between measures and countermeasures. “*In some ways information warfare is like classical electronic warfare. It’s a never-ending struggle for advantage between countermeasures and counter-countermeasures. On the other hand, EW has been like an organized street brawl while IW has been more like a mugging.*” (James Stekert)

Electronic warfare support measures intend to facilitate or support warfare missions. From the attacker point of view information warfare *support measures* refer to tools used to penetrate, misuse, or disrupt system operations. As an example, programs to detect weaknesses in systems (e.g., SATAN programs) can be used. *Countermeasures* are used to prevent the accomplishment of the adversary’s mission. Examples can be firewalls, intrusion detection, audit and strong authentication or antivirus programs. *Counter-countermeasures* are used to defeat the installed countermeasures. Examples can be insider or trusted path access and/or a new and unexpected virus.

4.3 *Some Scenarios*

4.3.1 *Natural Hazards and Unintended Threats*

Even though Y2K problems are among those in the low end of threat magnitudes, they have attracted much attention and unrest concerning what could happen. Many systems have been examined and corrected but it is virtually impossible to guarantee that all of the important fixes have been carried out. Old systems interconnect with new ones and failures can spread and affect new systems.

4.3.2 *Hacker Type Threats*

A more severe category of threats can evolve from the Y2K problem. Technicians working with the problems have had access to all areas of an organisation's information system. An organisation that lacks total knowledge of its systems could be manipulated and the systems compromised in various ways. Viruses, logic bombs, trapdoors, and backdoors could be installed and triggered, perhaps years later.

New malicious software is born and is introduced on the Internet. Hackers and crackers may use this software to covertly control or disrupt other computers attached to the Internet. This may be far more serious than when a 16-year-old English boy took down some 100 U.S. defence systems in 1994 and other hackers rerouted calls from 911 emergency numbers in Florida to Yellow Pages sex-service numbers in Sweden.

4.3.3 *Tactical Threats*

According to information warfare specialists at the Pentagon, an electronic Pearl Harbor could result from a properly prepared and well-coordinated attack. It is said that fewer than 30 computer virtuosos located around the world, with a budget of less than 10 million US dollars, could bring the United States to its knees. This scenario, also indicated by acts of hackers around the world, holds true for any high-tech nation and is a very real and increasing danger to national security.

Meanwhile new military capabilities are being developed to launch cyberattacks or counterattacks making use of the power of information warfare and information operations. Today almost a dozen nations have such capabilities – with or without political support - extending over a range of activities, often in conjunction with other measures. Logic bombs can be planted in foreign computer networks in order to paralyse parts of foreign civil and military information infrastructure. Systems are prepared to take over public radio and television broadcasts.

4.3.4 *Strategic Threats*

Dependencies on information technology systems coupled with inadequate defences create vulnerabilities. Strategic information warfare (SIW) consists of coordinated, systematic attacks through computers, communication systems, databases, and media. This corresponds to a potential threat unlike any previous threat just as the information age society is unlike the smokestack age society. With conventional thinking this new threat is easily underestimated.

Strategic information warfare is the most alarming threat to a whole nation. The enemy could be a hostile nation, a terrorist organisation, an organised crime syndicate or a highly motivated cult. The necessary means and tools to carry out an attack can be found as the proliferation of information technology and expertise is global.

Strategic information warfare in order to achieve major long-term objectives is thought to start with a careful long-range plan including covert reconnaissance missions in order to find critical information assets. Other elements would be long-term collection, analysis and exploitation of open-source intelligence information including but not limited to political, governmental, financial, industrial, societal, and personal activities. Strategic information warfare would then continue to develop as a campaign of covert strikes with a series of

coordinated and precisely executed operations for months or even years to gain as much advantage as possible before revealing the hostile operations. Strategic information warfare would finally be combined and integrated with other actions such as terrorism, diplomatic measures, and military operations for maximum synergy. This kind of warfare would more likely resemble Waterloo than an electronic Pearl Harbor. The reason is that there would be an associated strategic long-range plan, ultimately in order to achieve strategic power in some respect.

Strategic information warfare has special features in comparison with the other threats. Targets are selected for the ability to cause systematic collapse of an opponent's capabilities. Many interdependencies among systems could cause failures to spread widely. Goals are strategic in nature and could eventually result in changing the balance of financial markets, the balance of military power, or the stability of an international coalition. Combining information warfare with other military, diplomatic, societal, ethnic, or market tools creates synergy and increases effectiveness. Strategic information warfare represents an interesting and low cost asymmetric option for adversaries that cannot compete using other types of power.

The very nature of strategic information warfare is such that no hard evidence of activities is revealed until operations have increased to a certain magnitude. This makes it very difficult to convince decision-makers of the importance of investing in alertness and effective countermeasures. In the United States a number of hearings have pointed at structured attacks from unknown sources and that some of these attacks could be "state sponsored". A present known threat is that hostile organisations might try to exploit the Y2K problem and the connected window of opportunity at the millennium shift. Such operations could be well concealed. In Europe, the combination of Y2K and the start of the Euro present more information warfare opportunities.

Strategic information warfare concealment is expected to be better and detection more difficult the more serious the opponent. Many historical examples point at threats that were undetected. Encryption systems are widely available to permit groups to communicate among themselves and to plan attacks in secret. Nations such as the United States, Russia, China, Britain, France, Australia, and Canada have considerable resources to develop information warfare capabilities. Apart from these states, rogue states such as Iraq, Iran, Libya, and North Korea, would have motives to develop a strategic information warfare capability. Global terrorist networks such as those headed by Osama bin Laden or by very powerful criminal organisations in countries like Colombia, Russia, and Papua New Guinea are also significant players. The required technology, knowledge and tools are readily available. Industrial espionage has long been known and has increased considerably with the new IT tools at hand and with the number of people relieved from cold war intelligence activities and that now have taken on new assignments. Multinational corporations with loose national bounds are also powerful players on the arena, sometimes in cooperation with government intelligence facilities, sometimes not. State-sanctioned industrial espionage exists and may be increasing. It is easy to agree with the following wordings: "...we have created a global village without a police department." (Frank J. Cilluffo)

5. Countermeasures

5.1 Recommendations

5.1.1 Introduction

Information warfare is a new type of warfare and makes it vital for new kinds of defence in cooperation among the civil private, civil public, and military parts of a nation, and also between nations on an international scale. Both non-criminal and criminal economies have gone global. New groups of criminal organisations, activists, extremists and terrorists have emerged worldwide. Rethinking both civil affairs and military operations is a must. On a national scale recommendations to cope with the new threats could look like this:

- Increase awareness and understanding of the threats, especially among critical infrastructure providers and users.
- Develop and implement a national security policy for the information age and re-examine it constantly.
- Make information assurance a national security objective.
- Implement and exercise policies ensuring critical government services.
- Cooperate closely between civil and military government, industry and universities on methods, products and management concerning information assurance.
- Create an information age military capability, expected to be very different from traditional military systems and thinking, and re-examine it continuously.
- Create requirements, methods, organisations and networks for the information age intelligence community.

5.1.2 Awareness

Critical infrastructure providers and dependent users are familiar with hacking and computer viruses but largely unaware of the possible results of an information warfare attack. The visibility of the threat must be clear. Awareness must be raised to a point where actions are motivated and taken. Government must provide industry with information and incentives for taking action and make the private sector lead the way towards reasonable security measures.

“Many leaders and decisionmakers are not cyberfluent. They do not understand the technologies and the realm of possibilities, rendering them less effective in dealing with information warfare issues, policies, and future-focused directions.” (Brenton Green)

“Our best deterrence to the strategic information warfare threat involves continual emphasis on education, training, and awareness for all users; cyber legislation at all levels of government; and research and development in all areas of information technology.” (Mark Centra) However, Sun Tzu has stated: *“The best way to wage war is by attacking the enemy’s strategy.”*

5.1.3 Policies

It is imperative to respect and incorporate the strategic information warfare threat into overall national defence planning and doctrine. Discussion and policy concerning information warfare are unfortunately continuously centred on vulnerabilities, not on a long-term strategy for national security and dominance in national affairs. Such a strategy must cover the total

impact on the nation of the Information Revolution. A secure, strong nation is the best foundation for well being.

“Just as nuclear dominance was the key to coalition leadership in the old era, information dominance will be the key in the Information Age.” (Joseph Nye and William Owens)

5.1.4 Information Assurance

Information assurance is only one step in this policy that must cover the broader perspectives of defending against an attack of national interests. This is a new kind of defence that does not fit into existing traditional military and civil defence. It is vital to rethink national defence, the meaning of national security in the Information Age, the methods of achieving it, and to cover all these new perspectives. The United States Defense Science Board has marked the important difference between old and new thinking in this way: *“Current practices and assumptions are the ingredients in a recipe for a national security disaster.”*

5.1.5 Government and the Private Sector

There is a great difference between protection against strategic information warfare and protection against intrusions by a number of hackers. Protection against strategic information warfare requires extensive cooperation between nation organisations. Private companies play the most important role in development of information technologies. Government is not able to influence this to any great extent. However, government is more concerned about the threat than most of the private sector. Many people are not fully aware of the impact of a strategic attack on the telecommunications and information infrastructure. Thus the private sector must become aware of the problems, be involved in policy planning and take on a role of producing information assurance systems. In order to do so, collaborative partnerships between the public and the private sectors are imperative.

There are a number of obstacles to the development of good information security. Government has lost its leadership in information technology development and has difficulty in regulating security. The commercial sector sets standards mainly to gain market dominance and profitability. Market and profit change rapidly which makes it difficult to maintain a certain standard. It is even a question of whether a company can control standards for its own products.

“Acceleration is the consequence of reducing everything to its digital form and increasing the power of digital processors. Now, any transaction is instantaneous and markets can turn dramatically in seconds.” (David J. Rothkopf)

Just like cowboys enter and exit an arena, commercial systems do so on the multinational arena. It appears to be very difficult to ride the market for more than a limited time, and only a few well-known companies remain on the scene as years go by. Microsoft has been criticised for its market dominance, but this dominance has resulted in widespread common software products. On the other hand, unsecure parts of their software could have widespread negative effects.

Legal obstacles hinder improvement of personnel and operational security. Law has difficulties to keep up in pace with technological development and appears to be far behind in several security areas. Legal obstacles must be overcome concerning red-team exercises.

“At the bottom, allowing red-team testing of computer systems is no different from allowing the cop on the beat to stop and twist the doorknobs on every storefront. No one would tell the police officer to stop doing that for fear of invading the store owner’s privacy. We’ve got to develop a similar set of rules for cyberspace or the only people who will be trying the doorknobs will be the crooks.” (Stewart Baker)

5.1.6 Military Forces

Today military forces depend heavily on civil resources and commercial information technology and systems. Examples are systems for mobilisation, transportation, logistics support, and communications. Without perfect control of the security of these systems – and there is no such guaranteed control -- military operations are at risk. Military services depend to a large extent on commercial-off-the-shelf (COTS) hardware and software, and there are no special military requirements on these. The pace of development in the information technology (IT) area is such that items that were not even on the market two years ago represent 80 percent of the profits today. There is no possibility for the military to keep up with this pace in all respects.

In the 1980s discussions on the revolution in military affairs (RMA) started. Sophisticated information technology showed the way to new forms of warfare with high capacity computer and high fidelity sensor networks, and precision guided munitions. However, without guaranteed information assurance, the credibility of this new military power is undermined by information warfare.

The revolution in information affairs, RIA, extends over the whole society and will be even more developed and pronounced in the future. Along with the revolution in information affairs comes the revolution in military affairs. This is expressed in a true shift from platform centric warfare to information centric warfare which requires new doctrines, new organisations, new kinds of training and knowledge, and new technological tools. The primary prerequisites will be to use electrons and photons as bullets, not gunpowder and fire. The speed of operations will be quite different from what has been known until now. Targets will be the information components in any vital function. War will be permanently going on, mostly concealed and almost always without any declaration of war. Thus software, hardware and wetware attacks should be expected – in peace and in declared war - throughout all design, development, manufacturing, deployment and mission phases.

Life will be quite different from the old days and from conventional thinking. It is likely that the nature of warfare will change, just as most other things are changing in the information age. Operations and war will be carried out in diffuse ever-changing networks without any absolute front or identities of actors. In the blurred environment of information warfare it will be difficult to clearly identify the actor and the real objective behind an intrusion, intentional or accidental, and to respond with appropriate means. There will be diffuse boundaries between civil and military systems, actions, and responsibilities. The most important map of battlespace will be the instantly changing map of information concerning its sources, routes, carriers, receptors, importance, speed, concealment, strategy, and other factors. The most important command leaders in the networks will be those who have the ability to think faster, observe more facts simultaneously, and have the best quality of intuition and innovation. The campaigns will be using the synergy of a combination of hardware military territorial forces, software information forces, and political, societal, ethnical and similar wetware forces. There will not be a resemblance to today’s military and political traditional thinking. There will be

enormous conceptual problems, policy questions, and cultural issues. A great challenge will be to abandon deeply rooted traditional thinking and doctrines.

5.1.7 Intelligence

The intelligence community faces competition from new actors. It must form new continually changing alliances. This implies rethinking organisations and customising products. There is a certain relationship between information warfare, business intelligence, open sources scanning operations, and civil and military intelligence operations. Boundaries between these are not very clear, and it is likely that one activity can transform into another. The result of long-term intelligence operations can be useful for strategic information warfare even though the original objective for the operations was different.

Strategic information warfare requires changes in intelligence organisations and operation, methodologies and information sources, and personnel. A new breed of operators and analysts are needed. Threats throughout the cold war evolved in incremental steps, and intelligence adapted to this development. Information warfare threats can emerge very fast or instantaneously which requires different methods of intelligence. New forms of information sharing are needed between the military intelligence community, the law enforcement community, and the private sector. This could be done by stripping off and protecting sensitive details, while sharing generic targets, techniques, and sources of attack as well as effective assurance methods.

5.2 Swedish Activities

The Swedish government has recognised the increasing threat of information operations and information warfare. A Cabinet working group has issued recommendations for a strategy and for the assignment of responsibilities for defence and protection against information warfare. Some of the proposals follow:

- A high-level coordination group within the Cabinet Office and the Ministries for problems concerning public administration and for national crisis management should be created. The information infrastructure must be regarded as a national asset concerning safety and security.
- A national coordination of information warfare under the leadership of the Civil Emergency Planning Agency (ÖCB) should be created.
- A Computer Emergency Response Team for the Government (GovCERT) under the leadership of The National Post and Telecom Agency (PTS) and with support of the National Police Board (RPS) should be created. Private CERT:s should be invited and encouraged to add on.
- There should be an obligation to report all IT related incidents within the public administration to a designated Information Sharing Analysis Center (ISAC) which combines incident information from both the public and private sector. In both cases above – GovCERT and ISAC – a key element is the close cooperation with the Private Sectors Security Delegation, which serves as a one-stop-shop to the private sector.
- An active IT control function (Red Team) should be managed by the Armed Forces.

- Media coverage within the IT area at the National Board of Psychological Defence (SPF) should be encouraged.

Internationally there are challenges for international law, international cooperation, and the use of force. Doctrines concerning the use of information warfare and information operations under the United Nations or other international legal auspices are of interest. What could be discussed are international operations or upholding sanctions. Also of interest are principles of building regimes for defensive actions taken in cyberspace. This could involve actions like tracing and counterhacking. Some of these thoughts have been raised at workshops in Sweden.

According to an American view the basic term is information operations, and information warfare is one part of information operations in crises and war. One application of information operations in military operations is command and control warfare. All of these terms comprise both offensive and defensive parts.

The Swedish Armed Forces defines command and control warfare as offensive only and has made studies according to this. The Swedish industry is reluctant to use the term information warfare with regard to the previously mentioned drawbacks. In my personal view we ought to agree with international views as far as possible and primarily develop the defensive parts.

5.3 Emphasising the Information Defence

If it is true that we are standing on the edge of the deepest powershift in human history, we need rethinking for both the military and civil business. A new starting point and idea is to emphasise the importance of information forces by creating the Information Defence. The Information Defence consists of new civil and military forces. The military force must be integrated, with distinct and profound ingredients. These ingredients are force multipliers of land, sea and air forces serving as cement to join together land, sea, air and information operations.

The Information Defence must also include coalition forces and civil society. The civil information defence must defend finance, media, government, and all other functions associated with the information infrastructure including those parts, which are required by the military defence.

Military information forces have been associated with some kind of “hacker army”, but this might not at all be the task, or at least far from the only task. The information forces could be assigned a number of special and qualified tasks requiring new kinds of recruiting and training depending on the nature of the special areas. To begin with there would be no existing organisation to fit the new forces, and existing established organisations might resist the new information defence forces because of the fear that their own budget could be threatened in making room for a new organisation.

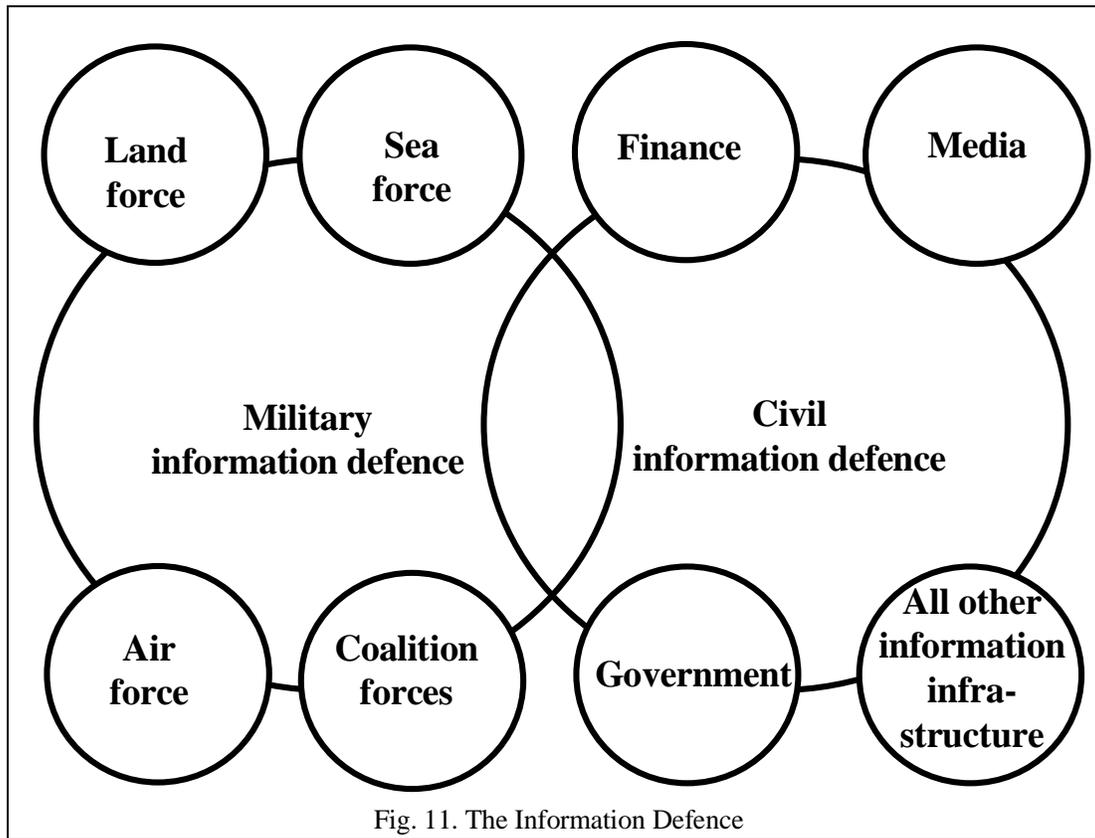


Fig. 11. The Information Defence

Concerning the military part of the information defence, there are several reasons to introduce it:

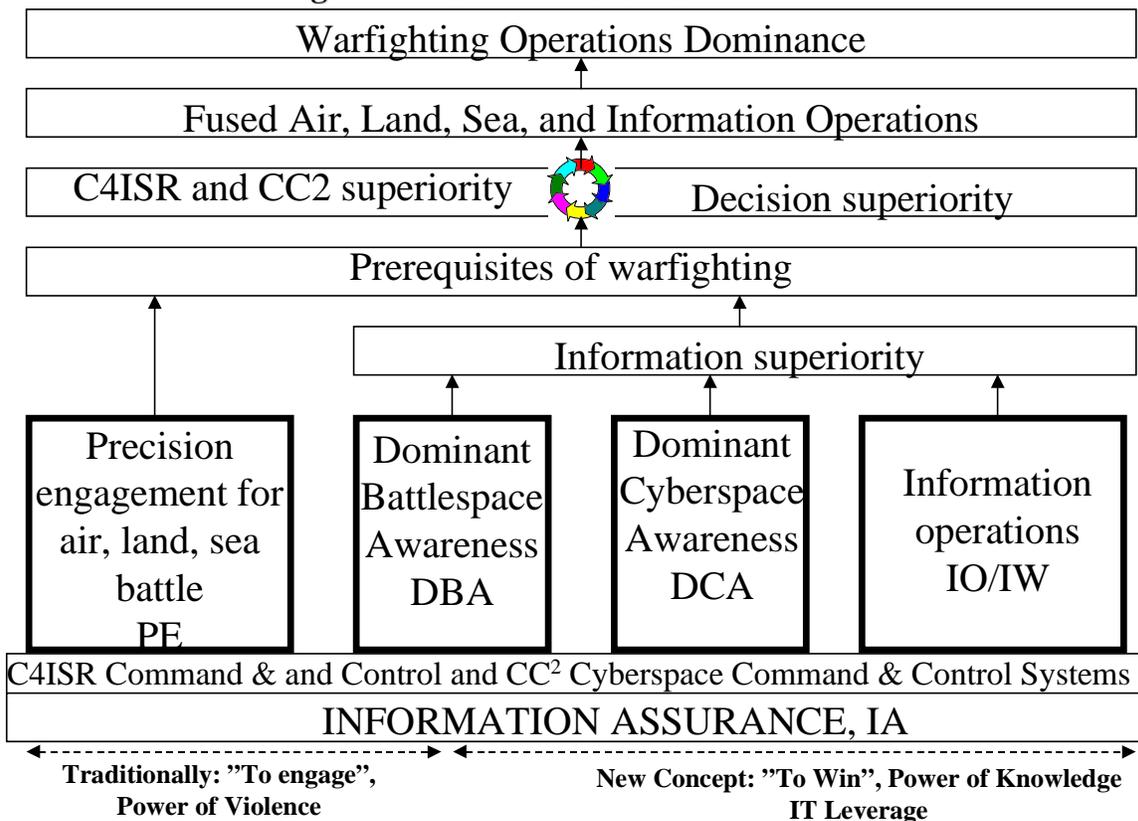
- Command and control and command and control systems are primary targets and must be protected and defended. Information warfare is in progress before a declaration of war and is harming the national information infrastructure. Thus the capability will be reduced to exercise military force in times of war.
- A prerequisite to conquer land, sea and air is to conquer the information and knowledge battle-space. This requires a shift from a platform-centric defence to an information-centric defence with information transparency and interoperability as features for the forces.
- Information forces are needed to fight enemy information forces without having a weak position. If one party is equipped with information weapons and the other is not, the competitive arena is sharply tilted. What should one do when unarmed and in front of such forces? Many special disciplines are needed.
- Emerging new military disciplines and weapons used in new ways require new types of knowledge, organisation and training. Innovations and development of new patterns of behaviour are also required.
- There is a gap between the revolution in military affairs and conservative military ideas and organisations. Futurizing and rethinking require a new starting point and new perspectives, not just incremental changes of what is already there. It is a question of inventing the future, not merely improving the past.

- The Information Defence main objective is to achieve information superiority and decision superiority as a foundation for planning and executing co-operative land, sea, air, and information operations. In order to do so the Information Defence executes information operations to achieve information assurance, produces dominant battle-space knowledge, and acts as a focal point for a true and common battle-space picture.

The following should be noted. Information and decision superiority is not an eternal realm, but rather a temporary condition within a limited space. Information operations are performed both as a precondition for joint operations and within joint operations.

Traditional battles involve land-, sea-, and air forces supported by command and control systems, intelligence, surveillance and reconnaissance and systems to acquire timely battlespace awareness. With the addition of the third main element -- information operations including information warfare -- and with information technology as a reinforcement for a vision of battlespace and for command and control systems, the art of war is revolutionised, and information superiority becomes a clear objective. Together with the fighting prerequisites this can in its turn provide for command and control and decision superiority. In peacetime only part of the main element information operations and dominant battlespace awareness are being used. In conflict and war these elements are used to full extent together with the land, sea, and air forces.

Fig.12 INFORMATION AGE WARFARE



There are vital differences between geographic systems and cyber systems. Cyberspace Information Superiority builds on Dominant Cyberspace Awareness (DCA) and Information Operations in the Cyberspace Command and Control System. In the cyber world objects are intangible in artificially created medium. Sensor systems are system log files, intrusion

detection systems, sniffers, user profile databases, network management systems, Internet traffic control etc. Weapons are logic bombs, Trojan horses, worms, virus, backdoors, sniffers etc. There are much different rules-of-engagement doctrines in cyber warfare. Examples are rules based on timeliness, fidelity, and accuracy of knowledge databases, short-term sensor information, and decision support systems.

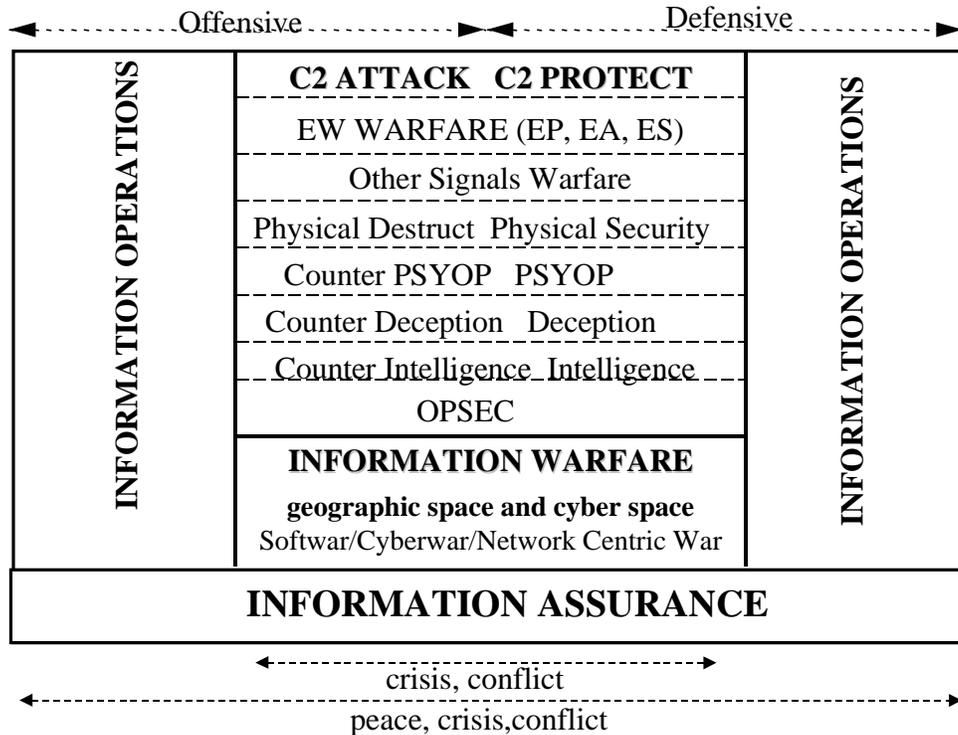


Fig.13 Information Operations / Information Warfare / Command & Control Warfare
Floating boundaries!

Information operations depend on information assurance and include command and control warfare, network centric warfare / softwarfare / cyberwarfare and other signals warfare.

Domain	Target	Battlefield Armed forces	Power	Examples
Wetware Brainpower Brainwar	Human thoughts, Perceptions	Political, Religious, Ethnical etc	Knowledge	Milosevic
Software Softpower Softwar	Information	Cyberspace, Media Information forces	Wealth	TV programs
Hardware Hardpower Hardwar	Land	Air, land, sea and its forces	Violence	Jugoslavia

Fig. 14. HARDWAR, SOFTWAR AND BRAINWAR

In my view a conclusion of this is that the geographical map and video images of battlespace must be supplemented by a map of human minds and perceptions, and that this requires a new attitude. We must proceed from power of force to power of mind, supplementing power of force with power of knowledge with the aid of information, information assurance, and information defence. We must be able to manage both conventional warfare and information warfare and other more concealed, disguised or masqueraded forms of conflict.

Conflicts can be complex and hard to grasp. One way to try to analyse different layers or classes within a conflict can be to divide it into hardware, software, and wetware (brainware). Within the hardware region the battle of territory is fought with land, sea, and air forces and power is conquered using violence. In the software region the battle is about information and information superiority, is fought with information forces – visible or invisible – and power is conquered using the control of media, cyber space, electromagnetic spectrum, and other carriers of information together with sources and receptors of information. In the wetware region the battle is about thoughts and concepts, and forces are camouflaged as political, religious, ethnic and other groups; and power is conquered using control of knowledge. In the worst case this can mean lack of freedom in an undemocratic environment and in the very best case free access to knowledge in a completely democratic environment.

At times of political elections when the politicians are quarrelling, it is a sort of camouflaged wetware war. The whole population is mobilised in order to participate in the elections. The victorious political group captures the power and occupies the political arena. Certain countries prevent its population from free access to information and from exercising the free word. That resembles an information blockade in the same way as for instance one speaks about an oil blockade. During the blockade, forces are in effect to mentally mobilise and arm according to the objectives of the rulers. When the objective is attained, a mental occupation is prevailing similar to territorial occupation; and the nation is equipped with mental forces not easily engaged using other types of forces. There are many examples of religious and ethnic forces in charge of occupying the population mentally and successfully. It can be very difficult to disengage such an occupation. Similar conditions apply to the political area in several cases.

5.4 Points of Similarity between Military and Civil Views in the Information Age

There are some fundamental points of similarity between military and civil activities in the information age, although the wording and terminology are often different. Fundamental is the utilisation of information leveraged by information technology. Fundamental also is the agility of business operations, the speed of development, production, and marketing of goods and services. Both sides need reorganisation, networking, and concurrent processes. Offensive spirit and action is vital in order to survive and prosper in the business world.

Both military and civil activities can be said to rest on five fundamental pillars in the information age:

Information assurance through

- Authentication – verification of originator
- Non repudiation – undeniable proof of participation

- Availability – assured access by authorised users
- Confidentiality – protection from unauthorised disclosure
- Integrity – protection from unauthorised change

Infrastructure protection concerns the government, the military, and business as all of them use the same national information infrastructure. Infrastructures are increasingly transnational and global.

Information dominance does not mean total dominance but rather sufficient dominance and superiority at the critical time and place. Information is a catalyst in a business process and the race goes to the swift. Information warfare can be regarded as the struggle for control in a decision space. Information dominance can be achieved through Business Intelligence, and speed and agility of product development, marketing, and finance.

Perception management is the ultimate goal of information operations and information warfare. In civil business this is done in several ways:

- Broadly informing through effective Public Affairs, which is a normal corporate function.
- Broadly persuading through coordinated Public Diplomacy, which is lobbying.
- Focused persuading through well-targeted Psychological Operations, which is advertising.
- Distorting the opponent's sense of reality through deception.

Finally *operational effectiveness* combines important features:

- In the modern market, any given enterprise can simultaneously be a competitor, customer, supplier, and ally.
- In the marketplace, effectiveness means being adaptable to early changing trends in technology and business practices.
- Being innovative and highly adaptive in product design, production, business practice and marketing.

6. An American View

6.1 Information Age Requires Information Operations

Telecommunications, automated data processing, sophisticated decision aids, remote sensors, and other types of information technology applications are rapidly developed today, are globally proliferating and being used, and are creating dependencies within an increasing number of areas for civil and military purposes. There are no firm boundaries in the world of information between civil and military systems, and the development results in a situation where no single authority has full control over the totality. New information systems and new technologies are continuously being introduced and offer almost unlimited possibilities to exploit the value embedded in timely, accurate, and relevant information.

Today information is a strategic resource of vital importance to national economy and security. This reality extends to civil and military business at all levels. Every system designed and deployed has some inherent weakness and vulnerability. In many cases this is the inevitable result of aspiration for increased user functionality, effectiveness, and convenience. The complexity and vulnerability of the information systems are often disguised by user-friendly software. Technical possibilities, system performance, efficiency, and decreasing cost result in an increasing number of users becoming dependent on them and running the risk of falling victim to latent/concealed vulnerabilities. All development has both good and evil sides, and it is clear that the arsenal of IT tools also finds applications for evil purposes.

The explosive global proliferation of information technology has a considerable effect on our actions in peace, crises, conflict, and war. Our reliance upon information technology creates dependencies and vulnerabilities in the whole of our modern infrastructure and generates requirements on information defence capabilities. Information warfare is a central and joint defence responsibility for the whole nation. Our dependence on information and information systems, and the exposure of vulnerabilities to a great number of threats, from computer hackers through criminals, vandals, and terrorists to nation states, makes it compelling and urgent to focus on the emerging disciplines of information warfare. Its unique characteristics demands information defence, and its double edged nature creates new powerful opportunities to enhance diplomatic, economic, and military efforts and to support conflict solutions in the future. Information warfare can be an important element to contribute to the defusing of conflicts and thus to avoid military confrontations. This requires close cooperation among a number of sectors in the society.

6.2 Some Basic Conditions

Information warfare involves actions taken to achieve information superiority by affecting adversary information, information-based processes, information systems, and computer-based networks while defending ones own information, information-based processes, information systems, and computer-based networks.

Information warfare focuses on vulnerability and opportunities offered as a consequence of increasing dependence on information and information systems. Information warfare aims at the information itself, at transmission, collection, and processing of information, and at human decisions based on information. The influence may have its greatest impact in peace and the initial stages of a crisis. If carefully conceived, coordinated and executed, information warfare can make an important contribution to defusing a crisis. Diplomatic and economic efforts can be enhanced and could forestall or eliminate the need to employ military forces.

Information warfare can be waged both within and beyond the traditional battlefield. Information warfare is applicable in all phases of war from mobilisation to deployment, employment, sustainment, maintenance, and regrouping, in all military operations and in all levels of a conflict. Defensive information warfare is constantly applicable in both peace and war and is a constant part of all protection and defence. Offensive information warfare may be conducted in a variety of situations in all military operations. When fully developed and integrated, offensive information warfare can offer an enormous potential and force enabler in support of the warfighter.

Defensive and offensive information warfare are two sides of the same coin, engraved by both threats and opportunities. Information and information systems are both targets for attack and for protection. Duels are fought between friendly and adversary information and information systems. In order to develop an integrated strategy for information warfare it is necessary to understand the fundamental parts of offensive and defensive information warfare and their capabilities.

Coordination among military defence, civil government and industry is imperative. Military defence relies on civil communications and networks, transport systems, and electric power. The technical complexity makes it impossible for a military commander to command and control all information and civil resources. Information warfare can involve complex legal aspects and policy requiring careful review and national-level coordination and approval.

Command and control warfare is a subset of information warfare and is an application in military operations that specifically attacks and defends the command and control systems. Apart from this the capabilities and disciplines employed in command and control warfare together with other less traditional ones related to information systems can be employed to achieve information warfare objectives that are outside the military command and control range of targets. Traditional disciplines in command and control warfare are psychological operations, deception, operations security, and electronic warfare. Examples of other disciplines related to information systems are other signal warfare, computer warfare, and media warfare.

Information operations can have many objectives, e.g.:

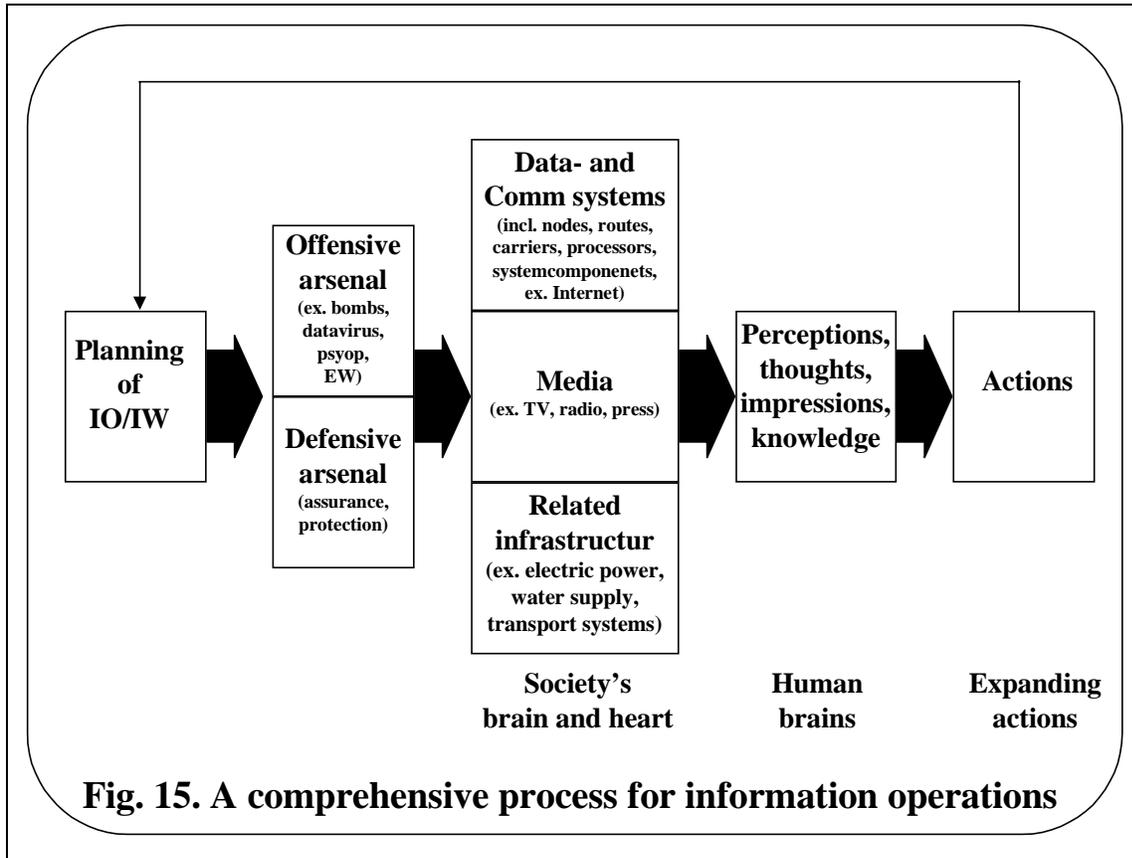
- Protect and defend the information infrastructure
- Deter war
- Affect infrastructure
- Disrupt enemy preparations of attack
- Support peace operations
- Expose enemy deception
- Degrade or destroy command and control systems
- Decapitate enemy national and military leaders from forces

My own thought in relation to this is that the arsenal of offensive and defensive information operations mainly affects three areas which in turn affects people. These areas are:

- Data and communication systems
- Mass media
- All other infrastructure in society directly or indirectly related to information operations

An organisation for information operations could thus comprise:

- Military information forces
- Civil society defence of the national information infrastructure
- The role of media in information operations



In the following mainly information systems and computer warfare will be discussed. The meaning of computer warfare is computer systems used against other computer systems. The systems can be interconnected through networks.

6.3 Information Operations, Information Warfare – Defensive Aspects

The threat against military and civil information systems constitutes a substantial risk for national security and calls for a national security strategy. Defensive information warfare must be organised as a system linking together policy, doctrine, technology, assessment, evaluation, training, simulation, and a mutually supporting national organisational infrastructure. Within military defence, defensive information warfare must be carefully considered, integrated at all levels of conflict, and applied to all phases of military operations. Along the way, information warfare can be integrated into all of national security and defence with the overall objective of capturing the latent potential of information warfare to enhance warfighting capability.

The objective of defensive information warfare is to achieve information assurance to protect access to timely, accurate, and relevant information wherever and whenever needed. Organising defensive information warfare as a system begins with a broad vision with collaborative efforts among the military defence, government, and industry. Visions and ideas are moved from abstract concepts to a set of specific questions and answers based on policy and standards. The five critical components that should be included in any attempt to form a defence system have previously been described:

- Authentication – verification of originator
- Non repudiation – undeniable proof of participation
- Availability – assured access by authorised users
- Confidentiality – protection from unauthorised disclosure
- Integrity – protection from unauthorised change

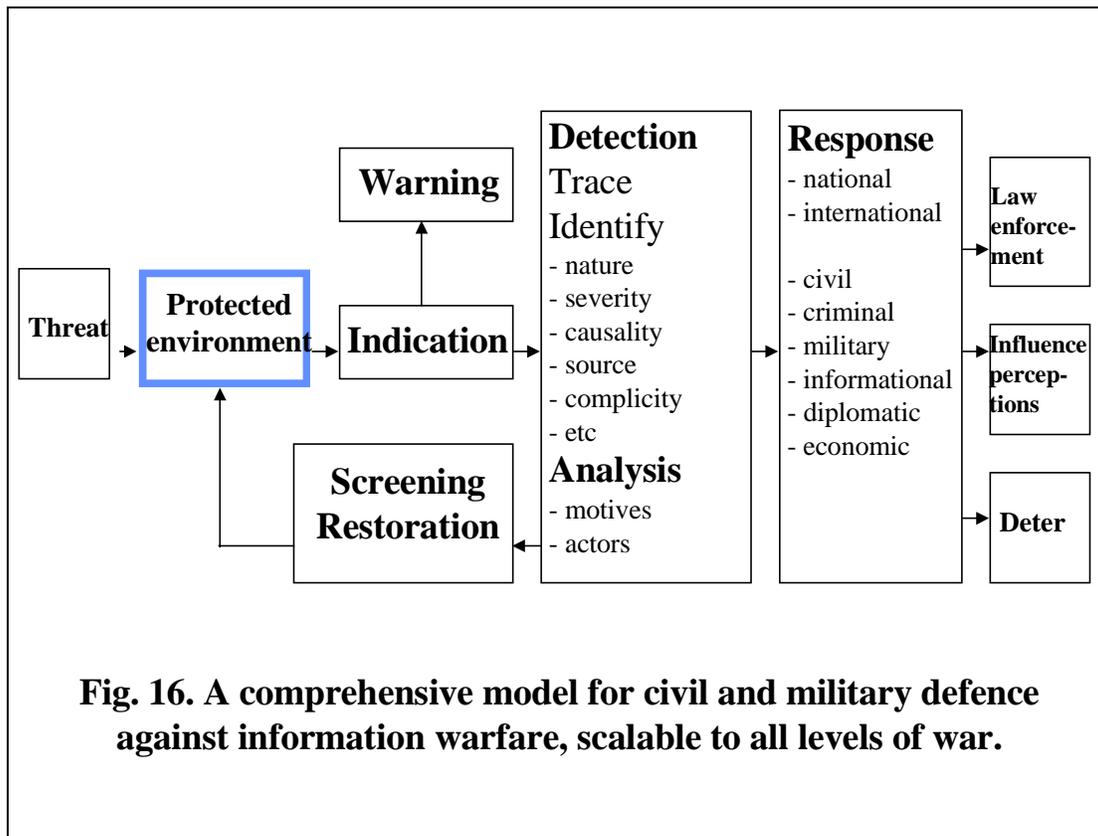


Fig. 16. A comprehensive model for civil and military defence against information warfare, scalable to all levels of war.

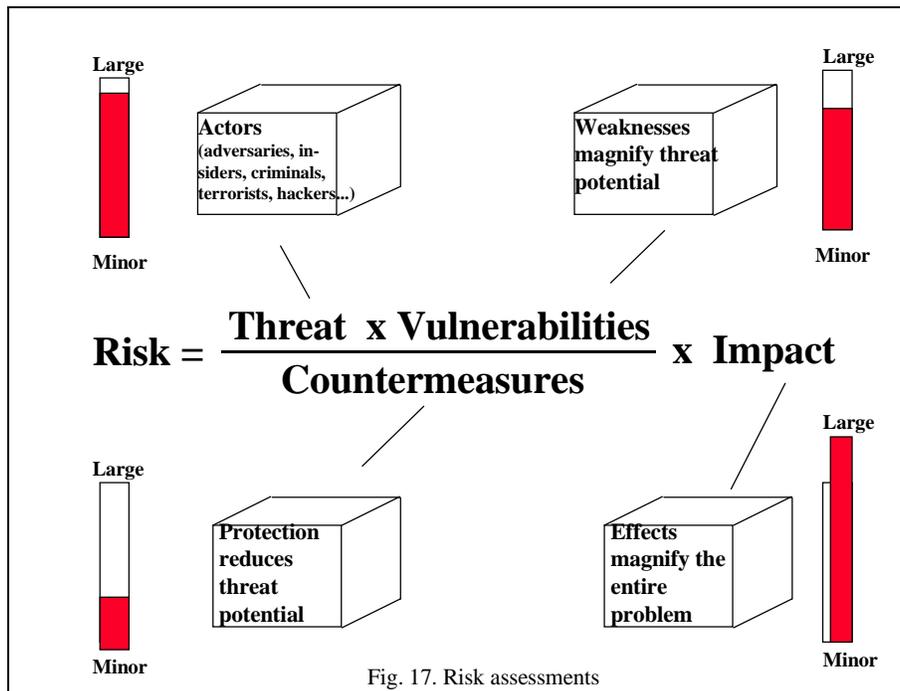
A model in order to manage risks and protect the national information infrastructure will be described in the following with the aid of a number of processes. The model is scalable and applicable for civil and military use at all levels of conflict and all forms of operations. It begins with a defined and appropriately protected and defended information environment. Those threats that can affect the information environment are continuously surveyed. Indications of any interaction with the protected environment initiates a process to disseminate warnings and a process to detect, track, identify, and analyse attacks and other degrading conditions. The nature, severity, causality, complicity, and other characteristics are

ascertained based on knowledge of the threat built upon information from various sources. Motives and actors are analysed. This starts a process to select an appropriate response. It can imply law enforcement, the influence of perceptions, and deterrence from further attacks. The detection process also starts a process to screen and restore the original information environment.

Often security chains are described by protect, detect, and react, including the need for CERT-groups (CERT = Computer Emergency Response Team). In several respects the overall process can also be applied for other forms of threat than from foreign computers and networks, e.g., for threats from electromagnetic terrorism. (Electromagnetic terrorism is the unlawful use of electromagnetic energy against property or persons to intimidate or coerce a government, the civilian population, or any segment thereof, in furtherance of political or social objectives.)

6.3.1 Protected Environment

The protected information environment is no impenetrable fortress that guarantees a hundred percent security, because that is neither practical, affordable, or even necessary. The focus is on defining the real needs and dependencies. The environment depends on what is critical with respect to national security and is a combination of physical systems and places, as well as abstract processes such as intelligence analysis. The protected environment shall not only provide protection commensurate with the value of its content but also ensure that there are resources available to respond to a broad range of attacks.



The protected information environment is founded in a valid approach to managing risks. The process to manage risks includes consideration of information needs, the value of information that may be compromised or lost if the protected environment is intruded, the vulnerability of the systems, the threats posed by potential adversaries and natural phenomena, and the resources available for protection and defence. In addition, the value of information changes

in each phase of an information process, which must be considered in the risk management process.

Hardly any of these parameters are quantifiable without appropriate methods of measurement. Without measurement values, risk management is a big problem. One solution is to use time as a measure of security. *The time during which security and protection functions must work shall be longer than the time it takes to detect an attack and to react in an appropriate way.*

6.3.2 *Threat Knowledge*

The protected environment can be threatened by a number of actors, e.g.,

- Insiders and authorised users
- Hackers, criminals, and organised crime
- Terrorists
- Foreign countries
- Industrial and economic espionage.

Articulation of a threat must neither be overstated nor underestimated and must be as comprehensively and reasonably defined as possible. Intelligence organisations must continuously pay attention to how the threat evolves. It is a dynamic mission that must adjust to changing conditions. In order to get at the essence of a threat, three basic elements must be understood:

- Identities and intentions of possible attackers
- Possible attack techniques and methods
- Potential targets, extending from the strategic to the tactical levels

6.3.3 *Indication and Warning*

Threat knowledge is an input to a process indicating deviations, intrusions, and attacks; it is important to disseminate warnings to persons, organisations, and processes that are considered to be at risk or require warning to other decision-making processes. Indication and warning must be executed automatically without any delay, as crippling attacks can occur at speeds exceeding the unaided human capacity to detect, analyse, and disseminate warnings.

A high quality system for information warfare indication and warning requires a policy establishing authorities, roles, and responsibilities across local and national jurisdictions. This requires close cooperation between law enforcement, intelligence organisations, and private enterprise. Indication and warning cannot be realised without good collaboration between government and industry.

6.3.4 *Detection, Tracking, Identification, and Analysis*

Automatic detection of attacks and the immediate issuance of an alarm are imperative considering that the time from the initiation of an attack to its culmination can be extremely short. In addition, automatic protective countermeasures limiting damage and propagation of attacks must be self-initiating. Defence against attacks depends on the quality of threat intelligence, how well associated indication and warning processes function, and the agility of system providers, users, and administrators in implementing protective countermeasures. Thus, detection, tracking, and identification of foreign activities require close cooperation between government, industry, and other parts of the society. Identification of signs of foreign activity, analysis of the signs, and dissemination of warnings constitute critical elements of the detection process. It requires knowledge based on information from various sources such as law enforcement, intelligence organisations, system providers, and users. The analysis is comprehensive and time consuming and requires central support.

6.3.5 *Restoration*

Attack detection initiates reactive processes. The first process is restoration of conditions. Restoration relies on a pre-established understanding of the desired levels and conditions of system performance and functionality. Availability and integrity of information may be prioritised, as well as the detection of when anomalous conditions have degraded system processes below a threshold of acceptable function. Example of an organisation of importance with respect to this in the United States is the National Security Telecommunications Advisory Committee (NSTAC).

6.3.6 *Response Aimed at Attacker*

Attack detection mechanisms initiate the response process. Timely identification of motives and actors is the cornerstone of effective and properly focused response. Results of the process for identification and analysis are limited to national-level decision-makers. Attacks cannot unambiguously point to motives and actors. Apparently similar events or indications may have quite different causes, complicity, and severity. Different implications for national security call for providing decision-makers with the best and most comprehensive information as a basis for the selection of response.

Knowledge of true motives and actors are very important for the design of response processes. However, there is no clear and unambiguous set of automatic response processes to choose from. The reason is that the seam between civil and military roles is blurred when it comes to national security with respect to defensive information warfare. An attack against a commercial system in service for both civil and military purposes raises legal and policy issues highlighting the need for increased interagency coordination and joint civil-military response operations. Through all of this, the limits of the proper and legitimate role of government to provide for the common defence must be recognised and respected, ensuring no violation of personal freedom and rights of privacy.

The effectiveness of the response process depends on the efficient integration of attack detection and analysis capabilities. Timely response is essential to influence adversary perceptions, establish user confidence, and maintain public support.

6.4 Information Operations, Information Warfare – Offensive Aspects

Military defence relies on information in order to plan operations, deploy forces, and execute missions. Advances in information technology have significantly changed these processes. Complicated information systems support powerful infrastructures that dramatically enhance defence capabilities. However, joint forces become more vulnerable as a consequence of the increased dependence on these new technologies.

Defensive information warfare incorporates a comprehensive strategy in order to protect and defend information and information systems. When combined with offensive information warfare, the net result is an opportunity to use information warfare to exploit situations and to win.

As with defensive information warfare offensive information warfare capabilities can be used at each level of warfare and across the range of military operations. This makes it important to carefully consider how these conditions can be exploited. Employment of information warfare can result in a decisive force enabler for the joint warfighter. Offensive information warfare capability can affect every aspect of an adversary's decision cycle by impacting its information centres of gravity. The focal point of information warfare is the human decision process. Traditional perception methods such as psychological operations and information system attack can produce synergistic effects and affect information systems, information links, and information nodes.

Offensive information warfare can have deterrent effect on a potential adversary during peace and crisis. The same threat applies to the own nation. In order to counteract this, both offensive and defensive capabilities are required. A strong information defence limits the adversary's possibilities to attack. The ability to respond quickly, effectively, and decisively will influence the adversary's disposition to use information warfare. Together with economic, political, diplomatic, legal, and military power, information defence constitutes an essential element of total national strength. Information warfare capability has a deterrent effect in the information age similar to nuclear weapons deterrence during the cold war.

Offensive information operations can be used in military operations in peace to deter the development of crises, control crisis escalation, project power, and promote peace. Examples of targets are financial and media systems. Such circumstances may require special authorisation and approval with support, coordination, cooperation, and participation by civil agencies. Offensive information warfare can also be employed to disrupt or stop drug cartels and other criminal activities.

There are many other targets than military for the application of offensive information warfare. Offensive information warfare in wartime is not just a matter of military targets like the adversary's command and control system. There are many other information systems that are of importance to the adversary and that might be easier to attack and might be more vulnerable. Examples are systems for production of critical necessities and systems for command and control of electric power and telecommunications.

6.5 Measures for Implementation of Information Operations and Information Warfare

Information warfare focuses on achieving information superiority to achieve a decisive edge in war while information operations form a strategy for peace. This makes it essential to

capture the latent potential of information operations and information warfare. Information superiority requires both offensive and defensive information warfare advantages and builds on amalgamating many traditionally separate disciplines. Five principles must be fulfilled to achieve superiority:

- Establish the necessary relationships, within government and throughout the nation, to secure the information needs of all constituencies. Seal those arrangements in law and policy, in order to preserve peace, security, and stability.
- Reduce the opportunities presented to the potential adversaries by educating, training, and increasing the awareness of people to vulnerabilities and protective measures, both military and civil.
- Improve measures to protect against and detect attacks by pursuing emerging technological capabilities in new ways.
- Improve information and information system attack capabilities.
- Increase capabilities of synergy created by integrated defence-in-depth solutions at all levels.

In order to incorporate information operations as a natural part of defence, they must be integrated in the following six major areas:

- Education, training, and exercises
- Policy
- Doctrine
- Assessments
- Organisational infrastructure
- Technology

It is interesting to note that these six areas are of importance in both military and civil business and thus are of general interest to the whole society.

Education, training, and exercises offer the greatest return on investment to develop information operations capabilities, and they focus on concepts, policy, doctrine issues, and the role of information operations throughout the range of military operations at all levels of conflict.

Policy issues are developed in cooperation with all parties concerned and deal with roles, instructions, and tasks in order to achieve capabilities to command and execute information operations.

A doctrine for information operations comprises principles for both offensive and defensive information operations and deals with organisation, responsibilities, coordination between

levels of command, planning considerations, integration and deconfliction of activities, and intelligence support.

Assessment focuses on the judgement of the role of information operations in overall missions. Special processes and their command are the prime analytical tools supporting the articulation of joint requirements.

The organisational infrastructure is based on merging separate disciplines to form a totality. This can be achieved by collaboration between tailored information operation cells. The building of information operation capability implies an amalgamation of traditionally separate disciplines. The intelligence business is one of the areas exposed to new challenges concerning information operations.

Information-based technology is a principle enabler of information operations. Close collaboration with academic and scientific organisations promotes ideas that may influence future warfighting strategy and doctrine.

Information operations and information warfare build by amalgamating traditionally separate areas of knowledge. Such areas are: Psychological operations, operations security, electronic warfare, network management, counter psychological operations, counter intelligence, computer security, deception, intelligence, physical security, counter deception, public affairs, and information attack.

6.6 Conclusions of the American View

Military defence is dependent upon information to plan operations, deploy forces, and execute missions. Advanced information technology has decisively altered these processes. Complicated information systems support powerful infrastructures dramatically enhancing warfighting capabilities. Meanwhile vulnerabilities increase as a consequence of the dependencies of those rapidly emerging technologies. Conversely many of such deficiencies also concern the adversary. Thus opportunities are presented to use offensive actions in ones own favour.

The information age presents opportunities to nations and military organisations to gain decisive advantages through access to timely, accurate, and relevant information. Information is a strategic resource driving a global competitive environment. This fact permeates every facet of warfighting in the new century.

In many places around the world information operations are being studied today. Principles for defensive information operations are being developed and introduced to protect and defend information and information systems. Combined with offensive operations opportunities are at hand to exploit situations and gain advantage.

Information operations and information warfare is a reality today and will be more important in the future. It impacts societies, governments, and the whole range of military operations at all levels of conflict. Implementing information operations capabilities is a challenging task. Man has much to learn in order to understand the essence of information operations and its relevance to survival and conflict, now and in the future.

When properly developed and applied information operations can serve as a fundamental strategy for peace and a decisive edge in war. We have not yet arrived at that point.

7. Epilogue

Concerning the military part of the information age vocabulary, what is the result of all these glorious phrases such as “*information superiority*”, “*dominant battlespace awareness*”, and “*revolution in military affairs*”? What is the answer when considering conflicts such as those in Somalia and Yugoslavia? Maybe it is not such an easy thing to win the information war, to gain information superiority, and to successfully implement new solutions when applied to old types of conflict. Maybe it will take time before development catches up with expectations. Rethinking solutions to conflicts is necessary now that the information age rebalances the proportion between knowledge, wealth, and violence. In that process international law and human rights must also be taken into new perspectives.

People have not changed appreciably; they have not learnt from mistakes by earlier generations, nor have they learnt to talk with one another rather than to or past one another. Those who search for something in the darkness of the night only under the light from the street-lamp are not always lucky to find what they are looking for. Maybe other areas should be illuminated in order to look for solutions leading to more peaceful relations in the world. Who is able to point the light in the right direction? *The deepest powershift in human history must be met by reinforcing the Knowledge Defence.*

8. Acknowledgements

The author wishes to thank Dr. William A. Radasky, Metatech Corporation (Goleta, California), sincerely for his valuable language review and Mr. Lars Nicander, The National Defence College, Sweden for his review of “Swedish Activities”. My sincere thanks also go to my wife Margareta Wik von Bornstedt for her kind support and encouragement.

9. References

1. US Joint Chiefs of Staff. *Information Warfare. A Strategy for Peace... The Decisive Edge in War.* (Brochure with remark from John M. Shalikashvili, Chairman of the Joint Chiefs of Staff)
2. Center for Strategic and International Studies task force report. *Cybercrime... Cyberterrorism... Cyberwarfare... Averting an Electronic Waterloo.* (Washington, D.C., 1998, ISBN: 0-89206-295-9)
3. European Parliament, Scientific and Technological Options Assessment, STOA. *Development of Surveillance Technology and Risk of Abuse of Economic Information.* (Luxembourg, April 1999, PE 168.184/Part ¾)
4. US Joint Chiefs of Staff. *Joint Doctrine for Information Operations.* (Joint Pub 3-13, 9 October 1998)
5. Toffler, Alvin. *Power Shift.* (Bantam Books, New York, ISBN 0-553-29215-3)

6. Office of the Under Secretary of Defense for Acquisition & Technology, Washington D.C. 20301-3140. *Report of the Defense Science Board Task Force on Information Warfare – Defense*. (November 1996)
7. The White House. *A National Security Strategy for a New Century*. Washington D.C., October 1998
8. Davies, Ian, and Parker, Rick. *Information operations*. (NATO C3 Agency, The Hague, The Netherlands. Oral presentation, 1999)
9. Devost, Matthew G. *Vulnerability Assessment / Red Team Experience*. (Infrastructure Defense Inc. Oral presentation, 1999)
10. Wik, Manuel W. *Mobilisation for a new era*. (Militaert tidskrift Nummer 1 - 1999, Det Krigsvidenskabelige Selskab, ISSN 0026-3850)
11. Wik, Manuel W. *Global Information Infrastructure: Threats*. (Global Communications Interactive 1997, Hanson Cooke limited, ISBN: 0946 393 893) (<http://www.globalcomms.co.uk/interactive/technology/firewall/280.html>)
12. Borg, L., Hamrefors, S., Wik, M., 1998. *Information Warfare - A Wolf in Sheep's Clothing!* (Link from <<http://www.infowar.com>> Also in Swedish: Kungl Krigsvetenskapsakademiens Handlingar och Tidskrift, 3. häftet 1998)
13. Wik, Manuel W. *Informationsoperationer – en strategi för fred; informationskrigföring – en avgörande spjutspets i krig*. (Kungl Krigsvetenskapsakademiens Handlingar och Tidskrift, 3 häftet 1999)

Some books on Information Warfare:

14. Schwartau, Winn *Information Warfare: Cyberterrorism: Protecting Your Personal Security in the Electronic Age* (Thunder's Mouth Press, ISBN 1-56025-132-8, 1994)
15. Denning, Dorothy E. *Information Warfare and Security* (Addison Wesley Longman Inc., ISBN 0-201-43303-6, 1999)
16. Alberts, David S., Garstka, John J., Stein, Frederick P. *Network Centric Warfare* (CCRP, ISBN 1-57906-019-6, 1999)
17. Campen, Alan D., Dearth, Douglas H. (editors), *Cyberwar 2.0: Myths, Mysteries and Reality* (AFCEA International Press, ISBN 0-916159-27-2, June 1998)
18. Greenberg, Lawrence T., Goodman, Seymour E., Soo Hoo, Kevin J. *Information Warfare and International Law* (CCRP, ISBN 1-57906-001-3, 1997)

ooOoo