INFORMATION OPERATIONS
Some Operational reflections

Brigadier-General Prof. J.M.J. Bosch
Royal Military Academy, Breda, The Netherlands

ABSTRACT

'Information Operations' can only be understood in the broader context of change and continuity. 'Cyberspace' is, like land, sea, air and space, a dimension in which war can be waged. Where defence is a necessity while attack is a possibility. There is a close relationship between 'Information Based Warfare' and 'Information Operations'. Information Operations do however not only impact the military domain, it may also use national, international and even global layers of connectivity to influence a state, an alliance or a global audience. In the end all layers need command and control to keep order in the system. Notwithstanding the value of information technology, it is finally man who still has to decide and act. Given our dependence on information and communications technology (ICT) and options to manipulate information and the human decision maker, we face new threats; the challenge is here and now. Frustration comes with the complexity of the challenge.

INTRODUCTION

There is an almost endless series of books, articles and other publications on information as a mean, target or weapon, in short 'Information Based Warfare' and 'Information Operations'. Secondly, one observes the complexity of a variety of changes that already influence or soon will influence command and control. The scope of this article is, in essence, a military one. It first of all deals with the perspective of a military observer, who tries to understand today and tomorrow; who is confronted with changes at the speed of a modern computer processor, with continuity and getting things done in spite of this. Thinking about solutions is only sensible if we understand the challenge. My goal is to describe the meaning and implications of Information Based Warfare and Information Operations as to foster 'awareness', nothing more, but also nothing less.[1] My observations may be sobering enough.

THE BROADER SCOPE

Some might argue that we live in an age of over-change. With the disappearance of the East-West confrontation, stability diminished and gave way to many changes. The present global environment has hundreds, even thousands of actors, each struggling for power, influence, money and attention. States are among them. In this complex arena economic, demographic and ecological, cultural, and technological developments may lead, in itself or in combination, to conflict. Wealth is quite unevenly spread if we compare west and east, north and south. There is a strong relationship between economic growth and demography. Changes for the better only occur where economic growth substantially surpasses population growth. The problem is, that poor more or less equals to growing populations. The third dimension is ecology. We are confronted with an uneven distribution of raw materials and energy. Water is a real concern, as there are shortages already and as there is no substitute for this commodity. Culture, a fourth dimension, deserves attention too. Where rich and poor coincides with

cultural boundaries, and where identity seems to be in danger, perceptions and religious convictions might generate forces with dangerous dynamics. The media are both spectator and commentator. They are sometimes strictly controlled and thus instrumental. As a bridge between 'the message' and audiences they do influence collective feelings and emotions and may thus foster or hinder decisions including those concerning the use of force. Then there is science and technology on which any society builds its capabilities to produce goods and services - also of a military nature -, to organise and to act.

TECHNOLOGY

Information and communication technology (ICT), the combination of - simply put - computers and telecommunication, affects all aspects of daily life, our society and the world we live in. Biotechnology holds both promises for medicine and agriculture as well as dangers of new weapons. Space technology may lead to new options for communications, surveillance and management of the environment, but also to space weapons. And then there is micro- and nano-technology which may affect all other domains. In 1998, the NASA Ames Research Center in California presented a concept for a revolutionary transmission system built from atoms and molecules. One millionth of a millimetre small, the artificial wheels could rotate with enormous speed, driven by the electrical field of a laser. This development alone could mean a revolution in itself: the 'nanonisation' of machines and systems. As technology means power and money, it is a potential source of conflict.

It adds to existing sources of conflict, like the uneven spread of population, living space, wealth and water. A last source in itself is history, as it left unsettled bills and brought - at least to some - hatred and anger. Given these observations, the traditional definitions and concepts of security are increasingly inadequate. Our greatest challenge is to understand the complex world and trends towards the future. Most probably there are different futures, depending on who we are and where we live. According to Van Creveld we live in the 'Age of Automation'; according to the Tofflers we are now part of a 'Third Wave', the Information Age. They are right. Yet it is both change and continuity that accompany mankind. The constants being, the struggle for power, influence and wealth, coping with realities, and the continuous need for adaptation to never ending change. So what about the military domain?

THE MILITARY REALM

There have been and will be lengthy debates on military technological revolutions. According to one author we are now witnessing the tenth. Others used time frames to illustrate revolutionary changes all using different measures. Dupuy described on the basis of the speed and the process of technological change four periodes.[2] Slipchenko, a Russian Major general, indicated that the Gulf War presented some of the sixth generation weapons.[3] Van Creveld describes four epochs: the 'Age of Tools', the 'Age of Machines', the 'Age of Systems' and, beginning around 1945, the 'Age of Automation'. According to the Tofflers we are now in the 'Third Wave'. A new technosphere, a new information sphere, a new industrial sphere, new institutions and new types of war in which information is the critical enabler, mark this wave, originating in the U.S.A. between 1955 and 1965.

There is ample discussion about the number, reasons, effects and final meaning of revolutions. There is however little debate that they do occur where vision and technology meet in new concepts, organisations and modus operandi, the way we act. In the end, all changes were the effect of a combination of factors; the understanding by some that a combination of technologies might bring an advance or a risk if used by others; strategic thinkers who positioned such a development within a policy context; doctrinal thinkers who translated the new alternatives in a first concept, and others who imbedded this new system in organisational settings fitted for operational realities. Finally, there was 'trial and error', where, rightly or wrongly, we learned lessons. The impact of revolutions, it comes with the definition, is decisive at a certain moment in history. In the long run - with the exception of the nuclear weapon - revolutions tend to be evolutionary milestones. State, and thus military, obtained more sophisticated means to use in conflict. Yet the word 'revolution' has a special meaning: who wants to be part of 'evolution'? In general, one can observe four trends. The first deals with getting beyond the physical and psychological limitations of the human being, the second with enlarging speed, distance, accuracy and lethality of weapons. The third deals with protection. The fourth deals with preserving command and keeping in control in spite of the weapons available, the environment, an opponent, surprise and friction.

MEANS AND METHODS

If we study means we again can expect a lot to change. The individual soldier may develop into what the RAND-Corporation indicates as 'the Jedi Knight'; all-sensing, covert, indestructible and lethal. We will see better and smaller sensor systems using microwave radiometry and data-fusion. We can expect directed energy weapons, such as laser weapons and electromagnetic weapons. Hypersonic air-breathing missiles may fly at mach 8. We may see the all electric weapon platform and very small systems like 'the Fly' and 'the Wasp' both being micro-electrical mechanical systems carrying different sensors or even a miniature 'Stinger'. We will see new and better non-lethal weapons to have a broad spectrum to attack man, machine or software.

Methods deserve attention too. One could find new ways to use 'old' methods like biological, chemical, and ecological warfare, guerrilla, and, as we will discuss later, information warfare. In the end, change within the military realm is always technology related. But war and conflict are marked by many constants. It always embraces wills, skills and kills. Command and control always deals with uncertainty and has to find ways to overcome the inevitable friction, 'this terrible friction' as we learned from Von Clausewitz. Friction is more than the effect of fear, of exhaustion and uncertainty about 'them' and 'us'. It also has to do with coincidence, fortune and bad luck. Friction now is much more complicated than in earlier years. Clausewitz did not have to deal with air warfare, space warfare, coalition warfare, the press, etc. Modern forces have to. Finally, there is always surprise to deal with. The essence of command is not to reduce friction, but to succeed against all odds. The last constant is - as within broader society - the continuous need for adaptation to never ending change. The constants are indeed man-related.

The real revolutions might be the mastery to wage ware in a new dimension. During WW1 armies came to understand the meaning of the third dimension. WW2 gave way to a fourth, the electronic dimension, setting the psychological dimension aside. It also gave way to first

thinking about the use of space. It is precisely the growing understanding that there is something like a 'Cyberspace', 'information sphere' or 'digital world' that makes information operations a real concern.

ABOUT CYBERSPACE

WW2 acted as a catalyser for many developments; mechanised warfare; combined operations, war in the air, war under water. It resulted in the introduction of radar, new communication systems, the missile and the jet engine, the modern rocket, and the computer. Earlier thinking by Charles Babbage (1792-1871) resulted in a 'difference engine' and, in 1834, an 'analytical engine'. Hollerith tabulating equipment existed as early as 1890. In 1939 Atanasoff, a U.S. mathematician and physicist built what some consider being a prototype of an electromechanical digital computer. 1944 saw the birth of the Automatic Sequence Controlled Calculator, the Harvard Mark I, leading in 1946 to the first all-purpose, all-electronically digital computer, known under the acronym ENIAC. Little known for long was the existence of another 'Mark I', the 'Transmitter, Telegraph, Mark I' developed for use at Bletchley, home of Ultra, for actions against the Enigma, the main German encryption system. In 1943, the first Colossus, using 1500 electronic valves, was introduced; three months later there was Colossus II, giving Hollerith's ideas a new dimension.[4] Both within and outside armies in East and West the computer developed from a rare, crude and sometimes secret 'thing' into what it is today. Its development is however outside the scope of this article. Computers, or better: information technology, are now a 'fact of life'. At the same time it is relevant to note that computers are machines. Everybody should know that bad input means bad output. Everybody should understand that software programs are not flawless. According to Welsh, a standard military program may count some 2% faults.[5] So there is no real foundation for the more or less absolute belief in what a computer 'tells'. There is even more. In 1998, a Dutch company developed software that transforms -through Internet - any personal computer into an instrument to eavesdrop.[6] This ICT influences modern armies, societies and the world at large.

Modern armies cannot operate without some 'information sphere'. The growing complexity of organisations as a result of a diversity of weapon-systems with long range precision capabilities and growing speed, the corresponding need of intelligence, of co-ordination and synchronisation, in combination with the time-factor gave finally way to the present digital world. It is through Information and Communication Technology (ICT) that Armed Forces are managed, commanded and controlled. ICT is more than the combination of computer technology, micro- and nano-technology, data fusion and artificial intelligence. It also embraces communications technology and sensor technology. Its application within the individual weapon and weapon-platform, in sensors, in the command system and their combination, is at the roots of the digitisation of the battlefield.

Then there are the modern nations. It is through ICT that we organise government, the supply of water and energy, transport, banking, finance, commerce and everything else that makes a modern society work. ICT connects the media and different audiences. All this is connected by some form of a national information infrastructure (NII).
Finally there is an international, and even a global information infrastructure (GII), connecting producers and markets, banking and finance, governments and other organisations, and - again - media and world wide audiences as well as many individuals. Internet with its 70 to 80

million users (1999) is only one of the elements of this infrastructure. Nations are only one category among the many institutions and other actors in these supranational spheres. It is important to note that the layers partly overlap, that they are interconnected and that the 'players' partly are common users of the same networks and other means of communication. These means create environments as users and audiences build some 'sphere' as they are connected to this structure. Modern technology makes it possible to enlarge an environment at very short notice. A small invasion of television and radio reporters, government and non-government officials with their means of communication simply connects to a distant information infrastructure. This combination of military, national, international and global information infrastructures and the environments they support, create something, which might be called 'Cyberspace'

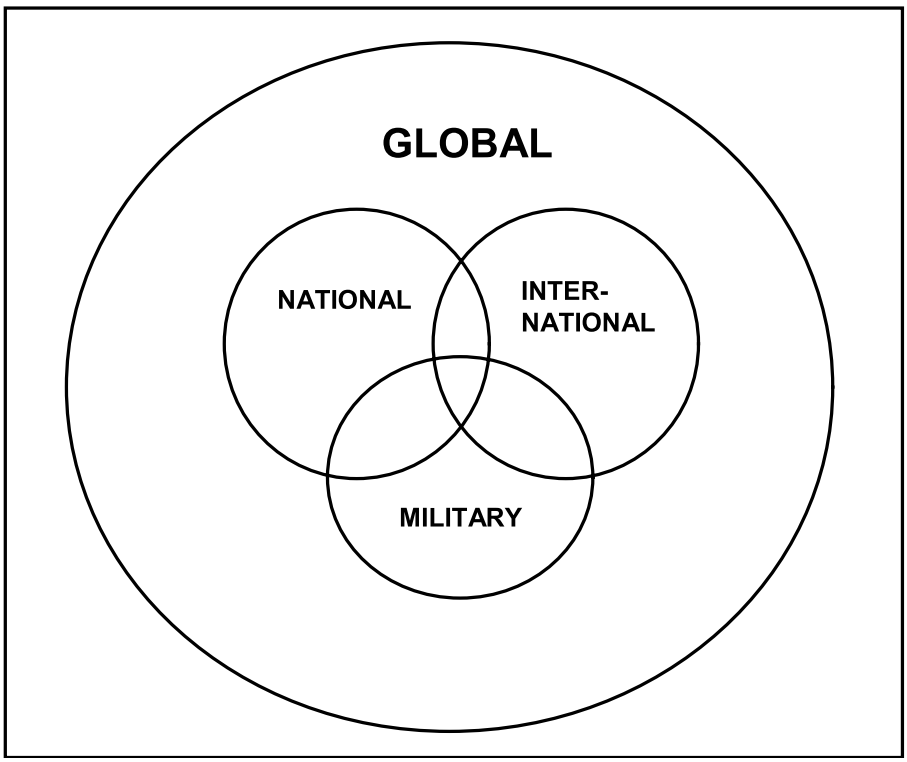

Figure 1: Information Environments

Within this space one can wage war as on land, at or below sea level, in the air, and in space, with command and control as the instrument to direct action. We witness thus a new dimension of war; the electronic and the psychological dimension fade away. And it is within this Cyberspace that Information Operations (Info Ops) play their crucial role.

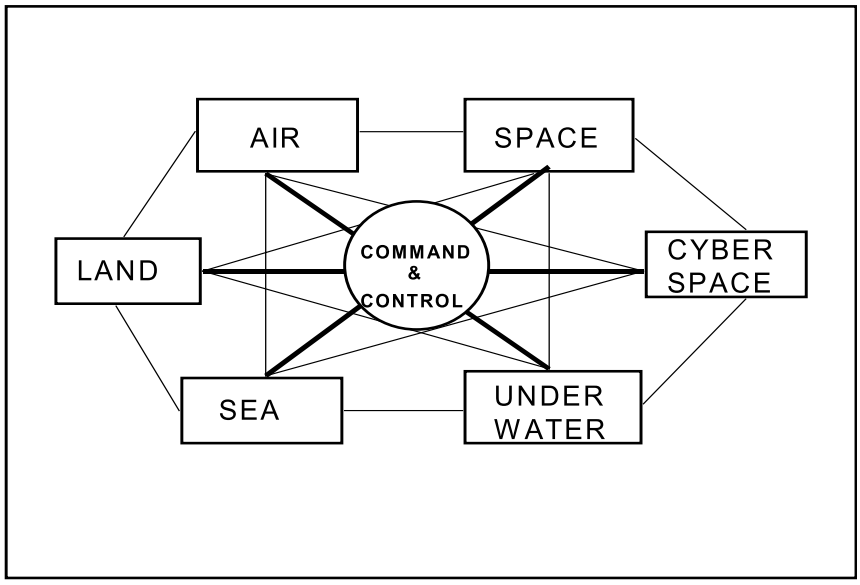

Figure 2: Dimensions of Warfare.

Before addressing conflict in this dimension, some remarks on Information Based Warfare.

INFORMATION BASED WARFARE

ICT in its broadest sense is at the heart of this development. According to the U.S. 'Joint Vision 2010', Armed Forces using the 'system of systems' will gain dominant battlespace awareness and will be able to decrease response time. The conceptual underpinning is TRADOC Pamphlet 52505, Force XXI operations, published on 1 August 1994. According to this document, all activities will ultimately produce a 'Total Force', capable of conducting land warfare in tough, uncompromising situations and environments. This Force will have five characteristics: doctrinal flexibility; strategic mobility; tailorability and modularity; joint, multinational and interagency connectivity, and versatility. The command system rests on new ways to use ICT. Collective unit images will form a battlefield framework based on a shared, real-time awareness of the arrangement of Forces. Thus commanders share a common, relevant picture of the battlefield. The focus is on spectrum supremacy. Combining these developments with concepts of deep operations and simultaneous attack creates a dynamic mode to extend the battlefield in space, time and purpose; to reduce, if not entirely eliminate, the time and need to shape the battlefield. This is the message.[7] But developments go even further. In the year 2025 there should be something like a 'living Internet', a jointly integrated multi-layered C4I infrastructure. According to Perricelli, the vision is that everyone on the battlefield can interact at anytime and in real time. This so-called 'C4I Information Sphere' provides ubiquitous information transport and information services to warfighters, independent of location, degree of mobility, or platform dynamics.[8]
Notwithstanding sincere admiration for these ideas and the enormous efforts that are taking place, there is reason for some reservations. Let me briefly touch on four elements: situational awareness, speed, information and the system as a whole.

SOME RESERVATIONS

Computer screens and databanks do not give the total picture. Some aspects, like motivation, estimates, feelings, personality and culture are hard to store or visualise. How and how fast can we store and retrieve the influence of weather and the effects of military actions, like blowing a dam, in this picture? And what about speed? How is speed influenced by human limitations, the influence of weather and terrain, the effects of good and bad luck, misunderstanding, system failures and our opponent? Please note that a decreased response time gives less time between any decision and the necessary next one. Speaking about humans in real war, it is always sobering to read 'Military Misfortunes' by Eliot A. Cohen and Richard Gooch. Many military forgot to translate experiences into action.

Next, there is the flow and use of information. Data and information alone do not yield decisions. Again and again, man will have to select, analyse, interpret and evaluate in order to decide and act. It may also lead to forms of 'information-pathology'. Army Times described in October 1995 how a HQ during a computer-assisted exercise was overrun without knowing it, while the commander was still busy obtaining further information through his computer. Already in 1985, Idenburg, a Dutch researcher, indicated five effects of the information revolution: the gap between what we know and what we could know is growing. Relatively, we increasingly know less and less. The gap between what we could know and what we can understand widens. The ability to produce information has increased; the ability to process information has not changed for the better. The extra flow of information enforces a feeling of powerlessness, and, finally, the growing amount of information also leads to more 'filthy' information.[9] Eleven years later, in 1996, in another survey, 1313 managers in several countries gave their opinion on information. Some 49% were often or very often unable to digest the available information; 65% expected the future to bring more stress.[10] But there is more to be said about this 'human decision maker' whom should be in control.

THE HUMAN FACTOR

A machine is logic; 'man' sometimes is. The human however differs in more than one respect from a machine. In logical terms he (or she) is inferior. It is not surprising that finally computers beat the best chess-players. Given the fact that rules determine the play, there is no endless series of possibilities. Some actions and counter-actions in war can be defined in logical terms: an incoming rocket engaged by radar in combination with a defensive weapon. Much in war however is outside this realm. In this 'man' is both the most precious, as well as the most limiting factor. Most precious while creativity and feelings do count, in more than one way, when armed conflict is there. Limiting too, as one is dependent on his character, intelligence, background and experience. As Dixon states: "*the ideal senior commander may be viewed as a device for receiving, processing and transmitting information in a way which will yield the maximum gain for the minimum cost. Whatever else he may be, he is part telephone exchange and part computer*".[11] Ideally, yes. In practice: hardly. There is more than one reason why most commanders do not meet these ideals.

Dixon mentions two. The first is that commanders have to fill a number of incompatible roles, including those of a 'heroic leader', military manager, technocrat, politician, public relations man, father figure and psychotherapist. The second has to do with 'noise in the system'. Noise

is what interferes with the smooth flow of information. It partly results from the fact that commanders are channels of limited capacity. Dealing with information takes time. Dealing with more information takes more time. But there is more. There is the problem of probability versus improbability. There is a tendency to resist 'new' information. It has - by definition, high informational content and therefore demands greater processing capacity. It threatens a return to an earlier state of uncertainty and it may confront the man in charge with the thought that he may have been wrong. Kam clearly illustrates the problems of conceptions, cognitive biases and over confidence in his book 'Surprise attack'.[12] But there is more noise to block the flow of information. This may be external in origin, ranging to quote Dixon: *"from static on a radio link to the delusions of a Chief of Staff. Or it may be the internal, ranging from such peripheral sources as poor eyesight (...) to such central and usually more disastrous causes as defective memory, brain disease, neurosis and alcoholism"*.[13] But the outside and inside might influence each other. In fact this commander has to cope with a complex set of organisational, physical, interpersonal and psychological stresses, ranging from mission drift and rules of engagement; from climate to fatigue; from command relationships to the loss of comrades and from ambition to fear.[14] So, the human decision-maker may be the victim of a human hazard - namely that attention, perception, memory and thinking are all liable to distortion or bias by emotion and motivation. Even more important however are the cumulating effects when we look at the 'system of systems' as a whole.

THE SYSTEM OF SYSTEMS

First, the shared battlespace awareness. Sharing a computer screen does not mean sharing the same interpretation. The picture of the environment is coloured by what we know, what we do not know, what we think we know and what we think we do not know. But also by character and background of those who share the screen and the circumstances that confront them.

Secondly, speed. How can we combine actions on different levels, both horizontal and vertical, in such a way that speed is synchronised? A difference in speed may lead to loss of momentum, may result in too hasty decisions, or may endanger the broader command and control. The sheer volume of information available alone, may lower the speed and lead to an operational 'information glut'. Could one suffocate from information? It is important to note that the physical speed of weapons and weapon-platforms may easily be confused with the speed of decision and the speed of execution. Any timely delivery of concentrated combat power involves the combination of everything: decisions and their dissemination, strategic aggregation, tactical positioning and fast, accurate fires.[15]

Next, command and control. The shared situational awareness, encompassing different levels, may be a mixed blessing. On the one hand, there may be misunderstanding on who has to decide on what, who sets priorities and gives orders to act. On the other hand, there is the risk of micro-management. Synchronisation is the key to combined action. It is not only the process that counts - managing action in terms of time and space - but also the effect, the result we want. There is no combined action without co-ordination and synchronisation; the realities of battle space may sometimes ask for initiative and immediate response.

And then, the other effects. In a fully digitised unit there are no real maps, there are hardly hard copy orders or instructions. This means that speed in such a unit depends on the least

digitised element. If the system fails, command and control may come to a standstill as it is all about computer-based information without an alternative. A military map with a hole in it is still a map. A computer may be killed by a bullet leaving nothing to act on. Even within the U.S., this could lead to units that cannot operate within the same environment at the same speed. You are digitised or not. Even more important, how will this effect coalition warfare? There are three types of technological asymmetry. The first is when coalition partners have a different degree of reliance on technology. A second type may arise when partners rely equally on a complex technology but utilise different forms. A third variant arises when partners, equally reliant on similar technology, use it for different purposes.[16] Digitisation certainly belongs to the first category.
Finally, a difficult one: can people trust the system and the information it produces? As stated before, the human is no computer and is liable to distortion or bias by emotion and motivation. But he may also be liable to manipulation. How do we prevent significant degradation or perhaps - even worse - manipulation? How can we 'attack' an opponent? How do we operate within the interrelated information environments? The answer to these questions must be found within the complex realities of modern command and control.

ON COMMAND AND CONTROL

In literature the so-called 'OODA-loop' (Observe, Orientate, Decide, and Act) is often used to illustrate the Command and Control (C2) process and cycle. Yet, this was the loop an *individual* U.S. pilot was trained to 'use' in the Korean War. Nothing less, but also nothing more. One might argue that this 'loop' is too simple an illustration of real C2. The first is the notion that within modern Forces there is no single 'OODA-loop'. In reality, a military organisation in action is a complex machinery where hundreds, even thousands of loops at different organisational levels - each having their own basic speed- have to be co-ordinated and synchronised. The speed of any individual loop is influenced by individual quality, organisational settings, the available technology, the complexity of the problems to be solved and circumstances. The second is very basic: the co-ordination within one single human being - for example a pilot - has to be done and can be realised in a very short time indeed. The co-ordination and synchronisation of the many loops as indicated above is of another dimension. Finally, and perhaps the most basic consideration: the OODA-loop was introduced to solve a problem: C2 has another scope. As soon as this function limits itself to problem solving, one is to lose freedom of action. A problem should be kept within the borders of friction, while the central focus remains the order or directive at hand. It is the desired end-state that counts. Problems will always be there. Clearing them is only one element in a broader concept of operations. Fig. 3 gives a more realistic illustration of the C2 process and cycle in the simplest situation: that of two opposing commanders.[17]

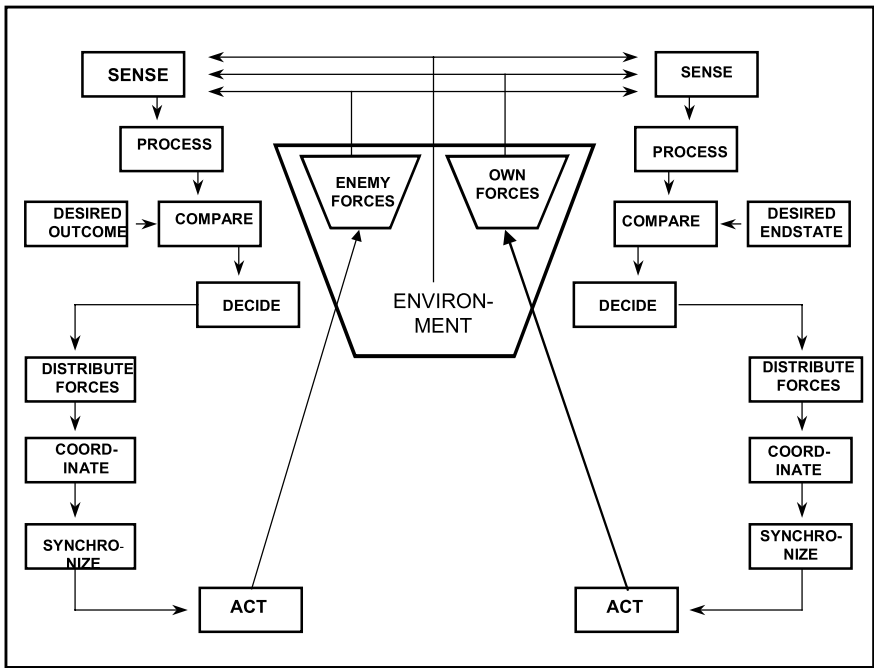

Figure 3:Opposing C2-cycles

Yet it illustrates both the theoretical process, as well as the resulting complexity. But even this illustration is also a simplification. It does not give credit to the fact that many cycles exist at different levels. It also neglects the fact that many are busy at the same time with protecting and sustaining Forces, administrative affairs as well as with plans for future action. Both cycles are intended to support action and to influence or neutralise the opponent. The final aim of command is to keep control. This is more than, as Van Crefeld states: "*reducing uncertainty*".[18] It is, in the end, about getting things done in spite of the odds. This is why the criteria for a perfect C2 system may be listed as follows:

- Preserving the order and cohesiveness of one's own Forces;
- Controlling the pace of battle and avoiding fatal blunders;
- Ensuring 'non-zero-effectiveness'; and,
- Optimising allocations, strategies, or force compositions.[19]

This brings us to the command and control complex that has to enable effective C2 and action.

THE COMMAND AND CONTROL COMPLEX (C2C)

One could have a lengthy debate about data, information, knowledge understanding and wisdom, and their ranking within a cognitive hierarchy. An acceptable generalisation for 'information' might be *"that which reduces uncertainty"* [20], in other words, filtered and organised data, relevant and - whenever possible - timely. Please note that 'that' need not be

digitised information. It could be a ‘real’ map, notes, or a verbal message. The more one nears the environment of direct violence, it may also touch on one or more of the five senses.

The information system functions like the veins and nerves of the broader command and control complex. The command and control process translates data and information into orders, and thus functions like the ‘brains’, as data and information are like oxygen and blood, without which neither brains, nor the rest of the body would function. In a more narrow sense any modern information system has seven basic components: sensors, processors, receptors, data and information, databases, transmitters and rules. There seems little value in a semantic discussion whether ‘it’ is Command, Control and Communications (C3), plus Computers (C4), and/or plus ‘I’ for either Information and/or Intelligence. (C4I or C4I2). The essence is Command and Control, which is supported by a C2-system, which unites sensors, ‘brains’ and shooters. The Command and Control Complex (C2C), as I prefer to use, embraces all: decision-makers, hardware and software, infrastructure, including power, means of transport, shooters and other users. Table 1 gives the separate elements of two opposing complexes.

Defend our	**Attack their**
sensors, processors, receptors, databases, transmitters	sensors, processors, receptors, databases, transmitters
Infrastructure, power, transport	Infrastructure, power, transport
data, information, software and rules	data, information, software and rules
commanders, advisers, and others that support the system	commanders, advisers, and others that support the system
shooters, other actors and users	shooters, other actors and users

Table 1: Opposing C2-complexes

That such a complex including its underlying structure and system is vulnerable to attack goes without saying. This vulnerability results from six basic considerations. As the system has to enable C2, it logically becomes a target. As data and information preclude action, these commodities become a target too. As a system is a structured combination of means; means as well as their cohesion can be attacked or used if one thinks about the collection of intelligence. Fifth, as technology is at the heart of the system, manipulation and degradation seems feasible. Finally, as it is humans who control, support and use those systems, it is those humans who are an important target too.

Information was always important; even in the Bible we read that spies were used to reconnoitre the terrain and observe the enemy. C2 was always a target; the Trojan Horse being a good example of early deception. Yet as the C2-concept increasingly became complex, one found new options for attack. This understanding led to the concept of ‘Command and Control Warfare’ (C2W).

COMMAND AND CONTROL WARFARE (C2W)

Within NATO, C2W is defined as '*the integrated use of physical destruction, electronic warfare (EW), deception, psychological operations (PSYOPS) and operations security (OPSEC), supported by intelligence, to deny information to, exploit, influence, degrade, confuse or destroy enemy C2 capabilities and to protect friendly C2 against such actions*'[21] The objectives of C2W measures are to open, maintain or widen the gap in C2 effectiveness in favour of friendly Forces and thus make a contribution to operational effectiveness. Offensive C2W is particularly effective, and often the most economical way of reducing an adversary's combat effectiveness. It is applicable at all levels of command. The primary objectives of C2W directed against an enemy's combat potential are to:

- Slow down the tempo of his operations.
- Disrupt his operations.
- Degrade the enemy commander's C2 cycle.
- Disrupt his ability to generate combat power.
- Lower his desire for combat.

Safeguarding of friendly C2 systems - defensive C2W - is a fundamental consideration, as failure is likely to result in loss of freedom of action and initiative, misdirection of effort, or failure of the operation. The primary objectives of defensive C2W are to:

- Reduce the vulnerability of C2 assets and installations to attack.
- Reduce the effects of enemy OPSEC actions against friendly C2.
- Nullify the effects of enemy EW actions against friendly C2.
- Deny the enemy's ability to exploit friendly C2.
- Ensure that the enemy's PSYOPS are ineffective.

Though defensive C2W indicates 'safeguarding friendly C2 systems', it is clear that the real concern is the broader 'command and control' as a whole.

Physical destruction does not need clarification. EW includes the effort to gain intelligence by observing and evaluating the enemy's use of the electromagnetic spectrum; degrade his use of this spectrum, and protect friendly use from enemy attack observation and evaluation.[22] Deception is to mislead the enemy by manipulation, distortion, or falsification of evidence to induce him to react in a manner prejudicial to his interests. The prime purpose of offensive deception is to achieve surprise, and maintain the initiative. The prime purpose of defensive measures is to improve security and set the conditions for future operations.[23] Deception must be directed at a specific human target that is normally the enemy commander and his staff and based on their likely reactions. Psychological operations have three purposes: to weaken the

will of the enemy, to win the support of the uncommitted, and to strengthen the resolve of the loyal. PSYOPS must also be co-ordinated with public information, civil affairs and CIMIC-activities. So what about 'Information Operations'?

INFORMATION OPERATIONS (INFO OPS)

There is no universally accepted definition of Information Operations. Though the U.S. Department of Defence issued DoD Directive 36.00.1. 'Information Warfare' in December 1992[24], it is not mentioned in the then current Army Field Manual (FM) 100-5, Operations, published in 1993. FM 100-6, Information Operations, June 1996, uses the following definition: *"Continuous military operations within the MIE (Military Information Environment) that enable, enhance and protect the friendly Force's ability to collect, process and act on information to achieve an advantage across the full range of military operations; Info Ops include interacting with the GIE (Global Information Environment) and exploiting or denying and adversary's information and decision capabilities"*.[25] The U.S. DoD came six months later with a joint Force definition, stating Info Ops are: *"actions taken to affect adversary information and information systems while defending one's own information and information systems"*.[26] The most recent U.S. definition is to found in the USAF Doctrine-Document 2-5 from August 1998. It states: *"Information Operations (Info Ops) apply across the range of military operations, from peace to all-out conflict. The Air Force believes that to fully understand and achieve information superiority, our understanding of information operations must explicitly include two conceptually distinct but extremely interrelated pillars: information-in-warfare-the 'gain' and 'exploit' aspects or other information-based processes - and information warfare - the 'attack' and 'defend' aspects".*

"Information Warfare (IW) is information operations conducted to defend one's own information and information systems or attacking and affecting adversary's information and information systems. The defensive aspect, defensive counter-information, much like strategic air defence, is always operative. Conversely, the offensive aspect, offensive counter-information, is primarily conducted during times of crisis or conflict. Information warfare involves such diverse activities as psychological operations, military deception, electronic warfare, both physical and information ('Cyber') attack, and a variety of defensive activities and programs. It is important to stress that information warfare is a construct that operates across the spectrum, from peace to war, to allow the effective execution of Air Force responsibilities"[27]'.

Reflecting on these definitions, it is interesting to note that they differ indeed. The common elements however are information and information systems. All focus on achieving an advantage. USAF thereby focuses on 'information superiority'. Such superiority being: *"the capability to collect, process and disseminate and uninterrupted flow or information while exploiting or denying and adversary's ability to do the same"*.[28] It is questionable whether the latter is right. 'Air superiority' indicates mastery and 'control' in a certain dimension. Information is more like a 'good' or asset. It gets meaning if used and through action. Information indeed may lead to understanding and insight. This insight - in combination with means, time and space - could create and preserve freedom of action and realise effective command and control. 'Ultra' (reading German Enigma signals) and 'Magic' (reading

Japanese codes) in WW2 did not, of itself, kill anybody; did not sink any ship and did not bring down any aircraft. Men and machines were necessary to do this job. If one accepts that there is something like 'Cyberspace', 'Cyber superiority' might be acceptable, though rather abstract in nature and only meaningful in combination with other elements like means, time and 'place'. Indeed, what is the real meaning of 'information superiority'? Finally it is understanding, insight or 'seventh sense' that counts. Chess players have all the information at hand; yet may not understand what a certain move may imply. War is much more complicated than chess. In the world of conflict we have several dimensions, we have means that may influence one or more of them and there are rules, some resulting from technological limits, some by law of war or ethical frameworks. But those rules do not dictate. They may or may not limit an almost endless set of options. Military operations are, to quote Holcomb: "not mechanistic, and command and control is much more than simply following established procedures, or gathering more information".

The Army digitisation hypotheses: if, within a digitised force, different technologies and doctrines are properly integrated across the Force, then increases in lethality, survivability and tempo will be gained - may rest on the false assumption that military operations are mechanistic. This is the so-called 'Newtonian paradigm': everything functions like a kind of machine, with well-understood laws that describe movements, relationships and forces. However, military operations are not mechanistic. They are - as Clausewitz indicated - to be described as countering friction. The whole concept of digitisation thus may be a simplistic conceptualisation. It is however here, that we must make a differentiation between the separate Forces. Up to a certain level, air and sea operations are indeed more mechanistic in character. The platforms, their weapons and other systems may be described in terms of speed, reach, height and accuracy. Thus battles at sea and in the air can be modelled. Battle at land and battle at the beaches are of a different character. The sheer number of 'actors', the manifold interaction with opposing elements, which may use deception or act unpredictable, and the complex interaction between man, machine, weather and terrain, sets limits to modelling and prediction. Computer simulations cannot really deal with thinking and creative commanders; their decisions are hardly replicable. The risk then exists that we do believe that if we have enough information, and good communications, we can, to quote Holcomb: *"predict all, respond to anything, and control everything. After we've achieved 'information dominance' over our enemy, then all that remains is the efficient functioning of the attrition systems we 'control' until the enemy recognises his defeat"*. In his opinion, the purpose of C2 is - as I indicated before - not information dominance, but to create, assemble and distribute combat power, while accepting that uncertainty will always be there. The commander should seek for sufficient information. Digitisation never should be a goal in itself. New automated C2-systems should only be introduced when there are positive answers to three basic questions:

- Does the Force effectiveness of the digitised force improve relative to an analogue baseline Force?
- Can the units accomplish their operational tasks better than analogue baseline units?
- Do the battlefield digitisation systems work as expected in an operational environment?[29]

But there is another consideration. What would have happened if Forces in WW1, WW2, Yom Kippur, the Six-Day War and The Falklands really had known all the odds? Knowledge may be an enabler; it certainly might be a heavy burden too. Are we really certain that our soldiers should know all information, all the time?
And then another question. What if we know but are restricted to use our knowledge because of deception, secrecy or other implications? Limited to the military realm, Information Operations thus encompass what Arquilla and Ronfeldt indicate as 'Cyberwar'. It includes all elements of C2W. There are however new options. High Energy Radio Frequency (HERF) weapons and Electro-Magnetic Pulse (EMP) transformation bombs may be used. Then there are viruses and other ways to manipulate data. However as stated before, there hardly is a separate military information sphere. Thus, military preparations and operations do not materialise within a vacuum.

OTHER DIMENSIONS

This connectivity of environments gives way to what the same authors indicate as 'Netwar'. This 'netwar' is intended to "disrupt, modify what a target population knows or thinks about itself and the world around it". In present literature this concept of influencing decision-makers, either directly or indirectly through broader audiences, is also referred to as 'perception warfare' or 'neo-cortical warfare'. In fact is has to do with state-of-the-art propaganda. Old concepts and new instruments to manipulate truth could meet. Even at this moment there are several 'battles' going on in the world of media. Both Sadam Hussein and Milosovich understand very well indeed the world of propaganda and media manipulation. So do others, even in the West. A good example of this kind of manipulation was the case of 'nurse Nayirah'. In order to build support for an invasion, the Kuwait Emirate succeeded in having the fifteen-year-old 'nurse Nayirah' present her experiences for a committee of the U.S. Senate. On October 10, 1990 she described how Iraqi soldiers killed fifteen babies in the Al-Addan Hospital. The filmed interview was used by several TV-stations. She later gave - accompanied by six other witnesses - the same testimony to the Security Council. Almost three months later the U.S. led the invasion to liberate Kuwait. Only in January 1992, the truth came out. The so-called 'nurse Nayirah' proved to be the daughter of the Ambassador of Kuwait in the U.S.A. One of her companions, 'Medical doctor Issah Imbrahim' who had described the burial of the babies, proved to be a dentist named Ibrahim Bahbahani. Five of the seven other eyewitnesses had false names.[30] Information as a weapon, it is a fact of life. A so-called cognitive virus may spread faster than a real one. Even at this moment there is no guarantee that a picture shows reality, that words we hear were really spoken and that 'facts' are 'facts' indeed. The real goal however remains the decision-maker(s). As stated in Russia: *"Information Warfare is a way of resolving a conflict between opposing sides. The goal is for one side to gain and hold an information advantage over the other. This is achieved by exerting a specific information/psychological and information/technical influence on a nation's decision-making system, on a nation's populous and on its information resource structures, as well as by defeating the enemy's control system and his information resource structures with the help of additional means, such as nuclear assets, weapons and electronic assets".*[31]

SOCIETAL CONNECTIVITY

But Information Operations might have a third dimension. As Harcknett indicates this kind of operations might be used for *"disrupting or killing societal connectivity, with transport, communication, energy and financial institutions as targets"*.[32] Given earlier statements about the different information infrastructures and the dependence on them, this concept is more than a theoretical framework. It is incorporated within the vision of the RAND-corporation, as it writes about *"the use of Cyberspace to affect strategic military operations and inflict damage on national information infrastructures"*.[33] There are indeed new opportunities for creative and evil minds. Any attack on societal connectivity might have severe consequences. It does not take much imagination to understand what a standstill of energy supply would mean for modern society. According to Swiss research certain branches of trade are quite vulnerable. A total brake down of computers would 'kill' banking activities after 2 days, commerce after 2½ days, modern factories in 5 days and the insurance business in 5½ days. Several authors discussed ways to take down America. Some of the vulnerabilities they listed are outside the realm of 'Information Infrastructure': bridges and dams, the Alaska Pipeline, the Panama Canal, critical railway switching points, etc. Looking at the information infrastructures there certainly are Achilles heels. Table 2 gives a 'top ten' of elements that are vital to broader command and control within the U.S.A.[34]

1	Culpepper Switch, handling all electronic transfers of Federal funds
2	Electronic Switching System (ESS), managing all telephony.
3	Internet, taking-out MAYEAST discounts U.S. Government and endangers Wall Street intranets.
4	Time Distribution System, upon which all networked computers depend.
5	Global Positioning System (GPS).
6	World Wide Military Command and Control System (WWMCCS).
7	Main satellite downlinks (Suitland, Bolling).
8	Federal Reserve Computing System.
9	Submarine Communications Centres (like Annapolis Golf Course).
10	TV-networks.

Table 2: 'Top ten' of U.S. C2-vulnerabilities

It is not surprising that several countries are studying these potential risks. Is there, or is there not a contradiction in having both a concept for C2W and Info Ops?

CONTRADICTION?

In some respect the answer is yes; both concepts finally focus on 'command and control' as something that can be attacked and has to be defended. There are however several arguments that have contributed to a new concept, that of Info Ops. The first has to do with the growing dependence of military organisations on ICT. Much of final quality of the Command and Control Complex rests on the quality and timely use of data, and information, on software and rules. There are new ways to manipulate and destroy this commodity. The present C2W concept does not envisage something like software attack. The second is the sobering conclusion that Info Ops is not restricted to times of crisis or conflict. Actions against command and control systems and the information within are taking place now. Several countries reported activities of hackers, crackers (hackers with malicious intentions) and possible state- or group-controlled activities to enter systems, to discover passwords and to get information. As stated before, there hardly is a separate fully secure military information infrastructure. The factual interconnectivity within the different information environments creates vulnerabilities that might be used at any moment. It might even be society, or the international community that is the target, as figure 4 illustrates. The state may find itself in severe danger without its Armed Forces being attacked. It is not surprising that C2W as a warfare concept does not give credit to these findings. The third has to do with another observation. The old clarity between 'friend' and 'foe' has gone. The complex political realities bring opponents, hidden supporters, and allies in different forms and neutrals on a gliding scale. These realities fuel the use of psychological warfare and propaganda even outside a real armed conflict. As indicated before, the international and even global information environments are there. This forces nations to reconsider their positions towards the media and the use and misuse of information.

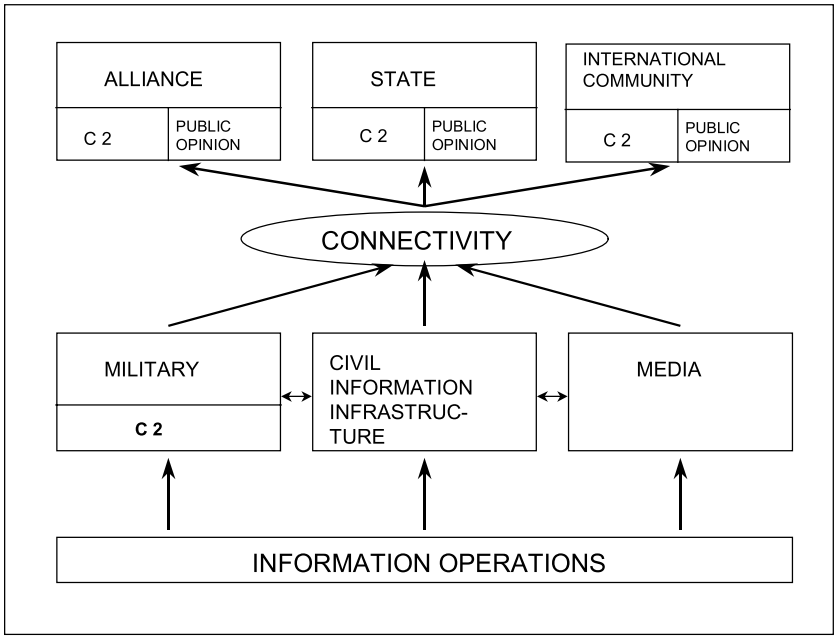

Figure 4: The scope of Information Operations

A further argument has to do with co-ordination and synchronisation. The C2W concept requires the 'integrated use of five principal military actions': physical, destruction, EW, deception, PSYOPS and OPSEC. It also stipulates the importance of co-ordination of PSYOPS with public information, civil affairs and CIMIC-activities. There are severe reasons to rethink how these separate actions and co-ordination should be synchronised. On the one hand, there must be an orchestrated approach to 'threat', friendly or third party action, and different audiences. On the other hand, one must safeguard the integrity of the different elements. In the world we live in, this orchestration demands a clear focus, a new concept and new guidelines. Bosnia Herzegovina and the conflict in Chechnya might demonstrate some lessons to be learned.

THE PEACE ENFORCEMENT ENVIRONMENT

The war in the former Yugoslavia gives a good example of the complexity of peace operations. The goal is to produce conditions that are conductive to peace and not to the destruction of an enemy. The enemy is the conflict itself. It has to do with the predominance of political and diplomatic considerations, with legitimacy and restraint and thus constraints on the Force. Transparency is necessary as a confidence and security building measure. Public scrutiny is a fact of life. The first Information Operations Compaign for U.S. forces in Bosnia-Herzegovina to follow the new Information Operations-doctrine of the U.S. Army began in October 1996 in the Multi-National Division-North (Task Force Eagle). The Land Information Warfare Activity (LIWA) at Fort Belvoir, VA, formed the backbone of the Info Ops-cell in the division. An 'Information Operations Working Group' included representatives of G2, G3, G5, Public Affairs, the Political Advisor, Psyops, etc. This group planned the overall Info Ops-effort, developed Info Ops-concepts, established Info Ops-priorities and determined the availability of Info Ops-resources. Given, for example, knowledge on an upcoming demonstration which might lead to a clash, LIWA would develop themes. The group would develop plans how to send messages to leaders and politicians ('you will be held accountable for your actions') and the population ('unruly demonstrations will harm the peace process'). Through radio and TV broadcasts, press conferences and pamphlets these messages would be spread. Own soldiers would be used to interact with locals, commanders might meet with local leaders. This combined and synchronised action should thus prevent a negative development. In this an own radio station, 'Radio MIR', could be used. Another instrument was the EC-130E, the 'Commando Solo'. This aircraft is able to jam or to broadcast at most TV, or AM and FM frequencies. The Commando Solo also relayed programs from 'MIR'. Helicopters and aircraft were used for aerial leaflet operations. Other instruments were a newspaper, 'The Herald for Peace', a monthly, 'The Herald of Progress' and press conferences to counter misinformation and propaganda. In some cases physical destruction was at hand. To counter propaganda, SFOR seized four Serbian Radio Television transmission towers and several transmitters used by pro-Karadzic elements.

As relevant as these communications with the outside world are, own soldiers and families are just as important. There were two internal publications, 'The Talon' and 'Tuzla Talk'. Through Internet, the 'Talon on-line' was a necessary information pipeline to families of deployed soldiers and to others. Deception was - 'off-limits', which illustrates the difference between a 'normal' operational situation, where friend, foe and neutral are easily to be indicated. This environment also brings new problems concerning information and

intelligence. There are many parties involved, thus all are of relevance. All parties may use radio, television and other media to spread information, which may true, partly true or false. Then there are the international media focusing in on the situation at hand. All those sources need to be monitored in order to get situation awareness. Then there is the 'normal' flow of information and intelligence. Through sub-units, the Joint Surveillance Target Attack Radar System (JSTARS), unmanned aerial vehicles, signal intelligence, gun-camera video on AH-64, human intelligence, etc. All this has to be collected, analysed and used, either in reports or databases or for direct action. For example there was 'Night Owl', a daily news digest of report summaries from broadcasts. It was distributed in paper copies locally and in digitised copies via the Internet to military, non-governmental organisations (NGO's) and other users. Finally there was the complexity of operations security (OPSEC). Again the absence of a clear enemy created security problems. Any civilian at the work force might be active for some party. Even international co-operation created some problems. Both because of different security perceptions and procedures, and the effects of combining different automated systems and communications. Yet the lessons of Task Force Eagle bring important conceptual lessons on the organisation, use and limitations of Information Operations.[35]

SMALL WAR

The war in Chechnya (1994-1996) may give some other clues to the complexity of 'information-based conflict' in the lower end of the spectrum of conflict. Both the Russians and the Chechens used psychological operations (PsyOps), deception, perception management and electronic warfare. As Arquilla and Karasik illustrate, 'old' and 'new' methods were combined.[36] The Russians used leaflets and loudspeakers. They also interfered with Chechen radio broadcasts. The Chechen spread rumours about the possession of nuclear weapons and an upcoming fundamentalist terror campaign. They also enlisted support of NGO's, thus reaching the Russian public and bringing pressure on the government. Both used deception. On the Chechen side by dressing in Russian uniforms, or by posing as Red Cross worker. But also by provocative fake radio messages that were intended to be intercepted. They also used radio jamming to influence Russian broadcast to the Chechen public and introduced small, mobile television platforms with Sony radio and television equipment to override Russian television programming. The Chechens used foreign mass media and computer networks to give warning messages that the war would spread to Russia. The Russians again 'captured' a database, including Chechen payroll lists, which led to sweeping arrests. Both sides used acts of brutality to attack the opponent's morale. The Chechens again were clever at using 'ham' radio contact and television feeds to relay information to fighters and their own population. The Chechen leaders understood how to unite local battle and the broader strategic dimension where it comes to the clash of governments and public support. Both examples indicate that there may be a specific dimension that deserves further study: Asymmetry.

ON ASYMMETRY

In principle, Armed Forces are organised to combat equals, in terms of means and concepts. The present situation forces to consider the a-symmetric conflict. The world of high technology is facing a dilemma. There is no progress without further digitisation; each step to

further digitisation creates new vulnerabilities. War certainly is more than a clash of technologies. It is a fact that technological supremacy is no guarantee for victory. As two American generals concluded: *"(technological) supremacy could not prevent Holland's defeat in Indonesia, France's defeat in Indo-China and Algeria, America's defeat in Vietnam, the Soviet Union's defeat in Afghanistan, or Russia's earlier defeat in Chechnya. All those episodes confirm that technological superiority does not automatically guarantee victory on the battlefield, still less the negotiating table".*[37] It does not take millions of dollars and hundreds of soldiers to attack any 'system of systems'. It also clear that it is very difficult indeed to develop some new weapon to surprise an enemy. Yes, the secret of Ultra was kept for over thirty years, though thousands of people were engaged in some way or another. But 1999, 2000 and the years to come cannot be compared with the 1940-1970 time frame. Even if one could conceal some new technology or weapon, there are many reasons why surprises are of relative value. As Hughes illustrates, there are many reasons why new weapons, secret or known, do not deliver what they promise: production limitations, testing limitations, the complexity, the simplicity and therefore its direct value to an opponent, the risk of failure, exaggerated expectations and the penalties for maintaining secrecy.[38] One could add the revolution of a 'secret weapon' too early and the problem of imbedding something new in a broader concept of operations. Technology is important. It is not decisive. Real war or conflict is first and for all a clash of wills, in which cultural aspects may dominate. There may be opponents who are not hindered by our democratic and bureaucratic principles and/or our values. What the West claims to be of value, like esteem for the individual and protection of the weak - like children - may be its Achilles heel. Others might understand that we do not want to risk our soldiers, that we do not want to risk non-combatants' lives and that we even have mercy with our military opponent. 'They' may think differently. Knowing this, one does not have to defeat the military forces of NATO, the United States or any other state. One could focus on the will of one or more countries to take risks. War, as stated before, always has to do with wills, skills and kills. These lessons however might contribute to new thinking and eventually new concepts, including a 'follow-on' MC-348 'Command and Control Warfare' (C2W). More basic is however that nations and coalitions have to study the real implications of Information Operations. In theory it may bring forms of conflict in which the role of conventional warfare is marginal, if not zero. There are two main reasons; the characteristics of information operations and the possible effects.

CHARACTERISTICS AND EFFECTS OF INFO OPS

The first observation is the low cost of an attack on our information systems and communication networks. They are trivial in comparison to conventional military means. A combination of computers and bright and imaginative minds may be enough. Some millions for bribery are again 'peanuts'. In fact, we are our own enemy by enforcing interoperability, our tendency to reduce safeguards in order to enlarge speed, our drive towards standardisation and our search for economy, thus reducing redundancy. All these mechanisms in some way favour an intruder. The time factor reduces more or less to zero. Where a conventional attack demands time to organise, displace and prepare forces, a computer attack may start seconds after the necessary decision. The same applies to distance. It is possible to act thousands miles away in almost real time. The defender thus has very little or no time to respond. Even worse, it will be very complicated to discover who and where the 'attacker' is. This makes counter actions and retaliation problematic, and a legal nightmare.

This retaliation is also hindered by the fact that information operations are more or less bloodless. The collapse of a financial system, the standstill of energy supply or the break down of computers in the military supply system may have devastating effects, they do not show - at least initially - the wounded and dead which result from conventional armed conflict. A combination of such an attack and information manipulation could have serious other effects. This information manipulation might be focused at creating different perceptions between government and population; might create distrust between governments and might endanger coalitions. In the end, a government might get paralysed, as it does not know who is friend or foe and what reactions might bring. Thus there are also opportunities. We could use the same instruments. A final characteristic is that information operations question our basic concepts of separation between military and civil institutions, and our ideas on the distribution of powers. In terms of the underlying networks those divisions are irrelevant, as are state boarders. So what can be some modest conclusions?

CONCLUSIONS

Information Operations can only be understood within the complexity of a broad range of changes. They not only influence the military, but also broader society and the international community. One of the effects of ICT is the creation of something one might call 'Cyberspace', one of six dimensions in which we may wage war. This Cyberspace has three inseparable layers: the Armed Forces; the nation and the international arena. At all levels command and control can be attacked and consequently need to be defended. At all levels it is finally man who makes decisions. This makes the concept of 'influencing' an option and a danger. Modern states are facing a dilemma. On the one hand, there is no escape from further digitisation. On the other hand, these developments create new and serious vulnerabilities. This certainly applies to modern military forces. Recent observations concerning information operations in Bosnia Herzegovina and Chechnya illustrate many of the problems that result from a-symmetric operations. Present C2W-concepts are not in line with recent developments. Whether the creation of a 'system of systems' is the answer, remains questionable. Given the characteristics and possible effects of information operations, especially if focused at societal or international connectivity, modern states face new threats. Cyber-terrorism and Information Operations are a real concern. There are no easy solutions. A first step however would be the understanding that new risks do exist. A next step might be a critical assessment of vulnerabilities within our digital world. International co-operation could be of value, as some countries have developed first conceptual thinking. Technology brings blessings as well as burdens. This is why technology will never be more than part of an answer. Since the Gulf War the Western countries came to understand that so-called 'wars' could be won without real losses. Neither the Gulf War, nor 'Kosovo' had much to do with a real armed conflict. In both operations 'the West' simply dominated. There may be circumstances however that technology is not the substitute for blood. Then we will understand that in real conflict there is no problem solving by the logical applications of scientific principles. Information Operations question many 'old truths'. We may face conflict in a new dimension. We even may face a new kind of warfare. We had better study the implications. The challenge is here and now. Frustration comes with the complexity of the challenge.

REFERENCES

Allied Tactical Publication 35(B), *Land Forces Tactical Doctrine*.

Arquilla, John and Theodore Karasik. *Chechnya: A Glimpse of Future Conflict?* Studies in Conflict & Terrorism, 22: 207-229.

Boyd, Morris J. and Michael Woodgerd. *Force XXI Operations*. Military Review, November 1994, pp. 17-28.

Bowdish, Randall, G. *The Revolution in Military Affairs*. Military Review, November-December 1995, pp. 26-33.

Breakwell, Glynis and Keith Spacie *Pressures Facing Commanders*. Strategic & Combat Studies Institute, Camberley, no. 29.

Creveld, Martin van, *Technology and War: from 2000 B.C. to the Present*. New York, 1989.

Dixon, Norman F. *On the Psychology of Military Incompetence*. London, 1991.

Dupuy, Trevor, N. *International Military and Defence Encyclopaedia*, Washington. Vol. 6.

Dying for Information? An Investigation into the Effects of Information Overload in the UK and Worldwide. Renters Business Information, London, 1996.

Field Manual (FM) 100-6, *Information Operations*, Washington D.C., August, 1996. [On-line] http://www.jya.com/fm100/

Foster, Peter. *Aber wahr muss es sein. Information als Waffe*. Huber, Stuttgart, 1998.

Grau, Lester W. and Timothy L. Thomas. A Russian View of Future War: Theory and Direction, *The Journal of Slavic Military Studies*, Vol. 9, No 3 (September 1996), pp. 501-518.

Harcknett, Richard J. Information Warfare and Deterrence. *Parameters*, Autumn 1996, pp. 93-107.

Holcomb, Robert C. *Operational Testing of Battlefield Digitisation Systems*. DSEi-Conference Proceedings (1999), vol 1, p. 101.

Hughes, Wayne P. *Fleet Tactics. Theory and practice*. U.S. Naval Institute, Annapolis, MA. 1986.

Idenburg, Ph. A. *Informatie-overlast*, Katholieke Hogeschool te Tilburg, The Netherlands, June 1985.

Kam, Ephraim. *Surprise Attack. The Victim's Perspective*. London, 1988.

Lewin, Ronald. *Ultra goes to War. The Secret Story*. Hutchinson & Co. London, 1978.

Marshall, Thomas J., Phillip Kaiser and Jon Kessmeire. *Problems and solutions in future coalition operations*. Strategic Studies Institute. Carlisle, PA, 1997.

Matthews, Lloyd J. *Challenging the United States Symmetrically and Asymmetrically: Can America be defeated?* U.S. Army War College, Strategic Studies Institute, Carlisle Barracks, Pennsylvania, 1998.

Military Committee (MC) Document 348, *NATO Command and Control Warfare Policy*. Brussels, June 1995.

Molander, Roger C., Andrew S. Riddle and Peter A. Wilson. Strategic Information Warfare: A New Face of War. *Parameters*, Autumn 1996, pp. 81-92.

Perricelli, Robert F. *The U.S. Army of 2025 C4I. An Integrated Approach*. DSEi-Conference Proceedings (1999). Vol. 2 pp. 34-39.

Pierantoni, Ferrante and Margherita. *Combattere con le Informaziono*. Il Centro Militare di Studi Strategici (CeMiSS). Rome, 1998.

Riper, Paul K. van and Robert H. Scales Jr. Preparing for War in the 21st Century. *Parameters*. Autumn 1997, pp. 4-5.

Shanahan, Stephen W. Information Operations in Bosnia. *Military Review*, November/December 1997, pp. 53-62.

Toffler, Alvin and Heidi. *War and Anti-War: survival at the Dawn of 21st Century*. New York, 1993.

Task Force Eagle. Information Operations. *Centre for Army Lessons Learned (CALL). Newsletter* No. 99-2, January 1999.

USAF, Air Force Doctrine Document, AFDD 2-5, *Information Operations*, 5 August 1998. [On-line] http://132.60.140.10/warfarestudies/iwac/afdocs\afdd2-5.pdf

Welsh, A.K. Digital Forces - Is the UK ready to support them? *The British Army Review*. Number 112, pp. 28-34.

NOTES

1 First thinking along this line was introduced by the author in '*Information Operations. Challenge or frustration?*' as published in DSEi Conference Proceedings (1999), Vol. 2, pp. 3-10

2 Dupuy, Volume 6, p. 2702

[3] Bowdish, p. 26 and endnotes 4-6

[4] Lewin, pp. 129-133

[5] Welsh, p 29

[6] *Tap through the Web*. De Telegraaf, 26 May 1998, p. T23

[7] For more details: Morris J., Boyd and Michael Woodgerd.

[8] Perricelli, Robert F. pp 34-39

[9] Idenburg, p. 5

[10] *Dying for information*, Executive Summary

[11] Dixon, p. 28

[12] Kam, p. 85-114

[13] Dixon, p. 31

[14] Breakwell and Spacie

[15] Hughes, p. 149

[16] Marshall, Kaiser and Kessmeire, pp. 51-52

[17] Lawson introduced the basics in 1977. Hughes introduced the combination of two cycles: the friendly and that of the enemy (Hughes, p. 187). The author introduced the distribution of force, co-ordination and synchronisation as essential elements.

[18] Crefeld van, pp. 235-249

[19] Hughes, p. 191 referring to Welch as quoted in Hwang et al pp. 4-6.

[20] Dixon, p. 28

[21] ATP 35 (B), chapter 2. See also MC-348

[22] p. 2-35

[23] p 2-36

[24] Alger p. 54

[25] FM 100-6, 1-6

[26] Bunker, p. 6 endnotes 9 and 10

[27] AFDD 2-5

[28] Bunker, p. 13, endnote 31

[29] Holcomb, p. 101-104

[30] Forster, pp. 19-22

[31] Grau and Thomas, p. 508

[32] Harcknett, pp. 95-96

[33] Molander, Riddle and Wilson, p. 84 and endnote 1

[34] Peter Black created a first 'top ten' in his article 'Soft Kill: Fighting Infrastructure Wars in the 2nd Century', *WIRED Magazine*, July/August 1993. I used this list, the article by Robert D. Steele *Take down, Targets Tools and Technocracy* in Matthews, pp 117-126, and own ideas for this construct.

[35] Task Force Eagle.

[36] Arquilla, John and Theodore Karasik, pp. 217-219

[37] Van Riper, Paul K. And Robert H. Scales Junior, pp. 4-5

[38] Hughes, jr., p. 203