Command and control and the role of information

On information as a means, target and weapon

J.M.J. Bosch

1. Introduction

On receiving orders or instructions to act, commanders have always had to deal with the problem of obtaining information and intelligence, positioning their forces, sustaining, protecting and steering them and using available fire power, while being subjected to the influence of enemy, weather and terrain, and the time factor. Julius Caesar, William III and Eisenhower had in common that they crossed what we now call 'The English Channel' in order to invade another country. Caesar landed in Britain in 55 BC, using 80 ships, 18 transports and 'slings, arrows and artillery'. William III sailed from Holland to England in 1688. He used some 49 men-of-war, with an average of 45 guns each, and some 300 smaller ships including 60 fishing boats that transported some 11,200 infantry and 4,050 cavalry (Kuijl, 1988: 79-80). Eisenhower invaded France in 1944 to open a second front in Europe. His armada was of other dimensions: 5,333 ships, ranging from battleships to transports and landing craft, were used to put some 175,000 men and thousands of vehicles ashore as elements of a first wave. Bombardments from the air and sea and airborne divisions supported this operation (Ambrose, 1944: 162,172) These three invaders faced more or less the same basic information uncertainties and intelligence needs: What about the enemy's intentions and capabilities, the own forces, the wind direction, daylight and tide? What beach to land on? What about Command and Control and information? Yet their organizations, their opponents as well as options and solutions were products of their time and thus the result of many changes. In 1944 the two-dimensional world of Caesar and William III had disappeared. Eisenhower had to deal with more dimensions: war in the air, electronic and psychological warfare. Present-day commanders face even more dimensions.
This article focuses on Command and Control and the role of information from a military perspective. I will first address the meaning and content of command and control. Next I will reflect upon developments over time in order to discover how change and continuity influenced both command and control and the search for information. I will then discuss the meaning of cyberspace in relation to my topic, Analyzing the role of information as a means, target and weapon. I will round off with some final observations.

2. On command and control

What is command and what is control? There have been many discussions indeed on the real meaning of command and control. What is command, compared to leadership, management, authority, responsibility, duty, and accountability? In Dutch Army Doctrine the command and control function covers the process of leading a military Organization towards achieving its objective. Command refers to the power and the authority to direct troops, take decisions about deployment and control the execution of an operation. Exercising command is a process of making decisions and impressing will. Command is a power - given or taken - leading to the authority, the responsibility and duty to act, or consciously to decide not to do so, in order to achieve – circumstances permitting - what has to be achieved. It is the art and skill of motivating all ranks and directing them into action. Taking charge and taking decisions are thus the primary responsibilities of command. In addition, the commander is responsible for

the controlling aspect of command. Control is the process used to organize, direct and co-ordinate the troops assigned to the commander as well as any support troops (Army Military Doctrine, 1996: 115) In other words, command encompasses, as Figure 1 indicates, three elements: leadership, decision making and control. As a leader, a commander projects his personality, his character, his professionalism and experiences on his subordinates in order to guide, motivate, and stimulate. As a decision maker, a commander takes decisions. He may do this in splendid isolation, in co-operation with his staff and/or subordinate commanders. He communicates these decisions and looks after the necessary co-ordination and synchronisation. As a 'controller', a commander oversees the execution and decides where and when adjustments to previous orders are called for. Finally – again according to Dutch Army Doctrine – command means that the commander can be held accountable for all actions of a unit. Authority and accountability are two sides of the same coin (*Army Military Doctrine*, 1996: 98-99) But this is not the only perspective.

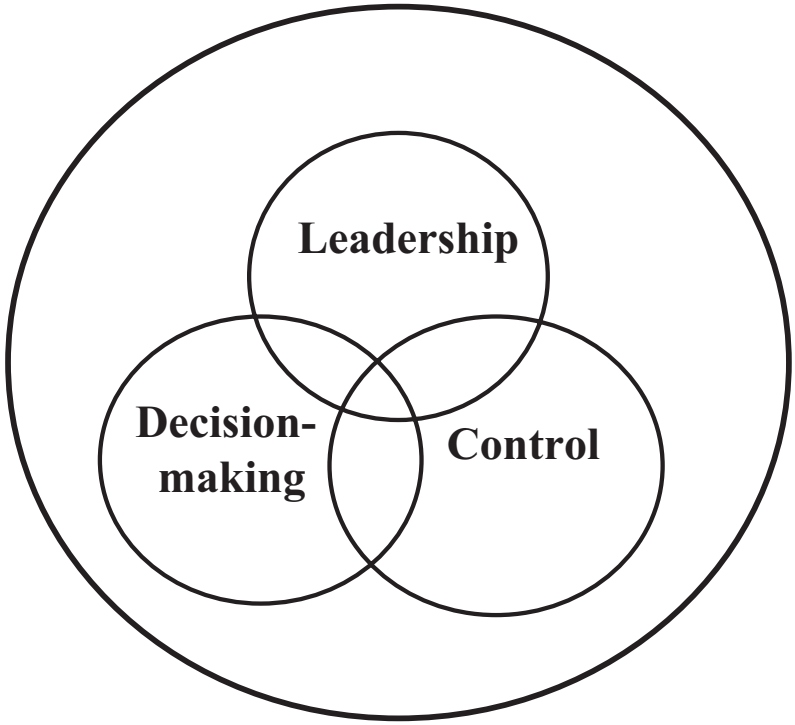


Figure 1: The elements of command

3. Other perspectives

From another perspective Command and Control encompasses three aspects: command, leadership and management. Nowadays it is hard to understand how absolute authority has sometimes been. In history emperors, kings, queens, popes, shahs and sultans combined political and military power. Both punishment and reward were in their hands. Only a dictator could nowadays project the same absolute power.

Leadership is first and foremost the direction of subordinates; it is what the Germans call *Menschenführung*. This again does not tell much about 'how' this leadership is projected. Sometimes leaders used the stick, others bargained, yet others rewarded or led by example. But leadership is certainly more than that: it is also expressed in the way commanders deal with broader human dimension in which superiors, peers and many others play a role. What

history shows is that some accepted any order, whereas others, for some reason or other, refused. Some commanders left colleagues in distress and others came to support them. There were those who neglected the broader human dimension, where others remained humane in spite of the conflict.
Management has to do with Organizing distributing and directing the available means and assets, such as time, space, information, infrastructure, personnel and equipment. As the Germans say, it is about *Mittelführung*. It is more or less the 'hard side' where calculations can be made, as it is all about quantity, numbers, distance and speed. Although most people may agree with these observations, there is still no common definition of Command and Control.
McCann and Pigeau use the NATO-definitions (Figure 2) to illustrate the problem of definition (McCann & Pigeau, 2000: 165) Analyzing the definitions, several observations can be made. Half the definition of 'command' is dedicated to the notion of 'control'; similarly, a large part of 'control' is dedicated to the notion of 'command'. But the question whether co-ordination is an element of control remains unsolved. The definition of 'Command and Control' does little more than restate the above. It is more about how Command and Control should be attained, than what it actually is. To complicate things even more: to command is in itself an act of control (McCann & Pigeau, 2000: 205). And what about its purpose? According to McCann and Pigeau 'command' is the authoritative and responsible expression of creative human will for the attainment of a mission.

Command: The authority vested in an individual of the armed forces for the direction, co-ordination, and control of military forces.
Control: That authority exercised by a commander over part of the activities of subordinate Organization […] which encompasses the responsibility for implementing orders or directives.
Command and Control: The exercise of authority and direction by a designated commander over assigned forces in the accomplishment of the force's mission. The functions of Command and Control are performed through an arrangement of personnel, equipment, communications, facilities and procedures which are employed by a commander in planning, directing, co-ordinating and controlling forces in the accomplishment of his mission.

Figure 2: NATO-definitions

'Control' is the application of structure and process for the purpose of limiting the mission's problem space. Based on these concepts McCann and Pigeau define Command and Control as 'the establishment of common intent to achieve co-ordinated action'. In other words: the essence of Command and Control is to realize common intent.
Van Creveld has another opinion. The history of command in war consists essentially of an endless quest for certainty about the enemy, his state, means, and intentions; certainty about one's own forces, and the many other factors that are relevant: weather, terrain, the threat and use of chemical and biological agents, etc. According to his observations, certainty can best be understood as the product of two factors: the amount of reliable and timely information available for decision making and the nature of the tasks to be performed. The history of command is one long demonstration of a race between the demand for information and the ability of command systems to meet this demand (Van Creveld, 1985: 264-268). There are, however, different opinions.
This small 'tour d'horizon' demonstrates that Command and Control is a complicated phenomenon. What is clear is that the definitions lack common ground. This is certainly the case in discussions on the essence of Command and Control. Is it simply 'achieving the

objective', or is it realizing common intent; is it a quest for certainty, the management of time, achieving the anticipated effect or even all of these and more? Command and Control can, however, only be understood within the framework of change and continuity. When looked at from this broader perspective, we may discover how change and continuity relate to command and control, information, and how commanders have responded through time.

3.1 On change

Change is a continuous companion of the military. Even if we study a rather limited time frame, say some 50 years, changes will be evident. If compared with a present-day F-16, the first planes in WWI have little more in common than the qualification that both are aircraft and that both use the air to project power. The same can be said of the tank. The first tanks were used in Cambrai in 1916; the most modern ones, the German Leopard 2A5 and the US M1A1/2 Abrams again only share the qualification of 'tank' and the use of ground. Speed, reach, lethality, resilience and other parameters are, as with the aircraft mentioned above, incomparable. When we study weapons we see the constant introduction of new ones or the search for increasing their potential: the bow, the crossbow, the (naval) gun, artillery of different kinds, the tank, the aircraft, the submarine, etc. War was rather two-dimensional until the introduction of the aircraft in WWI led to a third dimension. In the same war the electronic dimension brought a fourth, a virtual one and the submarine a fifth. Another dimension – the psychological one is almost as old as warfare itself. WWII acted as a catalyst for many developments: mechanised warfare, combined operations, war in the air, and war under water. It gave birth to radar, new communication systems, missiles, the time fuse, the jet engine, and the rocket. Modern armies had to learn, often the hard way, how to cope with those developments and to fight in all dimensions. Of course, the academic community studied the 'change'.

There has always been, is, and probably will be a complex relationship between social changes, military demands and technological inventions. Many authors have described the complex relation between technology, military thinking and military action. They have all tried to bring some order in the seemingly unordered realities through time. Dupuy used the speed and progress of technological changes as a starting point (Dupuy, 1993: 2702). Schlipchenko, a Russian general, focused on the weapons at hand, observing five generations and a glimpse of a sixth one (Bowdish, 1995: 26, endnotes 4, 5 and 6). Krepinevich identified ten military revolutions since the fourteenth century (Krepinevich, 1994: 3-36). In general they were all manifestations of four trends in relation to technology. The first deals with getting beyond the physical and psychological limitations of the human body and mind; the second with enlarging the speed, distance, accuracy and lethality of weapons and the third with protection and the fourth with preserving Command and Control. Those developments did not stop after WWII; they are still going on. The contribution of technology to warfare did not come without a price. It always resulted in rethinking tactics and doctrine, in training, in additional personnel, in bigger logistical problems. Armed forces grew into complex machines, increasing both the problems for commanders and the need for better command and control. War has little to do with chess. The opponents there have to deal with one board of 64 fields. The rules dictate and the number of moves only seems to be endless. Warfare consists of moves in one, more or all dimensions. Each action may result in effects in different dimensions. The moves in war are less bound by rules. Sometimes laws of war and opinions dictate, sometimes technical limits matter. If we focus on information and war, three publications deserve attention: Martin van Creveld's *Technology and War* (1989), *The Strategic Technologies for the Army Report (STAR)* (1992), and *War and Anti-War: survival at the Dawn of the 21st Century* (1994) by the Tofflers.

Martin van Creveld distinguishes four time periods while comparing military thinking and action: the 'Age of Tools', the 'Age of Machines', the 'Age of Systems', and the 'Age of Automation'. The first period, lasting until 1500 war was all about muscle power. The second (1500-1914) saw the emergence of armies and the state-in-arms. The third – somewhere between 1930 and 1945 – is characterized by integration; first by rail and telegraph, later by a combination of mechanisation, air power and communications. In his view, the world after 1945 is about 'automation'. The military Organization cannot be controlled and commanded without it (Van Creveld, 1989: 235-249).

In 1988 hundreds of American scientists co-operated in writing the *Strategic Technologies for the Army Report*. They presented their findings in 1992. The first topic they addressed was 'Winning the information War'. The message was that information superiority is a dominant factor for success. Two years later the Tofflers published their book *War and Anti-War*. According to them we now live in the so-called 'Third Wave', the 'Information Age'. The Tofflers used the Gulf War to illustrate their case. To them, and many others, this war indicated the arrival of a new type of war, in which knowledge plays the central role.

The Gulf War

In 1991 the world witnessed the Gulf War. The coalition got some months to deploy equipment and personnel, command and control systems and to use 'war games' to study what to do. As soon as the coalition was ready, it started an air campaign, intended to blind and demoralize the opponent. An offensive on the ground, lasting one hundred hours, finalised a six-week action. It was a 'joint' and 'combined' operation and it was the American dream war: intense, short and with light losses. It demonstrated the importance of satellites for navigation, weather forecasts and communication. It showed what precision weapons, stealth aircraft, cruise missiles, command systems and computer systems could contribute. To some, this was indeed the first information war, and as such it clearly was a child of its time: the 'Information Age'. To many people, especially in the USA the 'Information Age' is a fact of life, a reality. And indeed, there is a growing understanding that there is something like a 'cyberspace' or 'digital world'.The Kosovo-crisis in 1999 seems to support this idea. For a period of 78 days NATO conducted a multi-national air campaign. A total of twenty-two airbases in seven countries were used. NATO employed over 1,100 aircraft, which dropped some 4 million pounds of ordnance. At the completion of the campaign there had been - the sources differ - either one or no US casualties.

There are evolutionary changes between the crossbow and the cruise missile. The most fundamental change, however, seems to be the time factor, the compression of time. If and when modern systems engage in battle there is little time indeed to think, decide, command and act. Labbé (2000) discussed time, tempo and command (McCann and Pigeau, 2000:114-115). Referring to Boyd's Decision Cycle (Observe-Orient-Decide and Act) he observed how the time factor influenced command (Figure 3).

When	*Observe*	*Orient*	*Decide*	*Act*
American Revolution	Telescope	Weeks	Months	A season
US Civil War	Telegraph	Days	Weeks	A month
Word War II	Radio/wire	Hours	Days	Weeks
Gulf War	Near real-time	Minutes	Hours	A day
Tomorrow	Real-time	Continuous	Immediate	An hour or less

Figure 3: Time and command

I am rather critical of the use of the so-called 'OODA-Loop' to illustrate the problems of command and control. This is the loop *individual* US pilots were trained to 'use' in the Korean War. In 'real' command and control there are tens, hundreds and, sometimes even, thousands of loops at different organizational levels. Two other considerations are very basic. The first has to do with co-ordination and synchronisation. The co-ordination within one single human being - for example, a pilot – has to be done and can be realized in a very short time indeed. The co-ordination of different loops and the co-ordination and synchronisation of actions decided upon at different Organizational levels is of another dimension. The latter concerns the essence of command and control. The OODA-Loop was introduced to solve a problem: command and control has another scope. In spite of the problems at hand, the central focus should remain on the order or directive at hand. I also question the generalisations he presents concerning the time factor in the Gulf War, especially as he does not indicate which organizational level is used to illustrate his observations. I do, however, support his thesis that time came to be an increasingly rare commodity.
Labbé (2000) indicates that some armies continue to support their commanders with decision making processes that presume time to be a controllable commodity. This is, however, questionable as a commander is expected to make decisions faster than an opponent. Just as important is the observation that time is the essence of tempo – the rhythm or sequence of activities in operations, relative to that of the opponent. Tempo, then, seems to be both a state of mind and a function. It is a function of (a) the speed of decision, (b) the speed of execution and the speed of transition from one activity to the other. But, besides change there is continuity.

3.2 On Continuity

As stated before, change in itself is a constant companion of the soldier to which he or she continuously has to adapt. Apart from that, the history of warfare only presents two other constants: friction and the human factor.
It was Von Clausewitz (1780-1831) who introduced this concept in *On War*. He compares warfare to the working of a complex machine with enormous friction, the reasons for which are manifold. First, there is danger resulting in fear and its influence on decisions (Von Clausewitz, 1933: 56, 796). Then, there is the physical burden of combat, which, together with fear, forms part of the deepest sources of friction (1933: 57).The lack of reliable information is a third source, as information on the enemy often proves to be a lie, an exaggeration or a mistake (1933: 59, 718). But there is also uncertainty about one's own troops, as a result of which, one does not dare to act (1933: 718). Three further sources he mentions are logistical problems, throwing sand in the machinery, lack of time (1933: 720, 795), and finally coincidence, blind coincidence and thus fortune (1933: 16). The military machine is composed of individuals, who each introduce friction. This 'terrible friction' touches everywhere on chance, thus resulting in effects no one can 'calculate' or predict. Warfare thus more or less equals walking in water (Von Clausewitz, 1933: 60-61).
If some order is brought in his observations concerning command and control, and the role of information, we can identify three main 'sources' of friction: the individual, whether he be the commander or not, influenced by danger, exhaustion and lack of reliable information, the complexity of the military Organization, and, finally, blind coincidence and fortune, or - of course - bad luck.
All three deserve some reflection. Blind coincidence, fortune and bad luck belong to all times, however elusive. Fortune to one often means bad luck to another and vice versa. We have to accept that blind coincidence, fortune and bad luck do exist. They may be likened somewhat – as Kam stipulates – to natural disasters. We know that they happen, but we do not know when and where (Kam, 1988: 232). It is the same thing that tempts individuals to a casino: fortune

may be on their side. In reality no one dictates or controls events. They simply happen. But what about complexity, multi-nationality, the media and the human factor?

3.3 Complexity

Over time, military organizations have grown into much more complex machines than Von Clausewitz could predict. On the one hand, there was the sheer size of forces, on the other, the effect of technology leading, time and again, to further specialisation. During the Franco-Prussian War in 1870-71 the Prussian General Staff counted three colonels, eleven other officers, ten draughtsmen, seven clerks, and fifty-nine other ranks; not an over-large organization for the control of an army counting in total some 850,000 men (Howard, 1991: 62) A modern Dutch Mechanised Brigade, counting some 3,000 soldiers has a staff almost the same size. But there is more. Von Clausewitz knew about the 'old' battlefield. The only thing coming from the air was cannon balls. Modern warfare is waged in many dimensions: on the ground, at sea, from the air, under water and in space. There are the electronic and psychological dimensions. Adding to this complexity in terms of organization and dimensions of warfare are phenomena such as multi-nationality and the influence of the media.

3.4 Multi-nationality

Strangely enough, Von Clausewitz does not mention multi-nationality as a source of friction, although the Roman army already had foreign units in its organization. Von Clausewitz certainly could have reflected on the experiences with mercenaries. As history demonstrates, multi-nationality may and sometimes will result in friction. Different histories, different cultures, different sets of values, different approaches to warfare as formulated in doctrines, organizations and procedures, may lead to misunderstanding and hostility. This was the case in Ottoman warfare 1500-1700, as Murphy illustrates. Both the natural dispositions of the troops (e.g. Tatar, Timariot or mercenary) and factional infighting and leadership contests within the regular army, must be considered primary factors influencing the performance of the Ottoman armies. Such friction, though it was not always very overt or even discernible, often had very serious consequences (Murphey, 1998: 141). But the same happened during the Gulf War, as the memoirs of Colin Powell and Norman Schwarzkopf amply demonstrate. There is another factor Von Clausewitz does not mention, and that is the role of public opinion and the media. He probably had not witnessed the influence of media on public opinion, but less than twenty years after his death, this influence became very real indeed.

3.5 The media

The influence of the media goes back to at least the Crimean War (1854-1856), when British War correspondents used the telegraph to inform the public. The critical reports on the living conditions, the lack of adequate medical services and the huge losses led to public outrage. The Boer War (1899-1902) presented another example of the influence of media. Reporters, again using the telegraph, reported in neutral countries about 'David' (the Boers) fighting 'Goliath' (the British) for a good cause. This created heavy sentiments in countries such as the Netherlands. The scale of things has changed, however. Press coverage of 'Desert Storm' was unprecedented; of the 2,500 accredited journalists overall, 1,400 crowded the theatre of operations at the peak. Desert Storm correspondents totalled nearly four times the number covering Vietnam during the climax of that war. Compare this figure with twenty-seven reporters going ashore with the first wave in Normandy on D-Day (Powell, 1995: 528). Media influence is a fact of life. Words, sounds and pictures are used to inform, influence or even to manipulate decision makers and the broader public; 'friends', 'foes' and third parties. Decision makers cannot ignore what the media present. Certainly in situations where there may be more than one simple 'truth', the influence of the media is important. Decision makers

have learned the hard way that they can hardly keep up with the speed of the media. As the Yugoslav government presented a still burning F-117 - a stealth fighter which should not have been 'seen', let alone shot down -, on TV, perhaps a few people within NATO knew about it. Even fewer officials had any idea about *what* had happened, yet many wanted to know *why* this had happened. And they wanted the answer there and then. Governments and Alliances have to search for an answer to this reality. The images of the F-117 were real. More frightening is the observation that at this moment there is no guarantee indeed that an image represents reality, that words we hear are really spoken, that sounds we hear are 'real' sounds and that 'facts' are 'facts' indeed. In the digitised world any image, any sequence of images, and any sound can be manipulated. There are hardly any possibilities to 'prove' that what is presented is the truth and nothing but the truth, or indeed a lie. This sobering conclusion forces nations and alliances to reconsider their position towards the media and the use and misuse of information. And then, what about the human dimension?

3.6 The human dimension

A survey of modern conflict presents many different weapons and many ways to fight. Yet, behind every decision, action, weapon or supporting system there is 'man'. The human dimension is even broader. Conflict does not only influence the parties involved. Many more are subjected to the effects of an armed conflict. Von Clausewitz already understood how commanders were influenced by fear, exhaustion and lack of reliable information. He also understood that each individual could generate friction. In logical terms a human being is inferior to a machine. It is not surprising that finally computers beat the best chess-players. Much in armed conflict, however, is outside the realm of playing by the rules or simple calculation. In this world 'man' is both the most limiting, as well as the most precious element. Limiting because body and mind are influenced by the circumstances. Body as well as mind can easily be confronted with their limitations, though training, background, character, intelligence and experience do make a difference. Over time those burdens to commanders have grown. Coincidence, fortune and back luck kept on playing their role. Organizational complexity, multi-nationality and the influence of the media added further complications. But 'man' is also the most precious, as creativity may lead to unexpected solutions to problems at hand. There is more, however, and that is why feelings do count when a conflict is waged. In short this is the ethical dimension. Commanders have to decide when and where ethical 'borders' demand action. There is certainly no universal code of conduct in the face of violence. There is, however, some codification in the laws of War and on Armed Conflict. Long before Von Clausewitz there were already some regulations dictating what was, and what was not acceptable when fighting a war. In some cultures and times they existed; in others they were almost or completely non-existing. Real codification only came later. Modern commanders have to cope with ethical concepts and this kind of laws and other regulations. In his book *On the Psychology of Military Incompetence* Dixon held up a mirror to modern military commanders. The ideal commander may be viewed as a device for receiving, processing and transmitting information in a way that will yield maximum gain at minimum cost. It is not surprising that this figure, a human being, who has to deal with a complex set of organizational, physical, interpersonal and psychological stresses sometimes succeeds and sometimes fails. How did – at the organizational level – command respond to both change and continuity?

4. The search for solutions

It is possible to 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, in other words, filtered and Organized data, relevant and – whenever possible – timely'. It should be noted that 'that' need not be digitised information. It could be a 'real' map, notes, a verbal message or a picture. But it can also be a sound, a smell or anything else that activates our senses. From the beginning of conflict the importance of intelligence was obvious. In the Bible we can read how scouts or spies are used to reconnoitre terrain and enemy. It did not take long to understand the importance of spies and agents. As early as 1731 the French general De Feuquières devoted chapters to 'Des Espions', 'Des Guides' and to 'De La connaissance des Pays'(1731: 106, 108, 162). Gradually, national and military intelligence services and units began to emerge. Where codes were used, others tried to break them. When the radio was invented, others tried to eavesdrop or distort. The use of the electromagnetic spectrum brought electronic warfare, mainly focused on obtaining information. Weather services were introduced to get a forecast on weather conditions. As technology started to shape the battlefield, technical intelligence became important. What could weapons do? What were their limitations? How could they be countered? What defence was possible? But enemy, weather and terrain were only part of the problem; how were own troops to be controlled?

In order to do that, commanders at least needed to know their location, feelings and logistical situation. At first the horseback or hill would give oversight to the commander and messengers 'connected' commanders. Later a telescope would allow larger distances. Gradually, there was a need for more: command posts and other means of communication. Because of friction this system proved, time and again, to be unable to generate the necessary information and to communicate orders. There was a constant need for ad-hoc solutions. Napoleon used adjutants and liaison officers. Grant and Sherman did the same in the American Civil War. During WWI, Von Moltke used officers of the General Staff to oversee the situation. General Haig commanded 'by wire' and did not know the realities on the battlefield. General Joffre on the French side introduced a system of 'vertical liaison', young captains and majors sent to lower headquarters to spread instructions and to report. In WWII we see the Russians employed representatives of the General Staff, the STAVKA. The Germans used – again - the General Staff. The US Army relied on the so-called 'Signal Information and Monitoring (SIAM) units', while the British introduced the 'Phantom Service'.

There were those who tried to cope with these problems by detailed planning, yet others by overwhelming numbers and sheer force. Another approach was rethinking the command concept. The Germans introduced *Auftragstaktik* as a way to deal with uncertainty. They understood that only those on the spot would or might have insight into what was really going on, and should be given freedom to act. As Mission Command it is now part of the doctrine of many nations.

Commanders thus tried to find certainty amidst almost endless streams of false, misleading and accurate information. If accurate, often late or too late, irrelevant, unreadable, or considered unreliable (Griffin, 1991: 5-20).

4.1 The computer

WWII was, as stated before, a catalyst for many developments, and this is most certainly true for the introduction of the computer. Early efforts by Charles Babbage (1792-1871) resulted in a so-called 'difference engine' and, in 1834 an 'analytical engine'. In 1939 Atanasoff, a US mathematician and physicist built what some consider to be the 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. A well-kept secret for a long time was the existence of another Mark I, the Transmitter, Telegraph, Mark I, developed for use at Bletchley Park, home of Ultra, for actions against Enigma, the German encryption system. In 1943, the first Colossus, using 1,500 electronic valves, was introduced. Three months later there was a Colossus II, giving Hollerith's ideas a new dimension (Lewin, 1978: 129-135). Both within and outside armies all over the world the computer developed from a rare, crude and sometimes 'secret' thing into what it is today. In combination with information and communication technology (ICT) the computer changed the way in which we deal with information, paving the way for something that we now call 'cyberspace' or 'information sphere'.

4.2 Cyberspace

Modern armies cannot be managed, commanded and controlled without information and communication technology. ICT is more than computer technology, communication technology, micro- and nano-technology; it also encompasses data fusion, sensor technology and artificial intelligence. The reasons for its omnipresence are simple: the growing complexity of the organization as a result of a diversity of weapon systems with long-range precision capabilities and growing speed, the corresponding need of intelligence, information management, co-ordination and synchronisation; all this in combination with the time factor. In modern armies this development led to what I would call the 'Command and Control Complex'. Numerous information systems function like the veins of the broader command and control complex. The process translates data and information, common sense, battle experience and sixth sense into orders. It functions like the 'brains', as orders and situational reports on what happens are like oxygen and blood without which neither 'brains', nor the rest of the 'body', the organization in action, would function. A command and control system therefore is the 'central nerve system' that has to ensure that the 'body', the organization in action functions. The basic components of each individual separate command and control system are:

- sensors, processors, receivers, databases and transmitters
- infrastructure, power and transport
- data, information, software and rules
- commanders, advisers and others to support the system
- shooters, other actors and other users.

This complex embraces all: decision makers, hardware and software, infrastructure, power and energy, equipment, shooters and other users.

But it is through much of the same ICT and the resulting infrastructure that we organize government, the supply of water, energy, transport, banking, finance, etc. The same applies to the international level; ICT connects producers and markets, banking and finance, governments and other institutions and organizations. Finally, ICT connects the media and audiences, nationally and internationally. This web of military and civil, national and international infrastructures creates something that might be called 'cyberspace'.

The Internet with its 300 million users in the year 2000 is only one of the elements of this world-wide infrastructure. It is important to note that the layers are inseparable because they are in many ways interconnected and partly use the same elements of this infrastructure. So they also overlap. Finally, there is no central control of this complex environment. There are no borders other than by technological limitations. This digitised world offers new ways of communication and exchange of information, almost at the speed of light. Governments,

audiences and others are confronted with near real-time or real-time information on what is going on in the world. If we focus on the military realm there are many blessings. These advanced technological systems will increase significantly the battlefield effectiveness of:

- sensors, or 'finders', by increasing their capacity to see the battlefield, identify targets, and distinguish enemy from friendly forces;
- 'controllers', by decreasing their reaction time, improving their decision making, increasing their span of control and allowing direct communication by video-conferencing;
- shooters, by increasing their survivability, lethality and precision;
- planners, by giving new opportunities to simulate scenarios in order to find answers to strategic, operational or tactical problems;
- commanders, by giving opportunities to rehearse missions and to discover pros and cons of options for action;
- logisticians, by giving new tools to optimise support of a mission (Hosmer, 1999: 231-232).

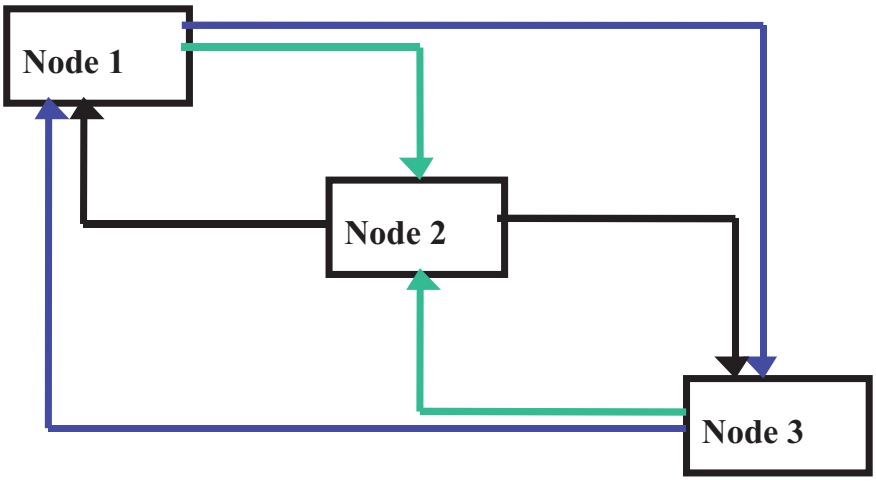
Another dimension concerns the psychological effects of advanced observation and detection systems on the motivation and morale of an opponent. He may face the following prospects: if we fly, we die; if we wire, we die; if we communicate, we die; if we radiate, we die; if we move our vehicles, we die and, if we remain with our weapons, we die (Hosmer, 1999: 233). Many blessings indeed. But from a military point of view they may also be mixed blessings.
The Gulf War did not only bring successes. It also demonstrated that friction is a universal problem. A third of all planned air sorties had to be cancelled, mainly because of the weather; Scuds could not be found; orders were misinterpreted or were never received. There was fratricide, rivalry, and multinationality created problems (Kellner, 1992: 161-163, 178-180; Watts, 1996: 67-74). The 'fog of war', 'Murphy's Law', human and system failure are, and always will be, the companion of the soldier. Who could have forecast that a laptop with the operation plan of Desert Storm could or would be stolen? It happened (Powell, 1995: 500). In addition automated systems may have some 'built-in' friction. An American report indicates that there are some 200 failures in every 10,000 software-codes. An Apache Longbow has some ten million instructions, to give some idea about the extent of this problem (Welsh, 1996: 29). The Gulf War also demonstrated that this cyberspace can be used in conflicts, creating new dimensions of war in which the electronic and psychological elements become integrated. To illustrate this observation I will discuss three topics that influence command and control and the role of information: Network Centric Warfare, Information Operations and Cyber-war, including Cyber-terrorism.

4.3 Network Centric Warfare

According to an American dream-scenario, a 'system of systems' emerges at some stage, combining all sensors, decision makers, shooters and supporting elements in order to gain information dominance, a shared battle space situation awareness and synergetic and simultaneous actions. In the year 2025 there will be something like a 'Living Internet', a jointly integrated multi-layered information-infrastructure. It is envisaged that everyone on the battlefield can interact any time and in real-time (Perricelli, 1999: 34-39). This leads to a new way of command and control.
This exciting development is sometimes indicated as 'Information Based Warfare', but Network Centric Warfare (NCW) is a better term for two reasons. First, armed conflict has always been 'based on information'. Second, the real core of this system lies in networking. NCW is defined as information superiority that generates increased combat power by networking sensors, decision makers, and shooters to achieve shared situational awareness,

increased speed of command, higher tempo of operations, greater lethality, increased survivability, and a degree of self-synchronisation. In essence, NCW translates information superiority into combat power by effectively linking knowledgeable entities in battle space (Alberts, 2000: 2).

Interestingly, proponents of this 'system of systems' use a comparison with civilian Network-Centric Enterprise to 'make their case'. According to their theory, information and IT are providing the means to create new value. The question 'Where does the value come from, and can it be quantified? is answered by use of Metcalfe's Law (Figure 4). It states that as the number of nodes in a network increases linearly, the potential 'value' or 'effectiveness' of the network increases exponentially (almost) as the square number of nodes. An upper limit information dominance in the information domain is reached as information relevance, accuracy and timeliness approach 100 percent. As this may be unrealistic, the objective in the commercial sector is to approach these upper bounds faster than a competitor in order to reach information superiority. This information superiority (see Figure 5) is a state that is achieved when a competitive advantage is derived from the ability to exploit a superior information position (Alberts, 2000: 29-34).



Network with N = 3 has
[N * (N-1)] = 6 Potential information interactions

Figure 4: Metcalfe's Law

I have several reservations, the first of which concerns the premise that the number of interactions, even if always based on relevant, accurate and timely information, automatically generates overall 'value' or 'effectiveness'. My second reservation pertains to the differences between a commercial enterprise and military forces. An enterprise is focused on a certain set of products or services. The military machine is focused on the effective use of functions in order to generate and use different kinds of power. The co-ordinated and synchronised use of different kinds of power is of another magnitude. My third reservation is based on the simple observation that a military organization must be prepared to confront an opponent. A civilian enterprise may be confronted with false or misleading information, even hackers or a virus, however, there is no need to consider the effect of enemy rockets, bombs, explosives and bullets. This is why armed forces do not fit into the so-called 'Newtonian paradigm': everything functions like a kind of machine, with well-understood laws that describe

movements, relationships and forces. Finally, information superiority in itself has little meaning. Information acquires meaning if used and through action.

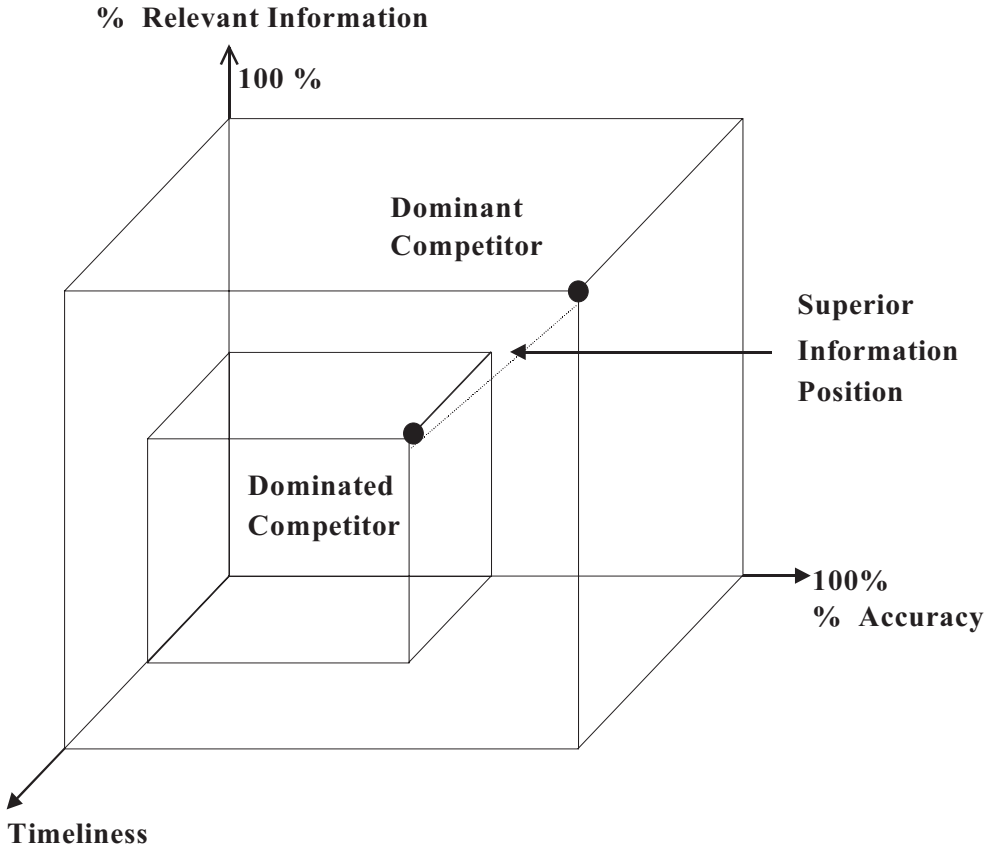


Figure 5: Superior Information Position

Information in itself does not generate the 'right solution', does not kill, sink ships, down aircraft. And there is another question: What if we know, but are impeded in using our knowledge because of deception, secrecy or other implications? But there are more questions in relation to NCW. How can we visualise 'morale' or actualise screens, given the speed of developments? How do we deal with ever less time to decide and new amounts of information? How do we select and Analyze? How do we synchronise action? And, last but not least: Can we trust the information? It goes without saying that any command and control complex, including its underlying structure and systems, is vulnerable to attack. The reasons are simple. As the system has to enable effective command and control, it logically becomes a target and because data and information preclude action, these commodities are liable to attack as well. A system is a structured combination of means, and, naturally, disrupting its cohesion can be profitable. Technology is at the heart of the system, so its weaknesses or limitations may be exploited. Finally, as humans control, support and use those systems, they can be targeted too, which brings me to 'Information Operations'.

4.4 Information Operations

Since there is no universally accepted definition of Information Operations I will use the NATO definition: 'actions taken to influence decision makers in support of political and military objectives by affecting other's information, information based processes, Command

and Control Systems and Communications and Information Systems (CIS) while exploiting and protecting one's own information and information systems'(MC-422, 1998).

There is indeed much similarity to the well-known concept of Command and Control Warfare (C2W). In this concept, physical destruction, operations security, psychological operations, military deception and electronic warfare – based on all source intelligence and communications and information systems – are used to deny information to, influence, degrade and or destroy an adversary's Command and Control capability. At the same time those instruments should protect the own system against similar action.
C2W is often an economic way of reducing an adversary's combat effectiveness because it hinders the necessary flow of information between commanders, staffs and units. In order to be effective, however, it must be well co-ordinated. What then is the difference with Information Operations? Information Operations is based on the new perception that C2W will remain important on all levels: strategic, operational and tactical. There is, however, a 'new world' where political-military consultations and decision making can and will be influenced by the media. In this world psychological operations and Public Information must be co-ordinated. Any opponent can use the media – to influence an Alliance like NATO, third parties or neutral states. Furthermore, Information Operations can take place at any moment, not specifically when there is a conflict. The 'old' clear distinction between 'friend' and 'foe' has gone. These realities fuel the use of psychological warfare and propaganda even without an open armed conflict.
Finally, there are new ways to manipulate and destroy data, information, hardware and software. The options range from manipulation, via viruses to electromagnetic pulse. Manipulation can be effected by entering false information into a system or by creating an 'information overload'. A situation, incidentally, that may occur on a technical level, as was experienced by the US Navy in the Gulf War. Here, AEGIS systems and surveillance aircraft provided so much information that command centre computers were overloaded and froze (van der Kley, 1999: 16). Information can be deleted in a literal sense but also indirectly. In a situation of overload some information will inevitably get 'lost'. On the level of the individual message there are various options for manipulation: change origin (which may influence readers' ideas about relevance and reliability); change the mailing list and/or change (part of) the content. There is also 'video morphing' in which video or still-picture information is changed. Then there are many types of viruses: the 'Trojan Horse', a code that has hidden side effects; a 'worm', a self-replicating code that uses network functionality, e.g. e-mail distribution mechanisms, to spread. A good example is the so-called 'Melissa-virus'. This type of macro virus, propagating by e-mail, was activated in March 1999. It may have affected some 100,000 computers. At least one US Airforce Base, supporting the operations in Kosovo, was 'down' for 24 hours (Luiijf & Klaver, 2000: 21). The 'logic bomb' and 'time bomb' are stealthy pieces of code that execute when a certain – externally triggered – condition, e.g. time, or the removal of a file, or the insertion of a code, occurs. There is the 'logic torpedo', a virus type that seeks out a certain system or program, and even a 'stealth virus', that can hide itself in a file, waiting to be activated. Then there is 'chipping', modifying chips in such a way that they contain a 'back door' or 'trap door', an opening in the system allowing unauthorised access, or a logic bomb. Finally, there are other weapons that would destroy information and information systems, such as High Energy Radio Frequency Weapons and Electro Magnetic Pulse (EMP) transformation bombs. The essence of all this is to disrupt command and control. The most dramatic effect might not be the slowing down of processes, but because of manipulation and other measures, the creation of distrust to *all* information.

The French offered an interestingly different definition of Information Warfare. They distinguished three types:

- war *for* information: to obtain information about the opponent's means capabilities and strategies in order to defend ourselves;
- war *against* information: the protection of own information systems and to disrupt or to destroy the opponent's;
- war *through* information: to conduct misinformation or deception operations in order to achieve 'information dominance'(Ehlers, 1999: 4).

Perhaps the US reactions are somewhat related to exercise 'Eligible Receiver', conducted by the Pentagon in the summer of 1997. A team of fictional hackers, the 'Red Team', was allowed to use only commercial-off-the-shelf' (COTS) equipment and information on the web and had to act within the US Law. According to one journalist, Air Traffic Control (ATC) systems were taken down, power grids made to fail, oil refineries made to stop pumping'. They also 'attacked' defence plans to move forces in response to a hypothetical international crisis, changed orders and interrupted the logistics flow. They also fed false news reports into the decision making process (Ehlers, 1999: 6-7).

Both Sadam Hussein and Milosevic understood very well how to manipulate the media. Sadam Hussein used the tragic bombing of public shelter no. 25 in Amiriya, used by civilians. He also demonstrated on TV that the Americans seemed unable to kill him. Milosevic also used civilian casualties to demonstrate NATO's 'perfidiousness', NATO's attack on the Chinese Embassy in Belgrad being a 'gift' to him and his followers.

Kosovo presented more examples of information operations. An indirect threat came in October 1998, when a Serbian group of hackers known as 'Black Hand' penetrated a Kosovo-Albanian web server and threatened to sabotage the 'Alliance's' Information system. NATO's' web site was down for two days. NATO also had to defend itself against macro viruses from FRY trying to corrupt its e-mail system. These attacks were possible because NATO was using the same server for the e-mail system and its web-pages. Yet it remains questionable whether those 'attacks' did have a real impact (Ehlers, 1999: 6, 11).

It is important to understand that the need for information is not only the result of growing complexity and the time factor. There are two other reasons. The first has to do with protection. Both the Gulf War and 'Kosovo' gave rise to the dangerous perception that armed conflict can be waged with little or no losses. Information is an important commodity to prevent losses. The second is that not only 'own' losses should be minimised; the same applies to non-combatants and even to 'the opponent'. A clear example was the four-lane highway leading out of Kuwait City toward the Iraqi city of Basrah. At the end of the Gulf War it had turned into what seemed a shooting gallery for allied airmen. Reporters began to refer to this road as the 'Highway of Death'. It shaped thinking about the end of military action (Powell, 1995: 520-521). At the very least there should be an awareness of the realities to prevent being 'outflanked'. But modern societies face another threat: cyber war or cyber terrorism.

4.5 Cyberwar

Again, there is a problem of definitions. It is clear to many that societal connectivity and even international connectivity can be a target. As both completely depend on ICT, this ICT, including the energy supply system which makes it work, is in fact an Achilles heel. Some label actions against society and broader connectivity as 'Net war', others see it as a subset of 'Information Operations'. I prefer 'Cyber war', as an indication that such activities might be a separate way to 'attack' a modern state or (part of) the international community. It would be much more devastating to the USA to lose Culpepper Switch, handling all electronic transfers

of Federal funds, the Electronic Switching System, managing all telephony and MAYEAST, an essential internet crossing, the loss of which would discount US government and endanger Wall Street internets, than to lose part of their military power. This is why President Clinton in 1996 introduced the President's Commission on Critical Infrastructure Protection (PCCIP). The commission presented its sobering findings in 1997. Based on them, Clinton signed, in May 1998, the Presidential Decision Directives 62 and 63, on Critical Information Protection, leading to the creation of new offices and agencies. There is now a Critical Infrastructure Assurance Office (CIAO), a National Infrastructure Protection Centre (NIPC) within the FBI and a functionality within US defence Space Command. On January 7, 2000, he launched a two billion-dollar action plan to secure systems and structures by the year 2003 (Cordesman, 2000: 57-64).

Germany, Canada, France, UK, Switzerland, Sweden, Australia, Norway, Israel and the Netherlands are among the countries studying vulnerabilities and possible solutions.

The good thing is that any country using this kind of warfare faces direct and severe retaliation by anyone who is attacked. Another good thing is that any such modern country might lose as much as it gains, as economies and financial markets are interconnected. The bad things are that identification of the attacker is difficult, that this kind of warfare only demands limited resources and an intelligent and perhaps evil mind, and that these kind of activities might be used within a broader armed confrontation between countries or alliances, or by terrorists.

5. Final observations

Command decides on what is needed from forces, and control transforms those needs into action. Command and Control needs information to be effective. It encompasses achieving the objective, Realizing common intent, the search for certainty, the management of time and Realizing the anticipated effect. But first and foremost, Command and Control is Focused on effectiveness in spite of friction, and on preventing fatal mistakes. Friction will exist as long as humans are engaged in armed conflict, and as long as chance, fortune and bad luck exist. Friction is a fact of life. It is a fiction that technology can eliminate this reality. It is the other way round: technology brings burdens in terms of equipment, supplies, personnel, training, doctrine, and even friction.

Fred Ikle wrote a book entitled *Every War Must End* (1971). He indicated that after starting a war, a government might lose sight of ending it. In his words:

> Thus it can happen that military men, while skilfully planning their intricate operations and co-ordinating complicated manoeuvres, remain curiously blind in perceiving that it is the outcome of the war, not the outcome of the campaigns within it, that determines how well their plans serve the nation's interest. At the same time, the senior statesmen may hesitate to insist that these beautifully planned campaigns be linked to some clear ideas for ending the war… Fighting should not continue long past the point where a rational calculation would indicate that the war should be ended (Powell, 1995: 519).

These messages are as relevant today as they were during the Gulf War or Kosovo. Both change and continuity are constant companions of any commander. Future leaders and commanders should understand these realities. Command and control is partly 'science'. In the study of logistics much can be quantified and Organized in terms of 'what', 'when' and 'where'. Yet armed conflict in a broader sense is an art. Even in the narrow sense of decision making most of the elements to build decisions on can only partly be quantified. The enemy is more than numbers, equipment, location and distance. Weather and terrain are not under any

nation's control, and the complex relationship between the two is beyond calculation. 'Own troops' is more than people, systems, vehicles, logistics and present location. Finally, both the opponent and the own forces might be creative or not, rational or not, in line with the laws of war or not, in sum predictable or not.

Today's environment is much more complex than ever. Conflict has to be 'fought' in many dimensions at the same time. 'Cyber space' is only one of the many dimensions. It should not be forgotten that an evil mind might turn to the 'old' instruments of conventional, nuclear, biological, or chemical attack. Or perhaps environmental warfare, as Sadam Hussein did, when he set fire to the oil wells.

Modern armies have to adjust to some form of 'Network Centric Warfare'. They understand that this development can create risks. A study of 'Information Operations' and 'Cyber war' shows that military organizations are nothing more than part of a problem. The clear division between politics and the military realm has disappeared. Worse even: societal connectivity might be a target while the military is not. At the same time nations and alliances have come to understand that they are no longer in control of either the information-flow, or the information infrastructure.

Digitisation will enhance our capabilities to execute manoeuvre warfare and mission command. In education and training we should increase emphasis on skills to deal with high technology and understanding digitisation. Even more important, we must train and train again to take decisions based on incomplete information, and to exercise initiative, based on professional expertise and experience. There is nothing wrong in doctrinal sessions or debate. The simulation technology is available and it is there to be used to learn how to deal with friction.

Commanders need information to act upon. However, information is only one of the 'means' a commander hopes to posses. Time, space, weapons, people, ammunition, food, water and infrastructure also count. Information is an important asset. It supports his actions, but also helps him to prevent losses, collateral damage and to safeguard 'third parties'. As a consequence information was, is, and always will be a target to be defended. On the other hand information - either as the truth or a lie - might be a weapon to confront an opponent or to manipulate him or others.

In conflict there is much at stake. Consequently, there are good reasons to look for ways to know as much as possible. Knowing 'all' is a dream. Commanders should be ready to act upon the information available. So did Eisenhower when he gave his 'O.K., let's go' to launch the invasion. As Ambrose writes (1994: 190):

> When the reporters left, Eisenhower sat at his portable table and scrawled a press release on a piece of paper, to be used if necessary. 'Our landings … have failed … and I have withdrawn the troops', he began. 'My decision to attack at this time and place was based upon the best information available. The troops, the air and the Navy did all that bravery and devotion to duty could do. If any blame or fault attaches to the attempt it is mine alone'. Putting the note in his wallet, Eisenhower went to dinner.

Indeed, it is all about the 'best information available'. Commanders should search for it. But, if and when decisions have to be made, what is available should be used. In the end there is more than information that counts. A simple plan, surprise, bravery and devotion to duty mattered in history. They will matter in the future.

References

Alberts, D.S. (2000), *Network Centric Warfare: developing and leveraging information superiority*. DoD, C4ISR Cooperative Research Program CCRP-publication Series, 2nd (revised)edition, Washington DC.

Ambrose, S. (1994), *D-day, June 6 1944: The climatic battle of World War II* Simon & Schuster, New York

Army Military Doctrine / LDP (1996), Part I – Military Doctrine SdU, Den Haag/The Hague

Bowdish, R.G. (1995), The Revolution in Military Affairs in: *Military Review*, November/December: 26-33

Clausewitz, C. von (1933), *Vom Kriege*, B.Behrs (Auflage 14), Berlin.

Cordesman, A.H. (2000), *Defending America. Exploring the Conceptual Borders of Homeland defence. Critical Infrastructure Protection and Information Warfare*. CSIS, Washington

Creveld, M. van (1985), *Command in War*, Harvard University Press, Cambridge, Mass.

Creveld, M. van (1989), *Technology and War: from 2000 B.C. to the Present* Free Press, New York

Creveld, M. van (1991), *The Transformation of War*, Free Press, New York

Dixon, N.F. (1991), *On the Psychology of Military Incompetence* Future Press, London

Dupuy, T.N. (1993), *International Military and Defense Encyclopedia*. (6 Vols.) MacDonald, Washington

Ehlers, V.J. (1999), *Information Warfare and International Security* Draft General Report, NATO Science & Technology Committee, Brussels

Feuquieres, M. de (1731), *Memoires sur la guerre, ou c'on a rassemble les maximes les plus necessaires dans les operations de l'art militaire*, Pierre Gandouin Libr., Paris

Gardeta, J. (1999), Information Operations, The NATO Perspective in: KMA, Breda, *NL ARMS* (Information Operations), 3, 1999: 105-115

Griffin, G.B. (1991), *The directed telescope: A traditional element of effective command* US Army Command and General Staff College, Fort Leavenworth, KA

Hosmer, S.T. (1999), The Information Revolution and Psychological effects in: Khalilzad, Zalmay M. and J.P. White, *The Changing Role of Information of Warfare*: 217-248, RAND, Santa Monica

Howard, M. (1991), *The Franco – Prussian War. The German invasion of France, 1870-1871*, Routledge, London

Hughes, W.P. (1986), *Fleet Tactics, Theory and Praxis*, US Naval Institute, Annapolis, Md.

Ikle, F.C. (1971), *Every war must end*, Columbia University Press, New York

Kam, E. (1988), *Surprise attack. The Victim's Perspective*, Harvard UP, Cambridge

Kellner, D. (1992), *The Persian Gulf TV-War*, Westview Press, Boulder

Kleij R. van der (et al.) (1999), *Information Operations: Threats to the effective use of information in command systems*. TNO-TM 99-A049, Soesterberg

Krepinevich, A.F. (1994), Cavalry to Computer. The Pattern of Military Revolutions. in: *The National Interest*, 1994, Fall: 30-42

Kuijl, A. van der (1988), *De glorieuze Overtocht. De expeditie van Willem III naar England in 1688* [The Glorious Crossing. William III's expedition to England in 1688] De Bataafsche Leeuw, Amsterdam

Labbé, J. S. (2000), Time, Tempo and Command
in: C. McCann & R. Pigeau (eds), *The Human in Command*: 111-126
Kluwer Academic / Plenum, New York
Lewin, R. (1978), *Ultra Goes to War*. *The Secret Story*, Hutchinson, London
Luiijf, H.A.M., Klaver, M.H.A. (2000), *Bitbreuk – De kwetsbaarheid van de ICT-infra-structuur en de gevolgen voor de informatiemaatschappij* [The vulnerability of the ICT infrastructure and the consequences for the information society].
TNO-TM, Soesterberg
MC 422 (1998), NATO Information Operations (Info Ops Policy), December, Brussels
McCann, C., Ross, P. (2000), Redefining Command and Control
in: C. McCann & R. Pigeau (eds.), *The Human in Command. Exploring the modern military Experience*: 163-185, Kluwer Academic / Plenum, New York
Murphy, R. (1998), *Ottoman Warfare* 1500-1700, UCL Press, Birmingham
Perricelli, R.F. (1999), *The US Army of 2025, C4I. An Integrated Approach*
DSEi, Chersey (Surrey), DSEI-Conference Proceedings, Vol. 2: 34-39
Powell, C. (1995), *My American Journey,* Random House, New York
Watts, Barry D. (1996/1997), Friction in Future War
in: *Brassey's Mershon American Defense Annual*
Welsh, A.K. (1996), Digital Forces – Is the UK ready to support them?
in: *The British Army Review*. No. 112: 28-34