NL ARMS

Netherlands Annual Review of
Military Studies
2000
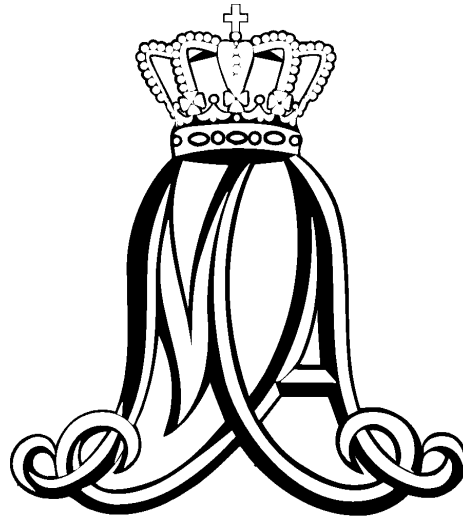
H.P.M. Jägers
H.F.H. Kirkels
M.V. Metselaar
G.C.A. Steenbakkers
(eds.)

Information in Context

The cover image of this edition of NL-ARMS is a diamond as a symbol of the concept of information in the present-day information economy. It symbolises the value of information and simultaneously its colourful splendour reveals a new facet of information with each new perspective.

NL-ARMS

1997: The Bosnian Experience
   J.L. Soeters, J.H. Rovers (eds.)

1998: The Commander's Responsibility in Difficult Circumstances
   A.L.W. Vogelaar, K.F. Muusse, J.H. Rovers (eds.)

1999: Information Operations
   J.M.J. Bosch, H.A.M. Luiijf, A.R. Mollema (eds.)

2000: Information in Context
   H.P.M. Jägers, H.F.H.M. Kirkels, M.V. Metselaar, G.C.A. Steenbakkers (eds.)

Contents

Part One

Information

Editorial preface

We live in exciting times. Change is all around us and it influences our world, our lives and our ways of thinking. For a decade now, the world's national economies have been integrating at an unprecedented rate. The increasing mobility of capital, deregulation and new communication and computer technologies have eliminated most of the barriers that used to keep these economies distinct. Some observers have labelled these developments the 'new economy'- an economy in which consumer incomes, corporate earnings and stock market valuations always rise, inflation never does and all emerging nations grow rapidly. In the old economy the information flow was tangible: cash money, cheques, invoices, waybills, accounts, analogous telephone, radio and television broadcasts, maps, photos and advertising. In the new economy information is digitalized in all its forms, it is reduced to bits in a computer and it races at the speed of light through networks. Information, in fact, has become an intangible asset for a company.

Some intangible assets, such as customer relations, reputation and brand values, can grow rather than shrink and for that reason they can provide a valuable basis for diversified expansion. Information has become the new basic resource. It becomes more valuable as more people have it and this fact implies that we will have to drastically revise economic theory. Information does not pertain to one industry or business. It does not have one end-use, nor does one end-use require a particular kind of information or depend on one particular kind of information.

In the recent past many authors have addressed the increasing importance of information in our rapidly changing society. Shapiro and Varian (1998) are perhaps the most important of them with their book *Information Rules*, in which they identify a number of striking aspects:

- Information is costly to produce (high fixed costs), but cheap to reproduce (low marginal costs). The implication of this is that information goods must be priced according to consumer value, not according to the production costs.
- With the rise of the possibilities for copying digital information and transmitting around the world, managing intellectual property becomes increasingly important. The goal should be to choose the terms and conditions that maximize the value of the intellectual property, not the terms and conditions that maximize the protection.
- Information is an experience good every time when it is consumed. The value of a good is established by the experience itself. Therefore we see free samples, promotional pricing and testimonials to help consumer learn about new goods.
- 'A wealth of information creates a poverty of attention', said the economist Herbert Simon. Nowadays the problem is not information access but information overload. The real values produced by an information provider lies in locating, filtering and communicating what is useful to the consumer. Attracting the viewers' attention has always been an attractive way to support information provision.

We find this same perspective in the discussion memorandum of the Ministry of Economic Affairs, published in October 2000, entitled 'The Economy of the 21st century'. In this document the increased role of information in society as a whole and in economic transactions in particular, is also pointed out. Castells (1998) expresses it as follows: 'In this new, informational mode of development the source of productivity lies in the technology of knowledge generation, information processing, and symbol communication'. ICT is crucial for information processing and it involves a broad domain of applications, ranging from micro-electronics, computer technology (hardware and software), telecommunication to audio-visual media. The enormous advance in the development of ICT proves to be the driving force behind the dynamics of knowledge production and distribution.

The defence organization is strongly influenced by these developments, precisely because it is an information intensive organization. This fact warrants a book which has 'information' for its central theme. In the ten articles in this issue of the *Netherlands Annual Review of Military Studies [NL ARMS]* the authors discuss the many aspects of this intriguing phenomenon. In his introductory article, **Jägers**, discusses at length the changing role and meaning of information in the information society. They not only strongly influence the functioning and designing of defence, but they also offer various new possibilities in the process.

Part two, with its emphasis on information in peacetime situations, opens with a chapter on collaboration in the armed forces (**Steenbakkers et al**.). They argue that collaboration in the armed forces increasingly adopts the form of a network organization. They discuss a variety of different types of network organizations, illustrated by examples from practice. **Mol** and **Van den Hooven** deal with financial information provision and in particular with the aspects of efficiency and effectiveness. The peacetime organization is Focused on efficiency, whereas deployment requires rigorous attention for effectiveness. The absence of an overall evaluation criterion for both has always been experienced as an obstacle for an adequate information provision for the management of the organization and in their article the authors indicate a possible solution for this problem. In recent years there has been much attention within the armed forces for result-responsibility, for reasons of efficiency and effectiveness. The pursuit of result-responsibility has not only been investigated in several reports, but there has also been research into how it works out in practice. **Heijnsdijk** and **Oonincx** describe the developments and the state of the art. Apart from offering a number of theoretical insights they present the results of a questionnaire.

In Part three the role of information in operational actions is discussed. Operational action is not any longer associated with large-scale conflicts, but with peacekeeping or peace enforcing operations. **Bollen** and **Vogelaar** discuss the role of information in the cooperation between military units and civil parties in humanitarian operations. They examine the concepts of confidence, trust and control from a theoretical perspective, after which they describe the role of information in fostering these crucial prerequisites for adequate civilian and military cooperation. Subsequently, **Soeters, Op den Buys** and **Vogelaar** take an every-day situation as their starting point for a discussion of the importance of cultural information. The deployment of British and Dutch units in Cyprus is the background for their analysis of the cultural frictions between the two contingents that occasioned an intervention from the Bureau Lessons Learned of the Royal Netherlands Army. **Metselaar** deals with information provision in crisis decision making. He states that there is a gap between theory and practice in intelligence and he proposes criteria for the evaluation of the intelligence process in order to fill it.

Deployment of forces is inextricably linked with technological developments in information processing and in Part four **Rogge** describes the relations that play a part in intelligence preparation of the battle space directed at what he calls 'information dominance'. In 1995 the Royal Netherlands Army established a programme directed at modernizing the fighting soldier. **Meijer** describes the developments in the so-called Soldier Modernisation Programme and he concludes that in the (near) future the equipment of the fighting soldier will not only allow him to become an effective warrior but also a highly valuable informant. **Bosch**, finally, considers the role of information in the context of a number of technological developments and their impact on the command and control cycle. The increasing potential of the information processing not only enhances the striking power of an army, it also makes it vulnerable. His conclusion is that information is not only a means or weapon, but also a target.

The editors would like to thank Wim **Visschers** and Robert **Smits** for their advice during the editing process.

Information: a many-faceted and fascinating phenomenon

H.P.M. Jägers

1. Introduction

In the last decade of the past century a number of developments took place which have converted our present-day society into an information society. Several authors use the word 'revolution' without any reserve when they discuss the influence of the developments in the field of information and communication technology [ICT] (Toffler & Toffler, 1993; Castells, 1998). With this characterization they not only point at the speed with which changes take place, but in particular at the more or less radical break with the past. The idea that the current technological revolution will cause a total unravelling of the structure of society and a redesigning of the existing social relations is widely proclaimed (Junggeburt, 2000).

Since the late eighties the use of ICT has grown enormously and the end of this phenomenon is not yet in sight. Probably, we are only on the brink of developments whose real meaning in terms of communication, transparency and permeability must still reveal itself. As to the possibilities of communication, they time and again offer wider perspectives and views and allow forms of collaboration across organizations which have hardly been conceivable. One of most important phenomena is the Internet, which gives access to real-time connective information processing. Consequently, the information processes and the social structure resulting from this phenomenon are connective and individual (De Kerckhove, 1996). But more important than these two qualities is an accelerated growth of intellectual production. The value of information has increased proportionally.

The importance of information within the information society is generally acknowledged. Some people think it is so extensive that they regard information as the fourth production factor. The value of information is determined by those who use it and place it within a certain context (Vuijst, 1998). The process of decision making in organizations forms an important element of this context (Choo, 1998). Information becomes more valuable to the extent to which it allows uncertainty in decision making to be reduced, allowing better decisions to be taken. At this moment, the determination of the value of information is affected especially by another vision on the concept of information, in which this concept itself is considered to be changing, both in meaning and goal (Jägers & Maes, 1995).

2. The concept of information: a shifting panel

Information has several meanings
Information does not present itself in one guise only. Dependent on the view that is chosen or the combination that is made with other parts of information, the concept can have different meanings; in fact, it is a many-faceted phenomenon. The days of starting from a categorical approach of information, in which it was stored in stable categories in a database and was accessible in one way, are over. The implementation of information and multimedia technology allows the combination of other, different forms of information transfer, exponentially increasing the number of possible images of reality. This has enormous consequences for the manners in which we organize. New possibilities lie within reach to choose from and combine into new forms of representation, resulting in the loss of meaning of traditional restore and collection media.

Information is subjective
Information is not a neutral phenomenon; it has always been related to a person's perception of reality and it is fed from the selection mechanism that is used in the observation (Van Hoorn, 1987). On this basis the idea of an information system as an objectified representation of reality is no longer tenable. At best it is an expression of a human agreement about the use of terminology around a question.

Information is ubiquitous and pervasive
Information is available for everyone and accessible for an almost negligible price on the Internet. The user is no longer waiting at the end of the value chain for what will be delivered, but he actively asks for the information needed at that moment. Incidentally, this is becoming a great problem, because of the enormous growth of the number of websites. It is an increasingly difficult task to gather the required and right information from the web. At the same time we see that information is not only complementary to a product or service, but that 'information' itself is the product. This demands a lot of the ways in which we set up information systems, place information at someone's disposal and organize the information infrastructure.

Information crosses the boundaries of organizations
Information is intangible and therefore it cannot be related to specific people, groups or locations. The sharing of information – electronic, written or oral – often takes place in a fluid and informal way, obscuring sight on what exactly is happening with it. The idea that we can retain information within our formal organizational boundaries is outdated, although there may be some objections from a legal point of view. This awareness has considerable con-sequences for the ways in which we deal with information within organizations, on the one hand, and how we approach employees about their use of relevant and available information, on the other. The currently popular 'information leak', mostly within the administration, has once again brought this aspect to the attention of society and it has evoked important questions about ethics. The situation after the Srebrenica mission of the Dutch army is certainly not the only relevant one, but it contains many lessons learned with regard to this aspect.
These changed views on information urge us to approach organizations in a different way than we have done for a long time. To think in terms of connections, interdependencies and processes, also across the boundaries of the organization, is a necessary condition for approaching, describing and analyzing the organizational reality. We see that organizations increasingly concentrate on the creation of value. In this context they realize that they have to deal with the required information in a conscious way. Drucker mentions four kinds of information and he sees them as diagnostic instruments (1999):
- *foundation information*; it affords an organization the possibility to know if a problem needs to be identified and treated, because it is abnormal;
- *productivity information*; it gives data on total-factor productivity by measuring the value added over-all costs, including the cost of capital;
- *competence information*; it rests on core competencies that meld market or customer value with a special ability of the producer or supplier;
- *resource allocation information*; it indicates the allocation of scarce resources, capital and performing people, which convert into action all the information that a management has about its business, because they determine whether the enterprise will do well or poorly.

Drucker's classification shows that information is embedded in everything, in products, in processes and in people, and in this way it proves an important basis for creation of value. The flows of information – facilitated by ICT – settle into these elements and this constitutes an integrated unit of them. These information flows also create relations within and between organizations.

3.   Changing defence

The army is one of the oldest forms of organization and already at the end of the 16th century. Prince Maurice carried through changes in the conduct of war which would be guiding for a long time to come (Mastenbroek, 1993). Maurice was obsessed by the wish to increase the combat strength and flexibility of his troops. The massive, unwieldy square formation was replaced by a shallow one. This, however, had great consequences for the type of soldier he needed. This soldier had to show more discipline and self-confidence, be able to react rapidly to orders and at the same time sustain the cohesion in the group. Already in these early times there was an awareness of the consequences of certain structural arrangements for performance, but also of the importance of a good real-time information supply.
Since Prince Maurice realized a different design in his lines of battle in order to guarantee success on the battlefield, many things have changed in the Dutch military organization. We do not find these changes in the principles for military operations, but only in the application of new technologies, in other ways of commanding and carrying out operations. The greatest changes, certainly in the mental sphere, have taken place in the way of employing units in areas of operation. This is also based on international and economic developments, making the security risks almost impossible to foresee, at least not before a conflict has broken out (Militaire Doctrine, 1996).

3.1.   Information in peace situations
In peace circumstances the defence organization has many features of a normal organization, in which efficiency and effectiveness take pride of place in the execution of the daily task. The realization of the operational management, however, is characterized by the demand to commit units operationally. Integral management, open and transparent accountability to higher management and steering on main lines are clear characteristics of this policy. They have to connect in such a way that the transition from the peacetime situation to operational action takes place faultlessly. Operational peacetime management and operational action are not only in line, but represent, as it were, one and the same reality which can only be divided in an analytical sense (Reitsma, 1996).
The occasional over-emphasis of the importance of the performance of the 'result-responsible units', in order to realize the aims of the management concept, has somehow caused this connection to be severed and two separate worlds of perceptions to emerge. This development has to be rejected from the perspective of information, because of the danger of the information provision getting entangled in the peace situation, losing its boundary-crossing character in the process. Information on operational management in peacetime circumstances in the context of result-responsible units and integral management must be equally meaningful for decisions that have to be taken for operational actions. The ability to link information systems across domains is therefore a prerequisite, necessitating great attention to infrastructures and architectures (Onincx, 1998). Coherence and interdependencies between operational processes and domains have to be given a central place, especially in times when complexity and changeability are the dominant factors to be dealt with.
In order to reach this, there has to be a thorough awareness of the fact that decision makers often have a restricted rationality, which means it is impossible to get a clear view on all the

alternatives and to survey the consequences of a certain choice. Moreover, the imbalance in the availability of information plays an important role in decisions. This disadvantage can be overcome to a large extent by the use of information systems that support the decision making process, arranging data in a significant and meaningful way (Jägers et al., 1997). The more prominent the use of information and communication technology in the daily execution of activities, the more new patterns of collaboration will grow within and between organization units. This is where the actions in peacetime and crisis situations come together.

3.2   Information in operational action

For many years the armed forces were predominantly oriented towards action in a sizable conflict, but this posture is obsolete now and partially superseded by action in crisis control and peace support operations, often in an international context. The various policy documents that were published over the past years, one after the other, have made clear that the Netherlands wants a complete army that can act in an important range of the conflict spectrum. The Netherlands forces would like to deliver modules that can be deployed in international missions in situations of regional collective defence and crisis operations – these two distinctive types of operation being more and more in line with each other. Besides, modules will have to be available for humanitarian operations and the army must be ready to carry out civil tasks where necessary. The national level of ambition allows a maximum of four simultaneous peacekeeping operations and this requires a whole range of employable units. It presupposes the availability of a high-quality technology, guaranteeing the required output to an army that is constantly shedding personnel (Sonneveld, et al., 1999).

Military units are strongly dependent in their way of action on information about terrain, circumstances and opponent, own means and so on. To be successful, real-time information is a prerequisite. In this respect operational units are information-intensive units. In C2 and C3, ICT plays an increasingly important role. More and more, the commander is supported to an increasing extent by information systems such as the Integrated Staff and Information System (ISIS) and Battlefield Management System (BMS) in order to process information and to provide units with a shared image of the situation in which they find themselves. They will give him the possibility to execute at greater speed processes like the analysis of factors of influence and command and control, thus increasing operational swiftness (Hoppenreijs & Tak, 2000). Obviously, the well-known dangers appear here: overload of information, making it difficult to make the right choices, the threat to the sustainability of the information because of fast-changing situations and, finally, loss of overview through too great an attention for details. The 'digitalization of the battlefield', begun in the 1990ties, brings real-time information at the level of the group and the individual soldier, and the right decisions can be taken on the spot. Also the use of, for example, video conferencing at brigade and battalion levels increases the speed of the decision making. Flexibility in actions is a must and optimal structures to enable it cannot be designed in advance (Fukuyama & Shulsky, 1997). Creativity, also based on experience and knowledge, is a more important aspect than structures. On this basis the optimum mix for an action must be established, first and foremost, on the spot.

In order to reach this it is important that operational units and individual servicemen learn to deal with information and to incorporate it in the familiar doctrines of analyzing, evaluating and revising operations (Richard & Barber, 1997). In doing so, they have to realize that information provision, to a large extent supported by ICT, is not a panacea (Bosch, 1999). A digitalized unit stands empty-handed when image and sound fall away. Then, a capacity and encouragement to think critically and creatively are essential conditions for handling a situation. This capability can only be acquired through training and education. Concepts of

learning processes will be acquired in order to counter the changeability and complexity in this information era.

4.   Perspectives

The development of information networks brings along new strengths and vulnerabilities. Electronic media give us the opportunity to reach across the boundaries of the own organization and of ourselves. In that sense there are new possibilities every day and we, as individuals and participants in organizations, change along with this broadening of perspectives and visions. Of course this is a great boon, but the openness and connectivity also proportionally increase the vulnerabilities. Separate, previously unrelated, units have now been connected and the disruption of that connectivity can set off a chain reaction that hits an organization much harder than before, when an onslaught was fended off with classical tools of battle. The growing attention for information warfare is expressed as follows: 'the offensive and defensive use of information and information systems to exploit, corrupt, or destroy an adversary's information and information system while protecting one's own' (Shaker & Gembicki, 1999).

This phenomenon will still have to looked into close by the defence organization, although the problem as such has been recognized and labelled as 'info-sphere' in the (American) military doctrine. The 'info-sphere' is described as the place where in the future wars will primarily be waged. The first signs that our 'opponents' are searching out this vulnerability and are no longer attempting to first reach disorder on the ground, in the air, at sea or in space, are already there. Destruction of strength by crippling the systems of these units themselves has become the paramount objective. In fact the daily air attacks during Desert Storm on vulnerable government communication centres and the Iraqi troops, preceding the actual ground war itself, signified a clear recognition of the importance of such systems, and their destruction, for victory.

The concept of 'information warfare' is also known in the world of business and has the same connotation as described above. Winn Schartau has written a most fascinating and instructive book, entitled *Information Warfare: Chaos on the Electronic Superhighway* and his website http://www.infowar.com/ is worth a visit. In his way of thinking there are many aspects which are just as much valid within the context of the defence organization. He sees 'information compromise' and 'information destruction' as two important threats that must figure at the top of the agenda of every self-respecting counter intelligence service.

A final element worth mentioning is the perspective of the change in the military war room. With the rise of modern means of communication and almost real-time information, these war rooms have become more and more a link in command and control activities instead of a support in long-term planning and strategy formulation (Shaker & Gembicki, 1999). Decisions relating to action on the battlefield can be taken on the spot. During *Desert Storm* this development was clearly illustrated by General Schwartzkopf giving briefings to the media on the basis of maps which had been updated only minutes before. It is already possbile at the moment to equip and have a 'high-tech war room' operate in the short term. This development will surely continue and still more advanced tools will be used, allowing a greater grasp on situations and better decision making.

5.   Conclusion

Information is a many-faceted and fascinating concept and it has acquired enormous power through the developments of ICT, which in the past decades has caused a great change in its applications and uses. It has progressed from (excessive) concentration on production increase

by means of all sorts of automation applications, via supporting information systems to multimedia applications with the help of information and communication technology – in other words, from support of basic activities to the creation of new possibilities and the bringing about of links via the growing synergy of network communication. 'In the enormous convergence of hypermedia, multimedia, virtual reality, neural networks, digital agents and even of artificial life, at this moment every medium changes different parts of our lives, our ways of communication, of labour and our entertainment', says De Kerckhove (1996). But more important is the fact the Internet affords access to an almost unlimited number of human intelligences, and because of that, it is the portal to as yet unknown and unrecognized dimensions. The influence of ICT on changes in internal and external functioning of organizations is enormous and touches on all the aspects of human functioning in organizations. The changes that already manifest themselves in the fighting soldier, who is equipped for the battlefield with the latest state of the art digital tools giving him a hold on his environment through a good information position, are clear signs of the recognition of the opportunities within reach at this moment in time.

Perhaps the most important problem in the present-day information economy is to find a way to get the required information in the right place and time in order to start transactions with the environment in every possible circumstance. This question is important both in peacetime and operational actions. Obviously, the creation of an adequate information structure and architecture is a basic demand in this. It lays down, as it were, the foundation on which the relation with the customer (stakeholders, collaborative partners) is realized and takes shape in a customer-specific way. The characteristics of the business process thus have a relation with the depth of the information that is needed in order to serve the customer as well as possible. This process of specification can be realized by the availability of information about relations, products/services and processes (De Vries & Stegen, 2000). The depth to which this information must be available depends on the situation in which a person finds himself. Information about relations/customers enables distinction between customers, so that products or services can be offered well-aimed and specified. Information about products and services offers the opportunity of presenting customer-made products/services and information about processes gives an insight into reliable prognoses about delivery.

Finally, information plays an important role in every organization. Both processes and products are dominated by it. Mostly we take the importance of information for granted, because it is everywhere, like the air that we breathe. The increase of the importance of information can be found more in the explosion of the connectivity and of the information standards which guarantee the open, almost free, exchange of a constantly growing world of rich information (Evans & Wurster, 2000). This phenomenon has greatly contributed to major breakthroughs and innovations and what we have seen until now only heralds much more. Therefore we must be aware of the importance of information as it can stimulate us to discover new possibilities and worlds.

References

Beleid Bedrijfsvoering Defensie (BBD) 2000 (1999), [Defence Operational Management
    Policy], DGEF, Directoraat Generaal Economie & Financiën, Den Haag
Bosch, J.M.J. (1999), De toekomst van de oorlogsvoering [The future of warfare]
    in: G. Teitler et al., *Inleiding Militaire Strategie* [Introduction to Military Strategy]:
    389-410, KIK; Den Helder, Rijswijk, Breda

Castells, M. (1998), *The Information Age: Economy, Society and Culture. Vol. III: End of Millennium*, Blackwell Publishers, Oxford.

Choo, Chun W. (1996), The Knowing Organization. How organizations use information to construct meaning, create knowledge and make decisions
in: *International Journal of Information Management*: 16, 1996, 5: 329-340

Drucker, P.F. (1999), *Management Challenges for the 21st Century*, Harper Business, New York

Evans, Ph., Wurster, Th.S. (2000), *Blown to Bits*, Harvard Business School Press, Boston

Fukuyama, F., Shulsky, A.N. (1997), *The Virtual Corporation and the Army Organization* RAND, Santa Monica

Hoppenreijs, J.G.M., Tak, N.W. (2000), De nieuwe leidraad commandovoering [The new command and control guideline], in: *Militaire Spectator*, 169, 2000, 10: 519–524

Hoorn, Th. P. van (1987), Paradigma's en portfolio: anders kijken naar hetzelfde [Paradigms and portfolio: etc.], in: *Mens & Organisatie*, 41, 1987: 424–442

Jägers, H.P.M., Maes, R. (1995), Integratie van Organiseren en informatiseren: onderkennen van en omgaan met dilemma's [Integration of organizing and computerizing: recognizing and dealing with dilemmas], in: *Management & Informatie*, 3, 1995, 1: 4–14

Jägers, H.P.M., Heijnsdijk, J., Steenbakkers, G.C.A. (1997), De invloed van informatietechnologie op de organisatiegrenzen: IT bezien vanuit de transactiekostentheorie [The influence of information technology on the boundaries of organizations: IT seen from the theory of transaction costs], in: *Management & Informatie*, 5, 1997, 1: 18–28

Junggeburt, H. (2000), *You've got no mail. Arbeid en arbeidsrelaties in de nieuwe economie* [You've got no mail. Labour and labour relations in the new economy]
Oratie, Universiteit van Amsterdam, Vossiuspers UAP

Kerckhove, D. de (1996), *Gekoppelde intelligentie* [Linked intelligence]
Stichting Maatschappij & Onderneming, 's-Gravenhage

Mastenbroek, W.F.G. (1993), Organizeren in historisch perspectief [Organizing in an historical perspective], in: *Mens & Organisatie*, 47, 1993: 161–171

Militaire Doctrine (1996), *Landmacht doctrinepublicatie, Deel I* [Army Doctrine Publication, Part I], Doctrinecommissie van de Koninklijke Landmacht, Sdu, Den Haag

Oonincx, J.A.M. (1998), Informatietechnologie in de Krijgsmacht [Information technology in the armed forces], in: *Militaire Spectator*, 167, 10: 506–513

Reitsma, R. (1996), Minder tanks, meer informatietechnologie? [Fewer tanks, more information technology?], in: J.A.M. Oonincx (red.), *IT in de krijgsmacht. Op weg naar de 21ste eeuw* [IT in the armed forces. On the road to the 21st century]: 45-49, KMA/VOI (Vereniging Officieren Informatica), Breda

Richard, J.S., Barber, H. (1997), *The Learning Army. Approaching the 21st century as a Learning Organization*, US Army War College, Carlisle Barracks, PA

Schartau, W. (1994), *Information Warfare: Chaos on the electronic superhighway*
Thunder's Mouth Press, New York

Shaker, S.M., Gembicki, M.P. (1999), *The War Room Guide to Competitive Intelligence*
McGraw-Hill, New York,

Shapiro, C., Varian, H.R. (1998), *Information Rules. A strategic guide to the network economy*, Harvard Business School Press, Cambridge/Boston

Sonneveld, H.C., Langen, T. van, Pasman, H.J. (1999), Kennisondersteuning voor de krijgsmacht [Knowledge support for the armed forces]
in: *Militaire Spectator*, 168, 9: 477–485

Toffler, A., Toffler H. (1993), *War and Anti-War. Survival at the Dawn of the 21st Century*
Little Brown, Boston

Vries, E. de, Stegen, F.S. (2000), Multi-channeling in de dienstverlening, het (pmc)2 raamwerk voor kanaalcoördinatie [Multi-channeling in the service sector, the (pmc)2 framework for channel coordination], in: *Management & Informatie*, 8, 1: 4–16

Vuijst, J. de (1998), *De waarde van informatie* [The value of information]
www.nbbi.nl,

Zee, H. van den, Strikwerda, H. (eds.) (2000), *Changing Business Designs for the 21st Century*, Addison-Wesley, Amsterdam

Part Two

The role of information in a peacetime context

Collaboration in the armed forces

An analysis from the perspective of network organizations

G.C.A. Steenbakkers, A. Koppe, H.P.M. Jägers, W. Jansen, T. Bijlsma.

Collaboration

Doctrinal thinking on the integrated deployment of combat helicopters, airmobile infantry and related transport helicopters is continually developing. One reason for this is an increase in experience in joint operations of the integrated 11 Airmobile Brigade/Tactical Helicopter Group (11 Air Manoeuvre Group, 11AMB).

Source: *Operational Principles 11AMB*

---

1.   Introduction

Collaboration in organizations is not a new phenomenon indeed. Processes in organizations have always required collaboration and co-ordination between people, activities and departments. The last few years, however, there has also been increased co-operation between organizations, the so-called inter-organizational collaboration. This involves boundary-crossing collaboration, in which several organizations together make a product or create a service, share knowledge or make expertise available to each other. In the literature this phenomenon is known as network organizations (Nohria & Eccles, 1992; Jansen & Jägers, 1995). We do not only find network organizations in commercial companies, but as often in government organizations, where the participants may be government institutions/ departments, and in organizations outside the government. The term is also used when it concerns the collaboration between (reasonably) autonomously operating departments of larger organizations, such as multinationals. Thus the collaboration between the AirMobile Brigade and the Tactical Helicopter Group (THG) as described in the box at the beginning of this article, is an example of inter-organizational collaboration in the armed forces.

In this article we intend to present a vision on internal and external collaboration in the armed forces from the perspective of network organizations. By means of several points of interest in the recently published *Defence Memorandum* we will demonstrate that in a number of areas network-like organizations, in many variations, are emerging between armed forces, between services and between international organizations (section 2). In section 3 a theoretical framework is presented for the positioning of the different types of networks. This framework will be applied to the armed forces in section 4 and we will conclude our article by indicating the significance of network organizations for them.

2.   Present plans for the (re)structuring of the defence organization

In the *Defence Memorandum 2000* the framework for the restructuring is given and with it the future structure of the armed forces. It offers a number of starting points for making an analysis of the armed forces from the perspective of network organizations. Based on the Coalition Agreement, the Memorandum will be guiding for the armed forces in the decade to come. Apart from reductions there will be room for innovation and intensification. As an

illustration a number of quotations from the 1999 Defence Memorandum (*Defensiekrant*, 29 November 1999) may suffice:

-    Modern armed forces have to be flexible. The Netherlands armed forces are founded on the modular concept: they form a system of modules that can participate on multinational levels. They have to fit in with NATO, UN, WEU, or ad hoc coalitions.
-    The Defence Memorandum contains several initiatives that underscore the increased importance of collaboration between the Services. An alert and flexible defence organization requires personnel that is capable of seeing and going beyond the boundaries of their own unit.
-    There are strong military-operational reasons for more collaboration between the Services, whose modules are also capable of taking part in 'joint' operations: modules such as, a mechanised battalion, a Patriot unit, the amphibious transport ship and parts of the Tactical Helicopter Group.
-    Our government is convinced that directing such a complex and dynamic organization requires centralised control and decentralised implementation. The latter ensures an alert and flexible response, clear responsibilities and greater efficiency and centralised control on main lines is therefore better than centralisation.
-    Collaboration between the Services can increase efficiency, amongst others in combat and logistic support.

The above quotations demonstrate that there is much attention for boundary-crossing co-operation and its control. In section 4 we will discuss the mainlines in greater detail from the perspective of network organizations.

3.   A model for network organizations

On the one hand, network organizations emerge as a result of important changes in the environment of organizations, such as internationalisation, globalisation, etc. Also the individualization of the customer's demands and the continuous development of products and services may entice organizations to collaborate. On the other hand, the possibilities for collaboration have increased for organizations, in a world where modern information and communication technology (ICT) ensures a communication and co-ordination independent of place and time. Collaboration can take place with partners all over the world. But it is almost completely impossible without the use of ICT, and as a consequence co-ordination and information provision are at the heart of network organizations.

In earlier publications we have presented a model for network organizations (Jansen, et al., 1997). In this section we will briefly summarize our model before applying it to the armed forces in section 4. For network organizations, as for all organizations, the environment largely determines the design. In our model the most important factors in that environment are complexity and changeability. Three types of network organizations are distinguished on the basis of the level of complexity and changeability. Complexity can be defined as follows:

Complexity is the extent to which an organization is confronted by various factors and relations, in particular the number of factors as well as the relations between the factors.

The environment of an organization can range from simple to complex – from the environment of the folding boxes manufacturer who only needs very basic knowledge for his simple products and who is only active in very simple markets, to that of a space travel organization that has to make use of the most sophisticated sciences in order to be able to generate a very complex output.

Changeability is defined as follows:

> The extent to which the organization is confronted with unpredictable changes in the environment.

Examples of this are unpredictable customer behaviour, a high personnel turnover, regular product changes, an unstable political situation and a fast changing technology. In a very dynamic environment it is difficult for an organization to anticipate on the future and it is almost impossible to fall back on previously developed doctrines and procedures.

On the basis of the key concepts of complexity and changeability three types of network organizations can be distinguished (Jansen, et al., 1997):

- Planet-satellite networks
- Strategic alliances
- Virtual organizations

The three types have been placed in the scheme below (Fig. 1).
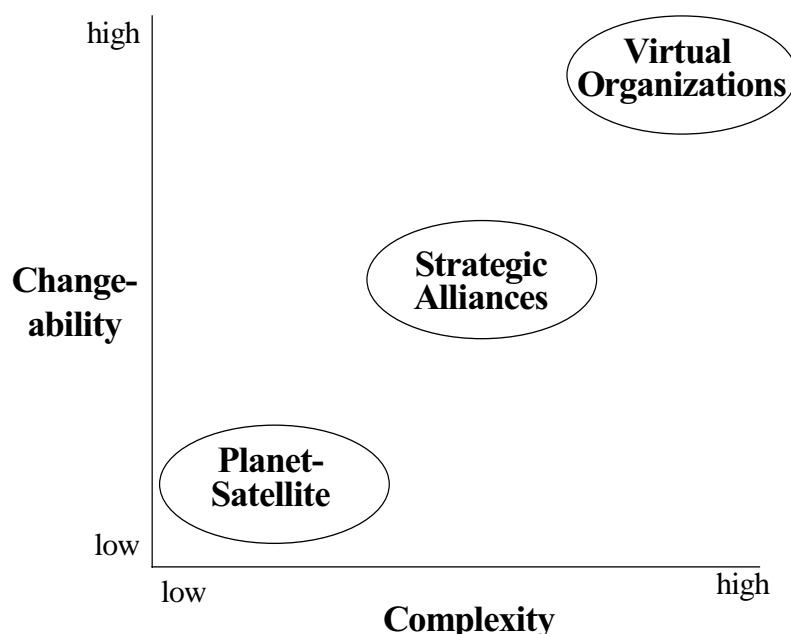
Figure 1: Three types of network organizations

Describing the network forms

3.1   Planet-satellite networks

In the planet-satellite there is one organization, the planet, which is dominant within the network and it has, as it were, a number of satellites around it. A good example of this can be found in Japanese production companies that work with subcontractors. The big companies determine the specifications, number, form, etc., of services/semi-finished products that are delivered by the suppliers. Due to the presence of a central party that holds all the power ('the spider in the web') there cannot be said to be a negotiation situation between the elements in the network. The division of power in this type is such that it seems as if there are departments or subsidiaries of one and the same organization, whereas of course there are several organizations 'bound' to the one powerful, central party in the network (Fig. 2).

13

Figure 2: Planet-satellite model

The role of ICT in planet-satellite networks
In planet-satellite networks control is increasingly supported by ICT by means of electronic connections between the central party and the decentralised units, aim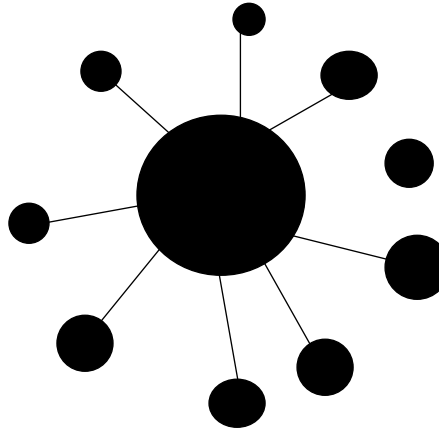ed at controlling the progress of activities (for instance, by workflow management), sales results, turnover, stocks, etc., and the giving of account (electronic report systems). Besides, there are shared customer databases and expert systems, enabling the users to supply customers of 'comprehensive services' in a decentralised way. The centralisation of power with the planet leads to the necessity of strongly standardised electronic communication (imposed by the planet), for which Electronic Data Interchange (EDI), in which computers communicate with computers, is eminently suitable. Placing and processing of orders are often cited examples of this form of ICT.

Characteristic	Planet-satellite networks
Purpose of collaboration	Efficiency and cost reduction (primary), increase of flexibility (secondary)
Environment	Low complexity; low changeability
Core competencies	Planet and satellite have different core competencies
Co-ordination mechanisms	Previously fixed rules and procedures; high level of standardisation and formalisation
Risk sharing	There is risk sharing between planet and satellites
Power	Lies with the planet (centralised)
Trust	Formal agreements reduce the need of blind trust between the partners

Table 1: Survey of characteristics of planet-satellite networks

3.2   Strategic alliances

In case of an increasing changeability and complexity organizations tend to choose for collaboration in a number of areas. Often they complement each other and by working together they can use each other's assets. In this type of networks there is a wider spreading of power among the participating parties than is the case in the planet-satellite networks. An example is the strategic alliance between KLM and NorthWest Airlines. This alliance improved the competitive position of the participants in that the occupancy of the air fleet improved by the combination of flights and the acquisition of landing rights on the permit of

one of the partners. These factors appear to be important arguments in the present cooperation boom among airlines (Fig. 3).
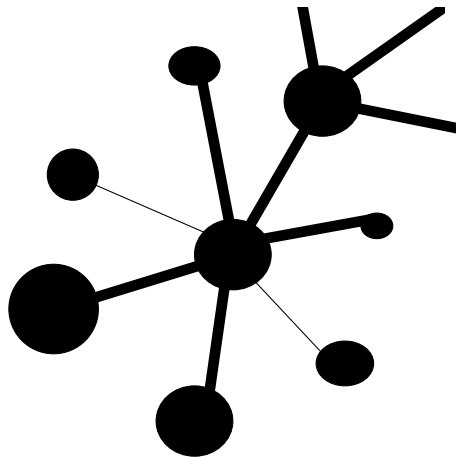

Figure 3: Strategic Alliance

The role of ICT in a strategic alliance
ICT plays a role in the communication between parties in networks. Allowing part of the activities to take place outside the organization necessitates the tuning of internal and external activities by means of ICT. The strategic alliance has existed for a long time now, and ICT has been the means to establish an optimal communication between the partners (E-mail, EDI, business-to-business E-commerce).

Characteristic	Strategic alliances
Purpose of collaboration	Market motives (primary), increase of efficiency (secondary)
Environment	Average complexity; average changeability
Core competencies	Parties have the same or complementary core competencies and can generate their own products independent of each other
Co-ordination mechanisms	Previously fixed rules combined with workgroups and committees
Risk sharing	There is risk sharing between the partners in the strategic alliance
Power	Power is shared between the parties or hardly present
Trust	Formal agreements reduce the need of blind trust between the partners

Table 2: Survey of characteristics of strategic alliances

3.3   Virtual organizations

In a sliding scale the increase of changeability and complexity finally leads to a virtual organization. Organizations have to operate more and more in unstable environments, in which it is not clear whether the existing knowledge of the single organization is applicable. In such a situation virtual organizations are playing an increasingly important role.[1] A distinctive characteristic is knowledge sharing and innovation. A common goal (often implicit), therefore, of virtual organizations is to experiment with new ways of collaboration.
In virtual organizations there is a relation of equality between the participants in the network. The difference with the strategic alliance is mainly found in the ever-changing composition of the network (Fig. 4). In strategic alliances the collaboration is much more permanent.
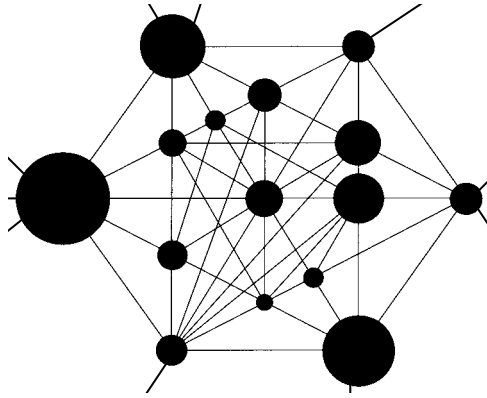
Figure 4: Virtual Organization

The role of ICT in virtual organizations
In virtual organizations, consisting of several organizations, ICT forms an essential prerequisite for the mutual co-ordination, facilitating the sharing of knowledge, in particular. ICT-facilities, such as E-mail, groupware, the Internet, videoconferencing and group decision support systems, are necessary for making quick contact with the partners about new or existing orders and ideas. Continuous co-ordination and monitoring of progress is also done by means of ICT.

Characteristic	Virtual organizations
Purpose of collaboration	Innovation and flexibility
Environment	High complexity; high changeability
Core competencies	Parties have different core competencies and CANNOT generate the product or service without each other
Co-ordination mechanisms	Mutual co-ordination, often with the help of ICT and committees or workgroups
Risk sharing	There is risk spreading between the partners
Power	Power is shared by the partners or hardly present at all
Trust	A high degree of trust is necessary because of the high uncertainty and high degree of dependency

Table 3: Survey of characteristics of the virtual organization

4.   Network forms in the Defence Memorandum

In this section attention will be given to the proposed developments in the Defence Memorandum and they will be held against the light of network organizations. Examples from the armed forces will be applied to the three types of network organizations discussed in section 3. As was seen, these types lie on a continuum, and it will not always be possible to match organizations or parts of organizations fully with one of the types, although a certain type will often be dominant. An organization, therefore, can have the characteristics of one or more types of network organization at the same time. It is also possible that in one organization more types exist or that organizations can take part in more types of network than one.

4.1 Planet-satellite networks in the armed forces

In the armed forces a great many planet-satellite networks can be identified. Often reductions have been the occasion for this form of collaboration. Many reorganizations in the armed forces are targeted at increasing efficiency, reducing costs and improving flexibility. A well-tried method for cost reduction was reorganization, with a personnel ceiling as a prerequisite. Many units sought an escape in task specialisation and, whenever possible, the putting out of (a cluster) of tasks. Especially in the case of the garrison business this was often used. The outputting of maintenance activities, barracks security, and the hiring of temps for general tasks in the messes may serve as examples.

Units must concentrate on their specialist, irreplaceable core competencies. When, as much as possible, secondary tasks are put out or executed by units of the garrison, the units themselves only have to concentrate on their main tasks, which increases flexibility (Fig. 5).

In planet-satellites there is extensive agreement-making and co-ordination and a high degree of standardisation is required in order to tune all the business processes adequately. As a planet-satellite functions in a relatively simple and not very changeable environment this is not a problem. Procedures, once developed, will hold sway for a considerable period of time.
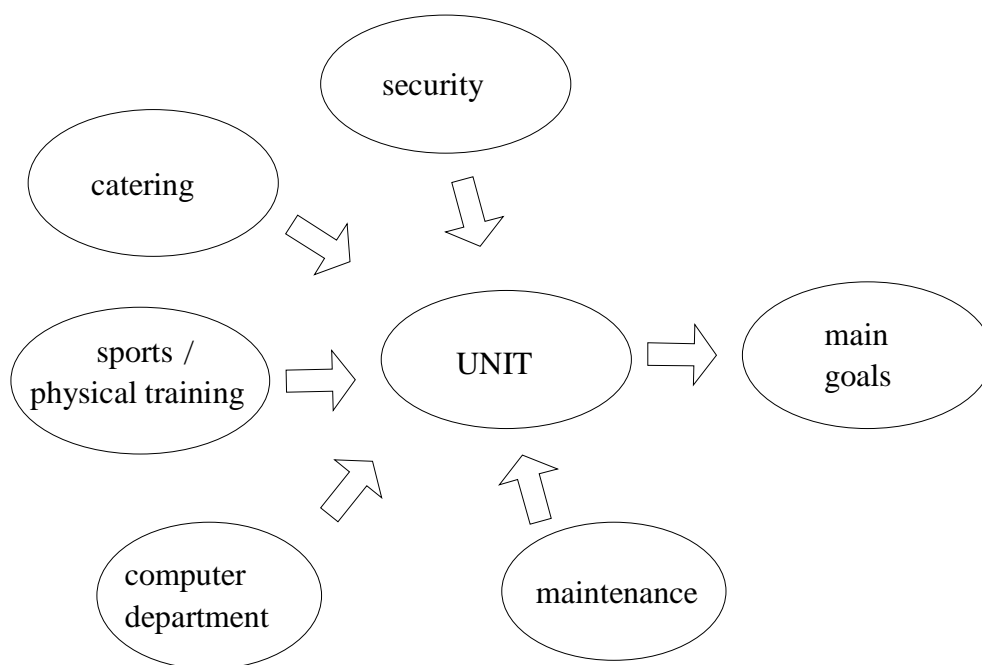
Figure 5: A unit and some of its satellites

4.2 Strategic alliances in the armed forces

The armed forces have always been used to working in strategic alliances. Examples can be found in NATO, UN, or WEU contexts. This network form is found in situations featuring an average complexity and changeability. Apart from these forms there are sufficient other possibilities for strategic alliances in the armed forces, in particular alliances in the field of special forces and airmobile infantry. Potential players in these alliances are:

- Special Security Assignment Brigade (BSB, of the Royal Netherlands Military Constabulary)
- Special Assistance Unit (BBE, of the Royal Netherlands Marine Corps)
- Commando Corps (KCT, of the Royal Netherlands Army)
- Royal Marines (Royal Netherlands Navy)
- AirMobile Brigade (Royal Netherlands Army).

A number of tasks these units train for are identical or at least similar. An analysis of the total task responsibilities and the collaboration based on them would most certainly benefit efficiency and effectiveness. Large gains are also to be reached in the areas of recruitment and training of personnel. As it is, all units are more or less 'fishing the same pond', in that the demands on personnel overlap and are often identical. Close collaboration is certainly possible here, also in the area of training, especially the basic training, where there are many similarities. An alliance in this area would create a 'win-win situation' for all parties involved.

4.3 Virtual organizations in the armed forces

The complexity and high degree of changeability of the environment of humanitarian aid organizations demand an approach for which virtual organizations are eminently suited. In the short term a product has to be delivered in an almost completely unknown area. Actors in a humanitarian or aid operation (HUMOPS) can be:

- the High Commissioner for Refugees (UNHCR)
- the International Red Cross (ICR)
- Médecins sans Frontières (MSF)
- a whole range of (Non-) Governmental Organizations (GOs and NGOs)
- military units
- local authorities.

These actors all fulfil an essential role in the administering of help, and most of the time they have a certain specialisation that makes them unique, whereas other aid organizations have a more general task and can be replaced more easily. This does not mean that when the task of one of the actors is not carried out, there will be no help, but the quality of the help offered does go down (Fig. 6).
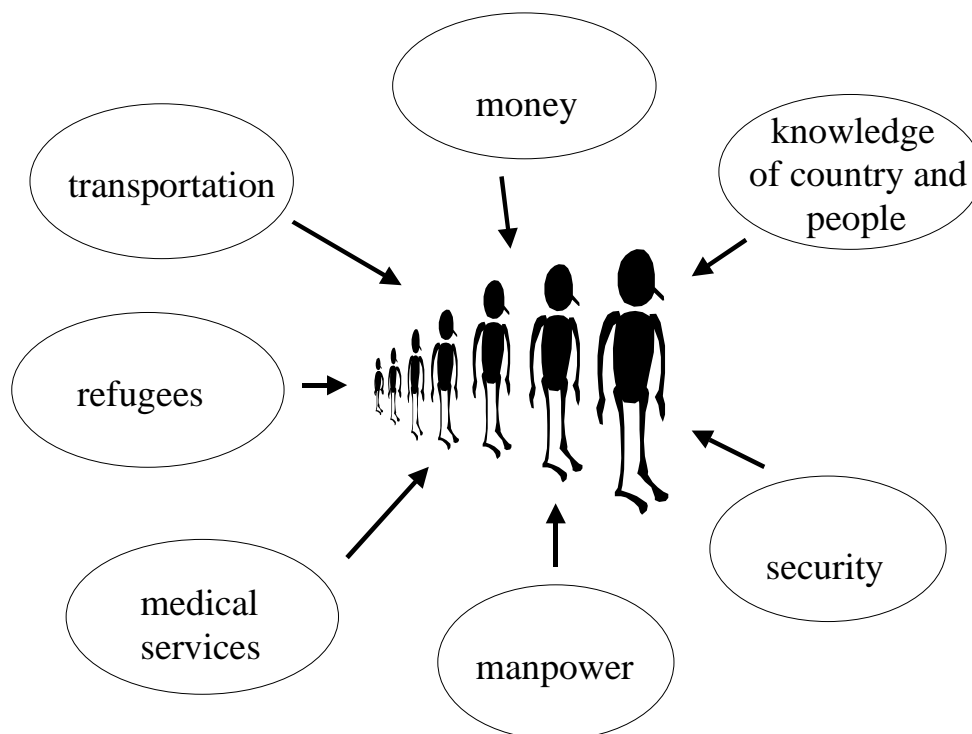
Figure 6: Virtual organizations in the armed forces

The armed forces have gained a lot of experience in working in virtual organizations during HUMOPS during the last ten years. A few examples are:

1991	Engineer Support Battalion	Iraq
1994	Provide Care	Goma
1999	Taskforce R	AFOR - Albania
1999-2000	Engineer Support Battalion	KFOR - Kosovo

As each of the actors has his own identity and home front, collaboration cannot be forced upon them or simply ordered. There is no centralised, let alone single-headed, control. Mutual dependency and common goals form the only binding factor between the actors who know and realize that collaboration is the only key to success.

5.   Conclusions

What, then, is the significance of network organizations for the armed forces? When the armed forces environment is considered, it is very likely that present trends and developments will continue. To an increasing extent the armed forces will be confronted with missions abroad, aid operations and multinational actions. It can be concluded that this ever-increasing complexity and dynamism of the environment will lead to units operating more and more in virtual networks.

Another development is the steady increase in the price for weapon systems, which forces defence organizations to make a choice with regard to deployment. This in turn forces countries to collaborate in the development and procurement of these systems. Specialisation will be the result, but also with respect to military operations countries will develop core competencies, which will lead to yet more strategic alliances.

Apart from this there will also be parts of the armed forces that will remain functioning in more stable and simple situations, where the emphasis on efficiency and scaling up will create planet-satellite forms of collaboration. Whichever network organization will be chosen, they all rely heavily on the use of ICT.

It is most certainly worthwhile to map out all the different forms of external and internal collaboration that have emerged over the last few years or lie in the near future and to study for which form a particular network organization and the role of ICT will be most successful.

References

Bouts, W., (1999), *Value Added Partnerships*, lezing congres 'De praktijk van netwerk-
    organisaties', [presentation held at conference 'The practice of network organizations']
    Nederlands Studie Centrum, Rotterdam
Defensiekrant (1999), Directie Voorlichting, Ministerie van Defensie, [Defence Journal,
    Information Service, Ministry of Defence], Den Haag; esp. 1999, No. 41
Defensienota 2000 (1999), [Defence Memorandum 2000], MoD, Den Haag
Fukuyama, F., Shulsky, A.N. (1997), *The virtual corporation and army organization*
    RAND, Santa Monica
Have, S. ten, Lierop, F. van, Kühne, H.J. (1997), Hoe virtueel moeten we eigenlijk zijn?
    (How virtual do we have to be?], in: *Nijenrode Management Review*, 1997 / 4: 85-93
Jägers, H.P.M., Jansen, W. (1992), Integratie van organisatiekunde en informatiekunde: Naar
    een nieuw paradigma [The integration of organization theory and computer science:
    Towards a new paradigm], in: *Informatie en Informatiebeleid*, 10, 1992 / 3

Jägers, H.P.M., Jansen, W., Steenbakkers, G.C.A. (1998), Wat zijn virtuele organisaties? Op zoek naar definities en kenmerken [What are virtual organizations? In search of definitions and characteristics], in: *Informatie & Informatiebeleid*, 16 (Spring) 1

Jansen, W., Jägers, H.P.M., Steenbakkers, G.C.A. (1997), Kennis, macht en informatietechnologie in netwerkvarianten [Knowledge, power and IT in network variants]
in: *Management & Informatie*, 5, 1997 / 5

Nohria, N., Eccles, R.G. (1992), *Networks and Organizations: structure, form, and action*, Harvard Business School Press, Boston

Operationele Grondslagen (1999), 11 AMB (Operational Principles 11 AMB]

---

[1] The publication of *The Virtual Corporation and Army Organization* (Fukuyama & Shulsky, 1997), commissioned by TRADOC, is an indication of the importance attached by the American Doctrine Committee to this kind of network.

Efficiency and effectiveness in the armed forces

The role of financial information

H.M. van den Hooven, N.P. Mol

1.   Introduction

The Netherlands defence organization has an annual budget of about 14 billion guilders – approximately 5% of the National Budget, an amount of money which more than justifies a closer consideration of the role of financial information in this organization. In doing so an age-old paradox immediately emerges: although the financial aspect dominates the allocation of resources for the military organization, it is largely ignored in the use of these resources in internal management control. Managers, even up to the highest levels in the organization, are only to a limited extent confronted with financial decision making. In times of peace the available personnel and material resources are largely fixed for organization units.   In financial terms, budgets do not give the unit commander more than a 'free margin' of expenditure of 5 to 6 per cent at most (De Bakker, 1998). In missions abroad, too, personnel and material resources to be employed are generally determined in advance to the smallest detail. The complementary financial consequences of deployment during the mission are settled on a reimbursement basis. In neither case, therefore, does financial information play a substantial role in management control on the executive level.

Nevertheless, from an economic point of view we may ask if this situation does not hamper an optimal - efficient and effective – allocation of resources. The economic use of scarce resources constitutes an obvious principle in any military doctrine. The opportunity costs of a choice between alternatives should, therefore, be given adequate attention.

In this contribution we will explore the possibilities for improvement of defence management control through an increased use of financial information. First we will distinguish the application of this information in government institutions in general from its use in for-profit companies. Subsequently, we will deal with the characteristics of economic behaviour in the armed forces that determine the specific application of that information there.

2.   Economic behaviour

Economic behaviour can be described in general terms as making a choice between various options of use of scarce resources. This choice mainly concerns the question which use contributes most to the objective(s) of the organization. In making it, two sides can be distinguished in economic behaviour (Fig 1, next page):

1.   Maximize the contribution to the objective, given the quantity of resources;
2.   Minimize the use of resources, given the contribution to the objective.

The first maximization problem starts from (exogenously determined) resources and tries to realize the greatest possible contribution. The second takes the given contribution as a starting point and aims at the minimization of the required (endogenously determined) resources. An optimal choice implies a mutual tuning of the used resources and the rendered contribution. In commercial companies, motivated by a pursuit of profit, this tuning can obviously be realized with the help of financial information. After all, the financial value of the inputs of resources

(costs) and the rendered contribution (benefits) forms the basis for optimizing management control in terms of output. The returns of the guilders spent, on the one hand, and the costs of

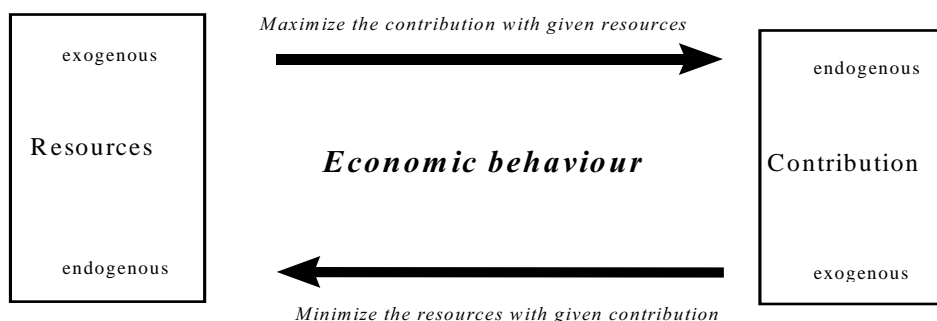| exogenous	*Maximize the contribution with given resources*	endogenous
Resources	*Economic behaviour*	Contribution
endogenous	*Minimize the resources with given contribution*	exogenous

Figure 1: Economic behaviour

the guilders gained, on the other, can be controlled simultaneously in the context of profit maximization. Resources and contribution can both be made endogenous. Thus, in the commercial business world, financial information forms the guiding principle of economic behaviour. It is based on market prices of both the buyer's market (resources) and the seller's market (contribution) (Fig 2).

Buyer's market	*Transformation*	*Seller's market*		
money ➡ input	➡ processes ➡	output ➡ effect (money)		
Resources		**Contribution**		

Figure 2: Economic behaviour in the commercial business world

Government organizations do not seek profit. In principle, as guardians of the public well-being, they have to take into account all relevant consequences of an action. Their products and services are usually not traded on a market, so that the market prices for the contributions are lacking. They are mostly directed at generating goods and services that the market does not or not sufficiently supply. Therefore, the societal contribution is, in principle, not expressed in financial terms, although there are occasional exceptions, notably where activities are of a market-conforming nature. In the armed forces this is particularly the case for the support services, such as maintenance and transport. The eventual product of the armed forces, however, remains problematical, because of its monopoly on violence. As a consequence, the significance of financial information in activities directed at fostering public well-being, is of necessity limited: only for the employment of resources can a financial equivalent be determined This limitation has far-reaching consequences for the optimization of economic behaviour in the management control of governmental organizations. An unambiguous criterion for this behaviour is absent, and the ensuing handicaps have been described by Anthony and Young (1999: 49-51) in the following five points:

1. Choices with regard to management control cannot be related to a single criterion, with the result that financial and non-financial considerations can continue to vie for right of preference, without the possibility of bringing them together under one clear-cut overall standard.

2. Quantitative assessment techniques that can enhance optimization in complex judging problems cannot be applied, when the relevant aspects cannot be subsumed under a common standard.
3. Performance measurements will fall apart in mere sets of indicators when they cannot be related to a single 'bottom line' (in the commercial world this sort of incorporation can be seen in the Dupont Charts).
4. Decentralization in the organization is hampered when the separate units cannot be given concrete tasks related to the general organizational objectives.
5. Benchmarking (or mutual comparison, in general) of activities will be obstructed when those activities are not similar.

At the end of the day the absence of a single overall measure of performance entails that the management and control of input and rendered contribution will take place in separate evaluation frameworks. The former happens in the budget cycle of the governmental organization, the latter in the policy cycle of the specific policy area. As a result the accountability with regard to management control is breaking up into a measurement of the financial control (based on a comparison of allocated and used budgets), and a measurement of generated activities (in terms of intended and realized objectives). This threatening divide and its ensuing partial approach of weighing issues can be illustrated by the usual systems approach (input - processes - output), as presented in Figure 2.

When the measurement of input and output is based on two different evaluations the assessment of management control will divide into two measurements:

- *Input measurement*. The value of the input is reflected in the available budget, so that measurement will only take into account that budget. The efficiency of the management control is identified with the economy in the spending of the budget and the objective of increasing the efficiency is made equivalent to budget reduction.

- *Output measurement*. The value of the management control is limited to the objectives realized with the output and the effectiveness of management control is identified with attaining these objectives. The extent to which the activities undertaken have contributed to a certain effect is not taken into account. Represented in a diagram (Fig 3)

Economy	*Transformation as a black box*		*Attainment of objective*
money ➡ input	➡ processes ➡	output ➡	effect (money)
Resources			**Contribution**
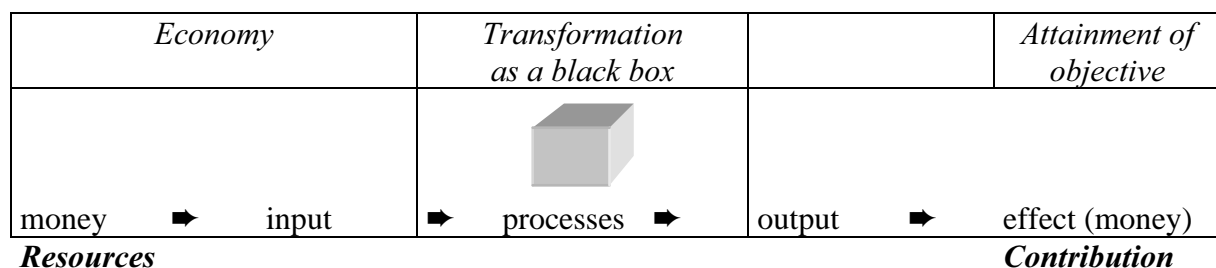
Figure 3: Economic behaviour in a governmental organization

In the following we will elaborate this divide and its consequences for management control in the defence organization.

3. Finance in military management control

The risk that assessment of management control on efficiency and effectiveness falls apart in two separate evaluations of the financial control and the military activities, is very real in the decision making on the Netherlands defence organization. After all, the decisions on the resources to be allocated are made while determining the National Budget, whereas the

contributions to be rendered are established in the NATO Defence Planning Process. An attempt to harmonize both these decision making circuits – complex as they are of themselves – is bound to run into many problems. The resulting shortcomings are, for instance, revealed in the calculation of the defence share in the national incomes of the member states. For the Netherlands, too, this share falls considerably short of the targets that have been established in NATO.

A good illustration of the isolated consideration of effectiveness and efficiency aspects in military management control can be found in the economy policy conducted in the first half of the nineties (Mol, 1995). After the – reduced - volume of the armed forces had been laid down in the *Defence Memorandum* (1991) and the *Priority Memorandum* (1993), a further budget reduction was imposed on the defence organization in the so-called November letter in 1994. Given the by now reduced volume of the operational units, this reduction could only be realized in the support units. Some thirty odd 'task forces' began to realize spending reductions in the budgets of these support units, laying down cuts in such activities as maintenance and logistic support, training and education, intelligence and research and accommodation and health care. These cuts were presented unreservedly as 'gains in efficiency' without further investigation into their effects on the actual combat power of the organization. In doing so, it was taken for granted that the effectiveness of the organization (in terms of motivation, quality and flexibility) would not be affected - and all this in spite of evident aversion these cuts appeared to encounter among defence personnel. For a sound decision making efficiency and effectiveness aspects should have been explicitly related. After all, a certain deployment capacity of operational units in terms of materiel and personnel can be seriously affected when the necessary support is undermined

The attempt to establish 'result-responsible units' in the defence Management Control Policy in the latter half of the nineties has failed to tear down the barriers between the resources and contribution compartments. Nevertheless, the evaluation of the allocation of resources on the basis of their output was the explicit objective of that policy. In order to achieve this, the application of contract management was to establish an unambiguous connection between the resources allocated and performance to be realized with them. This connection has not been established in the actual management contracts. As regards the performance to be realized, these contracts have been limited to inventories of performance indicators deemed relevant. However, so far, people seem to have been reluctant to introduce budgeting in terms of these indicators (Mol, 2000) There is no unambiguous responsibility of unit commanders for target levels with these indicators, nor has authority with regard to the allocation of means really been decentralized. It seems to be very difficult for the defence organization to make a definite choice for a management model. The traditional centralized model with its inherent bureaucratic decision making has by now been deserted, but the defence leadership seem to have second thoughts about the substantial decentralization that is at the heart of the result-responsible unit-concept. (*Sturingsconcept BLS,* 1999; cf. Heijnsdijk, 2000).

In our opinion it is this ambivalence that is hampering optimization at a centralized as well as decentralized level. Only an actual implementation of the drive for result-oriented management, widespread in public service, can effectuate a mutually coherent effectiveness and efficiency of management. In the next section we will describe how to achieve this implementation.

4. Efficiency and effectiveness in the armed forces

As is widely realized the management on 'result' in the armed forces faces the special problem that the operational employability of armed forces units can only with difficulty be translated into measurable results. In peacetime the actual result only consists of availability,

which in itself does not represent actual results. Crisis control missions are so frequently dominated by situation specific circumstances, that an assessment of their results remains precarious as well. Even if it can be established unambiguously whether and to what extent the 'crisis' – defined in whichever way – has been controlled, the contribution of the intervention to that control can still be open to discussion.

This has caused an extremely problematical relation between possible or actual effects of the activities of the armed forces and the allocation of resources for those activities itself. Most certainly so, in comparison with the business world that sells its products on a market and so gets immediate 'feedback' for the incurred expenses through the profits; but also in comparison with other public organizations, in which the performance measurement is less subjected to handicaps (such as the police, although, its activities are similar to the Royal Netherlands Military Constabulary, to a certain extent).

These limitations, however, do not imply there cannot be made a connection between resources and results at all. Even if the contribution of the resources cannot be defined in terms of the ultimate objective – the 'causa finalis' of the activities -, it can still often be expressed in intermediate targets as performance or activities. These intermediate targets consist of output or process indicators that can be seen as 'causa efficiens' of these activities. Control and assessment of the management on the basis of such intermediate targets have been schematically represented in the figure below.
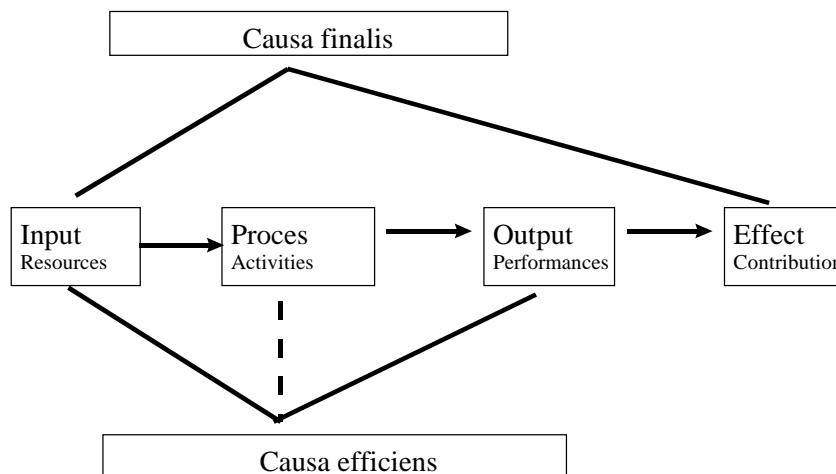

Figure 4: Intermediate targets

If it is impossible to make a causal connection between the activities rendered and the intended effects, the use of resources cannot easily be derived from these effects. In that case the use of resources and the matching result-responsibility will be based on the relation with the 'output' as intermediary management target. When the measurability of that output is defective, as is generally the case in the defence organization, that relation can be approached through an orientation on the activities [process indicators] (van den Hooven, 1999).

The key problem in determining efficiency and effectiveness in terms of those activities remains the question to what extent the indicators used can be deemed to adequately represent the intangible final objectives.

It goes without saying that in general the effectiveness of an organization must be measured on the basis of the eventual objective of its activities. Taking this as a starting point we could try to map the relevant aspects that determine the realization of that objective. To that end, Jägers and Jansen (1991), for instance, distinguish four criteria for measuring the effectiveness of an organization. The first criterion is the extent to which the demands and needs of the interested parties in the environment of the organization are met, in short satisfying

external demands. Following naturally from this is the second criterion, the extent to which an organization adapts and adequately reacts to its environment, the so-called flexibility of the organization. The third criterion concerns the way in which the needs of the internal participants are satisfied, the work satisfaction. Efficiency is the fourth criterion, which in this context refers to minimizing the claim on resources. Of course these four criteria mutually influence each other. Thus, the efficiency criterion will correlate negatively with other criteria. In the present tight labour market it proves to be difficult to recruit enough defence personnel and it seems the organization has trouble to present itself as an attractive employer. The criterion of work satisfaction is becoming increasingly more important for the effectiveness of the organization and it causes an increase in the labour costs as a result. When the willingness to make these costs is lacking, the recruitment of suitable personnel with the right qualifications is becoming more difficult which in its turn may affect the effectiveness of the defence organization.

The measurement of effectiveness in this sense will depend on the way in which the criteria are operationalized and the weight that is attributed to the distinctive aspects of the concept of effectiveness. The less concrete the final objectives are, the less relevance this measurement will have, making it all the more difficult to bring the use of resources unambiguously in line with the intended contribution. Especially in the defence organization this tuning is pre-eminently problematical, and a result-responsibility for the use of resources in terms of this ultimate effectiveness is beyond reach of the management there. However, in peacetime it is not the immediate deployment that is most important for the defence organization but only availability. Therefore the bulk of the defence expenditure is only related to that availability. An attribution of expenditures for the year 2000 to objectives, showed that an amount of almost 13 billion guilders out of a total expenditure of 14.2 billion guilders was related to availability (only 550 million guilders could be related directly to peace operations and international co-operation). In the allocation of resources it is this intermediate objective of availability that plays a prominent part.

With a view to this intermediate objective we can attempt to optimize the use of resources in the armed forces. The drive for efficiency and effectiveness expresses itself in the result-responsibility that is required of the units with regard to that availability. For operational units this responsibility can be described in general terms as the readiness of their personnel, materiel and operational readiness. A first initiative to quantify the availability is taken in the report *Operational employability of an F-16 squadron* (Visser, 2000). Here, operational readiness is divided into readiness of personnel and materiel. The readiness of personnel is subsequently specified with the help of indicators for 'proficiency' and 'realized training'. This initiative builds on an earlier – more theoretical – elaboration of the connection between means and contribution with the help of the 'value for money'-analysis (Van Slooten & Vijn, 1998). The amount of money required getting an F-16 ready for deployment was the central element in that analysis. This performance was subsequently broken down into economy, effectiveness and efficiency. This integral attribution of costs, however, does not yield any management information for alternative uses of the resources of production. In the short run the financial claim on the use of many resources is already fixed. The personnel costs, for instance, are largely unavoidable in the short term, as employees have permanent contracts. The alternative employment of personnel in terms of possibilities for use, however, can be influenced.

All the Services are currently setting up indicators for the readiness of personnel (manning, individual proficiency), readiness of materiel (employability) and degree of proficiency (operational readiness). At this moment the targets for both the operational as well as the support units are ready. Besides, the indicators for the operational units have been developed

and are being introduced. The indicators for the inter-service support units are still in the making, and their organization-wide introduction is scheduled for the budget for 2003.

Based on these indicators the units to be sent out could, in principle, not only be assessed on their readiness of personnel and materiel but also on their actual suitability for the operation. Thus the availability can, up to a certain extent, also be made concrete in criteria for operational readiness. The resources to be allocated can be related to the contribution that is intended with this readiness. The ensuing task budgeting of result-responsible units enables their management on the basis of financial information with respect to the avoidable costs. Thus, the effects the handicaps in management control summed up by Anthony and Young (1999: 49-51) can largely be reduced .

5.   Summary

In this article the role of financial information in the armed forces is discussed against the background of economic behaviour. Economic behaviour envelops the optimization of the relation between resources and contribution. If resources as well as contribution can be expressed in an overall criterion (money), a mutual tuning between the claim on resources and contribution can take place. In the armed forces the public contribution is in principle not traded on a market, so that the profits are not expressed in financial terms. The absence of this overall criterion makes it impossible to assess to what extent the claim on resources is justified by the contributions. Apart from that it is also very difficult to quantify the contribution of the armed forces in other terms and to link them to the claim on resources. This has led the present practice of the management control taking place in separated compartments of resources and contribution, where the concepts of efficiency and effectiveness have been degraded to economy and goal achievement, respectively. The creation of intermediate objectives allows a partial opening of the compartments. An intermediate objective par excellence is the availability of the armed forces in peacetime. A recent calculation has shown that approximately 91% of the expenditure is related to this intermediate objective. With the help of this intermediate objective efficiency and effectiveness can once again acquire meaning for the armed forces.

References

Anthony, R.N., Young, D.W. (1999), *Management Control in Nonprofit Organization*,
    Irwin/McGraw-Hill, Boston
Bakker, E.J. de (1998), *De rol van kosteninformatie bij de bedrijfsvoering van de krijgsmacht*
    [The role of cost information in armed forces management control]
    Ph.D. thesis, Tilburg University (KUB), KMA, Breda
Heijnsdijk, J. (2000), De rol van de financiële functie in de bedrijfsvoering van defensie.
    [The role of the financial function in armed forces management control],
    in: J.A.M. Oonincx (red.), *Militaire Accountancy & Control*: 3-43
    Tilburg University Press, Tilburg
Hooven, H.M. van den (1999), Geld speelt (g)een rol [Money does (not) play a role]
    in: *Parade*, 20, 1999, 2: 86-95
Jägers, H.P.M., Jansen, W. (1991), *Het ontwerpen van effectieve organisaties* [Designing
    effective organizations], Stenfert Kroese, Leiden/Antwerpen

Mol, N.P. (2000), Accounting voor resultaatverantwoordelijkheid [Accounting for result-responsibility], in: L.M.W. de Bie (red.), *Management Control voor Commandanten en Controllers*: 87-96; KMA, Breda

Mol, N.P., *Defence planning and budgeting in the Netherlands: the quest for efficiency*, paper presented at the 9th session of the Defence Economics Workshop, NATO Economics Committee

Slooten, G. van, Vijn, R.M. (1998), *De 'Value for Money-analyse toegepast op een operatio-neel onderdeel* [The Value for Money-analysis applied to an operational unit] Research Paper FMB 98-43, KMA, Breda

Sturingsconcept BLS (1999), [Management concept of the Commander in Chief of the Land Forces], Landmachtstaf, Den Haag

Visser, W.S. (2000), *Operationele inzetbaarheid van een F-16 squadron* [Operational employability of an F-16 squadron], Student thesis, University of Twente, Enschede, December 2000

Result-responsibility and integral information processes

J. Heijnsdijk, J.A.M. Oonincx

1.   Introduction

In recent research and discussions both authors have shown that choosing a management concept is only one side of the coin, and that implementing it is quite another. The way of handling information plays an essential role in this. It can be said that many commanders of result-responsible units within the defence organization struggle with the question of what constitutes the most suitable information design for internal management. But also the executive and commanding level above the result-responsible units is searching for an optimal information provision from and about these units. Finally, there is much intensive study into the most adequate information provision from the Secretary and Minister of defence via the so-called TOP-report.

In this contribution the question of internal and external information provision within and about result-responsible units in the framework of the BBD 2000 management philosophy is considered in more detail, from the angle of integral responsibility.

After a general description of the concept of information provision (section 1) the following topics will be dealt with in this contribution:
- The importance of and requirements for information provision (sections 2 and 3);
- The TOP-report of the MoD (section 4);
- Information provision within and about result-responsible units and empirical research (section 5).

2.   General

As a result of a number of calamities and serious incidents the former Minister of Defence, J. Voorhoeve, tasked J.A. van Kemenade to conduct an investigation into the truth-finding with regard to the Srebrenica affair. In his report of 28 September 1998 Van Kemenade states that the integrity of the armed forces is not under debate. There is no indication of a conscious obstruction, hindering or restriction of the truth-finding process by any persons in the defence organization. The report, however, does uncover a number of serious shortcomings and instances of carelessness that have occurred in the defence organization over the past years in the process of information gathering and information processing. Incidentally, these shortcomings can be explained by the radical change processes and the great time pressure under which people had to work.

Van Kemenade concludes that:
1. in the past years not all persons responsible were timely and adequately informed and that consequently the internal communication was seriously flawed;
2. information often has to be assessed under great time pressure, with modest resources and (too) few personnel;
3. information gathering and information processing have become increasingly complex in peace operations, involving several ministries and departments within the defence organization;
4. defence personnel sometimes dealt with the information in a cramped manner;
5. there is a tendency to label information on defence matters too quickly as secret.

Van Kemenade explains these shortcomings as stemming from the fear among defence personnel that reporting problems and incidents might harm one's own career, unit or service. Often, important information is mistakenly seen as an exclusive matter for the own unit or service. It goes without saying that the Ministry of Defence (MoD) is learning from these experiences (lessons learned), and the recommendations made in the Van Kemenade report have been implemented. Subsequently, measures have been taken to improve the situation with regard to the management information provision.

Information provision has the undivided attention of the MoD and any further measures yet to be taken may not have an ad hoc character, but must be based on the requirements and principles of adequate information provision during calamities and serious incidents. The implementation of the management philosophy, *the Defence Management Policy 2000* (BBD 2000), too, will lead to a considerable improvement of the information provision both within and about the defence organization. Within the organization there is a clear recognition and conviction that the adequate deployment of ICT will be at least a relevant, if not determining, factor for the success of its functioning. This applies to the military management, the command and control, the generating of combat strength and to national and international deployment in case of war and conflict containment. Fortunately, it is recognized within the organization that ICT determines striking power; that it has become the heart of the management, that it is the determining factor in the running of primary processes and that it forms the most important component of weapons and command systems.

3.   Requirements for information provision

What does the MoD, but also Parliament want to know about the defence organization?
a.   In any case there should be an insight into the performance indicators of the armed forces and the result-responsible units inside the organization by means of the annual reports.
b.   Furthermore, it is extremely relevant to be informed about the operational readiness and availability of the services.
c.   It should be possible to determine whether the targets have been reached.

If the target of information provision is to be reached, then well known requirements, such as relevance (meeting the information demand), completeness, accessibility, organization and consistency will have to be met. These requirements have been sufficiently documented in the standard literature, and therefore they will not be dealt with here. However, six requirements that are at present of crucial importance will be discussed below.

The information necessary for the organizational control as well as for the accountability has to be *transparent*. This transparency is attained through adequate implementation and TOP-reports. In the implementation report the (sub-)commander indicates whether the targets have been reached and at the same time account is given of the resources used. The reports are analyzed and, subsequently, targets or improvements are formulated. If necessary, corrections are made. In this manner the policy and implementation of the activities within the services and their result-responsible units are made transparent.

A second requirement is that the information provision meets the demands of the receiver with regard to *form* and *content* and it is preferably realized in good mutual understanding between the provider and the receiver of the information. The information provider, however, will be given a say in what is deemed relevant information about his result-responsible unit. The discussion about the report will reveal whether this corresponds fully with the needs of the receiver. The defence practice has been different for many years, when all too often the same rules, regulations and uniform report formats were applied, irrespective of the type of

result-responsible unit and the level in the hierarchy. It goes without saying that the receiver makes his information needs known to the authors of the reports in advance.

The third requirement concerns the *selectivity*. It should be prevented that everything that happens is reported, as too much and too detailed information usually gets in the way of the intended target. The information provision will mainly have to be directed at supplying mission-critical points of the unit, something that does not happen enough at the moment. Suitable indicators can play an important role in this.

Inside the defence organization *security* begins to play an increasingly prominent role. It concerns the security of persons, material, information and information systems. More and more the defence organization becomes dependent on the information systems used, and the systems are increasingly becoming vulnerable to all sorts of infringements. The dependency on continuous availability and trustworthiness of ICT has become so great that the collapse will be total is the systems go down. The security of the information systems has to reduce the vulnerability to acceptable proportions and to that end information security plans are set up for the vital systems.

The fifth requirement is that of *integration*. Until the present moment, there has been little integration between the accountancy, the management and the operational information systems. The complete separation of information systems for peacetime management and the operational battlefield information systems is not a felicitous one anymore at the beginning of the 21st century. It makes it extremely difficult and costly to get the necessary information, as, in new types of deployment, internal management and command and control are two sides of the same coin and operational and effectiveness aspects deserve equal attention. The commander cannot any longer rely exclusively on information from only one system, as this will confront him with a serious information problem in his decision making. Naturally, war and peace enforcement necessitate specific information about the adversary, the weather and terrain. The information itself on all relevant aspects has become an integrating factor in the decision making.

The last requirement is *interoperability*. In peacetime as well as crisis situations and operational actions the information systems should be able to communicate with each other. Interoperability, therefore, has become a crucial success factor for the future of information provision. ICT is only effective and efficient if it can be used by all the partners in an international mission.

These requirements are contributory to the future information provision in the armed forces. In the following section we will discuss the way in which the MoD tries to realize them in the so-called TOP-reports, by means of an analysis of a number of reports presented so far.

Subsequently, we have tried to describe the use of the information. The extent to which the information acquired was actually used to reach the objectives described in BBD 2000 is an indication of the quality of the information provided (section 5).

4.   TOP-reports

The first quarter of 1999 saw the advent of the TOP-report - integrated cyclical reports about past activities and present state of affairs in the business units, the definite form of which will be developed over a period of several years. The TOP-reports are written by the Chief of the Defence Staff, the CinCs of the four Services (Navy, Army, Air Force and Military Constabulary), the Chief of the Defence Interservice Command, as well as the Deputy Permanent Under-Secretary, and is presented to the Minister and the Secretary of Defence by the Chief of the Defence Staff and the Permanent Under-Secretary.

4.1 Content of TOP-reports

The TOP-report is intended to give an insight into the relation between the targets, activities and resources. In this way it is possible to realize the task and change objectives of the Defence Memorandum 2000. The result of this reporting on the policy areas of the inner department may be an adjustment of the targets, activities and resources. In order to be able to do this the TOP-report contains information on:

- the implementation of primary tasks
- important management aspects
- resource management

In the report use is made of so-called *indicators*. In the Royal Netherlands Army (RNLA) the most important of these are gathered in the *dashboard* of the Commander in Chief (CinC), and together they form his management tools. This procedure guarantees transparency and, as far as the RNLA is concerned, also integration of information.

In the reports of the Royal Netherlands Navy (RNLN) the realization of the primary product (deployable units) is described by means of tables and indicators. Here, too, there is a division into primary tasks, management aspects and resource management. Because of the orientation on output there is a selectivity of information, which satisfies the needs of the receiver (form and content).

In the Royal Netherlands Air Force (RNLAF) report information is given about re-organizations and personnel and of course about the three areas indicated above. As for the primary task, this involves operations and activities that took place under the responsibility of the CinC, exercises and preparation programmes and tasking targets of operational readiness. As to management aspects, it concerns information about the following: improved management project, workload and work pressure, reorganization, planning and control, audits, targets of the CinC for special projects, maintenance and progress reports on major materiel projects, the productivity of supporting units, training and education of personnel, safety, occupational health and environment.

Resource management in the Air Force involves personnel as well as financial resources and any bottlenecks in the three major areas will be reported. Possible solutions will be indicated and have to be accompanied by estimates of their effectiveness and efficiency. Because the focus of attention is on bottlenecks there is also selectivity of information and transparency. This selectivity allows the Air Force commanders to use management by exception. It should be possible to use an adequate TOP-reports an integral management tool in the assessment and possible adjustment of the strategy and policy. This also involves taking the necessary actions and translating them into measurable and checkable agreements. Of course the reports can never be complete without a prognosis about the future.

4.2 Information about the primary tasks

On the level of the Services primary tasks involve the units' or individual serviceman or woman's readiness for carrying out the tasks in the various operational areas and national tasks in the short or long run. It concerns information about missions abroad, logistic support, the degree of training and all other matters that determine operational readiness.

At the same time bottlenecks are reported. It is no secret that the quantitative and qualitative appointment of personnel gets much attention at this moment. Shortages of logistic, supply, ICT, maintenance and technical personnel as well as drastic reorganizations have a great impact on the possibility to send out units and individual service personnel on humanitarian and peace missions. The provision of information is in part intended to propose ways to remove these bottlenecks. With respect to personnel this can be done by further improving labour conditions and fringe benefits, increasing recruitment activities, reducing wastage during training, etc. Much used indicators in the RNLA are:

- level of practice in comparison to planning
- service personnel sent out
- support
- appreciation by society
- satisfaction of personnel.

In case an expectation is not (fully) realized, every indicator is accompanied by an explanatory analysis, which lends transparency and selectivity to the information.

In the case of the RNLN, information is given about the readiness term for the various business units. It shows how many days are needed to have frigates, ships, planes, battalions, platoons, etc. ready for deployment. The RNLAF works with tables showing the period of deployment in operations as well as the practice periods, specifying the name of the operation or exercise, units, number of personnel and other particulars. For both the RNLN and the RNLAF there is management control and information provision, directed at benchmarks with regard to previously specified indicators. This will guarantee transparency, selectivity and a suitable form and content of the reports.

4.3 Information about management

Under this heading information is given about the implementation progress of the *Defence Management Policy 2000* (BBD 2000) for the four Services. Many of the measures for improvement derived from the implementation targets are directed at increased transparency of the management of the Services. Possible topics in the information provision are authorization, transparency of targets and target attainment, integral management budgeting, cost insight, audit plans, integral quality management, information architecture, and the replacement of information systems.

Authorization implies that in the course of 2000 all units at result-responsible level will have the authority and resources (materiel, personnel and budgetary) to enable their commanders to bear integral responsibility (and with it, unequivocal accountability) for the implementation of their tasks. To this end all requirements and criteria for decentralization and management at arm's length will have to be met. In the last two years extra emphasis has been given to financial control, of which the orderliness, controllability and effectiveness must be guaranteed. Indicators use by the RNLA are:

- trained personnel
- pass rates
- targets of the Commander in Chief
- progress of BBD 2000.

In the RNLN this part of the report gives information about targets for change, productivity of support units and personnel. To every target for change (for instance, increase of percentage of female personnel in the RNLN, implementation of BBD 2000, the introduction of the Euro, and improvement of financial control) an indicator is attached with three positions: realization runs according to schedule, realization runs behind schedule, realization runs ahead of schedule. The action meter also indicates progress in the previous quarter, the present quarter and expected progress in the coming quarter. The productivity of support units mainly concerns information about maintenance, major materiel projects (running behind or on schedule) and personnel (actual strength, influx, flow-through, outflow). The information on management in the RNLAF is mainly of a descriptive nature.

4.4 Information on resource management

The information on resource management mainly concerns the influx and realization of financial (budgets), materiel (materiel projects) and personnel resources (appointments).

Indicators used by the RNLA are:

- cash realization
- budget realization
- appointment realization of short-term or long-term personnel
- progress of major materiel projects.

In the RNLN resource management mainly concerns financial budgets, subsidy and investment realization. Here, too, the information provision clearly seems to show transparency and selectivity.

In the RNLAF especially bottlenecks in supporting materiel and personnel, infrastructure and spare parts are given attention to. Besides, figures and facts are supplied about personnel, such as level of recruitment (level of occupancy), reduction of civilian staff, recruitment of military personnel, influx and outflow, sickness absence, etc. The financial information concerns budget realization and cash prognosis of expenditures and receipts.

In conclusion it can be said that the most recent developments within the framework of TOP-reports have led to more transparency and a better form and content of the information provision. By working with indicators (amongst others, for the benefit of the 'dashboard') selectivity has improved; the information provision has been adapted as far as possible to the demands of the decision makers (the top of the defence organization). Integration and interoperability requirements still deserve attention. The interaction between information systems (management, command and control, international adjustment) remains vital for attaining integral management on all levels of the defence organization.

5. Information provision within and about the result-responsible unit

In this section the information provision within the result-responsible unit will be dealt with. In doing so, the characteristics befitting an integral manager commander in an organization where the management is reasonably decentralized, will be described. The results of empirical research are also subject of discussion here, and commanders (and up to a certain extent also their controllers and accountants) will indicate in how far they are of the opinion that the information provision does indeed meet the requirements of the integral manager.

First of all in 5.1 the use of information by commanders is discussed and it will be seen to what extent commanders use information for the benefit of strategy and policy, accountability to the higher level and other interested parties. After that the criteria for the information of the commanders will be dealt with: legitimacy, efficiency, effectiveness and quality (5.2). The subject of 5.3 is the extent to which commanders make use of financial, operational and management audits. Finally, in 5.4, (modern) management techniques used by commanders in managing their units will be discussed: indicators, balanced score card, SWOT-analysis and scenario planning.

5.1 Use of information by result-responsible units

The information provision in the TOP-reports is based on the information received from the commanders of the result-responsible units. In such a result-responsible unit information is gathered in order to manage the unit and to give account about this management. Since its introduction in 1993 the application of a decentralized integral management concept with authorized competence, also for the financial function, has been at the heart of management. The commander bears integral responsibility within this decentralized management concept for the realization of the output as agreed upon in the management contract or covenant. A commander may be explicitly held accountable as he is not only responsible for the results, but also for the financial control and the financial consequences of his actions within the apportioned budgets. This implies that the information for the benefit of the commander is not only directed at the accountability to a higher echelon, but also towards the strategy and

policy of the result-responsible unit and the internal process control within the framework of the management. The commanders and controllers were asked to indicate for what purpose they used the information gathered, allowing them a choice from among the following possibilities:

- strategy and policy
- process control
- accountability to the higher level
- accountability to other interested parties.

'Strategy and policy' and 'accountability to other interested parties', in particular, are elements that belong to the integral manager in the armed forces. In Table 1 the answers of the commanders and their controllers are presented.
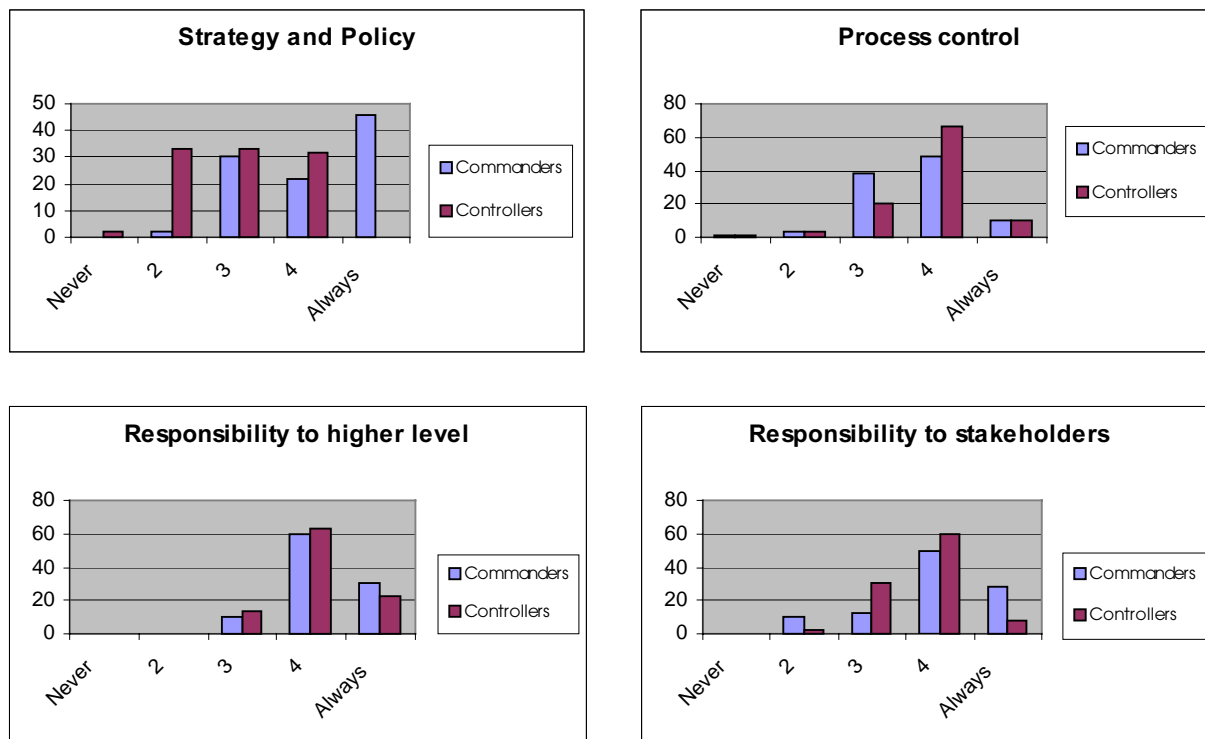

Table 1: The use of information

It clearly indicates that commanders to a large extent (67%) use information for formulating the strategy and policy within their unit; controllers, incidentally, score considerably lower in this respect. This means that the commanders do indeed involve themselves in strategy and policy matters and do not limit themselves to waiting for assignments from a higher level and in doing so, they use the information to give form and substance to their own strategy and policy.

In the opinion of the commanders (90%) and controllers (82%) information plays an important role where the accountability to the higher echelon is concerned. The score for 'other interested parties' is also high, which indicates that the commanders interpret their responsibility to be wider than only to the next higher level.

5.2 What does a result-responsible unit commander use his information for?

For the commander integral management within the context of result orientation implies that he will have to answer a number of main questions for his result-responsible unit, such as:

- what targets is my management directed at?
- what do I want my commander to steer me on in my unit?
- what are the consequences of this for the organization of my unit?

In order to be able to answer these questions the commander needs information and information systems. As not all commanders have an equally well developed sense of financial administration, information systems, economic control and budgeting, it is likely that a controller or an information expert will be employed in this. Integral management is not possible without adequate management reports and ICT takes up an important position in this. The management will have to be supported by adequately analyzed and documented figures. This brings us to integral information provision, management information provision, the application of management accounting, use of indicators, administrative organization and internal control. Every result-responsible unit, therefore, faces the challenge of developing a system of internal and external information provision. This implies the designing or purchasing of suitable management information systems, amongst others, a cost information system, which can give the commander cost information to be used in answering the question whether good products are delivered at the lowest possible cost. Important criteria to assess the functioning of a unit are:

- legitimacy of expenditure (this has always been important for the controller)
- efficiency in the form of the relation between planned and realized cost
- effectiveness as an indicator of the extent to which the targets have been reached
- quality (of all processes).

The latter three criteria, in conjunction with the integral responsibility of commanders, have become increasingly important over the past few years. Simultaneously, the role of the controller has expanded. Apart from legitimacy, the commander and his controller have to see to efficiency (cost reductions), effectiveness (output management) and quality (at the moment formulated in terms of the INK model Netherlands Quality Institute). The extent to which commanders, controller and accountants use information in order to assess units on these aspects is shown in Table 2 (next page).

It is clear that the commanders of units have a high score for each of the criteria for information gathering – legitimacy 63%, efficiency 74%, effectiveness 79% and quality 67%. This proves that the military commanders keep a good eye on each of these criteria when doing justice to their integral responsibility. The commander who is only interested in 'funken, fahren and schiessen' appears to have become obsolete. Indeed, in managing their units the majority of commanders clearly bear the quality and efficiency of the management process in mind.

For the controllers of the units the scores for 'legitimacy' and 'efficiency' compare to those of their commanders, whereas they score considerably lower for 'effectiveness' and 'quality', As is to be expected, accountants score very high for 'legitimacy' (100%), but, compared to commanders and controllers, considerably less for the other three criteria. It appears that, except for legitimacy, accountants in the armed forces (still) have insufficient means to assess units on the above-mentioned management criteria.
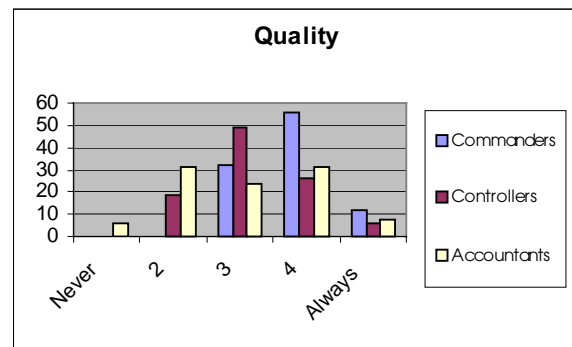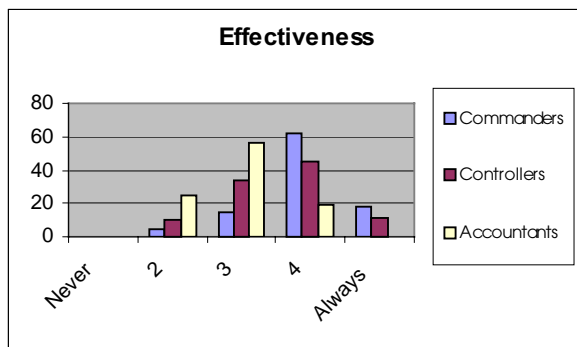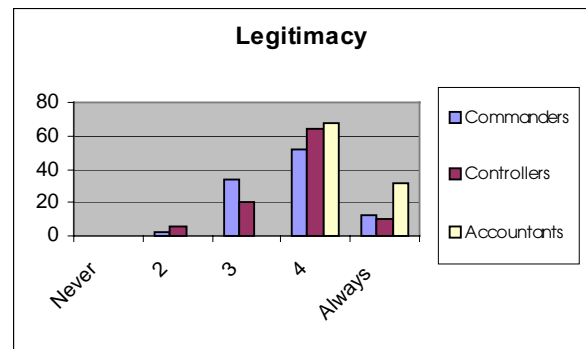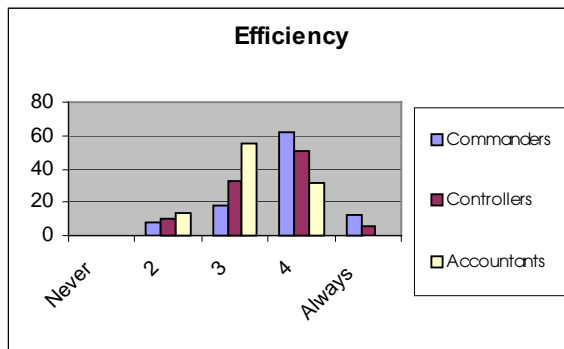
Table 2: What is the information used for?

5.3 What role do audits play in the information gathering of commanders and controllers?

In the 1993 and 2000 BBD audits form an important aid to measure the criteria of efficiency, effectiveness and quality. There are three types:

- financial audits, which concern the quality of the financial policy and control in a unit
- operational audits, directed at the quality of the management processes
- management audits, lending a certain value to the quality of the organization and the management of the result-responsible unit.

It can be expected of an integral manager that he will gather information with the help of these audits. After all, he manages the processes in his units (operational audits), he has to attend to efficiency (financial audits) and the quality of his organization (management audits).

Table 3 (on the next page) shows that many commanders make use of financial audits (56%), operational audits (59%) and management audits (44%). Operational and management audits are used considerably less by controllers of units and by accountants in the armed forces. These scores indicate that many commanders are not only interested in operational affairs, but most certainly also in the costs (efficiency) and, to a somewhat lesser degree, the quality of the organization (management audit). It confirms the impression that a large number of commanders are developing into the direction of integral manager.
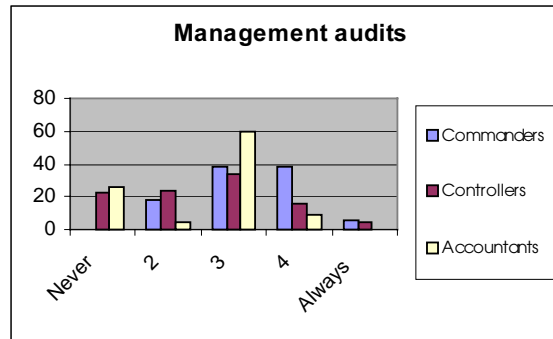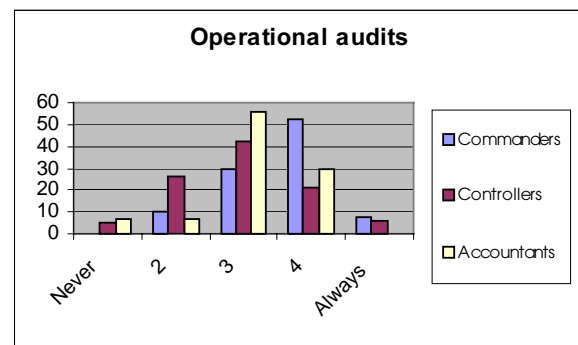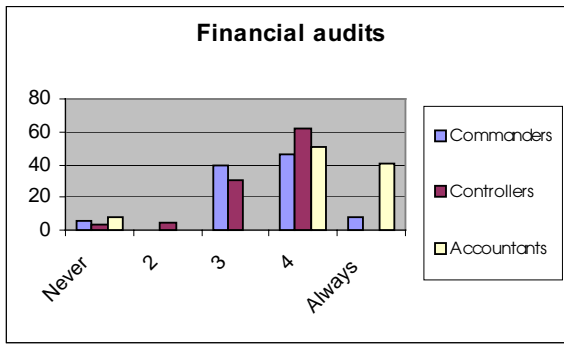
Table 3: Use of audits by commanders

5.4   Management methods and techniques used by commanders

Information about the performance of a result-responsible unit is essential. In a number of situations this is a problem in that this performance must be measured. In particular in operational units this has not sufficiently been solved yet. The designing of measurement and assessment norms is not always easy either, which may cause an information hiatus. The use of indicators as information providers is emerging strongly. When they are used as a means of obtaining information the principle of the selectivity of indicators is violated more often than once in the armed forces. On the basis of the critical success factors in a unit it is usually possible to determine the essential indicators. Making long lists containing lots of indicators is, generally speaking, not useful at all. Nor is it sufficient only to use financial indicators.

Other performance norms will have to be developed as part of the strategy, especially with a view to measuring effectiveness, a factor in the management process ('balanced score card'). Using this card yields a coherent set of performance norms particularly directed at financial, economic, internal, customer and other development perspectives. When filling out the card the manager is forced to concentrate on the essence of the strategic policy and the ensuing targets for improvement. The commander can also use the balanced score card in the information section of his report as an instrument for giving account of the implementation of the management contract. Of course the information provision can also be realized by means of other models. In the armed forces the INK model is also being studied or even used as a medium for reporting. In our empirical research we have asked the commanders to what extent they make use of:
- indicators
- balanced score cards
- SWOT-analysis
- scenario planning: a means to prepare a result-responsible unit for possible alternative expectations for the future.

These techniques are mentioned in BBD 2000 and earlier policy document with regard to modern management forms within the armed forces. Table 4 gives a survey of the results.
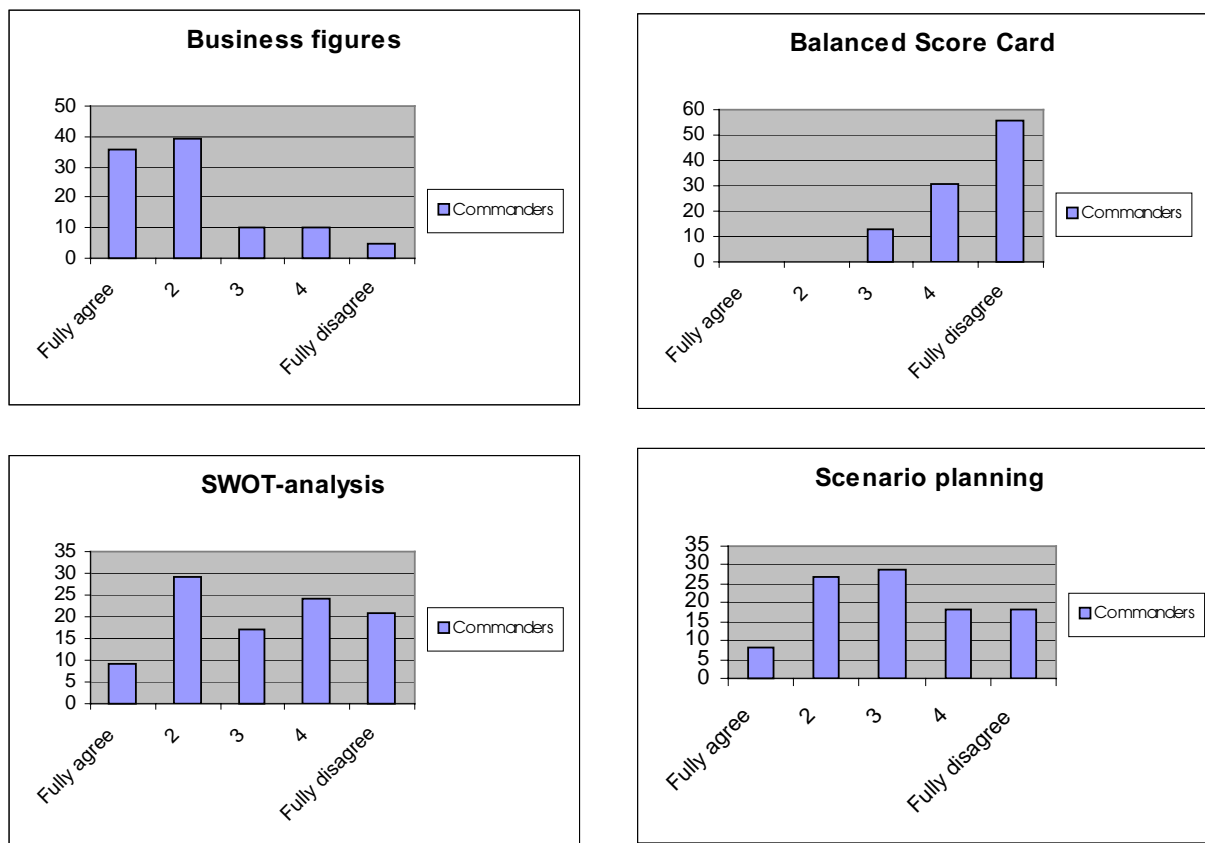
Table 4: Use of modern management tools

Many commanders (78%) make use of indicators. For scenario planning and SWOT analysis this lies just below 40%, while the balanced score card is hardly used. It is clear from these figures that modern methods and techniques to support and foster integral management are only used by an as yet limited number of commanders.

6.   Conclusions

It is possible to draw a number of conclusions from the following data. First of all, managers do not only assess the legitimacy of management processes, but also the efficiency, effectiveness and quality on the basis of the information they obtain. Secondly, apart from using the information for process control and accountability to higher echelons, the commanders also use it for their strategy, policy and accountability to other interested parties. Finally, next to operational audits the commanders make use of financial and, to a lesser extent, management audits.

These findings justify the conclusion that many commanders are developing into integral managers and are learning to pay attention to multiple aspects that determine the effectiveness of their units. Form, content and transparency of the information allow the top managers and commanders of the result-responsible units to manage their units. The simultaneous use of indicators, in particular, ensures a high degree of selectivity of the information provision. The

linking of the information from management information systems and command and control systems (integration) in non-peace situations, still causes considerable problems. Solving them can lead to an integral approach to management problems within the result-responsible units (especially in peace situation), which would realize a major target of the defence management policy.

References

Heijnsdijk J. (1999), Resultaatverantwoordelijke Eenheden: papier of werkelijkheid? [Result-responsible units: paper or reality?], in: *Militaire Spectator*, 168, 9: 494-500

Heijnsdijk J. (1998), *RVE binnen defensie; stilstand of vooruitgang?* [RVE within the armed forces; standstill or progress?], KMA, Breda, Research Paper FMB 98-46

Heijnsdijk J. (1998), Beleid Bedrijfsvoering Defensie; Transparant en integraal management in de defensietop? [Defence Management Policy: Transparent and integral management at the top of the MoD?], in: *Militaire Spectator*, 167, 11: 468-472

Heijnsdijk J. (1999), Sturingsconcept BLS: einde van het RVE tijdperk [Management concept of CiC Land Forces: the end of the Result-responsible unit-era]
in: *Parade*, 20, 3: 43-48

Heijnsdijk J. (2000), De rol van de financiële functie in de bedrijfsvoering van defensie; een empirisch onderzoek onder RVE-commandanten, controllers en accountants [The role of the financial function in defence management; an empirical survey (etc.)]
in: J.A.M. Oonincx (ed.), *Militaire Accountancy & Control*: 3-43
Dutch University Press, Tilburg

Kemenade J.A. van (1998), *Omtrent Srebrenica; een rapport over de verzameling en verwerking van informatie door de defensie-organisatie over de gebeurtenissen rond de val van de enclave Srebrenica* [About Srebrenica; a report on the processing by the MoD of information about the fall of the Srebrenica enclave]
Ministerie van Defensie, Den Haag

Oonincx J.A.M. (1997), Commandant, bedrijfsvoering, RVE en VEB [Commander, management, Result-responsible unit and Improved Economic Control]
in: *Militaire Spectator*, Vol. 166, 7: 310-316

Oonincx J.A.M. (1998a), Informatie-adviseur: toch maar niet [Information consultant; I think not], in: *Komma*, 20, 1: 24-28

Oonincx J.A.M. (1998b), IT in de krijgsmacht: evolutie of revolutie? [IT in the armed forces: evolution of revolution?], in: *Militaire Spectator*, 167, 10: 506-513

Oonincx J.A.M. (1999), Controller, control en informatievoorziening [Controller, control and information provision], in: *Militaire Spectator*, 168, 9: 486-493

Part Three

The role of information in an operational context

The role of communication and information in civil-military cooperation in humanitarian operations

M.T.I. Bollen, A.L.W. Vogelaar

1.   Introduction

Ten years into the post Cold War era have shown many humanitarian disasters caused by war. In the wake of these disasters many relief organizations emerged to give humanitarian aid. Nowadays, there is a great variety of actors working in the field of humanitarian operations in order to cope with the demands made by the security environment of the 21st century.

The players in the humanitarian field have many origins: international military and civilian organizations, like the United Nations, whose members are nation states; non-governmental organizations (NGOs), like Memisa or Médecins sans Frontières (MSF); the International Committee for the Red Cross; transnational corporations; and the authorities of host nations. They are in fact any group that has the will and the potential to help in specific crises. All the organizations providing aid in crises have their specific working field, operating alongside each other and, where and if necessary, collaborating with each other. They are in some instances very different from each other and often they are not traditional collaboration partners at all.

Two reasons seem to account for the growth of organizations in this area and the resulting non-traditional coalitions that are necessary. Firstly, the transnational characteristics of the new security issues require another division of labour in which neither the military nor any other single organization or nation is able to solve the problems on its own and a multi-actor approach is called for. Consequently, a wide variety of civilian and military actors, who generally have not met before, find themselves working on a shared problem. Secondly, because of the uncertainty amongst the traditional players regarding the approach to the new security issues, new actors have stepped into the void.

In this article we will examine one field of such non-traditional multi-actor collaboration: the military's relationship with civil organizations and institutions in humanitarian operations. In the British Joint Warfare Publication - an important pillar on which the Dutch Army Doctrine on peace support operations is founded - humanitarian operations are defined in the following way:

> Humanitarian operations are conducted to relieve human suffering. Military humanitarian activities may accompany or be in support of humanitarian operations, conducted by specialized civilian organizations (JWP 3-50).

It is in the interest of the military as well as the civilian organizations and institutions that good civil-military cooperation relationships are established in the operation for a number of reasons. Firstly, humanitarian emergency situations may be too dangerous for civilian organizations to handle on their own and they may require security. For instance, the military may provide for the safety of the environment in which medical treatment is given by MSF. Also, other specialized help from the military, such as the clearing of mines or logistical support may be required and complementary tasks of this nature imply good relationships. Secondly, humanitarian help and the resulting build up of a country often require a long-term response, whereas military assistance to humanitarian operations may only be needed on a temporary and complementary basis. This means that military humanitarian missions often have to be supportive of other organizations and short-term oriented. After a certain period of

time the international military community may leave the area of operations. Humanitarian organizations usually stay involved over a longer period. It is important for the military to timely transfer their responsibilities to civilian authorities and humanitarian organizations.

Below we will present a number of measures that may help to improve the cooperation between the military and civilian organizations during humanitarian operations. Our arguments centre around the concepts of building confidence, trust, and control between the organizations and we will go into the roles of communication and information exchange within and between the organizations in this process. First we will outline the complexity of civil-military relationships during humanitarian operations, after which we will describe the concepts of confidence, trust, and control and analyze how these concepts contribute to the mutual cooperation between members of different organizations. In the final section of this article the importance of the role of interorganizational and interpersonal communication and information exchange in the process of creating partner confidence, trust, and control is discussed.

2.   The complexity of civil-military relationships during humanitarian operations

Although in recent years there have been examples of mutual benefits to be gained by civil-military cooperation in humanitarian operations (e.g., both the logistical support of the military during Operation Support Hope in Northern Iraq in 1991 and the logistical assistance provided by NATO in Albania and Macedonia in 1999 facilitated the work of humanitarian organizations), there are many instances to show that good working relationships in the field do not occur naturally. One of the circumstances preventing satisfactory civil-military cooperation may be differences of opinion among civilian relief organizations about the appropriateness of the involvement of military troops. To some humanitarian organizations, association with the military remains a sensitive matter to be limited as much as possible. For instance, in the case of the above-mentioned military support by NATO during the Kosovo refugee crisis, MSF have remarked: 'Although heavy logistical assistance has been useful, NATO is first and foremost a military organization which is currently involved in conflict and not a humanitarian actor.' The NGO believes the military is neither responsible for nor able to coordinate relief activities for the refugees (Press conference Skopje, April 9, 1999; in: Minear et al., 2000). During the same crisis the United Nations High Commissioner for Refugees (UNHCR), on the other hand, considered collaborating with the military to be necessary in order to support the refugees more adequately. As a result, the UN-organization was criticized widely by aid agencies for giving up too many of its humanitarian responsibilities to NATO (Minear et al., 2000).

In an article on cooperation between the military and UNHCR Wolfson (1997) identifies yet other circumstances standing in the way of civilians and the military cooperating. According to this author, problems between civilians and the military may arise from differences in organizational behaviour in both types of organizations. Like most NGOs, UNHCR approaches its humanitarian tasks in a utilitarian way. By this Wolfson means that relief goods and funding will be deployed in such ways that as many refugees as possible will be able to benefit from the aid given. Because of the high degree of uncertainty concerning the amount and timing of humanitarian means and funding, UNHCR and NGO staff are expected to be flexible in the extreme. The operational conduct of the military, on the other hand, is based upon maximum preparation and planning. Means and funding are calculated beforehand and the designations are fixed. Military staff is expected to behave in accordance with their mission and within their given mandate, until officially revoked by their superiors.

Other problems may arise as a result of diverging organizational cultures which manifest themselves, amongst others, in different views on leadership and decision making processes.

NGOs and UN-organizations, such as UNHCR and the World Food Program (WFP), rely heavily on decentralized field offices to coordinate the humanitarian tasks at hand. Field offices are staffed to a minimum and more often than not field workers are stretched beyond their limits in their efforts to solve the problems. Under these circumstances civilian staff has to operate highly autonomously. Therefore, the role of field-managers cannot be compared to the role and functioning of military commanders because the chains of command and the formalized decision making processes which the military are accustomed to are lacking.

Not only do the military and civilian institutions differ on these and other organizational root-aspects, at the same time both parties are attached to their own way of life. They often appear to be ignorant of the organizational patterns of behaviour of their counterparts or else regard them with disdain. Because of these differences civil-military cooperation in humanitarian operations usually does not occur naturally, and relationships prove to be far from simple.

Based on the above mentioned aspects, on literature on crisis management and civil-military cooperation (Seiple, 1996; Gordenker & Weiss, 1993; Frerks, 1998; Maynard, 1999), and on the influence of crisis-situations on the development of trust (Webb, 1996; Mishra, 1996; Creed & Miles, 1996), we propose the following set of characteristics to account for the complexity of civil-military cooperation in the field:

- *Context-related characteristics*: humanitarian operations are mostly characterized by the following stressors: human suffering, threat, time pressure and the lack of resources and supporting structures. Under these conditions the humanitarian support goes on around the clock. At some time both sets of actors are overcome with exhaustion, which provides fertile soil for mutual grievances and frustration to fester.

- *Organization characteristics*: Hierarchical relations between civilian and military organizations are non-existent. Therefore, interorganizational processes during operations cannot be coordinated by traditional mechanisms. Furthermore, representatives from both kinds of organizations have different working styles, originating from the hierarchical structures of their own organizations, e.g. a fully autonomously functioning person from an NGO may have to work together with a person from the military with far less autonomy to make decisions. Finally, civil-military cooperation involves temporary relationships, dissolving as soon as the operation ends for one of the parties. Chances of renewed cooperation between the same participants are slim. Up to the present moment interorganizational monitoring and evaluation of cooperation processes between the civil and military organizations has not been an issue of interest. As a result, (inter)organizational processes of learning and change have hardly had any impact amongst the actors in the humanitarian field (Minear, 1998).

- *Task-related characteristics*: the job that has to be done consists of unfamiliar tasks that are often difficult to understand. In the military, this may be so because of the fact, that there is relatively little experience in humanitarian operations, compared to civilian fieldworkers. Civilian institutions are not only aware of what should be done, but also how. For NGOs, however, the difficulty of the tasks may originate from their relative unfamiliarity with coordinating and managing the whole gamut of humanitarian activities and actors involved, whereas the military are used to organizing. Furthermore, the tasks to be performed are often interdependent, while time is short.

- *Actor-related characteristics*: civilian and military actors alike are attached to their own different identities. Their operational habits differ widely, they come from various fields of expertise and their motivation to take part in humanitarian operations varies. Often, the members of the NGOs are opposed to military forces from the outset.

Apart from the above-mentioned sets of characteristics, civil-military cooperation involves collaboration at different organizational levels, which adds to its complexity. All parties

involved have to cooperate at two different levels at least. People at the top of the organizations have to provide a policy for working together. Furthermore, they are the spokesmen for their organizations. However, the real work has to be done in the field. The civilian and military field workers have to meet during work and cooperate.

3.   Confidence, trust and control

In an article about partner cooperation in alliances Das and Teng (1998) formulate a model from which several suggestions for better partner cooperation may be deduced. They describe partner cooperation as 'the willingness of a partner firm to pursue mutually compatible interests in the alliance rather than act opportunistically' (Das & Teng, 1998: 492). They see confidence in partner cooperation as central to successful cooperation. Confidence is defined as 'a firm's perceived certainty about satisfactory partner cooperation' (1998: 492). This means that confidence is inversely linked to perceived uncertainty about a partner's behaviour. The more an organization knows that the other organization performs in a reliable way, the less uncertainty there is and the better the alliance works.

Das and Teng introduce two mechanisms that play a part in building confidence in partner cooperation. The first mechanism is control: 'a regulatory process by which the elements of a system are made more predictable through the establishment of standards in the pursuit of some desired objective or state.' (1998: 493). Two measures that enable control are the defining of specific goals and objectives for the organizations or of specific rules and regulations for working together. The second mechanism mentioned by Das and Teng is trust, defined as 'positive expectations about another's motives with respect to oneself in situations entailing risk.' (1998: 494). So trust is about the goodwill of the other. It is especially valuable when organizations have to rely on their partners' performance and they themselves remain vulnerable to their partners' actions. For parties to trust one another they have to know that in the cooperation the other party will be reliable in the execution of its tasks, that it will not abuse information, that it will respect the interests of both parties, et cetera.

In the literature several kinds of trust have been described. Lewicki and Bunker (1996) distinguish three different kinds of trust.

Calculus-based trust is founded on rational choice of the parties, the fear of punishment for violating the trust and the rewards to be derived from preserving it. Knowing that cooperation is the best option will keep the parties working together. However, this form of trust is very fragile. A single violation is likely to terminate the exchanges between the parties.

Knowledge-based trust derives from repeated interactions over time between trustor and trustee. In this way reliability and dependability are formed in previous interactions, and the other's behaviour may be anticipated. This form of trust is based on repeated cycles of communication and information exchange. It develops over time. Dimensions of this kind of trust are: information about each other, predictability, and understanding that has been developed over repeated interactions. Exchanges based on this form of trust are more resilient when a violation of trust occurs.

Identification-based trust means that a party identifies with the other party's desires and intentions. Trust exists because the parties effectively understand and appreciate each other's wants. The other party can be confident that its interests will be fully protected and that no surveillance or monitoring of the other is necessary.

For the purpose of our analysis we would like to add two other kinds of trust that have been mentioned by McKnight, Cummings, and Chervany (1998): cognition-based and institution-based trust.

Cognition-based trust means that trust relies on rapid, cognitive cues or first impressions, as opposed to personal interactions. A person knows what to expect from another person on the basis of the reputation of the category to which the other person is perceived to belong.

Institution-based trust refers to knowing what one can expect from representatives of a certain organization. This kind of trust is based on two forms of beliefs: *structural assurances beliefs* imply that the necessary impersonal structures, such as regulations and guarantees about the behaviour of the other party, are in place to enable one to act in anticipation of a successful future endeavour. *Situational normality beliefs* imply that members of the organizations perceive the situation as normal, so that both their own roles and positions and those of the members of the other party are familiar. This leads to the expectation that cooperation will be successful.

To these categories of trust we would like to add yet another aspect which is often forgotten in the literature about trust. Lewicki, McAllister, and Bies (1998) distinguish between trust and distrust as two separate dimensions and not as two opposite ends of the same continuum. In their terms, trust is described as confident, positive expectations regarding another's conduct. Hope, faith, confidence, etcetera, in this conduct characterize high trust. Distrust, on the other hand, is characterized by confident, negative expectations regarding another's conduct. A distrusting person is sure that the other person will not behave as he would wish. It is possible to both trust and distrust a person with respect to different facets of interaction. In cooperation relationships there are often shared but also separate objectives. For instance, it is possible to trust a representative of a partner organization in professionally completing his task, and yet at the same time this person may be distrusted because he is working for an organization which is seen as a competitor. So, both trust and distrust may be necessary in this cooperation.

From the above categorization can be concluded that trust and control are not very well distinguished. Under the 'flag' of trust many elements of control have been included. The structural assurances beliefs are hardly more than control elements: the other organization can be trusted because of the many controls that exist between the two organizations. Also, calculus-based trust is hardly more than a control mechanism: people are pushed or pulled towards cooperation because of some extrinsic reinforcements. Furthermore, the distinction between trust and distrust points at the fact that members of the cooperation partner have to be checked or controlled for those aspects in which they are distrusted.

Both trust and control contribute to a high level of confidence in partner cooperation. We think that a successful cooperation relationship has to start with the necessary control mechanisms in place. When this cooperation succeeds trust will develop. However, control mechanisms, such as rules and regulations, may prove their value in stable situations, but they may be inadequate when flexibility is required. So, when the cooperating organizations are very interdependent in very uncertain and changing situations, trust has to develop quickly because control mechanisms may be too inflexible and therefore insufficient for successful cooperation. Such situations require swift trust to develop. Meyerson, Weick and Kramer (1996) describe *swift trust* to be strongly action oriented. Instead of putting energy into the development of close interpersonal relations, the emphasis is on action, absorption in tasks and the avoidance of too much personal openness. Thus, swift trust can be considered to be a pragmatic strategy to cope with high levels of uncertainty. In such situations successful cooperation between two organizations requires a certain level of trust amongst the collaborators to be able to create the necessary flexibility.

4. What are the requirements for confidence, trust, and control in civil-military cooperation?

In this section we analyze what qualities and quantities of confidence, trust, and control may be necessary for a successful partnership between the military and the civilian organizations during humanitarian crises. At first sight, it may seem ideal when two organizations adapt fully to each other. However, it is our opinion that the different organizations should adhere to their own ways of working, which are most adequate for dealing with the situations for which they have originally been designed. For instance, the military should be and remain able to cope adequately with dangerous situations, such as combat situations, and the NGOs should remain focused on their own tasks. In spite of this, however, ways should be found to create effective cooperation between the organizations based on confidence in partner cooperation and mutual trust.

According to Seiple (1996) relationships between the US military and NGOs in humanitarian interventions are governed by two principles. The first concerns the notion that apart from the goals both parties may share during the humanitarian operation, they will also adhere to their own specific interests and agendas at the same time. The shared goals are of a temporary nature, causing temporary civil-military alliances to evolve. With regard to the second principle ruling civil-military cooperation, Seiple introduces the concept of *altruistic self-interest*. By this the author means that civilians and the military will agree to cooperate when they are convinced that by supporting the other party they will also further their own interest. However, due to the simultaneous presence of conflicting interests and motives, chances are for the interorganizational cooperation to succumb to opportunistic behaviour. It is because of these dynamics, that civil-military relationships constitute the kind of alliances that are characterized by the emergence of both trust and distrust at the same time. An employee of one organization trusts employees from the other organization on certain aspects, but distrusts these same persons with respect to others. Thus, officers trust the medical professionalism of MSF employees, but they may distrust the way in which they regard security. Because of this distrust, the officers will emphasize certain control measures, aimed at maintaining security, and introduce measures to ensure that everybody lives up to them. These measures may generate some active or passive resistance from employees of the civilian organizations, which in turn may result in more controls, etcetera.

Working together in humanitarian crises may evoke rather high levels of uncertainty amongst the participants, which may interfere with cooperation on the tasks at hand. Therefore, measures should be taken to promote confidence in partner cooperation, thereby keeping the alliance from falling apart prematurely (e.g. before the shared problems are solved in a mutually satisfactory way). Because civil-military cooperation cannot be coordinated by traditional hierarchical mechanisms, the necessary safeguards to prevent these relationships from falling apart have to be based on other sources. We propose different forms of trust mentioned in the former section as main sources to instigate initial cooperation as well as for keeping interorganizational alliances together over some period of time.

Two kinds of trust may account for the emergence of initial interorganizational cooperation. The relation between *calculus-based trust* (Lewicki & Bunker, 1996) and the principle of altruistic self-interest seems to be immanent. Driven by rationality (for instance, because both the military and civilians cannot afford the costs of not collaborating and therefore not reaching their goals, collaboration may seem to be in their best interest) both partners may decide to cooperate. Since some degree of trust is a prerequisite for cooperation we assume that cooperation on the basis of altruistic self-interest involves at least some degree of calculus-based trust. Cooperation on the basis of calculus-based trust does not require a great deal of personal commitment or involvement with the organizational norms and values of the

partner. Both parties may either view civil-military cooperation to be the lesser of two evils or else a pragmatic strategy for achieving much coveted results. Therefore, relationships based on calculus-based trust will tend to be fragile and easily dissolved. Moreover, since this specific form of trust is to a large extent based on self-interest it may in fact promote opportunistic behaviour. Although collaboration may seem to be a rational decision regarding the need for complementary expertise and capabilities, at the same time it increases dependency on the partner's cooperative behaviour. High levels of dependency cause vulnerability and uncertainty, thereby creating the need for additional forms of trust.

In our view *cognition-based trust* and parts of *institution-based trust* (McKnight, Cummings and Chervany, 1998) often have to accompany calculus-based trust in initial cooperation and trust formation. First impressions and second-hand information play an important role in reducing uncertainty about what behaviour to expect of the unfamiliar partner. For instance, based on their reputation, the military may foster positive expectations about the humanitarian expertise of NGOs. Based on hearsay about former military assistance, relief workers may look favourably upon any military offer regarding logistical support or security. Cognition based trust relies largely on this kind of tentative assumptions and indirect sources of information. However, by working together on a daily basis, direct information on the behaviour of the unfamiliar partner becomes readily available to all parties involved in collaboration. Perceived differences between direct and indirect sources of information will be interpreted in favour of the own direct experiences. Furthermore, *certain structural safeguards* have to be in place to regulate the cooperative behaviour of both parties, which reduces uncertainty about opportunistic behaviour. As a result, the partner's behaviour is becoming more predictable, which increases the perceived level of control over the relationship.

Because of the urgency in humanitarian operations to achieve the objectives, it is vital that the collaboration between civilian and military organizations starts quickly. Although they often do not know each other, representatives have to be able to work together at very short notice. Therefore, initial civil-military relationships require swift trust. In view of the above, we propose that calculus-based trust, cognition-based trust, and the structural assurances (*institution-based trust*) play an important role in initial trust formation between civilian and military partners unknown to each other. However, as more direct information becomes available or shared objectives are being partly achieved, another form of trust may develop between the partners providing additional support for more robust civil-military relationships. The tasks to be performed require informal interaction and exchange of information on a daily basis. In this way both parties are able to familiarize and mutual respect based on proven expertise may grow, leading to the development of yet another form of interorganizational trust: *situational normality* (institution-based trust). Situational normality makes both sets of participants not only feel comfortable with their own role and functioning in the alliance, but also at ease with the role and functioning of the partner in the alliance.

Both other forms of trust, viz. *identification-based trust* and *knowledge-based trust*, which we have introduced, have in common that they only grow and develop over time between individuals. They rely heavily on the building of close interpersonal relationships by which means the partner's behaviour in the alliance becomes fully predictable and understandable at all times. Because of the symbiotic nature of partnerships based on these forms of trust, the alliance has no need for control mechanisms such as monitoring or surveillance of the partners' actions. However, civil-military relationships during humanitarian operations are of a temporary nature. Collaboration takes place in a temporary system, the objective always being to get the job done. Although the military and civil organizations do indeed share some goals during humanitarian operations, at the end of the day they are highly separate organizations and likely to remain that way. Born out of totally diverging needs and motives,

besides having their own missions and goals towards society, both the military and humanitarian organizations naturally adhere to their own identities and look upon each other critically and with a sound distrust. Therefore, only knowledge-based trust may play some role between those few individuals of two cooperating organizations who have to deal closely with each other over an extended period of time. In our opinion, identification-based trust will hardly ever play any role of importance in civil-military relationships.

How much confidence in partner cooperation is required in civil-military cooperation? Regarding the necessary level, Das and Teng (1998) state that it is dependent on the type of alliance. The authors propose three different types of dependency that affect the necessary level of confidence in partner cooperation. The first regards the extent to which non-recoverable investments have been made into the alliance. The more alliance-specific investments there are, the more risk there is for partner firms, the more confidence in partner cooperation is necessary. The second aspect is the level of embeddedness and connectedness of both organizations. The more the organizations are embedded and connected, the more difficult it becomes for them to freely exit the relationship. Finally, there is the risk involved in opportunistic behaviour by one partner, abusing the resources of the other.

Since neither civil organizations nor the military will ever be closely connected in any strategic way, we presume the level of non-recoverable investments in the cooperation to be low at all times. However, because of external and political pressure the level of embeddedness and connectedness between both organizations is much higher. They are condemned to each other in concrete humanitarian aid situations and so they have to work together, whether they want to or not. They cannot openly state that they will not cooperate with the other party. Both parties also run some - but not high - risk that one party makes use of the resources of the other party. One of the risks that the organizations may see is that they may be each other's competitor in the acquisition of certain assignments. Another risk may be that an organization may perceive a loss of credibility by cooperating too closely with the other party. So, they have to be certain that they can retain their own identity in the cooperation.

This leads to the conclusion that civilian and military organizations have to have moderate - neither high nor low - confidence in the other organization. They have to form a moderate level of swift trust to be able to cooperate from the start. This level of trust requires a lot of communication and information exchange, both in the field during the operation and between headquarters before, during and after the operation. Communication and information exchange have to overcome the difficulties in cooperation which arise because of the above-mentioned characteristics, such as the stressful context in which the cooperation has to take place, the unfamiliar, fluctuating, and interdependent tasks that have to be performed, the great differences between the cooperating organizations and the actors within these organizations.

5. Role of communication and information exchange in the promotion of trust, control, and confidence in civil-military cooperation during humanitarian operations

In this section we will discuss the important role of communication and information exchange in promoting trust and confidence in civil-military relationships, thereby facilitating the ways in which the military and civilian organizations cooperate during humanitarian aid interventions. In our opinion a high level of communication and information exchange between the representatives of the cooperating organizations is a sine qua non. We will make a distinction between top levels of the organizations and the field workers and we will suggest six opportunities for increasing the flow of daily communication and information-exchange

between the military and civilian actors. We believe that by making use of these opportunities interorganizational trust and confidence will be promoted.

First, it has to be recognized that communication and information sharing between the military and civilian organizations are impeded in circumstances where civilian organizations feel the military are trying to take over responsibilities and tasks that belong to them. In their view the use of military assets to assist in the humanitarian sphere is designed to supplement, rather than to supplant the work of traditional humanitarian agencies. From a functional standpoint, military assets can make four major kinds of contributions:

- foster the development of a protective framework of overall stability within which civilian populations are protected and humanitarian activities are carried out;
- support humanitarian agencies and the host government with logistics, personnel, construction and security counsel;
- carry out relief activities on their own initiative;
- assist humanitarian agencies and the host government with regard to crisis management.

Assuming the host nation and other parties involved agree with the military presence, the former two military contributions evoke relatively little resistance on the part of humanitarian agencies. As to the latter two, however, things are much more sensitive. Traditional humanitarian actors share a common conviction as to the lack of humanitarian expertise of the military. Besides, as stated before, civilian agencies are divided amongst themselves about the appropriateness of military involvement with humanitarian affairs. Whereas some level of consensus might be reached concerning a purely supportive role, military involvement with regard to the planning, coordination, and management of humanitarian activities will soon meet with resistance. By the same token, civilian agencies generally object to the military undertaking relief activities on their own initiative. Contributions in these areas may be viewed as an attempt from the military to unrightfully take command, or else humanitarian agencies may suspect the military from trying to steal their turf. In other words, any amount of military initiative displayed in this field will be likely to evoke high levels of distrust, thereby severely impeding communication and information sharing. Under these circumstances civil-military cooperation is hardly likely to take place. At the same time the opposite is true. Because of the supportive behaviour of the Albania Force (AFOR) military and because of repeated assurances expressed by the commander of AFOR (COMAFOR) regarding the humanitarian mission of AFOR, the Albanian civil authorities, as well as international humanitarian agencies proved themselves willing to communicate with the military and - in many cases - were in favour of cooperating with them.

Secondly, military as well as civilian organizations do recognize the importance of communication and information exchange, as the emergence of conferences and meetings on civil-military cooperation in recent years has clearly shown. On these occasions high-level managers and high-ranking military commanders meet and familiarize. These gatherings are important for discussing and evaluating cooperation experiences. Furthermore, representatives may formulate policies there on working together in future operations, which they can then communicate to their organizations.

Although the conditions for trust may be provided from the top, real trust can only be developed amongst the field workers, which brings us to the third opportunity. We assume that continuous interaction - the extent to which both sets of partners communicate and take part in information exchange - has a positive effect on the level of confidence in partner cooperation and the emergence of trust. This recognition has led to an increase of *formal* structures in the field, such as military-led centres for Civil-Military Cooperation (Cimic) or their American pendant Civil-Military Operations Centers (CMOCs). Exchange of infor-

mation and communication with national and local authorities, NGOs and international organizations is a key element of the job of Cimic officers. From a military point of view Cimic is considered to be a valuable asset in areas where military forces are or plan to be employed (*MC 411 NATO CIMIC Policy/AJP 1 Definition*). On the civilian side there exist parallel structures, called On-Site Operations and Coordination Centers (OSOCCs) and Humanitarian Operations/Information Centres (HOCs/HICs). Needless to say, civilians are in charge of these information channels. On top of this, different departments of UN-organizations, preferably in collaboration with local authorities, disseminate information and organize meetings regarding their specific topics of interest, such as water and sanitation, food distribution, security, repatriation, et cetera.

In view of the above, it is our opinion that difficulties in civil-military cooperation do not stem from a lack of formal structures for communication and information exchange. Instead, we propose that an overabundance of these formal structures, each led by either military or civilian actors, creates confusion and uncertainty as opposed to transparency and a certain degree of trust. For the formal structures to fulfil the need for communication and information sharing, they have to be *freely admissible* to all collaborating partners. This means, they have to operate on a local level to be of any use in case of an appeal for help. Instead of isolating themselves from the civilian actors by being based at military headquarters, centres for Cimic or CMOC should be based 'outside the wire' (Devendorf, 1996). In their evaluation of the humanitarian operations that took place in Albania, Macedonia and in Kosovo in 1999 (Minear et al., 2000) compare the functioning of Cimic structures there. In Macedonia Cimic was based at the Headquarters of Allied Command Europe Rapid Reaction Corps (ARCC) and KFOR in Kumanovo. In Kosovo, too, Cimic was based inside the wire at KFOR Headquarters. In Albania, however, COMAFOR decided that, rather than establish a separate Cimic centre, Cimic officers should participate in already existing structures. As a consequence, Cimic officers were assigned to the Emergency Management Group (EMG), set up by the Albanian government to coordinate the crisis management, and to the Humanitarian Information Centre, an NGO-initiative. Situated in the centre of Tirana, the HIC-offices are freely accessible to the military, humanitarian organizations and local authorities.

For each of the above-mentioned settings relationships with civilian authorities differed. In Macedonia the authorities were viewed as resisting cooperation on humanitarian issues, in Kosovo the authorities were non-existent. In Albania, on the other hand, they proved to be eminently cooperative. In July 1999 the first author of this article conducted interviews with Canadian, British, German, American and Dutch Cimic officers in Albania. In these interviews all officers expressed their satisfaction about the smooth collaboration with civil agents and organizations. They also showed themselves appreciative of AFOR's involvement in the EMG and HIC. A British Cimic officer, appointed to the EMG, compared the advantages of being assigned to the civilian-led structures to working at a military led Cimic-center. According to him, 'Cimic could have played that role (in information-exchange), but the HIC-chairman represents all those NGOs in person. They are 100% behind her, whereas they would never have been behind a military-led Cimic.'

Fourthly, we suggest improvement of civil-military relationships in the field may be found in the increase of communication, information exchange and personal contacts in more informal settings, in which the parties involved interact on a daily basis. Michael Toole, an American MD, who has cooperated with the military throughout the world stresses the importance of informal personal communication and information exchange between the military and civilian actors. Describing his experiences with the US military in Goma (1994), he comments,

Many attempts to have NGOs and the military become more familiar with each other have been made […], but those meetings and exercises mainly involve the higher level managers and the upper ranks of the military. The real familiarization has to be made among field people. […] In Goma there was almost no social mixing of the two groups. Without these personal relationships organizational relationships will never work. In a field of human endeavour so stressful and emotional, the personal linkages are even more important (Seiple, 1996: 165-166).

By actually working shoulder to shoulder, daily civil-military interaction becomes a natural phenomenon. This means that *situational normality* may set in. Under such circumstances the participants in the alliance will consider cooperation as a matter of course. For instance, both the Cimic-officers and the civilians appointed to the HIC in Albania worked together in extracting, gathering and distributing information. After a while, because of positive results, they voiced their respect for the degree of professionalism shown by their counterparts. Although both parties did not take part in generalizing their mutual experiences to comprise the entirety of each other's organizations, at the work floor a good deal of fraternization took place and it continued after the work for the day had been finished. Mijs observes some form of confrontation is to be expected between cooperating mutually divergent parties (Lammers, Mijs, van Noort, 1997). Therefore, the author suggests interorganizational relations should allow for differences of opinion and conflicts of interest. Informal settings are needed to enable partners to feel at ease with one another. Thus, informal settings may facilitate the processes of coping with the confrontations Mijs regards as unavoidable. Moreover, informal settings may promote feelings of *situational normality*, which in its turn affects the development of confidence in partner cooperation. However, it is our opinion that *situational normality*, one of the characteristics of institution-based trust, cannot be taken for granted in the early stages of civil-military cooperation. We suggest both calculus-based trust and cognition-based trust are needed for initial trust formation in civil-military relationships. Only by working together on a daily basis and each party contributing the required expertise, an insight is gained into actual behaviour and organizational safeguards. Information of this nature reduces uncertainty about the partner's cooperative behaviour and minimizes the risks of opportunistic behaviour. Eventually, due to continuous interaction situational normality may come about. Apart from feeling comfortable with the partners' behaviour, situational normality also results in parties assuming that structural assurances, necessary for risk-taking, will be met under such circumstances.

Fifthly, therefore, for any structure to fulfil the need for communication and information sharing there has to be *open personal contact* between all parties involved. Openness increases the transparency of civil-military relationships, allowing mutual understanding to grow. By means of open communication direct feedback is facilitated, which allows a different course of action when needed. During former humanitarian operations open personal contacts have already proven their value. For instance, the high degree of openness in the relationship between the Dutch military and Memisa in camp Mugunga (1994) led to the formation of interorganizational trust of a rather resilient nature. After the Dutch military had supported Memisa in constructing a field-hospital and supplying medical equipment, the idea was to have Dutch orderlies assist the NGO in its medical work. In this capacity the untrained orderlies could benefit from the medical expertise of the relief-workers. However, after a short period of time Memisa made it clear they preferred para-medically trained refugees to support them instead. Although faced with a serious management problem, the commanding officers trusted Memisa up to the point of understanding its underlying motives and, without relationships deteriorating, untrained military personnel were withdrawn from the field-

hospital. In an interview conducted four years after the event, the senior medical officer of the Dutch contingent motivated his decision:

> *We took too many inexperienced orderlies along, relatively speaking. The NGOs use local people on those jobs. We should have brought more highly specialized medical staff. For me this was an important lesson* (personal communication with the authors).

When asked, the former logistical officer of Memisa also remembered this particular incident. Due to the actions of the commanding officers and the support received, he declared to be highly in favour of cooperating with the military during humanitarian operations.

Finally, in order to create an open communication and information exchange there has to be common acceptance of the use and objectives of the information gathering. The military consider NGOs to be rich sources of information, needed, amongst others, for force protection. NGOs, on the other hand, feel reluctant to share information if they suspect it will be used for military intelligence, as this could endanger their much-coveted neutrality in the area. By the same token, NGOs often refrain from informing the military about planned activities out of fear that this might attract undue attention from indigenous groups.

6. Conclusion

In conclusion, communication and information exchange between civilian and military organizations are important in order to be able to formulate the necessary control mechanisms, and to build the required trust and confidence between both organizations. Without the required levels of confidence, trust, and control cooperation will not be successful. Furthermore, since the parties involved have little or no previous experience in working together, we propose that, at least at the onset of the cooperation process, a certain level of control is as important as a certain level of trust to reduce uncertainty. However, it has to be taken into account that, up to a certain extent, both the military and civilian institutions will have to adhere to their own interests to be able to also fulfil the goals they do not share. As mentioned before, both sets of partners come from highly disparate organizations. They have their own missions and goals towards society and no amount of communication and information sharing may ever be able to fully reduce uncertainty between civilian actors and the military.

The phases of the humanitarian operation itself may also add to the uncertainty about the cooperative behaviour amongst civilian and military partners. In our view the initial emergency-phases dictate the need for cooperation, since they exceed the capacities of any single organization to cope with the problems at hand. As a consequence, traditional relief agencies and civil authorities in host nations may appeal to the military for support. Usually, reception and accommodation of refugees will be the main goals during the first phases of a humanitarian operation. Under these circumstances of acute emergency civilian organizations and the authorities in host-nations may feel highly dependent on military assistance to reach their humanitarian goals. Compared with many civilians, the military lack humanitarian expertise. Therefore, they may be dependent on civilian organizations for the way in which their support should best be given. Interdependency for reaching shared goals is a characteristic of interorganizational cooperation. Moreover, during this highly ambiguous novel situation, both the military and civilian actors will require daily interaction and information-sharing to be able to perform their interdependent tasks. However, at some point the acute emergency is over. Refugees have been provided with shelter, their basic needs are seen to and some degree of stabilization may set in. The demands for support are changing from massive relief into specific specialist needs. Besides, as the operation proceeds over time

the number of civilian aid-agencies increases. The same applies to the financial funding supplied by donor-organizations. As a consequence, civilian institutions may feel better prepared to cope with the situational demands. Their dependency on cooperating with the military may be reduced, which in turn may affect their need for daily interaction, communication and information sharing with these partners. All of a sudden, the military may find themselves in a situation in which the tables have been turned overnight. Their ongoing support of humanitarian tasks may now even be considered as competition or as undue interference with the rightful domain of humanitarian agencies. Under these circumstances it can only be expected that the military will experience a certain degree of uncertainty as to the behaviour that is expected from them.

Humanitarian operations take place in a fluid context, causing different demands and needs for civil-military cooperation. In our view, civil-military cooperation may always be limited to certain areas under specific circumstances. The same can be expected with regard to the established levels of trust and confidence in these temporary alliances. Communication and information sharing between the parties involved before, during and after the operation may increase the awareness of these dynamics, enabling both civilians and the military to cope with the consequences of the temporary nature of their relationships.

References

Creed, W.E.D., Miles, R.E. (1996), Forms, Philosophies, and Costs of Controls in: R.M. Kramer, T.R. Tyler (eds.), *Trust in Organizations: Frontiers of Theory and Research*: 16-38, Sage Publications, Thousand Oaks, 1996

Das, T.K., Teng, B.S. (1998), Between Trust and Control; Developing Confidence in Partner Cooperation, in: *Academy of Management Review*, 23, 3: 491-512

Devendorf, G. (1996), *The NGO/Interagency Interface*, Workshop on Humanitarian & Peace Operations, April 18-19, InterAction, Washington DC

Frerks, G.E. (1999), *Refugees between Relief & Development: Continuum or Discontinuity?* Landbouw Universiteit, unpublished paper, Wageningen

Gordenker, L., Weiss, T.G. (1993), *Soldiers, Peacekeepers and Disasters*. MacMillan (in association with the International Peace Academy), London

Joint Warfare Publication 3-50, MoD (UK), London, 1999

Lammers, C.J., Mijs, A.A., Noort, W.J. van (1997), *Organisaties Vergelijkenderwijs* [Comparing Organizations], Spectrum, Utrecht/Antwerpen

Lewicki, R.J., Bunker, B.B. (1996), Developing & Maintaining Trust in Work Relationships, in: R.M. Kramer, T.R. Tyler (eds.), *Trust in Organizations: Frontiers of Theory and Research*: 114-139, Sage, Thousand Oaks, 1996

Lewicki, R.J., McAllister, D.J., Bies, R.J. (1998), Trust and Distrust: New Relationships and Realities, in: *Academy of Management Review*, 23, 3: 438-458

Maynard, K.A. (1999), *Healing Communities in Conflict; International Assistance in Complex Emergencies*, Columbia University Press, New York

MC 411 NATO CIMIC Policy/AJP 1 Definition, NATO, Brussels, 1998

McKnight, D.H., Cummings, L.L., Chervany, N.L. (1998), Initial Trust Formation in New Organizational Relationships, in: *Academy of Management Review*, 23, 3: 473-490

Meyerson, D., Weick, K.E., Kramer, R.M. (1996), Swift Trust and Temporary Groups in: R.M. Kramer, T.R.Tyler (eds.), *Trust in Organizations: Frontiers of Theory and Research*: 166-195, Sage, Thousand Oaks, 1996

Minear, L. (1998), *Learning to Learn*, Discussion Paper Seminar Lessons Learned in Humanitarian Coordination; Office Coordination of Humnitarian Affairs (OCHA) and Swedish Ministry of Foreign Affairs, April 3-4, Stockholm

Minear, L., Baarda, T.van, Sommers, M. (2000), *NATO and Humanitarian Action in the Kosovo Crisis*, Institute for International Studies, Brown University, Providence

Mishra, A.K. (1996), Organizational Responses to Crisis: The Centrality of Trust in: R.M. Kramer, T.R. Tyler (eds.), *Trust in Organizations: Frontiers of Theory and Research*: 261-287, Sage, Thousand Oaks, 1996

Seiple, C. (1996), *The US Military/NGO Relationship in Humanitarian Interventions*, US Army War College, Carlisle Barracks, PA

Webb, E.J. (1996), Trust and Crisis, in: R.M. Kramer, T.R. Tyler (eds.), *Trust in Organizations: Frontiers of Theory and Research*: 288-301, Sage, Thousand Oaks, 1996

Wolfson, S. (1997), Samenwerken: UNHCR en de krijgsmacht, [Cooperating: UNHCR and the armed forces], in: T. van Baarda, J.Schoeman (eds.), *Werelden Apart?*: 43-52 Stichting Maatschappij & Krijgsmacht, Sdu, Den Haag

The importance of cultural information in multinational operations: a fragmented case study on UNFICYP

J.L.M. Soeters, T.P. Op den Buijs, A.L.W. Vogelaar

1.   Introduction

In an ever-increasing world, organizations must work together. This is equally true for accountancy firms, industrial companies and retail enterprises. When, on top of that, organizations are faced with shrinking instead of growth, there is an even greater imperative for cooperation and this is the situation that most western armies find themselves in. The decrease of the number of personnel employed in the western defence sector since 1990 can truly be called spectacular. But even before that year there was an unmistakably downward trend. Cooperation, therefore, is the buzz word for the military.

This cooperation in the defence sector happens jointly between the services (e.g. the land and air forces), but to an increasing extent also combined, between units of several countries. The cooperation sometimes assumes very far-going structural forms, as is demonstrated by the formation of the German-Netherlands Corps. Usually, however, international units meet – on a more incidental basis – in exercises, and increasingly also in actual missions. The closing decade of the last century showed that military operations – from peace enforcing to peace support operations – cannot be conducted by an individual country anymore. In an international context military personnel are dependent on each other in the realization of their targets, usually because there is a lack of adequate (personnel) resources to conduct independent action, and sometimes, as in the case of the United States, to strengthen the legitimacy of an operation.

The result is that the military has thoroughly internationalized, making know-how regarding international management from the business sector also applicable to the armed forces. One of those knowledge domains concerns the influence of national cultures on the structure and functioning of international alliances. Research based on insights into cultural differences in multinational companies has established that national armed forces show substantial cultural differences. These differences concern the loyalty of the personnel to the organization, the structure and functioning of the organization, the relation and social distance between the leadership and rank and file, as well as the extent of formalization and rule orientation. In this respect the cultural heterogeneity between national armed forces is at least as great as that in the profit sector.[1] In all likelihood the impact of this cultural heterogeneity is greater in military operations than in structural cooperation in the business sector. This is related to the fact that in military operations the missions and targets are not always so concrete and measurable. Besides, military units always have to keep up a national line of responsibility, the time frames of the operation tend to be rather tight and the sense of urgency is very high, whereas the personnel is constantly rotated.[2]

At the same time, however, there is also, quite emphatically, something like a supranational military culture. In comparison with profit businesses, military culture in all countries is rather bureaucratic, hierarchic and institutional (i.e. relatively less inclined towards income, career and private life). This means that even before entering a specific multinational force, officers may have undergone vicarious anticipatory and actual socialization to work in such frameworks.[3] The consequence of this is that military personnel of different origin can often function with each other without too many problems. Charles Moskos, for instance, found that the most serious tensions during the UNFICYP operation took place between military personnel and the local population, not between personnel of the various contingents.[4]

Apparently there is – according to Moskos – a certain military professionalism that, at least to a certain extent, can surmount national borders and cultural differences.

Up to a certain extent, and this is an important point. In the present article we intend to show how cultural differences, in this case between British and Dutch army personnel, could give rise to such friction that interference by the Dutch Army Staff was deemed necessary. This interference was occasioned by an investigation of the Bureau Lessons Learned, directed at providing cultural information on the British Army.[5] The intention was to give direct culture guidelines to Dutch personnel on how to improve their contacts with the British. It so happens that the location of this Anglo-Dutch cooperation is Cyprus, and the international framework that of the UNFICYP mission; indeed, the same mission about which Moskos had expressed so much optimism with regard to the effects of an international military professionalism, some 25 years ago.

The build-up of the article is as follows. We begin by describing the nature of the conflict in Cyprus as well as the task and composition of the UN mission there. Subsequently, we will address the Anglo-Dutch cooperation in this mission based on some fragmented research material. In doing so, we will make use of data obtained from interviews with ten Dutch servicemen conducted shortly after their return from deployment on the first rotation. In addition, we have made use of the experiences of two Dutch lieutenants during the second and third rotation respectively, described in a study paper. Moreover, we have had the disposal of material from a survey held among the Dutch contingent during the first rotation. Taken together, these data yield a fairly good impression of the dynamics of the Anglo-Dutch cooperation in Cyprus. A subsequent section gives a description of the intervention by the Bureau Lessons Learned with regard to this cooperation. Finally, there is an observation on the use and necessity of cultural information in multinational military operations.

2.   Cyprus and UNFICYP

The nature of the problem in Cyprus goes back a long way.[6] Cyprus became an independent republic on 16 August 1960. Fairly rapidly it became clear that the interests of both ethnic entities in the island – Turks and Greek-Cypriots – were not easily reconcilable. In the background the two "mother countries" unmistakably played a role. In 1964 the UN Security Council passed resolution 186, which gave birth to the United Nations Peacekeeping Force in Cyprus (UNFICYP). The mission was intended 'to use its best efforts to prevent a recurrence of the fighting, and […] to return to normal conditions'. These normal circumstances were far from returning, certainly when in 1974 a Greek-Cypriot coup favouring union with Greece was followed by a Turkish military intervention, which resulted in the island being divided into a Turkish-Cypriot part in the north and a Greek-Cypriot part in the south. After a cease-fire a buffer zone was established, varying in width between 20 metres and 7 kilometres. The total extent of the cease-fire area amounts to approximately 180 kilometres. As a formal cease-fire has not been agreed upon, annually hundreds of incidents take place in the buffer zone, ranging from the throwing of stones, to shouting of abuses, moving of positions and sometimes real firing incidents. More than once large numbers of civilians are involved, regularly forcing UNFICYP to exercise crowd control. UNFICYP uses a range of means to counter incidents: investigation, negotiations with both parties and also direct troop movements. It tries to keep the military status quo in a more structural way by manning observation posts, and by carrying out foot, mountain bike and mounted patrols. Apart from that, its tasks involve supplying escorts and the carrying out of routine matters such as barrack duty and administrative affairs and the giving of training. At this moment UNFICYP is composed of British, Argentine and Austrian units, each with their own buffer zone. To the Austrian sector Hungarian units and a platoon of Slovenian personnel have been attached. The

total strength of the mission amounts to 1,273 service personnel and 33 police monitors. The British battalion is deployed in the central sector, in which the capital Nicosia is situated. It is in this area that the bulk of the incidents take place, not least because the buffer zone is narrowest in and around the city. Nevertheless, for the British serviceman deployment in Cyprus is very popular: 'a holiday destination in combat kit'.[7] Since 1998 the Royal Netherlands Army have made a company available to replace part of the British regiment there, for a period of three years. This company is under command of the British sector commander. The Dutch personnel are attached as national platoons in the British order of battle, or have been allocated to platoons that are completely international in composition. During the third rotation Sector 2 has come under Dutch command (with its own HQ). Although UNFICYP is explicitly multinational – the commander being a Nepalese bears witness to this – the binational cooperation with the British is an everyday reality for the Dutch.

3.   Anglo-Dutch cooperation

This cooperation is not going very smoothly, in any case not in the beginning. A survey carried out among a sample of 77 Dutch army servicemen who were deployed in Cyprus when the research was conducted, showed that some 60% disagreed with the statement that the cooperation with the British was smooth. Even more pregnant was the fact that more than 85% stated that they did not like the British way of acting. Only a small minority thought that the British soldiers were very skilful, whereas only 50% found that British and Dutch soldiers did get along very well. This cannot have been caused by language; in less than 10% of the cases English was a problem. These data concern the first Dutch detachment, a company of the AirMobile Brigade, deployed in Cyprus from June until December 1998, and they can be made more concrete by means of more elaborate 'stories' of servicemen. To that end we have conducted open interviews with ten servicemen, varying in rank from private to lieutenant, who had likewise all been part of the first Dutch UNFICYP detachment.

From these 'stories' several salient points emerge, mostly related to the relatively great distance between the leadership and the rank and file in the British Army. Earlier research among a great many military academies had already shown that the hierarchical or power distance between the leaders and the led as well as the emphasis on discipline were nowhere greater than in the British Army.[8] This distance in the army doubtlessly mirrors the strongly stratified British society. The working class in the UK definitively is a working class, much more so than in many other countries, and the British working class culture with its specific characteristics can be found - possibly even somewhat stronger – in the British Army, in particular in what was once so splendidly labeled the 'squaddy syndrome', a working class culture at platoon level.[9] On top of that the social dynamism of the British class system is not only visible within the platoon, but also in the way the commanders address their subordinates. Privates, junior NCOs and subalterns, have to listen to and obey their superiors inexorably, regardless whether they think the orders sensible or fair. He is punished, who does not obey, usually severely. That is how things are in the British Army.[10] It is not for nothing that the commanders issue orders with the standard addition, 'If not, disciplinary actions will be taken.' A private's direct refusal to comply with a command is going to propel him into one direction only – into the clutches of the Regimental Police.[11] It is evident that in the British Army there is steering by coercion, and not so much on the internalization of the logic and necessity of regulations and orders.

It will not come as a surprise that this manner of doing things is alien to the Dutch. The Dutch culture –the 'Dutch approach' if you will – has for centuries been characterized by the three Cs: consensus, consultation and compromise.[12] It is this cultural difference in particular that

has given occasion for what could be called 'cultural friction' between Dutch and British military personnel. This friction concerns subordinates – privates - as well as officers and NCOs. A few examples.

A Dutch sergeant comments on customs in the British Army:

> *It is not the bloke himself, but clearly the British system that irritated, the clear division between privates, officers and NCOs. Especially in that hotel* [HQ in Nicosia: the authors] *this is noticeable, because you had the separate mess halls and canteens. It was not appreciated at all if you went for a beer with the men you had worked with all day.*

A Dutch private on British manners which tend to be rather different from the jovial tone and 'yes, but-attitude' of the Dutch:

> *Yes, the British is quite a different story; especially the gunners; the privates, say, they are normal, but as soon as they are only slightly higher in rank they think they are the world; they yell at the men and if you don't follow their orders you're bound to get trouble.*

This is a far cry from what the Dutch are used to. In Dutch units many decisions are taken in consultation, which increases support and ensures that the bulk of the tasks are carried out as comfortably as possible. The other side of the coin is that the Dutch have comments on anything, and that a sort of 'culture of complaint' seems to be rife.

The distance between the several layers is also seen in a more operational sense. Providing information to the rank and file is felt to be more important in the Dutch army than in the British. Besides, status and competence issues can come into play more easily in a strongly stratified organization. This is how a second lieutenant of the Dutch company got into trouble:

> *At a certain moment I had made an order and written down tasks for the battery staff, one level up. We needed transport, but I immediately got my wrist slapped, for I should have written a request; after all I could not give tasks to a higher level. On the paper it had to read 'request' and not 'task'. That major was pretty pissed off about it, so I crossed out 'task' and wrote 'request'. But, no way, that was not good enough: I had to make a new print and have it signed by the captain.*

This may seem childish, and it certainly is so in comparison with the dilemmas and conflicts of loyalty that young Dutch platoon commanders have to face when they get caught in between their Dutch subordinates and their British commanders:

> *I have to say this, 'Listen, this is how it is', and the men think and say, 'The lieutenant is just chinwagging along with the Brits and carries out all their little plans.' But at a certain moment I try to tell them that this is the way the British want it and that I myself don't agree. But it's difficult to be disloyal to your* [British: the authors] *commander. Every day you are fighting for your platoon there, but well, it may sound blunt, but in a meeting you try to get your own way in order to get the best for your men out of it.*

The following shows that the Dutch servicemen do not fully trust their leaders anymore because of their contacts with the British:

What I thought was very bad of our cadre was that they said things like, 'we are Dutch, and we remain Dutch', but after a time they began to change and show British behaviour. When you said this to a sergeant, he would deny it and say he had remained the same, but that just isn't true.

Internal tensions for young Dutch officers really become great when matters of discipline and punishment come into play:

Their way of punishing is quite different from ours, for we have our military penal and disciplinary law and that is what we use when we punish. We don't make them run a hundred rounds in the hot sun, or what have you. At one time a bloke had accidentally driven his car into a fence. Very stupid, but there was no damage done. Things like that can happen, so this bloke is given a bollocking, and that's the end of the story as far as we're concerned. But then he had to report immediately to the battery commander, and he was completely flattened and abused, and had to pay 500 pounds on the spot. So I went up to the commander and said, 'This is not they way we handle these things. We are under your operational command, but when we punish someone we do this under our own penal system, not by clearing a lot of money straight away.' They could have said: if that is the damage, then we hold you, the Dutch unit as a whole, responsible. That's when the tables were completely turned and they offered their apologies, but only to me, not to that bloke

The collective punishment for offences committed by individuals, too, was something the Dutch found hard to understand.

It's really nonsensical that we are punished each time for something we cannot do anything about. There was the two-can rule [a maximum of two cans of beer per day: the authors]. *Because the English got drunk each time, we were not allowed to have anything anymore, although we just stuck to the rules. The Brits got pissed every night and at one time they were punished, but so were we, although we were ready to go every morning, but they weren't. In this way the atmosphere became worse by the day.*

The so-called Out of Bounds areas were also difficult to explain to the Dutch servicemen. They are areas, always places of entertainment, where British soldiers are not allowed to come, because in the past excesses like fights, excessive drinking or rapes took place there. Because the Dutch UNFICYP servicemen are under British command, these Out of Bound areas also hold for them.
There are more frictions of a (semi-)juridical nature, in particular about the severity of the punishment, which in Dutch eyes, is often extreme and especially intended to instil fear. This is characteristic for the British 'squaddy culture'. In the British army, soldiers can be made to do their duty through fear of coercive sanctions, based on the application of military law, only.[13] Occasionally this can lead to a situation in which the Royal Netherlands Military Constabulary, also present in Cyprus, blows the whistle on a Dutch commander, who has gone along with the British system of punishment (doing extra shifts).

Sometimes these punishments are in conflict with Dutch policy on working conditions.

When a person had finished his shift and was entitled to a six-hour rest period, he would get a punishment of a six-hour painting job immediately following his shift. This would mean he'd only have a few hours' sleep. Well, in the Netherlands this is

impossible, of course. When a person gets a punishment shift, it can only be a maximum of three hours prior to or following his shift, taking into account a minimum of six hours' sleep.

Problems of this kind are regularly reported. Thus, there are misunderstandings and disagreements around working with asbestos and caustic substances. In Dutch eyes – and, amongst others, on the basis of Dutch rules and regulations – this kind of activities cannot be conducted without protective measures. The British are more relaxed about it, which gives rise to disagreements and revoking of British orders by Dutch commanders.

As with the divergence of rules and views regarding working conditions, the Rules of Engagement, including firing instructions, are not identical for the British and Dutch troops. Although these differences in phrasing of the instructions for the use of violence (which, incidentally, are minor) have not yet led to any serious problems, it is conceivable that in specific situations they may do just that.[14]

A last striking difference between the British and Dutch cultures concerns the difference in value attached to what could be termed external discipline, as expressed in saluting of superiors (also when they are in civilian clothes) and the pomp and circumstance surrounding official occasions. The highlight of outward show for the British is the so-called Medal Parade. There is intensive practising weeks prior to this three-hour drill parade in which the servicemen receive their UN-medal. The result is that during the practice sessions about 100 persons cannot work shifts.

In view of the above, it is not surprising that the success of a mission for a British commander is determined, to use his own words, next to the absence of excesses in breach of discipline, by the success of the Medal Parade and the Regimental Cocktail Party.[15]

4.   The 'intervention' of the Netherlands Bureau Lessons Learned

The above has clearly shown that a smooth cooperation between the British and Dutch army personnel is not something that goes without saying. Cultural differences, and differences springing from them, of a legal and disciplinary nature, are too great for an easy cooperation. Signals about cultural friction and various concrete incidents occasioned an intervention from the Staff in The Hague. One of the incidents concerned a relationship between a Dutch servicewoman and a higher-ranking British serviceman. The relationship in itself but in particular the difference in rank, proved to be the fuse of the incident, as this situation was unacceptable in British eyes.

The intervention was a low-key operation; it consisted of working visits to the mission area of representatives of the Bureau Lessons Learned, specifically aimed at studying the "cultural issue". It was conducted during UNFICYP-IV, but information regarding UNFICYP-I to III was also included in the investigation. As British and Dutch troops also cooperate in an SFOR-context in Bosnia, there were also working visits and investigations in Banja Luka and Sipovo. On the basis of these visits and investigations a report was written and a host of hints and tips formulated on how to deal with representatives of the British Army.[16] The most important and valuable principle derived from it is: *For a fruitful cooperation it is of the utmost importance that one gets to know one's own culture first, then the other culture and subsequently attempts to find a solution for the cultural differences together.*

The Bureau draws a number of conclusions, which in view of the above, will not come as a surprise. Nevertheless, it is worthwhile to present a number of them briefly here. It is pointed out that, in contrast with the Netherlands, the British Commanding Officer is still very much on a pedestal. He often takes decisions, regardless of the plans and programmes of others. He is used to planning meetings and consultations without taking into account anyone or

anything. It is found that his cadre accepts this kind of behaviour, although not always wholeheartedly. Furthermore, the Bureau Lessons Learned finds that British servicemen often have strictly defined tasks and responsibilities and they will immediately carry out any order they may get without discussion. The checking of the implementation of the orders is not always very consistent among the British, the report says. Hierarchy is much more important for the British than for the Dutch, as is shown in more formal manners with regard to saluting, forms of address and the use of first names. Also the difference is pointed out between the regular soldier and the reservist who seems to be more receptive to suggestions and contradiction.

With regard to everyday routine a number of interesting observations are made. Thus, it appears the British commander manages his staff in a much more direct way, instead of taking decisions on the basis of preliminary work of his staff, as is more usual in the Dutch armed forces. Meetings in the British Army are short, and the chairman has the floor most of the time. Compromises are less common than in the Dutch army and at the same time there is a very open atmosphere; there is no beating about the bush when things go badly and corporals and privates can give their opinions unreservedly in such cases. This observation confirms another aspect of British army culture: craftsmanlike pride among all ranks, leading to a concern to carry out all the core activities central to the military role, which is considered to be 'real soldiering'.[17]

The report also points to striking differences with regard to barracks matters. The British stick more to the normal barracks rhythm and during missions abroad they carry on with their normal business, such as courses and training. Officers, NCOs and privates have separate quarters, messes and sanitary facilities and social intercourse between the ranks is generally limited because of this. Apart from that, the report makes mention of a number of peculiarities - at least peculiarities in the eyes of the Dutch: the absence of the ritual coffee drinking during work, common among the Dutch, the ban on smoking in the open air, conservative views on homosexuality, a reluctant acceptance (which is in actual fact no acceptance) of relationships between service personnel on missions, problems with long hair, and in fact with the presence of female soldiers at all. The report states, for example, that the British are very surprised when the Dutch female soldier joins in the conversation, whatever the subject. Dutch humour, directed at playing someone a trick, does not exist in the British army, let alone between the ranks. Conversely, the Dutch are probably incapable of fathoming the typical British humour. The British also have a great sense of history, especially in things military, and of course in particular with regard to their own regiment.

So far the report of the Bureau Lessons Learned. It is as brief as it is clear and the similarity with our own findings regarding the first rotation and those of the two lieutenants during the second and third UNFICYP rotation, respectively, is remarkable. One caveat should be mentioned, however. All observations were made by Dutch people and what has been described says as much about the Dutch as about the British (military) culture. In order to get a complete picture it would be necessary to have the British tell about their cooperation with the Dutch. It is to be expected that they would address the same subjects, and their findings would probably mirror ours.

Apparently we are dealing here with a stubborn phenomenon, which can only be approached by giving it specific attention. The Bureau Lessons Learned tries to do this by supplying a list of hints and tips as an annex to its report. The list is not presented as a regulation, but it is expressly brought to the attention of commanders and we would not withhold the reader some items from it:
- the Dutch and British service personnel should know about each other's cultures and subsequently attempt to find solutions for the differences;

- take into account that a British person higher in rank does not accept contradiction when issuing orders;
- take into account that British service personnel hardly takes initiatives beyond their own tasks;
- show your professionalism, it will speed up integration with the British;
- respect customs and views of a culture other than yours, and never ridicule them;
- operate within your tasks and responsibilities. Do not deal with matters that concern others, as this helpfulness can quickly be explained as subversive;
- be polite when addressing British officers and NCOs;
- go through the (Dutch) hierarchical channels, even when the functionary is not there for the moment; and, finally, probably the most important tip;
- always be yourself, be open and honest.

5.   Concluding observations

In an essay on national differences in military cultures[18] it has been suggested that in a cultural and structural respect military organizations go through a development from a coercive bureaucracy to an enabling bureaucracy. In the coercive bureaucracy hierarchy as well as rules and regulations coming from above play an important role. Compliance with the rules and orders is achieved in a coercive way, i.e. with much emphasis on disciplinary measures and punishments. In contrast, in the enabling bureaucracy rules and regulations are also important, but there is more emphasis on internalization, achieving inner conviction of the (effective) rightfulness and (moral and legal) legitimacy of assignments and orders. When the two-can rule is issued, for example, compliance can be enforced with punishment. But it should also be possible to stimulate those to whom it applies to become convinced of themselves of the use and necessity of such a rule. In an enabling bureaucracy it is therefore very important to get rid of bad rules and to steer on good ones, i.e. rules that are accepted by everyone to be inevitable and right. Another difference between good and bad rules is the extent of detail. Bad rules specify everything, whereas good rules function more as frames of reference within which the personnel has room for manoeuvring.
The above mentioned empirical research into 18 military academies has shown that certain national armed forces clearly find themselves on the coercive side of the scale, whereas others display a more enabling bureaucratic military culture.[19] It will not come as a surprise after the above that the British Military Academy in Sandhurst proved to be the academy with the most explicit coercive culture, whereas the Royal Netherlands Military Academy in Breda took up a middle position, with tendencies towards the enabling culture. However fragmented the information presented in the present article may be, the first-hand data of four UNFICYP missions unambiguously confirms the truth of the empirical findings of the military academies research.
At the same time this account has shown the importance of paying attention to the stubborn phenomenon of cultural differences between armed forces. The attention begins with the production of information and this brings us to the over-all theme of this book. The intervention by the Bureau Lessons Learned with regard to the Anglo-Dutch cooperation can be considered as a way to provide cultural information that is extremely relevant for the performance of the multinational military operation in question. If the other side, the British, organized the production of cultural information about the Anglo-Dutch cooperation in the same manner, the chance of optimizing the cooperation would be increased considerably.
But not only must the information be produced, it is equally vital that it is disseminated as well. It is not sufficient to write reports, however interesting in themselves. The information must also be brought across in education and training and during the actual work up for the

mission. In this respect the role of the commander, at all levels, is crucial. If anyone can contribute to the internalization of the rules of conduct it is he. With great force of conviction and especially by setting the example he will have to motivate his people to show the right sort of behaviour with the help of the provided cultural information. General aspects of importance in this respect are: an emphasis on the combined nature of the operation, as well as the equal status of all those concerned, regardless of their nationality; boundary crossing, i.e. attempts to unite, reconcile or transfer knowledge between the various groups by means of emphasising shared experiences, directly asking others about their cultures and comparing the own culture to the other in a neutral or flattering way; and, in general, tolerating ambiguity.[20] That is what commanders, active in multinational military operations should do and for which they have to be trained. The importance of fostering their cultural awareness cannot be emphasized enough.

These aspects of multinational leadership do not prevent other contextual or structural matters from playing a part in the effects of culture in multinational military operations. First of all there is the time factor: as is well known, Dutch and British marines have worked together intensively for about twenty years now, reportedly to the satisfaction of all concerned. What we possibly see here are the effects of a strong Marine Corps culture that counters any Anglo-Dutch cultural differences, but more probably it is the longer duration of the cooperation that has brought both cultures closer together. A parallel example of such a successful cooperation is the British field hospital at Sivopo, where the medical staff are equally divided over the two nationalities. Again, it may be the sense of belonging to a certain medical brotherhood that suppresses mutual irritation, although even here, the Dutch have resorted to setting up their own bar. What is striking in the various reports on the Anglo-Dutch cooperation in Cyprus is that, from time to time, it is found that the own unreasonableness (on both sides) is admitted, that sometimes people adapt and quite simply begin to get used to one another. Whenever people work together for a long enough period and cultural differences are not exaggerated, a certain hybridization of cultures tends to emerge. From this perspective it would be a pity if the Anglo-Dutch cooperation in Cyprus came to an end after only three years, as was originally intended.

The second factor is the organizational structure. It seems noble, but in reality it is sometimes a little naive to have people of different origins cooperate with each other just like that. In general this does not improve cohesion and mutual trust, as is clearly shown in military social research going back as far as half a century ago. It can sometimes be more opportune to create an organization-structural separation between the various groups. In this context the remarks of a lieutenant in the first UNFICYP rotation are quite relevant: 'international integration at a level lower than the company is not successful in my view'. This may be somewhat exaggerated, but the organizational structure most certainly is a factor of importance, especially with regard to cultural differences. It was not for nothing that during the transfer of UNFICYP-II to UNFICYP-III one sector (West 2) came under Dutch command in its entirety. And as far as the Anglo-Dutch marine cooperation is concerned, there has always been a separation of lines of command.

Thirdly, the importance of giving attention to the legal differences cannot be emphasized enough. Many of the disagreements and misunderstandings described above are directly related to this aspect. Both partners should be well aware of the differences between the own and other rules and regulations if these misunderstandings and disagreements are to be avoided. As legal rules reflect the views of a society or organization, there is most certainly a relation between cultural and legal information.

Finally, the context in which the multinational operation takes place requires some attention. When there is little tension in a mission and much boredom instead, cultural friction will manifest itself much sooner than when there is a certain risk and a sense of uncertainty for all.[21] As for this aspect, UNFICYP, with its relatively light and safe character, is perhaps not the most favourable operation with regard to the integration of cultural differences and the forming of cohesion and mutual trust. As said, uncertainty and risk bring people together, but there are also limits there. When the danger is so great that actual fighting comes into play, and, consequently, one's own life is at stake, the tolerance with others diminishes again.[22] Possibly the relation between danger and cultural integration can be represented as a U-shape: when there is little danger, there is little integration; when there is some danger and uncertainty, there is integration; when there is much danger, there is again no integration. This relation is very important in an operational sense, but it has not been properly investigated yet. Once again, this last point emphasized as importance of the attention for cultural differences in multinational military operations. Most definitively, on the eve of the formation of a European Rapid Reaction Force this aspect of production and dissemination of information should be high on the agenda of the policy makers. The many victims of acts of violence that will have to be protected by this Force in the future, will be grateful for it.

Notes

[1]   J. Soeters, 'Value orientations in Military Academies; a thirteen-country study', in: *Armed Forces & Society*, 24 (1997): 7-32; J. Soeters & R. Recht, 'Culture and Discipline in Military Academies: an international comparison', in: *Journal of Political and Military Sociology,* 26 (1998): 169-189

[2]   E. Elron, B. Shamir & E. Ben-Ari, 'Why don't they fight each other? Cultural diversity and operational unity in multinational forces', in: *Armed Forces & Society*, 26 (1999): 73-97; see also, D. Winslow & P. Everts, 'It's not just a question of muscle: cultural interoperability for NATO', paper for the 50th anniversary of NATO conference, Brussels, May 1999; E. Elron, B. Shamir & E. Ben-Ari, *Cross–cultural differences in the multinational peacekeeping forces: faultlines or seamlines?,* unpublished mimeo, Hebrew University, Jerusalem, 2000

[3]   E. Elron et al., 'Why don't they fight each other', (1999): 85; J. Soeters & R. Recht, 'Culture and Discipline in Military Academies', (1998)

[4]   C.C. Moskos, *Peace Soldiers; the Sociology of a United Nations Military Force*, University of Chicago Press, Chicago, 1976

[5]   It may perhaps come as a surprise that cultural tension may exist between western countries that seem to be so close and have such a long history of cooperation within NATO. However, there are comparable experiences, for instance with regard to Danish-US military cooperation. See: H. Soerensen, *Warriors in peacekeeping operations: points of tension in complex cultural encounters,* unpublished mimeo, Kopenhagen, July 1999

[6]   http://un.org/Depts/DPKO/Missions/unficyp/unficypB.html. See also: A. James, 'The UN Force in Cyprus', in: *International Affairs*, 1989: 481-500; M. Evriviades & D. Bourantonis, 'Peace-keeping & peacemaking: some lessons from Cyprus', in: *International Peacekeeping*, 4 (1994): 394-412. A recent publication is: C.H. Dodd (ed.), *Cyprus. The need for new perspectives*, Eothon Press, Huntingdon, 1999

[7]   A. Beevor, *Inside the British Army*: 278-280, Corgi Books, Reading, 1991

[8]   J. Soeters, 'Value orientations in military academies', (1997); J.Soeters & R. Recht, 'Culture and Discipline in military academies', (1998). In the following ample use is made of a term

paper written by two Dutch lieutenants who have been on a mission to Cyprus: the Lieutenants D. Brink & F. van Rosendaal, *Binational cooperation during UNFICYP-II and UNFICYP-III*, term paper (student thesis), KMA-II, Breda, November 2000

[9] J. Hockey, *Squaddies. Portrait of a subculture,* University of Exeter Press, Exeter, 1986

[10] For an interesting inside view on recruitment, discipline and training, see: A. Beevor, *Inside the British Army*: 13-27, Corgi Books, Reading, 1991; A. McNab, *Immediate Action*: 7-32, Corgi Books, Reading, 1995

[11] J. Hockey, *Squaddies. Portrait of a subculture*, (1986): 153

[12] A. van Iterson, 'Rules of action in Dutch work organizations', in: *Netherlands Journal of Social Sciences*, 36 (2000): 176-187

[13] J. Hockey, *Squaddies. Portrait of a subculture*, (1986): 17

[14] D. Brink & F. van Rosendaal, *Binational cooperation during UNFICYP-II and III*, (2000). In the British instructions for the use of violence, open fire is only allowed when the situation endangers one's life or the lives of other UN personnel under one's protection. In the Dutch instructions for the use of violence this is possible in situations that can lead to death or serious wounding of oneself, or other UN personnel or persons under one's protection. These are salient differences indeed.

[15] D. Brink & F. van Rosendaal, *Binational cooperation during UNFICYP-II and III*, (2000)

[16] Document presented in circular letter by Brigadier General W. Bek, 27 March 2000

[17] J. Hockey, *Squaddies. Portrait of a subculture*, (1986): 142

[18] J. Soeters, 'Culture in uniformed organizations', in: N.M. Ashkanasy, C. Wilderom & M.F. Peterson, *Handbook of Organizational Culture and Climate*: 465-481
Sage, Thousand Oaks, 2000

[19] J. Soeters & R. Recht, 'Culture and Discipline in Military Academies', (1998)

[20] J. Soeters, 'The commander's responsibility in multinational operations', in: A.L.W. Vogelaar et al. (eds), *NL ARMS*, [The commander's responsibility in difficult circumstances], 2, 1998: 181-191. See also: E. Elron, B. Shamir & E. Ben-Ari, *Cross-cultural differences in the multinational peacekeeping forces: faultlines or seamlines?*, (2000)

[21] D. Meyerson, K.E. Weick & R.M. Kramer, 'Swift trust and temporary groups', in: R.M. Kramer & T.R. Tyler (eds), *Trust in organizations. Frontiers of theory and research*: 166-195, Sage, Thousand Oaks, 1996

[22] E. Elron, B. Shamir & E. Ben-Ari, *Cross-cultural differences in the multinational peacekeeping forces: faultlines or seamlines?*, (2000)

Preventing poor intelligence cycles during crisis decision making

Evaluating prescriptions and bridging the gap between science and practice

M.V. Metselaar

1.   Introduction[1]

The quality and efficacy of political-military decision making and command depends to a large extent on the quality of the ongoing intelligence cycle. In other words, the more errors organizations and decision makers make during the ongoing cycles of information collection, analysis, information dissemination, and information utilization/response, the more these processes will result in poor decisions, unanticipated risks, costs, outputs and outcomes. This widely accepted assumption is particularly relevant for crisis situations in which the combination of various types of increasing crisis-induced stress can easily result in a dynamic chain of uncontrollable escalations and entrapment. It is therefore hardly surprising that the stream of studies on foreign policy crises which started in the early 60s of the past century produced a wealth of policy prescriptions in order to prevent many of the traps that tend to undermine the quality of C3I cycles and decision making in almost every situation in which policy makers, commanders and their organizations are confronted with serious dangers, time pressures and uncertainty, as well as increasing risks of uncontrollable escalation.

Strangely enough, publications of systematic meta-evaluations with regard to the content and the quality of (specific parts of) the prescriptions that have been offered thus far, have almost been non-existent up to the present moment. Insofar as books, review articles, and conference papers have discussed the state of progress on these aspects of crisis research, it was usually in quite general terms.

This article represents a first attempt to fill this gap. It presents several tentative findings of a research project at the Royal Military Academy that was started two years ago. The article opens with a brief introduction of the main features of the research project. The next section discusses the framework that has been applied hitherto in order to evaluate the quality of policy prescriptions. It will emphasize the importance of logical consistency between the conceptual framework that has guided empirical studies on crisis decision making, the clarity and quality of its key concepts, case selection, main empirical findings and prescriptions. Other criteria that will be examined are, amongst others, (un-)ambiguity of the prescriptions, practical usefulness, range of applicability, etc. (section 3). This set of criteria is applied to a number of (sometimes widely quoted) prescriptions with regard to (a) decision making structures; (b) communication/information aspects; (c) cognitive-psychological dimensions of decision making. The article continues with an evaluation of the quality of prescriptions (section 4) and concludes with some observations on improving it (section 5).

1.1   When the quality of intelligence cycles and information-processing
becomes critical

Serious failures in intelligence cycles and decision making during potentially stressful events are anything but unique. To a certain degree, they can be regarded as a fact of life, almost inevitable and unavoidable, no matter how gladly politicians, the military, researchers, and members of the press would like to close their eyes to them. Military history contains numerous examples of crisis situations and disasters in which the sometimes overwhelming pressures on military commanders and policy makers resulted in tragic mistakes in

information processing and decision making. For example, the onset of WWI in 1914 reveals an impressive chain of poor communications, tragic intelligence failures, and fatal miscalculations and decisions in the centres of command of each of the key players. Whether it concerns the decision makers and planners in Berlin, St.Petersburg, Paris, London, or Vienna, they all became entrapped in an escalatory game which no one could control any more (Holsti, 1965, 1972, 1975; Farrar, 1972; North, 1967). Each of the command centres was confronted with what Von Clausewitz once characterized as 'friction' and 'the fog of war'- situations with a dynamic, almost uncontrollable conflict spiral, combining an overload of information (including noise, rumours, after-the-fact information, deception, etc.) with a sometimes dramatic underload of intelligence and diplomatic messages about the latest state of events. A recently published, more than 500-page-thick, report of a Dutch Parliamentary Commission that describes and evaluates Dutch political-military decision making on peacekeeping operations during the past decade, sums up many – more or less comparable - shortcomings in the quality of intelligence cycles, interdepartmental communication and decision making (Tweede Kamer [Second Chamber] 2000). Shortcomings such as these unmistakably played a role in one of the most tragic and traumatic policy fiascos for the Netherlands, namely the fall of the Srebrenica-enclave in July 1995. It accumulated in one of the greatest post-War genocides in Europe. Similar 'classic' illustrations of what may go wrong when cognition is boiling hot, can be found in crises such as the Barbarossa offensive in 1941, the Chinese intervention in the Korean War, the Bay of Pigs crisis in 1961, the Yom Kippur crisis in 1973, the Rwanda genocide in 1999 or the Russian wars in Chechnya in 1994 and 1996.

These historical experiences illustrate that the quality of political and military decision making, and more in particular its effectiveness, outputs and outcomes may be closely related to the quality of information scanning, processing, and communication. The more shortcomings there are in the collection, processing, dissemination, and utilization of crucial data, the more likely it is that policy makers, as well as military commanders on all levels in the chain of command, will be confronted with tragic miscalculations and painful surprises (De Rivera, 1968; Jervis, 1976; Herek, Janis, & Huth, 1987; Janis, 1989; Betts, 1977, 1978, 1980a, 1980b, 1982; Kam, 1988; Wirtz, 1991; Heuer, 1999). This commonly accepted pattern tends to be particularly relevant in situations in which first-line soldiers and officers, as well as high commanders and politicians are almost 'forced' to take more radical, consequential decisions under risky, dynamic, stressful, and often highly uncertain circumstances (Janis, 1989; Janis & Mann, 1977; Brecher & Geist, 1980; Brecher, 1993; Brecher & Wilkenfeld, 1993, 1997; Hermann, 1972; Holsti, 1972; Holsti & George, 1975; George, 1980, 1991). And they are decisions in which every minor mistake could easily put the well-being and lives of many subordinates, non-combatants, and the decision maker himself at stake.

1.2   The Cuban missile crisis 1962: the trigger for research on crisis decision making

For several reasons, the Cuban missile crisis in October 1962, during which any mistake in the information processing and decision making of political leaders, such as US president John Kennedy and Soviet leader Nikita Krushchev, could have triggered the start of an uncontrollable nuclear and conventional escalation, marked the beginning of scientific research on information-processing during crises. It prompted scientists, historians, socio-logists and social psychologists into setting up systematic research, focused on the way policy makers and their organizations cope with a wide variety of crises (Metselaar, 1997a). One of the main motivations behind this still ongoing research was certainly scientific curiosity and the ambition to build up a body of knowledge about human behaviour under severe collective stress. At the same time, however, it can be concluded that practical orientation, in the form of a strong drive to improve the quality of decision making during crises and to prevent poor

decisions and erratic judgements, formed another dominant incentive for crisis research (Hermann, 1972; Metselaar, 1997a; 't Hart, 1986, 1987). Most (if not all) pioneers in crisis research (e.g. Hermann, Brecher, Holsti, George, Lebow, De Rivera, Janis; Wohlstetter; Lazarus) were strongly driven by questions like: How and under which conditions do policy makers react to signals of impending danger? What patterns and regular traps can be observed in crisis situations themselves and in the decision making and crisis management activities of policy makers, military commanders and their Command, Control, Communication, & Intelligence systems (C3I)? How and to what extent can policy makers, commanders, and their advisors become more aware of possible 'misfits' and 'failures' that regularly occur under crisis pressure? And, last but not least: How can decision makers in key positions, as well as their information supporting systems, be prevented from becoming so overwhelmed by the situational pressures and distress that they make bad decisions with far-reaching negative consequences? How can the risk of normally intelligent leaders becoming entrapped in an almost unavoidable spiral of uncontrollable (nuclear) conflict escalation be reduced? (Axelrod, 1970; Bell, 1971; Betts, 1978; 1980a, 1980b; Brecher, 1977, 1979a, 1979b; Frei, 1978a, 1978b, 1982; Hermann, 1969a, 1969b, 1972; Kintner & Schwarz, 1966; Parker, 1977).

1.3   A blind spot in crisis research

Four decades after the start of crisis research, at the beginning of a new millennium, we can conclude that the study of decision making in crises has become a very productive, diversified field of interdisciplinary research, dominated by aggregate comparative studies (e.g., Gilbert & Lauren, 1980; Brecher & Wilkenfeld, 1988, 1989; Brecher, 1997), as well as many in-depth single and multiple case studies (e.g. Brecher & Geist, 1980; Dawisha, 1984; Holsti, 1972). This research tended to be focused on a wide variety of events: i.e. domestic and local crises, various sorts of international and foreign policy crises, natural disasters and so-called man-made conflict crises, etc. (cf. Rosenthal, 1984; Rosenthal et al., 1986, 1989).

Strangely enough, however, systematic attempts to collect, categorize and evaluate the content and the quality of all the prescriptions that have been produced thus far, have been minimal. Insofar as crisis studies, disaster studies and review articles have discussed the state of progress in crisis research, the examinations on the scientific and practical value of the prescriptions tended to be rather fragmented, brief, superficial, unsystematic, and formulated in quite general terms (see: Tanter, 1975, 1976; Gilbert & Lauren, 1980; Holsti & George, 1975; Holsti, 1975, 1980; Milburn in: Hermann (ed.), 1972; George, 1972; Robinson, 1970; Roberts, 1989; Levite, 1987; Kam, 1988). Given the fact that producing useful policy prescriptions has been one of the major incentives for the start of crisis studies, this omission is remarkable, to say the least. At the same time, however, it can be concluded that, in particular during the past 15 years, there has been a rapid rise of so-called *'How to do it'* handbooks that involve many aspects of crisis decision making as well (e.g. Ten Berge, 1988; Lagadec, 1993; Heath, 1995). These studies tend to provide a wealth of heuristics and descriptions which may be quite relevant and usable for policy makers. Unfortunately, they seldom define the precise conditions in which the provided prescriptions will be more or less valuable, nor do they warn decision makers of situations in which handling in line with the prescriptions may be (or may become) absolutely counter-productive.

In sum, there are various reasons why it is necessary to begin more serious attempts to evaluate the state of the art regarding the scientific and practical value of prescriptions for decision making in crisis situations. First, because it may help to create a more balanced insight into current research on crisis decision making in general, and the quality of the prescriptions that have been offered in particular. Second, it may offer guidelines and ideas for research agendas for the near future (Where are the gaps? What are we doing well, and What should we do better?). Third, it may help policy makers, advisors, and scientists to

answer the fundamental question to what extent the prescriptions that have been largely based on past events, will still be relevant for crises that can be expected in the new millennium. Trends such as the rapid increase of mass media effects (CNN!), the widespread application of modern information technologies and its implications for communication, organization structures and cultures, as well as the increasing quest for information dominance and real-time battlefield awareness, are important elements in this (Pfaltzgraff & Schultz, 1997; Bosch, 1997; Metselaar, 1999a, 1999b). Fourth, it may stimulate mutual learning about methods and experiences within the usually largely separated sub-fields, focused on different dimensions of crisis decision making (i.e. research on [political-military] foreign policy conflict-crises and international crises, research on early warnings and early warning responses, research on surprise attacks and on natural and man-made disasters). Last but not least, it may generate better prescriptions for policy makers, analysts and their organizations and (as far as possible) prevent the danger that they are applying prescriptions that are outdated, not suitable or only usable for a limited time, given the specific conditions and situation at hand.

1.4 Research questions

This article can be regarded as a first attempt to take up the challenge. It is based on a research project that I started two years ago at the Royal Netherlands Military Academy with the help of two research assistants. The research project is guided by the following research question:

> *To what extent have the scientific studies that have been conducted during the past four decades on 'decision making in crisis situations' resulted in policy prescriptions; how are these prescriptions formulated and what is the quality and applicability of these prescriptions, when evaluated from a scientific and practical point of view?*

This central research question is divided into the following set of sub-questions:

1. What criteria can be developed in order to evaluate the scientific and practical quality of policy prescriptions that have been produced in crisis research?
2. What types and areas of research can be distinguished in crisis research and which prescriptions have been formulated with regard to which potential traps in crisis decision making?
3. What is the quality of these prescriptions, when evaluated from a scientific point of view?
4. What is the quality of these prescriptions, when evaluated from a practical point of view? More in particular, are they applicable to peace-keeping or full-scale war operations, and if so, when, where, how?
5. How can the scientific and practical quality of prescriptions be improved in the new millennium?

1.5 Methods and limitations

The research that has been conducted so far, is mainly based on content analysis of the prescriptions that could be found in approximately 270 publications (articles and books) in the area of 'international conflict crisis' (i.e. conflict-crisis studies), military surprise attacks, disaster responses, and early warning responses. Research directed at the fourth and the fifth question has not begun yet. The answers to these two questions will be based on a combination of surveys with semi-structured interviews among policy makers, military commanders and key advisors in the field. This part of the research is scheduled for 2001.

Given the fact that this article reflects 'work in progress' and for reasons of space, the reader should be aware of the following self-imposed limitations:

- Since the meta-evaluation of the prescriptions will be in progress until the end of 2001, the findings that are formulated in this article should be regarded as tentative.
- This analysis will *not* pay attention to prescriptions that have been formulated with regard to crisis *management*. I will only focus on decision making processes that may (but not necessarily have to) lead to crisis management. Nevertheless, it should be kept in mind that there tends to be a close relationship between crisis decision making and crisis management (cf. Herek, Janis, & Huth, 1987; Janis, 1989; Milburn, 1969, 1972; Hermann, 1972; Holsti, 1972; Parker, 1977; George & Smoke, 1974; George, 1980, 1997; 't Hart, 1987). In other words, despite this self-imposed limitation, it is wise to regard weaknesses and traps in crisis management as a continuous and crucial part (or link) in the chain.
- Since it is impossible to mention *all* the prescriptions that have been formulated during the past four decades in this article, I have decided to mention only the ones that have been mentioned in more than one publication in order to give the reader some idea about their content, wording, domain, degree of ambiguity, etc.
- The evaluation review in this article will be focused on only two of the four sub-fields of research on crisis decision making (prescriptions in conflict crises, and prescriptions in surprise attacks). That implies that this article will *not* pay attention to the ever-increasing number of prescriptions (in particular in disaster studies) with regard to one dimension of decision making in crises that tends to become more crucial than ever before: i.e., the transaction between the media and public opinion and decision making (cf. Lagadec, 1993; Crisis Research Team, 1997).
- I will only briefly discuss the empirical studies on which the prescriptions are based. I will not go into detail either with regard to the patterns and traps in decision making and information processing the prescriptions (more or less) refer to.

2.   Evaluation criteria

Evaluations – including the meta-evaluation that will be presented in this article - are almost by definition arbitrary. They may be largely 'coloured' by subjective preferences, knowledge and knowledge gaps, time, culture, and space (cf. Bovens & 't Hart, 1987). However, they may be *even more* arbitrary and random if it remains unclear on which set of criteria they are based. As long as there is no explicitly formulated frame of reference, what are we talking about and how can we learn to improve the quality of the prescriptions? Although this point of departure seems to be common sense at first sight, it was obviously completely overlooked in the few state of the art reviews in crisis research that have been published thus far. Even Gilbert and Lauren (1980) who published a pioneering provocative review article in *Journal of Conflict Resolution*, twenty years ago, failed to formulate even one criterion on which their judgements were based. So, one of the first challenges for this research project was to develop a set of relevant criteria, based on a combination of criteria that can be derived from many standard books on social scientific methodology, policy evaluations, as well as publications about obstacles in the practical utilization of scientific knowledge.

Criterion 1:   *Valence of the prescriptions*
Criterion 2:   *Degree of clarity, instead of ambiguity, of the prescriptions*
Criterion 3:   *Specification of contingencies- and problem dependency of the prescription(s)*
Criterion 4:   *Explicit mentioning of advantages and disadvantages of the application of the prescriptions*

Criterion 5: *Quality of the empirical studies on which the prescriptions are based*
Construct validity: To what extent are the constructs of theoretical interest explicitly operationalized in a manner that decreases intersubjective differences as much as possible?
Internal validity: To what extent does the research design permit us to reach causal conclusions about the effect of the independent variable on the dependent variable?
External validity: To what extent can we generalize from the research sample and setting to populations and settings specified in the research hypotheses?

Criterion 6: *Strength and consistency of the linkage between the formulated prescriptions and the (self-imposed) research limitations, and patterns and traps that have been found in the research on which the prescriptions seem to be based*

Criterion 7: *Practical value of the prescriptions (i.e. possibilities for policy makers to translate them into the practice of decision making)*

3. Six dimensions of crisis decision making

Most studies in the four sub-fields tend to distinguish the following, closely related, dimensions of crisis decision making (e.g. Brecher, 1980, 1997; Rosenthal, 1984; Rosenthal et al., 1989; 't Hart, 1986, 1987; Lagadec, 1987; Kam, 1988):

1. the communication dimension
2. the perception process
3. the group dynamics process
4. the organizational dimension
5. the media (and public opinion) dimension;
6. the choice process.

Each of these dimensions of decision making can have a deep impact on the quality of intelligence cycles and information processing. However, given the limited space of this article, this review will mainly focus on the first two dimensions.

3.1 Regularly observed patterns and traps in intelligence cycles during crisis decision making

Empirical research in all four sub-fields reveals a wide variety of traps that can be regularly observed when policy makers, military commanders and their organizations are coping with (and anticipating on) the subsequent phases of crisis situations. Some of the most common ones that can be observed in almost every studied *surprise attack* is the so-called false alarm/desensitisation/or cry wolf syndrome. Other types of regular traps in information-processing are: more active, but more random and simplified information search, intelligence-to-please syndromes; structural and incidental misperceptions and miscalculations with regard to the enemy's intentions and capabilities, versus one's own intentions and capabilities, in particular in dynamic situations; lack of time; pathological secrecy; information overload and noise (Pearl Harbor and the overload of high-qualified signal intelligence), as well as underload; cognitive rigidity, misperceptions and wrong anticipations (partly) as a consequence of successful deceptions by the enemy; and cognitive indifference, superficiality, hyper-vigilance, as well as avoidance and denial; over-reliance on face-to-face communications with trusted - and liked - sources (e.g. Milburn, 1972; Wohlstetter, 1962; Whaley, 1975; Handel, 1989; Wirtz, 1991; Kam, 1988; Levite, 1987; Metselaar, 1997a, 1997b, 1999a, 2001; Heuer, 1999).

Unlike studies on surprise attacks, studies on *conflict crises* tend to pay more attention to *all* phases of crises (in other words, not only the pre-crisis or anticipation and warning phase, but
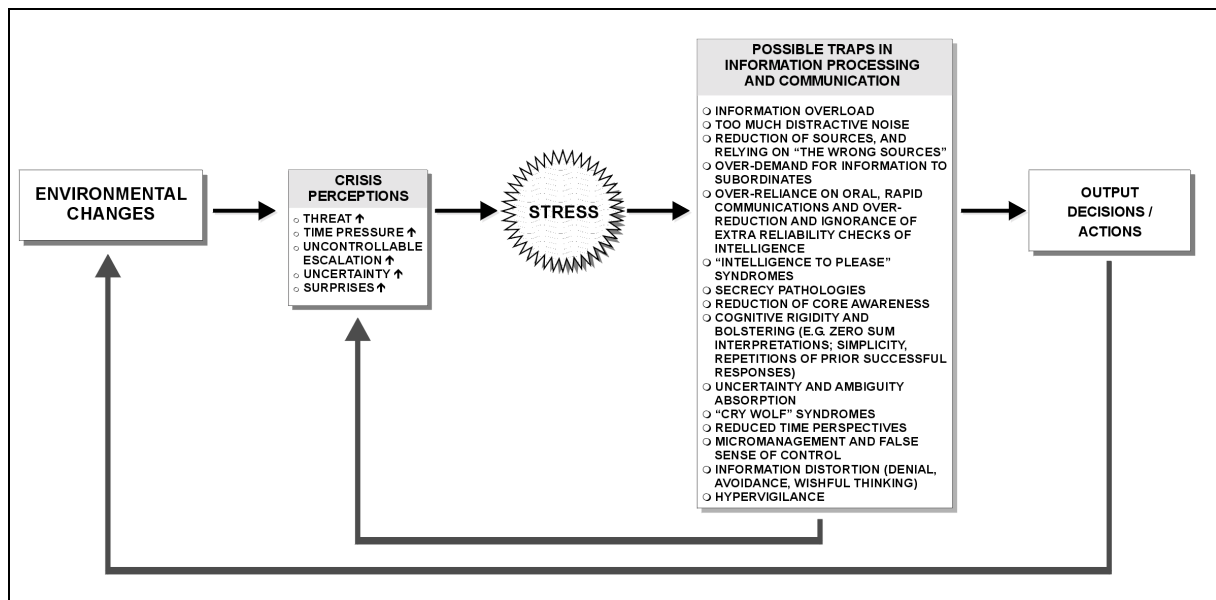

Figure 1: A simplified summary of regular traps in information processing during crises

also the escalation phase, as well as the de-escalation and post-crisis phase) and the impact of crisis-induced stress. They focus in particular on the so-called confrontation/escalation phase, the period in which decision makers often experience increasing peaks of distress. Furthermore, in general the data collection and analysis of conflict crisis researchers tend to be more dominated by a top-down perspective, whereby they focus in particular on the behaviour of policy makers in the top the organizations (e.g. Presidents, Prime Ministers, Ministers of Defence and Foreign Affairs, etc.)[2] As we shall see in the next section of this article, their prescriptions tend to focus mainly on improving the information-processing and decision making quality of the key decision makers and their senior advisors.

The general assumption is that there tends to be a curve-linear (or inverted U-like) relationship between the level of distress a policy-maker or a commander experiences during an operation and the quality of his information-processing, communication, and decision making. Up to a certain level, stress helps decision makers to function well. That is, too little or no stress tends to result in a relatively low quality of information processing and decision making. Increases from low to moderate levels of stress tend to make policy makers and intelligence analysts more alert to the existence of challenges or problems that require attention, decisions and action, and the need to increase vigilance and preparedness to cope with them. However, if the stress that a decision maker or a commander experiences becomes too high (and/or continues for too long) the quality of his performances tends to decline significantly and he and his colleagues may easily fall victim to several well-studied traps. Some of the traps that are described in almost every empirical study on conflict crises are: micro-management (over-concentration on small operational and tactical details, while largely neglecting more strategic information), the tendency of policy makers to fill in blind gaps in their knowledge and intelligence with historical analogies and stereotypes and – partly as a consequence of this – to downplay contradicting intelligence; cognitive rigidity, premature closure (groupthink), failures to recognize cultural differences between oneself and the enemy, etc. (Brecher, 1974, 1979b; Brecher & Geist, 1980; Brecher & Wilkenfeld, 1982,

1997; DeRivera, 1968; Holsti & George, 1975; George, 1974, 1980; Janis, 1982; Vertzberger, 1989; 't Hart, 1989; Roberts, 1989; Heuer, 1999).

Overall, the number of traps that have been described, and that according to most authors, may – at least potentially - undermine the quality of decision making and information-processing in most – if not all – current and future crises is quite impressive. In fact, so much so, that one may wonder how it is possible that the costs and negative consequences of coping with crises are not much greater than they already are (cf. Bovens & 't Hart, 1997).

3.2 A summary of available prescriptions

What types of prescriptions have been produced during the past four decades of empirical research, and what is their content? This section will briefly describe several prescriptions that have been produced in two of the four sub-fields, notably research on surprise attacks and research on conflict crises. As stated above, I will mainly focus on those dimensions of decision making that tend to be the most directly related to information-processing and organizational communication.

Sub-field 1: Research on surprise attacks

In comparison with their colleagues in the area of conflict crises, researchers on surprise attacks and intelligence failures tend to be somewhat more productive in the formulation of policy prescriptions. The following prescriptions appear to be the most relevant ones:

Prescriptions with regard to the perception process
- Attempt to raise the awareness of policy makers and analysts of the problems inherent in the warning *evaluation* process and introduce review procedures, dissent channels, periodic reappraisal, and post mortem analyses, etc. (cf. Lauder, 1985; Shmuel, 1985; Kam, 1988).
- 'In the event that receivers engage in substantial protective behavior, attempts should be made to perceive the danger as a highly cynical one' (Breznitz, 1984: 222).
- 'Training for the search of the uniqueness of each threat can reduce false alarm effects' (Breznitz, 1984: 226).
- Incorporate quantitative methods into the evaluation of incoming warnings (cf. Heuer, 1981a; Singer & Wallace, 1979; Hopkins, 1980; Jodice, 1982; Levite, 1987: 168).

Prescriptions in order to prevent malfunctions in the communication process
- Improve the dissemination stage of the warning communication process through the application of modern computer technologies and other advances in the area of secure real-time communications in order to improve the speed, scope and reliability of information transmissions (cf. Belden, 1977; Gravely, 1982; Levite, 1987; Metselaar, 1999).
- 'The warning system should attempt to delay issuing the threat as long as possible. […] The longer the time interval between the request for protective behavior and its onset, the lower the probability that individuals will engage in it. Thus, protective behavior ought to be limited […] in terms of 'last chances' when it can still be effective. However, such a deadline must not be too close, otherwise it could lead to panic behavior' (Breznitz, 1984: 221, 223).
- 'By identifying a particular segment of the warning system as responsible for the false alarm and by indicating that this segment is being corrected or replaced, the lost credibility can be partially restored' (Breznitz, 1984: 223).
- 'Individuals should be given full information about the false alarm effects and the parameters that influence its magnitude' (Breznitz, 1984: 226).

- 'Ensure a pluralistic intelligence system and parallel analysis and assessment also with the same data' (Kam, 1988: 225-226; George, 1982).
- 'Strengthen cooperation between senior analysts and policy makers' (cf. Kam, 1988; Dror, 1980: 17; Knorr, 1979: 87).

Overall, it will be obvious that both categories of prescriptions are aimed at making policy makers and analysts better aware of various potential traps in the information processing (i.e., perception process) and to improve their insight into factors that may enhance the chances of decision making actually being undermined by these traps. Furthermore, the prescriptions offer several techniques that may help to improve the quality of perception and communication and to reduce (a) gaps between analysts and policy makers; (b) chances on information overload; (c) cry wolf syndromes, (d) dependency on too few sources, (e) failing communication channels, and (g) premature closure and group think tendencies.

Sub-field 2:   Conflict crisis research
In comparison with early warning research and disaster research, the number of studies in decision making during conflict crises providing prescriptions, is remarkably low. For instance, Michael Brecher and his associates from the International Crisis Behavior (ICB) Project have produced several high-quality case studies since 1980. Still, they do not offer any policy prescription. The prescriptions that ICB provides are only directed at improving the quality of future studies on crisis decision making.[3] Another conclusion that can be drawn is that by far the biggest part of the prescriptions that have been formulated thus far, were provided in the period 1972-1975. The bulk of the prescriptions were produced during the first wave of publications in the area of conflict crises. In particular Milburn (1972) presented a lot of still dominant prescriptions. Alexander George, Irving Janis (1977, 1989) and Jonathan Roberts (1989) are among the few exceptions in the field of conflict crisis to formulate some prescriptions after 1975.

Prescriptions in order to prevent malfunctions in the communication process
- 'Avoid channel overload by reducing the communication traffic concerned with non-crisis issues and by increasing the number of channels used'(Milburn, 1972: 273).
- 'Make all communications in a crisis explicit, consistent, and transmit them through redundant channels to reduce the chance of being misunderstood. Remember that perceiving him correctly is not the same as ensuring that he perceives your moves correctly' (Milburn, 1972: 275).
- 'Do not rely on any single method or channel of information, nor upon a single point of observation (Milburn, 1972: 272).
- 'Use several techniques for evaluating the situation and conduct checks on the fidelity of information sources' (Milburn, 1972: 272).
- 'To the extent feasible, keep audiences restricted during a crisis until audience support is needed or until public announcement is desirable to add to the credibility of a commitment' (Milburn, 1972: 273).
- Set up a log book in order to write down quickly the procedures undertaken, steps already decided upon, and elements of information received and do so throughout all parts of the entire organization or network that is involved. If this is not done well enough or not done at all within a few hours, no one will be able to know what is going on, how procedures have been implemented, who said and did what, when, where, how. Writing a log book will (a) force those who are involved to try to see clearly through the mental fog and to put some mental distance between themselves and what they are doing and the course of events; it may (b) force the writers to look more objectively (as

far as possible) about events; it may (c) help to share information and to provide for a smooth transfer from one team to another in a crisis that drags on (Fink, 1986: 146; Parry, 1990; Lagadec, 1993: 202-204;). This may significantly reduce chances of bad coordination.

Prescriptions with regard to the perception process
- Perform according to the kind of crisis that is faced (Milburn, 1972: 272).
- A decision maker's understanding of a crisis increases as his awareness of prior and related events is increased. Consider, therefore, a wide and detailed range of contextual factors (Milburn, 1972: 272).
- 'Study available resources in terms of how readily available they are and what substitutes exist. Check rapidly with allies and others to survey what potential resources they might contribute' (Milburn, 1972: 272).
- 'Be sceptical of 'solutions' transferred from other situations exclusively for the reason that they 'worked' in earlier cases. Be careful of 'facts' in the present situation that seem to suggest that the previous situation is exactly like the present one. If there are no basic similarities, screen out that reference' (Milburn, 1972: 274; cf. Neustadt & May, 1986; Kam, 1988; Vertzberger, 1989; Heuer, 1999).
- 'Attempt to look beyond the crisis. Anticipate future relations and long-term consequences. Avoid contradictions of time perspective and over-emphasis on those things likely to occur in the immediate future' (Milburn, 1972: 274; cf. Holsti, 1972; Hermann et al., 1972; Holsti & George, 1975).
- 'Do not treat the crisis as an isolated incident, never forget to consider the aftermath of the crisis and the way this may determine the method you use' (Lagadec, 1993: 289).
- 'Use simulation and imagination to explore possible costs and dangerous side effects. It is essential that value not be restricted to one kind of benefit or cost. For example, to restrict ourselves to economic, technical, or material costs and benefits may irrationally exclude important human values we also treasure. Quite apart from knowing the costs-benefits of alternative potential 'solutions' to the crisis, we may also want to consider costs and benefits associated with the crisis itself. The costs of the existence of a crisis may include those associated with the centralization of the lines of command and communication. They could also include the creation of intense feelings of bitterness among opponents, which could prove exceedingly difficult to eradicate (Milburn, 1972: 273-274).
- Apply the following five special procedures (Janis & Mann, 1977; Janis, 1983):
  - awareness of rationalizations procedure in order to counteract rationalizations, cognitive bolstering and denial and avoidance (Janis & Reed, 1974);
  - emotional role playing;
  - balance-sheet procedures in order to examine the pros and cons of available alternatives;
  - outcome psychodrama to discover neglected consequences;
  - stress inoculation to prepare decision makers to cope with post-decisional consequences.

In addition, Janis advises to apply seven rules that have been extracted from brainstorming techniques: (a) Do not evaluate at the beginning; (b) Generate as many alternatives as possible; it is always possible to cut down the choices to a smaller, manageable set that contains the most promising alternatives in a later stage; (c) deliberately try to think up a few original, far-out alternatives to include on the balance-sheet, frequently such alternatives turn out to be more practical in a later stage than they initially seemed to be; (d) use the

alternatives that have already been generated as springboards for new alternatives; parts of old alternatives can be combined, broken apart, or shifted around to avoid their flaws; (e) consult other people about consequences of the alternatives or produce other alternatives; (f) use contemplation as a source of ideas; (g) avoid dichotomies;. although many alternatives fall into two dichotomous classes, there are always different ways to choose and implement them and different ways of not committing and implementing them, for example, by relating them to specified conditions, graduality and timing, etc. (Janis, 1983: 169-170; Wheeler & Janis, 1980: 43-48).

4.   Evaluating the quality of the prescriptions

What tentative conclusions can be drawn about the quality of the prescriptions that have been evaluated so far in both sub-fields? I will now discuss 'their performance' on information processing and communication in both sub-fields.

Criterion 1:   Valence of the prescriptions
In comparison with most disaster studies, prescriptions that are provided in research on conflict-crises and surprise attacks tend to be significantly more 'hidden' and fragmented all over the texts of the articles and the books. Specific chapters or sections referring to prescriptions are the exception rather than the rule. Given what we know nowadays about the gap between scientists and policy makers, military commanders and intelligence analysts, omissions like these probably significantly reduce the chances of appropriate utilization of scientific knowledge and insights, in general, and the chance of policy makers, commanders, or intelligence analysts utilizing these prescriptions, in particular. Perhaps, the regular contacts during conferences, courses and working groups between the researchers and military commanders, policy analysts and senior and junior advisors may somewhat compensate for this omission, because they may indirectly encourage mutual understanding in each other's cultures and worlds of action, and because they may increase the chances of dissemination of knowledge, however slowly. Still, this does not preclude that there are some missed opportunities here.

Criterion 2:   Degree of clarity, instead of ambiguity, of the prescriptions.
Most prescriptions are formulated in rather general terms. This may be a logical consequence of the ambition of the researchers to generalize and to offer prescriptions for a wide variety of circumstances. Instead of developing prescriptions that contain a more subtle balance somewhere 'in the middle' between relevance for very specific situations and moments, most researchers apparently seem to formulate prescriptions that cover a much wider range of situations. The implication is that many of them can indeed be criticized for containing 'oracle of Delphi-like' formulations. Whether this has actually led to serious misunderstandings and bad coordination cannot be proven, given the present stage of this meta-evaluation. However, at least in theory, this seems to be quite likely.
Furthermore, especially if the prescriptions are studied in complete isolation from the empirical studies they are derived from, many of them look so general that they can easily be regarded as complete understatements. It is therefore hardly surprising that several reviewers in both sub-fields have qualified some of the prescriptions as mainly 'open doors'. Schroeder (1972: 539), for example, once commented that most of the prescriptions in conflict-research that had been provided at that time (in other words, the majority of prescriptions produced in conflict crisis research during the past four decades!) '[…] *are about as useful as general advice to hospital emergency personnel - keep calm, have equipment ready, make no premature diagnoses'* (Gilbert & Lauren, 1980: 538-539). A clear example of these types of

understatement is, for instance, Milburn's (1972: 260) advice to avoid making decisions while fatigued. On the other hand, it will be obvious that there are several prescriptions that do not deserve to fall into the 'open door' category. Breznitz's prescriptions to reduce the false alarm trap, for instance, go much deeper than this.

The risk that policy makers, commanders and staff members might stereotype most (if not all) of these prescriptions as open doors and common sense may have serious implications. It may easily convince them that, somehow, they readily and fully understand how to manage crisis situations, without grasping the essence of what the author actually meant, or without the lessons that could be deduced if the underlying empirical research had been studied more deeply and critically (cf. Gilbert & Lauren, 1980: 657). Many scientific insights and prescriptions may lead to responses like 'that's just common sense for us,' 'we knew and have done just that all along.' Yet, the same persons who react like this, may easily neglect or forget all the prescriptions they once called 'open doors' and 'common sense' and become entangled in many avoidable traps, when they are actually confronted with the sometimes dazzling dynamics of crisis situations. At the same time, however, at least to some extent, stereotyping may have certain – unintended – positive and paradoxical side-effects as well. The tendency may help to create some false sense of control over the crisis situation and in many cases this has proven to be more productive than situations in which actors are well aware of many of the traps they have become entangled in, but feel relatively helpless and distressed because they realize that there are hardly any or no alternatives to improve the situation.

Criterion 3:   Specification of contingencies- and problem dependency of the prescription(s).
Studies in which the prescriptions are explicitly related to specific features of the crisis situation and antecedent conditions as well as specific features of the decision making process and the organization that is involved are rather scarce. At best there are some promising attempts to accomplish at least part of this (for instance, Janis & Mann, 1977)

Criterion 4:   Explicit mentioning of advantages and disadvantages of the application of the prescriptions.
Whereas conflict crisis studies in general tend to focus exclusively on the advantages of the prescriptions they provide, surprise attack research seems to be much more balanced, realistic and specific in its presentations. The fact that the prescriptions of researchers on surprise attacks seem to be more dominated by a holistic and contingency-prone perspective may play a significant role in the more realistic-pessimistic, 'it all depends'-like tone of their argumentation. For example, several authors in the field of surprise attacks have warned that most prescriptions proposed to obviate intelligence dysfunctions are in fact two-edged swords: in reducing one vulnerability, they often increase another (cf. Betts, 1978: 73; Kam, 1988: 225-226). One of the underlying causes of this different approach may be that surprise attack researchers regularly pay much more attention than their conflict-crisis oriented colleagues to self-critical, but constructive, evaluations of the practical value of their own prescriptions (e.g. Betts, 1978: 83; Kam, 1988; Levite, 1987). They seem to have developed a 'sadder and wiser' attitude towards their possibilities to reduce serious mistakes in the so-called intelligence and preparations cycle. As a consequence, they seem to be somewhat pessimistic about the possibilities to prevent unpreparedness and surprise. They do not seem to have any illusion that unpreparedness in case of an enemy attack or a disaster will ever be completely eliminated. As George and Smoke once claimed, such ambitions can be regarded as highly unrealistic:

Procedural and other efforts to improve recognition and utilization of warning can hope to meet with some success, but it would be dangerous to assume that the fundamental difficulties [...] can be fully […] eliminated (George & Smoke, 1974: 576).

Jervis is another authority on misperceptions and cognitive rigidity in conflict-crisis to strongly discourage any optimism by pointing at the complexity and ambiguity of the ongoing stream of incoming signals and its complex interactions with the cognitions and emotions of the decision makers. 'There is no way to eliminate misperception. The world is too complex and the available information too ambiguous for that' (Jervis, 1977: 184). Richard Betts, an expert in surprise attacks, is obviously even more sceptical about the effects of prescriptions. He suggests that the implementation of a prescription can be counter-productive from a more integrated and macro-point of view, even if it appears to be successful at first sight. He claimed, for instance, that, 'Curing some pathologies with organizational reforms often creates new pathologies or resurrects old ones' (Betts, 1978: 63).

The use of prescriptions such as those mentioned above brings along the risk of becoming no more than an intellectual exercise that does not really affect persistent beliefs. As Knorr put it, 'The danger is that, if these things are done, they will be done routinely and without keen alertness to the likely obsolescence of all preconceptions' (Knorr, 1979: 85). Depending on the conditions, the stage in the decision making process, or the style and character of a decision maker, decision units or the type of organizations, most - if not all - prescriptions will have advantages as well as disadvantages. In sum, the best thing surprise attack researchers seem to long for is to somewhat reduce many of the biases and mistakes that may lead to serious shortcomings in preparedness.

Criterion 5:   Quality of the empirical studies on which the prescriptions are based

Construct validity
In general, it can be concluded that ambiguous concepts are rarely clearly defined and seldom, if ever, operationalized in the same sections or chapters in which the prescriptions are presented. This omission is often somewhat compensated for by the fact that some of the key concepts (such as 'crisis', 'escalation', 'danger', 'warning', 'time pressure', or 'surprise' and 'unprepreparedness') are regularly defined (but seldom operationalized) in earlier parts of the publications, or – in the worst case - in earlier publications of the author himself or publications of others he explicitly refers to (cf. Levite, 1987; Metselaar, 2001). So policy makers, commanders, or staff members who want know more precisely what an author means with his or her prescription, have to invest more of their scarce time in looking elsewhere.[4] For example, studies on surprise attacks, early warnings, disasters, as well as handbooks and procedures and doctrines on C3I, crisis decision making, or crisis management, regularly refer to 'unpreparedness' and various types of 'warning situations'. Yet, explicit, detailed, and cogent definitions of (un)preparedness are hard to come by in most of these publications. What situations - in time and space - should we have in mind when we want to acquire an insight into a defender's state of (un)preparedness? What dimensions, tasks, and responsibilities does preparedness encompass? What are the most crucial features of warning situations? What types of data or signals can be labelled 'warnings'? Partly as a consequence of these conceptual (and operational) shortcomings, the way in which (un)preparedness as well as warnings are often labelled, applied, discussed and evaluated, is often arbitrary. Consequently, given its specific position in both (ex-ante) procedures and (often post-hoc) research, it is hardly surprising that unpreparedness is frequently used as a value-loaded, one-dimensional, black-and-white container term. Moreover, unpreparedness, readiness, preparations, under-reactions, decision making, outcomes and even labels like policy fiascos

are frequently intertwined in a fuzzy way,[5] in which gross simplifications, stereotypes, hindsight bias and even wishful thinking can easily continue to play a dominant role.[6]

Internal validity

To what extent do the research designs permit the researchers to reach causal conclusions about the effect of the independent variable on the dependent variable? This question is difficult to answer, i.e. it should be made more explicit than it is now when exactly it is permitted (or not) to reach such conclusions. Furthermore, it is probably better – for various reasons – to evaluate a criterion like this, with an inter-coder procedure. Nevertheless, if only for the sake of triggering discussion, I would like to put forward at least some tentative impressions about this scientific quality criterion.

A first tentative conclusion that can be drawn is that the sometimes rather loose definitions and poor (or even completely neglected) operationalizations of key concepts and expected effects in many of the case-studies in both sub-fields have at least an undermining effect on the internal validity. Another omission in a lot of case studies in both sub-fields is that many alternative causes are not, or hardly, taken into account. For example, Janis' studies on the effects of groupthink on information-processing mainly concentrate on all the factors that are directly related to the groupthink syndrome. However, some research in order to compare the validity of the groupthink-cause with the potential validity of other causes - on, for example, Admiral Kimmel's failure to take warning signals that the Japanese would attack Pearl Harbor more seriously - is almost completely forgotten.

External validity

The issue of generalizations in social sciences is still developing. Especially during the last 15 years many significant steps forward seem to have been taken. In order to generalize and enhance the external validity of research findings (and derived policy prescriptions!!) case designs need to be developed and formulated more carefully. Criteria for case selection need to become more explicit and logically deduced from the research questions, the theory, and the set of hypotheses, etc. In general, both sub-fields unmistakably gain from this developing insight. At the same time, however, there is a lot that needs to be improved on this point as well. It may certainly have the possible side-effect that prescriptions become more specific and justified.

Criterion 6:   Strength and consistency of the linkage between the formulated prescriptions and the patterns and traps that have been discovered in the research on which the prescriptions seem to be based.

In both sub-fields there is a more or less logical linkage between the theoretical framework, the findings, and the prescriptions that have been formulated. So, in general these findings are positive. Still, as always, there are some things that can certainly be improved. For instance, George and Smoke (1974: 589) have observed that

> It is the nature of any theory that it must simplify some aspects of the reality it seeks to comprehend. But if policy use is to be made of a theory, those elements of the real-life phenomenon that were left out or oversimplified in the formulation of the theory must be identified, and their implications for the theory's content and its use must be noted.

George and Smoke's remark is certainly relevant for the work of both sub-fields. The implications of the explicit or implicit simplifications or selections made by an author, are seldom if ever discussed. Nevertheless, they may have far-reaching consequences for the external validity and value of the prescriptions that have been derived. For instance, at least a part of a deduced prescription may be based on deductions and theory, instead of empirical research.

Criterion 7:   Practical value of the prescriptions (i.e. possibilities for policy makers to translate them into the practice of decision making)

To what extent do policy makers and other practitioners regard the formulated prescriptions as understandable, useful and easy or difficult to translate into practice? To what extent have the formulated prescriptions actually been utilized in order to reduce the chances of traps and serious failures in decision making during crises? At this stage of the research project it is rather difficult to conclude anything regarding this criterion. Of course, some insight into the political world of decision makers sometimes appears to be sufficient to conclude that, for example, some of the prescriptions that are provided by Irving Janis (like the use of psychodrama or emotional role playing) are unlikely to be applied by policy makers and their advisors. The same can be said of Milburn's prescription (1972: 270) that 'psycho-pharmacological aids can be useful to improve the quality of performance' of decision making (cf. Roberts, 1989; Janis & Mann, 1977). By far the most influential prescription seems to be George's well-argued recommendation concerning the benefits of using a devil's advocate and multiple advocacy in information processing and decision making in a small group context (George, 1982, 1985; Janis, 1982, 1989; 't Hart, Stern, & Sundelius, 1997). There are various examples in which policy makers deliberately attempted to structure parts of the information-processing and decision making process in crisis situations in line with these prescriptions.

5.   Challenges for the near future

So, given the prescriptions and analyses that have been discussed, what can be done better in the future? How can we improve the scientific and the practical quality of prescriptions? So far, I have formulated the following tentative recommendations.

- Formulate basic moral and cultural values that may guide the author's conceptions and analysis of crisis decision making as explicitly as possible. Milburn (1972: 271) has commented that prescriptions about crisis decision making and crisis management tend to be based to a large degree upon value premises and cultural values of the researchers who offered the advice: 'Hypotheses concerning crisis management are not like conventional scientific statements; rather, they are imperatives - recipes for action. They are prescriptive and often hortatory as well. Although they are based, in part, on descriptions of real world events – what happens in a crisis – they are also based on value premises: for example, the belief that crises are largely bad and those which are mismanaged worse.' Milburn is probably right. An author's basic moral and cultural values often have a significant impact on his way of data collection, data reconstruction, and, more in particular, evaluations and the prescriptions that will be offered. Consequently, it will be useful to link prescriptions more explicitly to the author's conceptions with regard to the essence and functions of crises themselves – insofar as the author is capable and willing to make his values explicit. For instance, it can be valuable if an author is explicit about the way he looks at crises in general, and the crisis he has studied in particular. Does he regard crises as 'a potential disaster for all parties'; or does he regard them as 'competitions of risk-taking and opportunities to win'; or 'a mix of potential disaster and opportunities to win' (cf. Gilbert & Lauren, 1982; Williams, 1980; 't Hart, 1986, 1987).
- Furthermore, both for scientific and practical reasons, it is necessary that both sub-fields pay more attention to the developments of definition and operationalizations and the motivations behind them.

- Continue with various means to make policy makers, military commanders and advisors as much aware as possible of the more or less regular patterns and traps of crises and decision making in crises;
- Try to study to what extent political leaders, military commanders and advisors have been actually aware of regular patterns and traps in decision making in crisis situations and prescriptions that have been formulated (cf. Haney, 1997; 't Hart, 1987; George, 1972, 1980). Insofar as they are aware of them, try to illuminate how and to what extent they have become so; to what extent this knowledge was actually utilized in concrete crisis-like situations and to what effect. Insofar as they are not aware of them, try to study how this can be explained and how these gaps can be bridged in the future. This important research area is still relatively unexplored. It will be obvious that this is a serious omission because it can be a crucial form of feedback and double loop learning.
- Link sets of prescriptions to a widely accepted taxonomy of crises.

As Gilbert and Lauren (1980: 660) stated twenty years ago, the first step toward curing the ills of research and theory lies in proper diagnosis. Their idea to start this process with the development of a taxonomy of crises still seems to be sound. It requires identifying the symptoms and subjecting the theory to more rigorous testing against reality in order to make it and its prescriptions more sophisticated, differentiated, and capable of addressing the practical needs of policy makers. Hermann's famous 'three-dimensional crisis box' of key elements of crisis, as well as Lebow's typology of crises, and the distinction between cynical and naive dangers (cf. Breznitz, 1984) may become quite relevant dimensions in such a taxonomy. On the other hand, experiences in early warning research indicate that the complexity of such a methodological challenge should not be underestimated.

- Link sets of prescriptions as much as possible to phases in the crisis and crisis management process.
- Be explicit about strengths, weaknesses (including internal inconsistencies), opportunities and threats with regarts to each prescription, and try to make decision makers and analysts aware of them.
- Study the usability and effectiveness of prescriptions that have been applied over the past years (select so-called 'failure' as well as 'success' cases) and apply SWOT analyses to them.
- Try to rehearse at least once a year in as realistic a setting as possible with the key decision makers and their advisors and teams.
- Try to get and provide a more 'holistic system-like perspective' of the vulnerabilities that characterize a 'crisis decision making system' and the impact that the application of prescriptions may have (cf. Perrow, 1984).

Ariel Levite (1987: 171-172) has made quite a valuable remark regarding the utility of remedies to the collection, communications and responses to potential warnings, while drawing on an analogy to the characteristics of a chain:

> The strength of a chain is equivalent to the strength of its weakest link. When significant weakness exists in all or most of the links, improvements in only some of them, as drastic as they may be, will not result in any significant difference in the strength of the chain as a whole. Improvements are required across the board.

In other words, Levite supposes that to make a real difference, potential weaknesses and traps in every stage and dimension of the information processing and communication process, as well as the decision making process need to be addressed and that the prescriptions ought to

be considered complementary and utility interdependent. In general, Levite's remark is sound. Of course, the question which links in the chain will turn out to be the weakest in a crisis will depend very much on the magnitude of the danger that the crisis involves, the domain of the danger, etc (Perrow, 1984).

In general, the art of preventing poor intelligence cycles and information processing during crisis decision making is still full of complex challenges and old as well as new obstacles. In various respects, 'the art of reducing the risks on such failures by learning and formulating better, more precise prescriptions' can - and always will be - a rather frustrating one. Thus, it remains to be seen whether, and to what extent better prescriptions will really reduce the chance of unacceptable and unwanted horizontal and vertical crisis escalations during the new millennium. We should never forget (nor become fatalistic about it!) that decision making process is not the same as outcome (cf. Janis, 1989; Janis, Herek, Wheeler & Huth, 1987; Snyder & Diesing, 1977). In a world that is becoming as interdependent, complex and tightly linked as ours, many other factors will affect processes, outputs and outcomes (cf. Perrow, 1984). Probably, the art and task of providing well-balanced, usable prescriptions will become more difficult and ambitious than ever before. Consequently, no matter how difficult it sometimes may be, the quality of research prescriptions has to be improved in both sub-fields in order to increase the chances that policy makers, military commanders, and their staffs will be appropriately prepared for future dangers, crises and disasters. More regular, critical but constructive self-evaluation is one absolute necessity to accomplish this ambitious mission.

References

Betts, R. (1982), *Surprise Attack: Lessons for Defense Planning*
	Brookings Institution, Washington DC,
Brecher, M., Geist, B. (1980), *Decisions in Crisis: Israel, 1967 and 1973*
	University of California Press, Berkeley
Brecher, M. (1993), *Crises in World Politics: Theory and Reality*
	Pergamon Press, Oxford
Brecher, M., Wilkenfeld, J. (1997), *A Study of Crisis*
	University of Michigan Press, Michigan
Breznitz, S. (1984), *Cry Wolf: The Psychology of False Alarms*
	Lawrence Erlbaum, London
Davies, J. L., Gurr, T.R. (eds.) (1998), *Preventive Measures: Building Risk Assessment and Crisis Early Warning Systems*, Rowan & Littlefield, Oxford
George, A.L. (1980), *Presidential Decision making in Foreign policy: The Effective Use of Information and Advice*, Westview Press, Boulder
Gilbert, A.N., Lauren, P.G. (1980), Crisis management: An assessment and critique in: *Journal of Conflict Resolution,* 4, 1980: 641-664
Hermann, C.F. (ed.) (1972), *International Crisis: Insights from Behavioral Research*
	Free Press, New York
Heuer, R.J., Jr. (1999), *Psychology of Intelligence Analysis*, Center for the Study of Intelligence, CIA, Washington DC
Janis, I.L., Mann, L (1977), *Decision Making: A Psychological Analysis of Conflict, Choice, and Commitment*, Free Press, New York
Kam, E. (1989), *Surprise Attack: The Victim's Perspective*
	Harvard University Press, Cambridge, Mass.
Lagadec, P. (1993), *Preventing Chaos in a Crisis*, McGraw-Hill, London

Metselaar, M.V. (1997), Understanding failures in intelligence estimates: UNPROFOR, the Dutch, and the Bosnian-Serb attack on Srebrenica
in: J. Soeters & J. Roovers (eds.), *NL ARMS* [The Bosnian Experience], 1997: 23-50

Metselaar, M.V. (1999), Is more information necessarily better? Advantages and disadvantages of the explosion of information technologies for political and military preparedness, in: J.M. Bosch, H.A. Luijf & A.R. Mollema (eds.), *NL ARMS* [Information Operations], 3, 1999: 259-276

Tanter, R. (1975), Crisis management: A critical review of academic literature
in: *Jerusalem Journal of International Relations*, 1975 / 1: 71-101

---

[1] This article is based on two conference papers which were prepared and presented during the Convention of the International Studies Association in Los Angeles, California, March 2000 and at the West Region Conference of the International Studies Association in San Francisco, in October 1999. The author wishes to thank the participants of these workshops for their helpful comments and suggestions. Furthermore, I have mentioned only a small part of the articles and books on which this article is based in order to reduce the length of the list of references as much as possible. Readers who like to have the complete list are invited to contact the author (mv.metselaar@mindef.nl).

[2] The perspective of researchers in surprise attacks seems to be more dominated by a bottom-up approach, with a key role for the intelligence agencies and military commanders in the field.

[3] Perhaps Brecher c.s. decided already from the start of the International Crisis Behaviour project in 1978/1980 not to invest time and energy in the formulation of policy prescriptions. In the future I hope to find out whether this was actually the case and if so, why they decided to do so.

[4] Of course, I am taking for granted here that the authors are consistent and unambiguous in the way they have applied and referred to these concepts (which is not always automatically the case!).

[5] See, for instance, Janis, 1962; Janis & Mann, 1977; Lagadec, 1993; Holsti, 1972. Positive exceptions to this rule are, for instance, the studies of Kam (1988) and Levite (1987).

[6] Bovens & 't Hart, 1997 have analyzed many of these types of traps that may seriously undermine the quality of evaluations and prescriptions in their trail-blazing book on understanding policy fiascos.

Part Four

The role of information in technological developments

Information dominance

What it is and some examples on how it can be achieved

J. Rogge [1]

1.   Information dominance and situational awareness

Information dominance and information superiority are closely related terms. The *US Army Field Manual 100-6* on *Information Operations* defines information dominance as:

> The degree of information superiority that allows the possessor to use information systems and capabilities to achieve an operational advantage in a conflict or to control the situation in operations short of war, while denying those capabilities to the adversary.

In his well-known book *Information Warfare, Principles and Operations*, E. Waltz (1998) quotes the US DoD:

> Information superiority is the capability to collect, process and disseminate an un-interrupted flow of information while exploiting or denying an adversary's ability to do the same.

The objective of this flow of information is to provide *dominant battlespace awareness* (the understanding of the current situation based, primarily, on sensor observations and human sources) and *dominant battlespace knowledge* (the understanding of the meaning of the current situation, gained from analysis).

The benefits of information superiority are to be found in the following operational areas: intelligence preparation of the battlespace, battlespace surveillance and analysis, battlespace visualisation and battlespace awareness dissemination. A key step towards achieving information dominance is reached when one commander's level of battlespace visualisation is significantly greater than that of his opponent's (*US Army Field Manual 100-6*, 1996).

Depending on the source, the quality of the information and the contribution to information dominance can vary. Important *quality assessment criteria* are:

- accuracy (does the information convey the true situation);
- relevance (does the information apply to the mission, task or situation at hand);
- timeliness (is the information available in time to make decisions);
- usability (is the information in common, easily understood formats and displays);
- completeness (does the decision maker require more information);
- precision (does the information have the required level of detail).

From the technical point of view, sensor systems are important sources of information. They can be mounted on different platforms, either space-based, airborne or ground-based. The accuracy, timeliness, completeness and precision of the information are highly dependent on the sensor/platform combination that is used. This is elaborated in the following sections where emphasis is placed on the large class of sensors that use electromagnetic radiation.

After a brief description in section 2 of the general properties of sensors and platforms, some selected topics will be treated in section 3. Intelligence Preparation of the Battlespace (IPB) is an ongoing activity, using existing databases and accurate (but not necessarily real-time) information. Reconnaissance and Surveillance (RS) produce actual information with a (near) real-time character. Some examples of both IPB and RS will be presented; it is clear that in practice these processes show mutual interference and overlap. The final topic in section 3 is Vehicle Positioning Systems, using GPS, as a basic information system for a Battlefield Management System (BMS). Apart from GPS, no ground-based sensors will be considered in this paper.

2.   Sensors and platforms

2.1   Sensors
The timeliness of information depends greatly on the ability of the sensor to function during day and night and in adverse weather conditions (fog, rain, clouds). The accuracy of information in general decreases with time, unless it can be updated regularly within intervals consistent with the rate of change of the situation. Precision (information details) strongly depends on the resolution that is offered by the systems.

Optical sensors include (analog) photographic systems and (digital) CCD cameras for daylight operation and image intensifiers and night vision goggles (mainly for individual use) for night time. Their use is limited to clear weather conditions: no fog, no rain and (depending on the height of the platform) no clouds. These restrictions can have severe consequences for the timeliness and accuracy of the available information, especially if (near) real-time information is required. An advantage of the optical sensors is their good performance as far as the geometrical resolution is concerned: they are, in principle, capable of offering very detailed information. The resolution, measured in meters, is range dependent.

Panchromatic optical sensors use a relatively broad wavelength band, containing a lot of energy, to generate a black and white image. Due to the large signal-to-noise ratio that is available a good geometrical resolution can be obtained. *Multispectral* sensors make observations in different, relatively narrow, wavelength bands of the electromagnetic spectrum. Because these bands contain less energy, the required signal-to-noise ratio can only be achieved at the expense of the geometrical resolution. Since the elements in the terrain have different reflective characteristics in different wavelength bands, the sensor signals can be used to discriminate between these elements. *False colour images* are generated when three sensor signals, originating from three wavelength bands, are displayed in red, green and blue respectively. The same technique can also be used to generate false colour polarimetric SAR images or fused images from different sensors (image fusion). The composition of these images must be carefully chosen in order to highlight the required information, thereby using the relevant sensor properties in an optimal way.

Thermal infrared sensors (thermal imagers) can operate during day and night and are slightly less vulnerable to weather conditions (light fog can be tolerated). Completeness of information is sometimes better than for optical sensors since thermal camouflage is (still) less effective. Geometrical resolution is not as good as for optical systems.

Active microwave systems can be used during day and night and under nearly all weather conditions (except heavy rain). This favours the timeliness of information. Detection performance is good, but geometrical resolution is in general insufficient for object recognition. In

(conventional) side-looking airborne radar (SLAR) the geometrical resolution in azimuth direction (flight direction) is range-dependent and the use of these sensors is restricted to airborne platforms. The azimuth geometrical resolution of synthetic aperture radars (SAR) is range-independent; this sensor can be mounted on satellites, airplanes and RPVs as well. SAR signal processing is very complex and requires more computation facilities than the platform can generally carry. Therefore, high capacity storage facilities or data links are necessary. Real-time operation is not yet possible.

2.2 Platforms

Commercial satellite services show an explosive growth, both in communications and intelligence (spaceborne remote sensing). Satellites are very well suited as a platform to monitor large areas on a regular basis. The orbit of these platforms is elliptical in shape, but satellites carrying image forming sensors are usually put in orbits which very much approximate a circle. Gravity laws cause a high orbiting satellite to take considerably longer to circle the earth than a low orbiting satellite. The orbital period of a geostationary satellite at a height of nearly 36,000 km is (of course) 24 hours, while for the SPOT satellite, having an 830 km altitude orbit, the period is approximately 100 minutes. SPOT is a typical example of the class of image forming remote sensing satellites. Quite often these are placed in a sun-synchronous orbit, which is a low altitude polar orbit that allows the sensor to take repeated images at the same time of day. Since the orbital period is much less than one day, images can

System	Timeliness/accuracy	Precision/completeness
Optical sensors	daytime; clear weather	high geometrical resolution, range dependent; high radiometric and spectral resolution
Thermal infrared sensors	day and night; weather dependent	Medium geometrical resolution; high thermal resolution; less vulnerable to deception and camouflage
Side looking airborne radar (SLAR)	day and night; all weather	good detection performance; low resolution
Synthetic aperture radar (SAR)	day and night; all weather	Medium geometrical resolution, range independent; polarimetry/interferometry/MTI
Airborne platforms	Depending on access to the area of interest	Depending on the sensors on board
Spaceborne platforms	Depending on the revisit time	depending on the sensors on board

Table 1: Selected characteristics of some sensors and platforms

be acquired of several ground tracks within 24 hours. After a number of days (for SPOT: 26 days) the ground tracks are repeated; the revisit time (the minimum time between two observations of the same area) can be much shorter, depending on the capability to steer the sensor's field of view. For SPOT, the revisit frequency can be as high as 11 times in the track repeat period of 26 days.

The revisit time is an important parameter with respect to the timeliness and accuracy of information. A second important parameter is the geometrical resolution: high precision information, showing many details, requires a good (i.e. small) geometrical resolution. For electro-optical sensors, the geometrical resolution gets worse as the range to the scene increases, which favours low flying platforms. The resolution of SAR systems is independent of the range: 'SAR on a satellite is as good as SAR on an RPV', but the resolution cannot match that of electro-optical sensors.

Compared to airborne platforms, a great advantage of satellites is their extraterritorial status: an essential asset in nearly all stages of a (potential) crisis situation. Data can only be transmitted to a ground station when a line-of-sight is present. This requires either a storage capacity on board of the platform or an adequate number of ground stations. For real-time operations in a certain area, a (semi)mobile ground station can be a good solution. Airborne platforms may have the possibility to adapt their position (height) in order to establish a line-of-sight.

3.   Selected topics

3.1   Intelligence Preparation of the Battlespace (IPB)
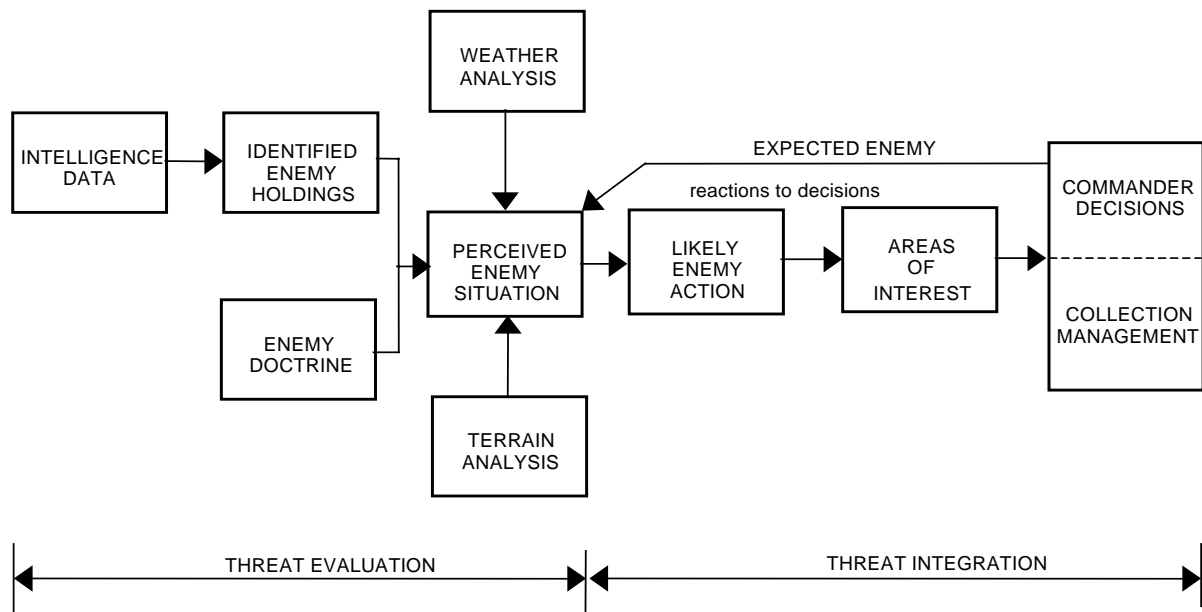The major elements of IPB are shown in Figure 1 (Waltz & Llinas, 1990).

Figure 1: Intelligence Preparation of the Battlespace

Intelligence preparation of the battlespace comprises two major parts: threat evaluation (using multisource intelligence data, providing an initial assessment of the situation) and threat integration (leading to the identification of areas of interest and priority information

requirements. The IPB process is continuous. It concentrates on building the IPB data base prior to hostilities and outlines its applicability in support of tactical operations.

This section will focus on the element labelled 'terrain analysis' in figure 1. Geographic Remote Sensing (GRS) from spaceborne or airborne platforms provides input for Geographic Information Systems (GIS) which form a basis for systems such as ISIS (Integrated Staff Information System) and BMS (Battlefield Management System). A GIS can also be used in the mission planning process to predict terrain trafficability estimated from soil type, slope gradients, tree size and distance, road width, ditch size, etc. (provided this information is contained within the GIS). Important features in a GIS can be selected from a DIGEST database (Digital Geographical Exchange Standard); they can be grouped in several categories:
-       culture: buildings, roads, bridges,…
-       hydrography: rivers, lakes,…
-       relief: contour lines,…
-       land forms: soil type, soil condition,…
-       vegetation: cropland, trees (including height, stem diameter, spacing,…),…

Airborne and spaceborne remote sensing examples will be given in the categories landforms/vegetation, culture/hydrography and relief. The actualisation of an existing topographic map will be demonstrated as an application.

Figure 2 shows three images of the area around the city of Olst (size 3 km by 2 km). The sensors were mounted on *airborne* platforms. From top to bottom:
-       a false colour image, generated by a multispectral optical sensor; geometrical resolution 3 m;
-       a thermal infrared image; geometrical resolution 5 m, thermal resolution 0.15 K;
-       a SAR image; geometrical resolution 6 m.

Classification of ground elements in a false colour image is based upon knowledge of the reflective properties in the different wavelength bands, supplemented by collected ground truth (field checking), for example: maize fields are displayed in brown, pasture in red, barren ground in green.

The thermal infrared image reveals the (radiation) temperatures in different grey-levels. Culture elements (e.g. buildings) are shown in white, just like barren land (heated by the sun), while pasture, having a lower temperature, is nearly black.

Buildings exhibit strong backscatter of the microwave radiation and appear as white spots in the SAR image. In some systems the SAR transmitter and receiver are both operating in the same (vertical or horizontal) polarisation mode (single channel mode). A polarimetric SAR has three channels for three combinations of vertical and horizontal polarisations. Examples of images are given in Figure 3 (Smith et al, 1999), showing a larger area around the same city as in figure 2. From top to bottom: three channel mode (avaraged polarimetric channels, featuring less noise than the one channel mode), false colour (using the outputs from the three channels independent of the classification of the ground elements) and the 'classification image' (using the signals of the three channels for the classification: water is blue, grass is light green, forest is dark green, barren ground is black, etc.). The geometrical resolution in all three images is 6 m.
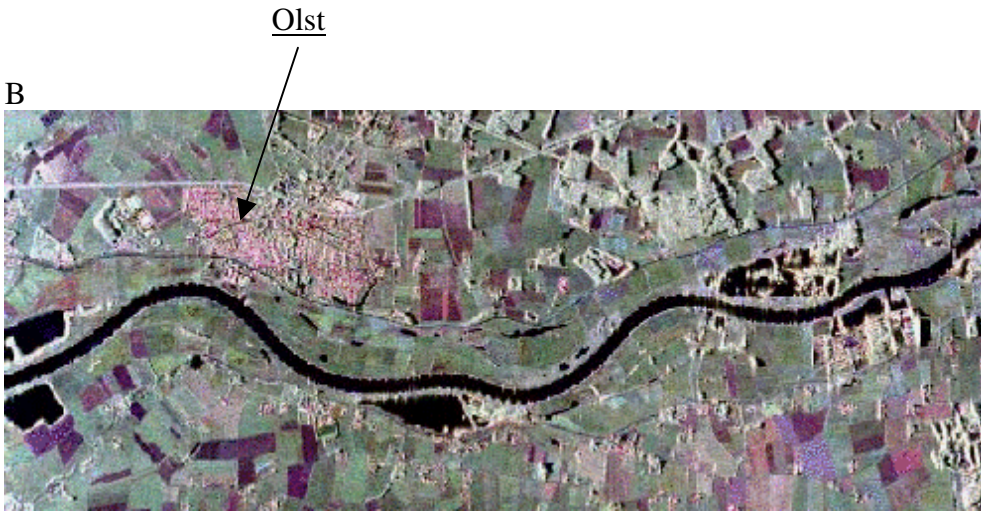
A

Olst

B

C

Figure 2:   Three images of the area around the city of Olst
              A.   False colour optical image
              B.   Thermal infrared image
              C.   SAR image

A

Olst

B

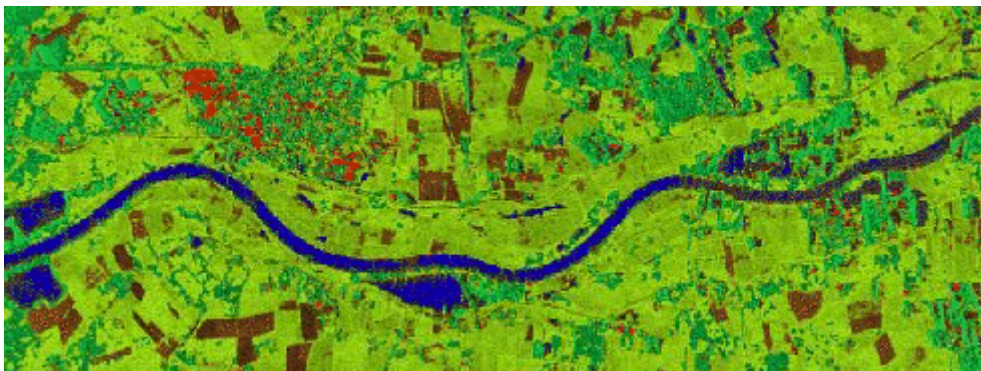C

Figure 3:   SAR images of a larger area around the city of Olst
            A.   Three channel mode
            B.   False colour
            C.   Classification result

Examples of *spaceborne* remote sensing are given in Figure 4 (Wijnhoud, 1995); the city of Olst is indicated.

In each of the images the false colour is generated by combining in red, green and blue the signals from three out of the seven wavelength channels of the LANDSAT/TM satellite (land observation satellite/thematic mapper). The ground resolution is 30 m. Specialists use these false colour images to classify and monitor landforms and vegetations. LANDSAT images are available from one of the many commercial satellite services that are in operation.
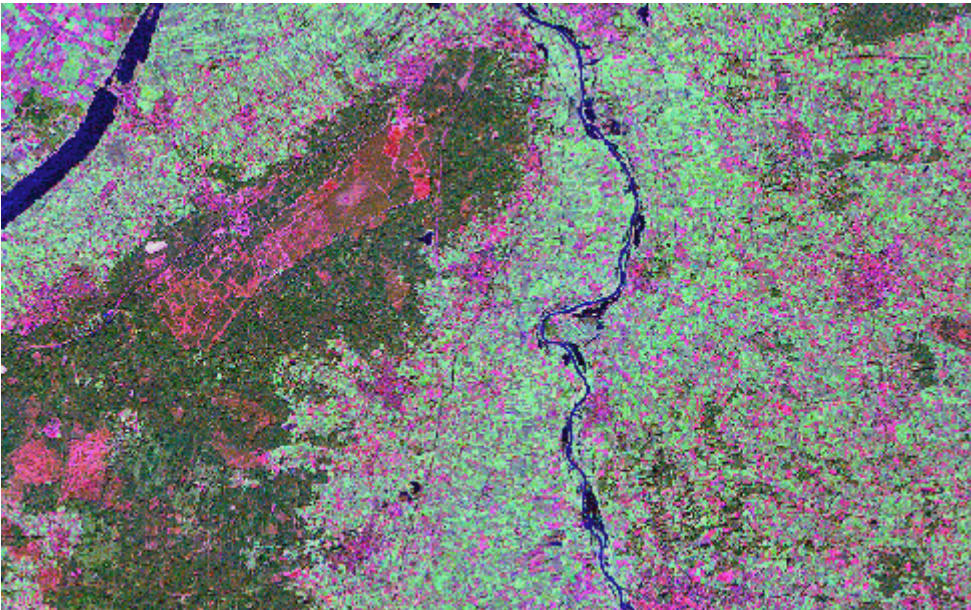
A
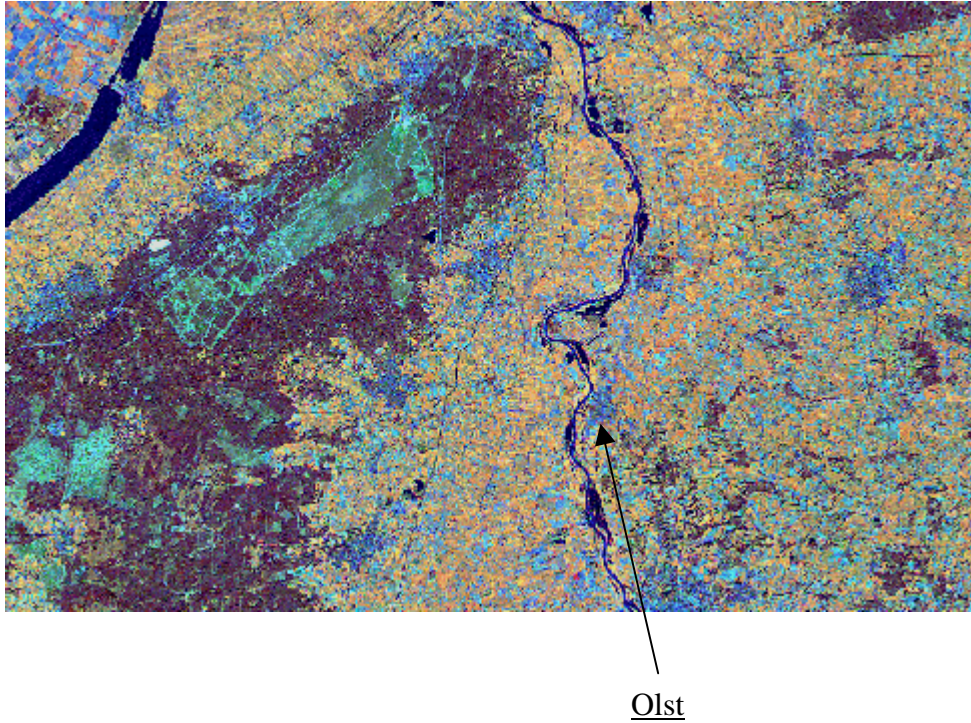
Olst

B

Figure 4: Examples of spaceborne remote sensing of the area around the city of Olst

Figure 5 (van de Broek et al., 1998)) shows satellite images of a power plant and the corresponding topographic map. The sensor/platform combinations are LANDSAT/TM (optical/false colour, resolution 30 m), SPOT XS (optical/false colour, resolution 20 m), SPOT PAN (optical/ /panchromatic, resolution 10 m), KVR (optical/photographic, resolution 2 m), ERS (SAR, resolution 25 m) and JERS (SAR, resolution 25 m).
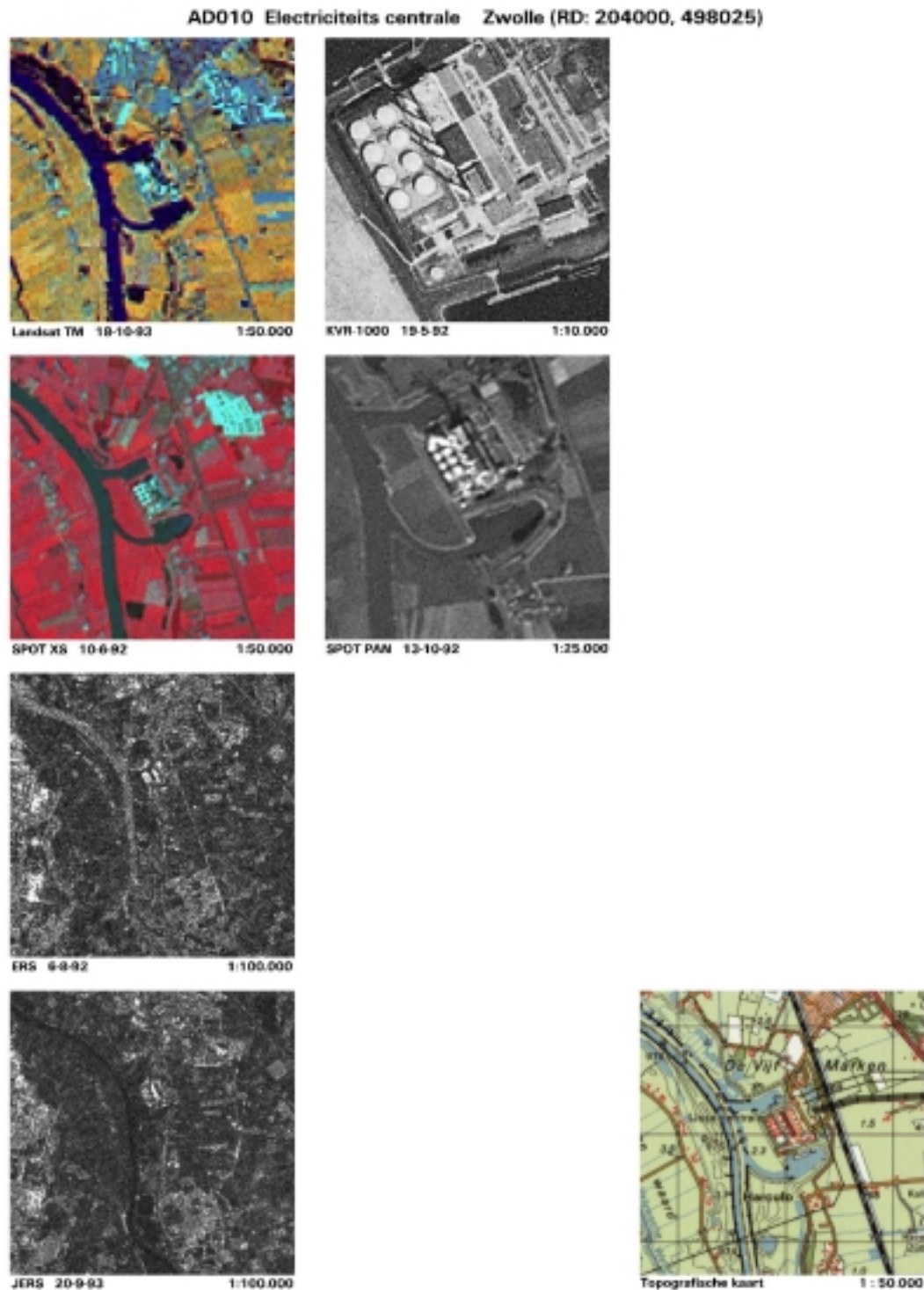

Figure 5: Satellite images of a power plant and the corresponding topographic map

Feature extraction from airborne and spaceborne imagery can be an essential element in the process of updating topographical maps. From the given examples it may be clear that in order to achieve completeness of the information, landform and vegetation features require good sensor performance with respect to spectral and radiometric resolution, while culture and hydrographic features require good geometrical resolution. In addition to this, the relief is of great importance for different reasons.

Distortions of airborne and spaceborne imagery occur when height differences (relief) are present in the terrain. These distortions can be corrected if a DEM (Digital Elevation Model) is available. Furthermore, a DEM can be used to generate relative and absolute height maps (slopes, height contour lines) and synthetic environments for the purpose of mission rehearsal (flight simulation for aircraft, helicopter or RPV as part of the mission preparation).

Both optical and microwave sensors can be used to generate a DEM. The most important techniques are optical and microwave shadowing (mainly for small scale height determination such as tree height), optical stereo and microwave interferometry. The latter two methods require images from the same area, taken under different viewing angles. SPOT satellites produce 'repeat pass' stereo images: the same area is observed during different orbits. Appropriate optical stereo image pairs are not always available in existing databases, but can be obtained from present spaceborne systems within a number of weeks, depending on the weather conditions. Future planned optical satellite systems will often have forward-backward viewing capabilities so that stereo-pairs can be acquired during one overpass. Present sensors offer a height resolution of about 10 m with a grid size of 100 m.

ERS 1 and 2 'repeat pass' microwave interferometry can, in principle, produce a DEM with an accuracy of about 10 m. Small environmental differences in the repeated passes (vegetation!) introduce noisy figures, degrading the accuracy. Single pass interferometry (which requires two antennas on the platform, separated by some distance), does not suffer from this effect. In an experiment in 1999/2000 the Space Shuttle carried two antennas, 60 m apart, providing a height resolution of 15 m and a ground resolution of 30 m. A 'world wide' DEM will be created, covering the area between 60^0 North and South latitude.

An important application of geographic remote sensing products is the actualisation of existing topographical maps. In a demonstration experiment, conducted by the Topografische Dienst Nederland (Dutch Topographic Service) and GeoPerfect TWI b.v. (currently ESRI Nederland b.v.), an older map of the former Yugoslavia was taken as a starting point. SPOT satellite images of the same area were selected from an existing catalogue, on the basis of a quick-look via Internet. With two overlapping images a DEM was constructed and used for the distortion correction of the SPOT images. These images were then compared with the (digitised) topographical map. The two products are shown in Figure 6 (a, b):

- an updated map
- an adapted satellite image, including selected features
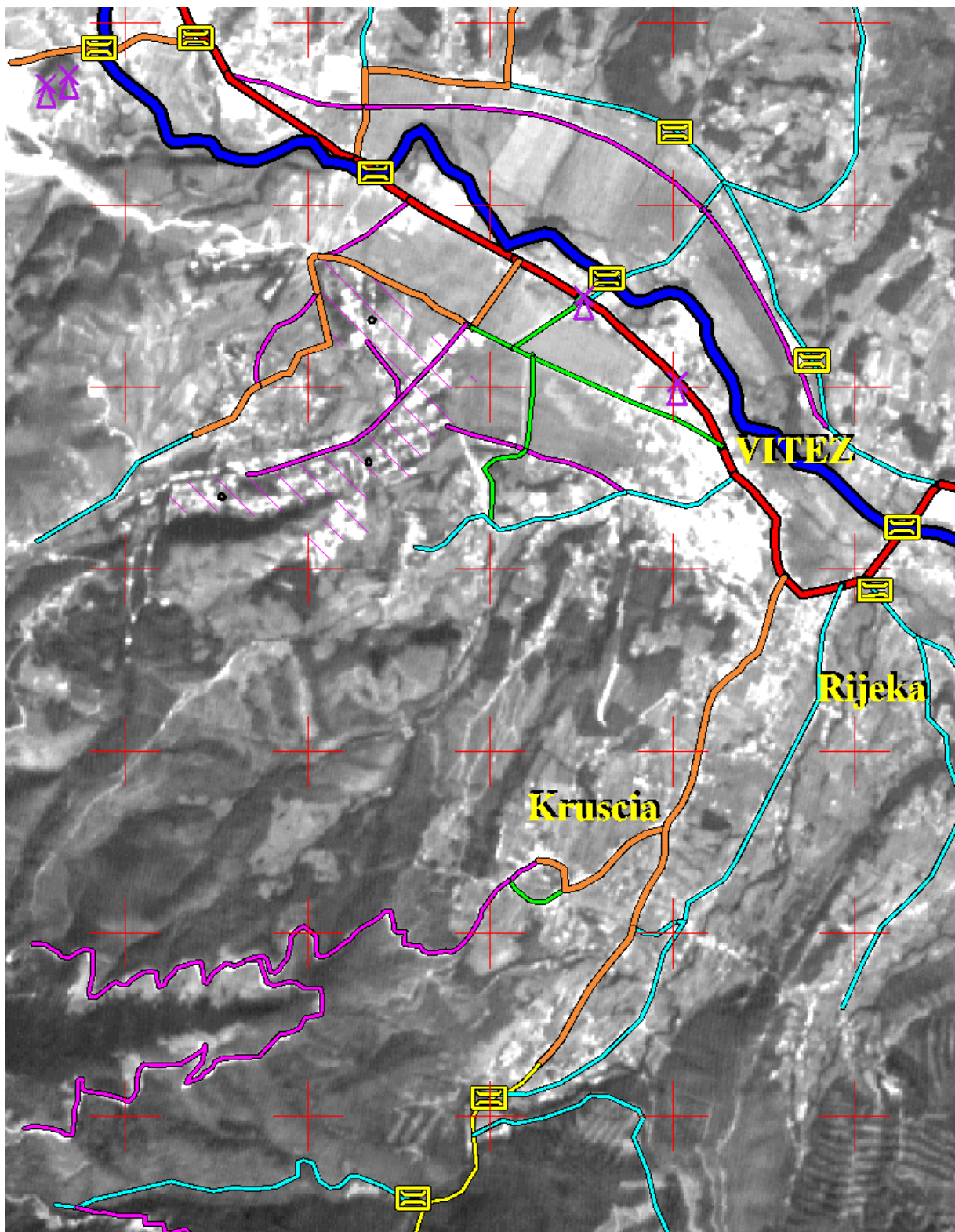
© Spot Image
© Nationaal Lucht- en Ruimtevaart Laboratorium (NLR)
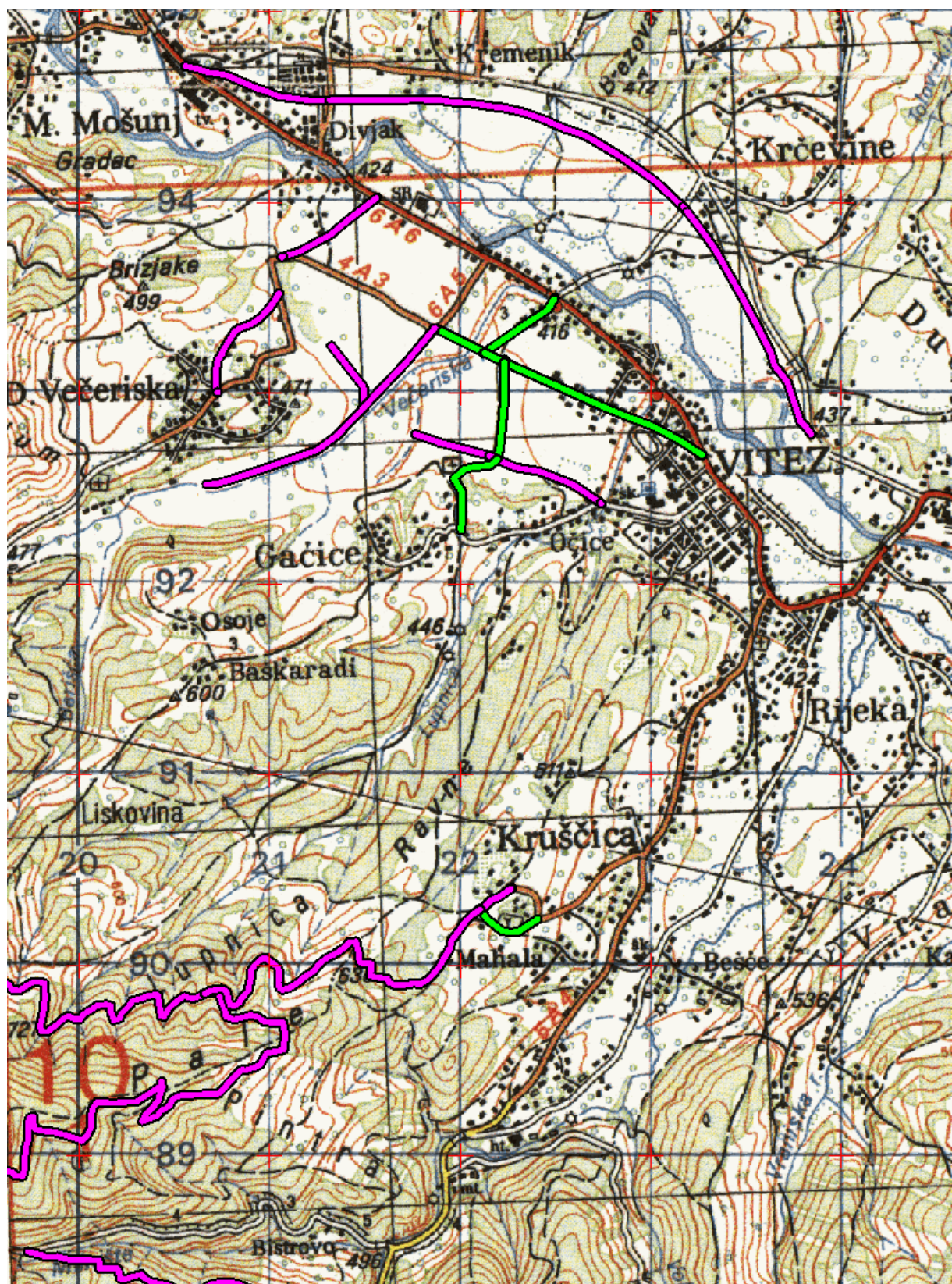
Figure 6a: Satellite image

Figure 6b: Topographical map

3.2   Reconnaissance and Surveillance

Waltz (1998) distinguishes two categories of intelligence sources: *open sources* (radio, television, newspapers) and *closed sources*. IMINT (IMagery INTelligence) is supported by sensor systems on spaceborne, airborne and ground platforms. In this section emphasis is placed on a rapidly developing class of open IMINT sources: commercial satellites. They provide services for military and civil organizations, friendly and (potentially) hostile alike.

'A New Era in Satellite Imaging' was announced in *Aviation Week & Space Technology* (Anselmo, 2000) on the cover page with an Ikonos image of London as background. Space Imaging Inc's Ikonos optical satellite was launched on the 24th of September 1999. It is the first of several high resolution commercial spacecraft that will be looking at the globe from space. In the panchromatic mode the geometrical resolution of the optical sensor is less than 1 meter; the revisit time is about 3 days (or shorter when poorer resolution is acceptable). After appropriate processing the digital imagery is available to the customer within one day after the image was taken. Figure 7 shows the centre of Amsterdam, taken from the Ikonos satellite (http://neonet.nlr.nl/npoc/News/ikonos_amsterdam.html).

© Space Imaging Europe
© Nationaal Lucht- en Ruimtevaartlaboratorium (NLR) 2000

Figure 7: The centre of Amsterdam, taken from the Ikonos satellite

In the coming years the number of commercial satellite platforms will increase significantly. The following list has been compiled from Anselmo (2000) and Hewish (1999).

COMPANY	SYSTEM	PROPERTIES	SCHEDULE
Space Imaging	Ikonos (optical)	Geometrical resolution 0.8 m (panchromatic) and 3.2 m (multispectral),revisit every 3 days, swath 11 km	Launched September 1999
	Ikonos (optical)	geometrical resolution 0.5 m (panchromatic) and 2 m (multispectral)	launch: 2003/2004
Orbital Imaging Corporation	OrbView 3 (optical)	Geometrical resolution 1 m (panchromatic) and 4 m (multispectral), swath 6 km	launch: end 2000
	OrbView 4 (optical)	as OrbView 3, but in addition hyperspectral sensor for chemical analysis of ground elements	launch: 2001
Earth Watch Inc.	QuickBird 1 (optical)	Geometrical resolution 1 m (panchromatic) and 4 m (multispectral), swath 22 km	Launched November 2000 (Failed !)
	QuickBird 2 (optical)	as QuickBird 1	launch: 2001
Spot Image	Spot 5 (optical)	high resolution stereoscopic payload for relief measurements, resolution 5 m (panchromatic) and 10 m (multispectral)	launch: 2002
RadarSat International	Radarsat 2 (SAR)	Geometrical resolution 3 m	launch: end 2002

Table 2: List of commercial satellite platforms

An indication of the commercial importance of these projects comes from the US National Imagery and Mapping Agency (NIMA), which expects to spend $ 1 billion during the period 2000–2005 for commercial imagery and derived products, such as geographical data production, imagery analysis products and services (*Aviation Week's Space Business*, April 3, 2000).

A drawback of spaceborne platforms might be the duration of revisit intervals in certain areas. Another disadvantage is the time it takes to transmit imagery to the ground as the satellites occasionally take several orbital revolutions to arrive within the range of the ground stations. These problems can (partially) be overcome by putting more satellites in orbit, placing more

receiver stations at strategic intervals or by setting up mobile ground stations near (potential) crises areas or even in the theatre of operations to acquire data in near-real-time. *Timeliness* of information, which is a very demanding requirement in fast-moving military situations, can thus be improved considerably.

In a demonstration project in June 1999, under the umbrella of the German-Italian-Netherlands-Norwegian EUCLID Research and Technology Project RTP 9.8, the Dutch National Aerospace Laboratory (NLR) showed the mobile RAPIDS (Real-time Acquisition and Processing Integrated Data System) ground station at Volkel Air Base. This ground station has been developed under a United Kingdom/Netherlands program and consists of a mobile tracking and receiving antenna and smart mini-terminals for dedicated, tailored, pre-processing of the raw data, followed by automatic extraction of information.

Figure 8:   Real-time Acquisition Processing Integrated Data System ground station
(http://www.neonef.nl/rapids)

In the demonstration, SPOT and ERS overpasses were captured; one of these overpasses included a SPOT multispectral image of Volkel Air Base (figure 9). A fulle-scale EUCLID demonstration is scheduled for 2002.
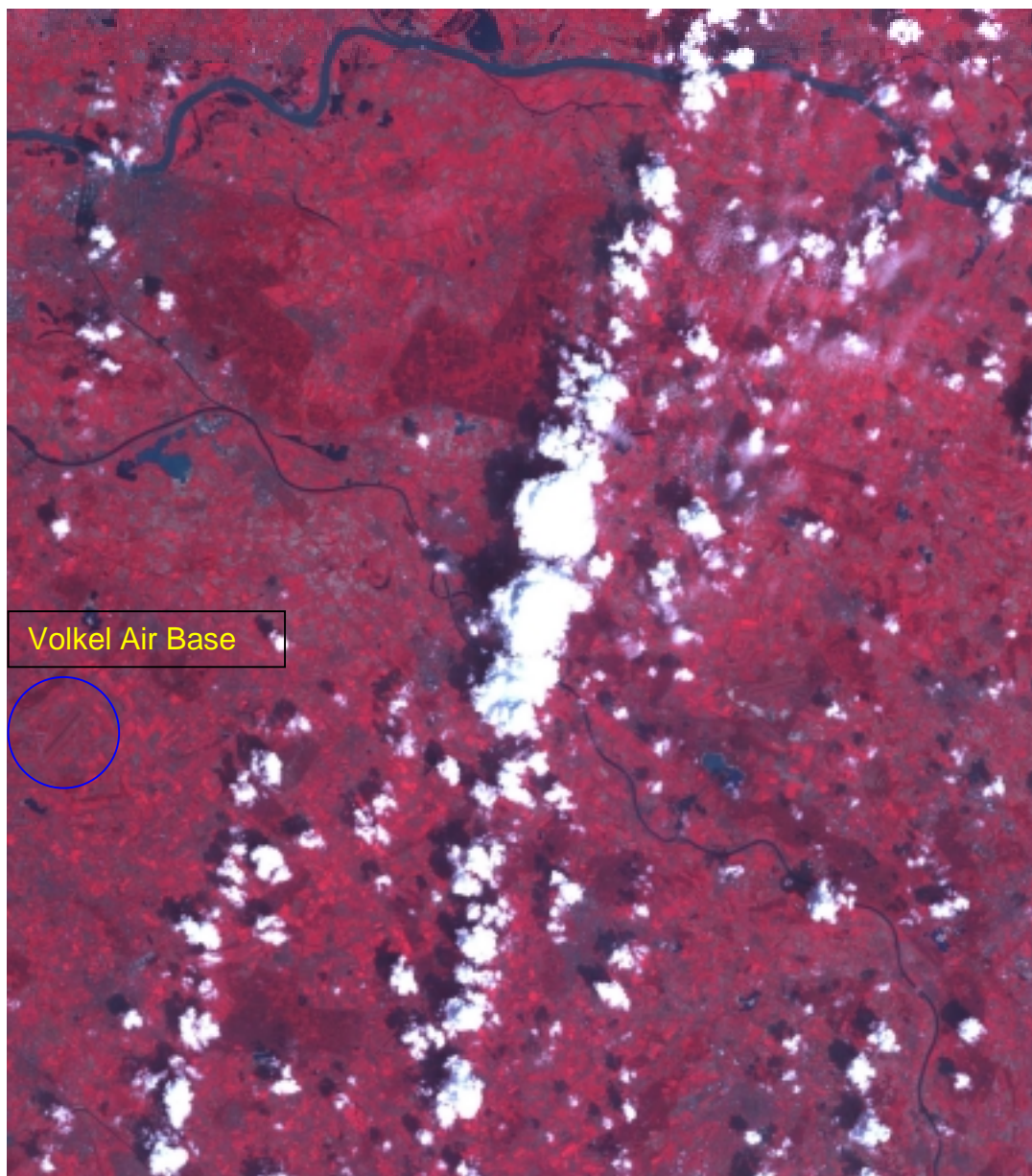
© Nationaal Lucht- en Ruimtevaartlaboratorium (NLR)
© SPOT image

Figure 9: SPOT multispectral image of Volkel Air Base and a large area to the east

Commercial satellite intelligence is an example of COTS (commercial off the shelf) activities within the military environment. Intelligence as well as communication depends increasingly on civilian, commercially operated systems. The (technical) specifications of these systems are much more openly known than is usually the case for military systems. A few countries have military satellites at their disposal; the specifications are not advertised and the collected information is generally not made available. Knowledge of technical specifications in theory offers the possibility of (offensive and defensive) operations to decrease the capacities of the systems. Similarly this is also true for the Global Positioning System (GPS), which is the subject of the next section.

3.3 Vehicle Positioning Systems

In 1998 *Jane's International Defense Review* Foxwell and Hewish published an article with the worrying title: 'GPS: is it lulling the military into a false sense of security?'. The message is summarized as follows:

> Activities […] are well under way to equip all (US) military forces with GPS receivers […] However, as dependance on GPS increases, so does the advantage that an enemy can gain by preventing its use.

Jammers can be used for this purpose.

А В И А К О Н В Е Р С И Я
Общество с ограниченной ответственностью
103009 г.Москва ул.Тверская дом 27 строение 2 офф.88
тел/факс. (+7-095) - 299-54-54, E-mail: aviaconversiya@mtu-net.ru

A V I A C O N V E R S I Y A Ltd.
Russia 103009 Moscow Tverskaya str. 27-2 off.88
tel/fax. (+7-095) - 299-54-54, E-mail: aviaconversiya@mtu-net.ru

Portable Jammer for GPS/GLONASS User's Receivers

The advertised jammer is described in the *Journal of Electronic Defense* (1999); the output power is 8 W in the four frequency bands of the GPS and GLONASS systems. According to the advert 'this power is enough for suppressing the normal operation of the receivers at the range of several hundred kilometers if the direct radiation from jammer to receiver will be ensured'. In (Kaplan, 1996) the required jammer-to-signal ratio for effective jamming has been calculated for different modes of operation of some generic GPS receivers: acquisition (C/A) mode, tracking mode (both for civil and military receivers) and for different jamming signals (e.g. wide band noise, single frequency). Each of these scenarios requires a specific jammer-to-signal ratio for the jamming to be effective. Figure 10 (adapted from Kaplan (1996)) indicates the dependence of the effective jamming range on the radiated power for a few required jammer-to-signal ratios.
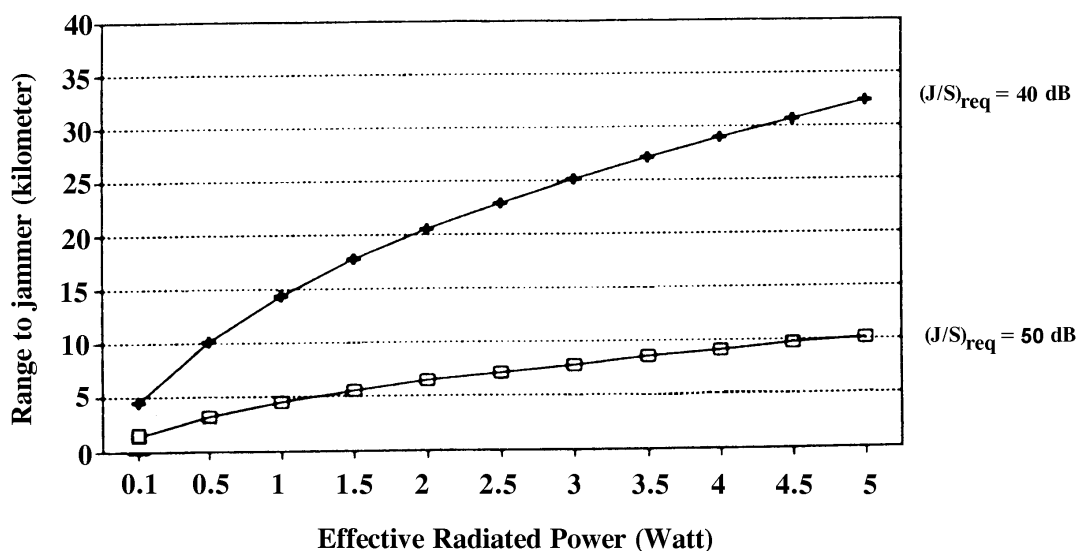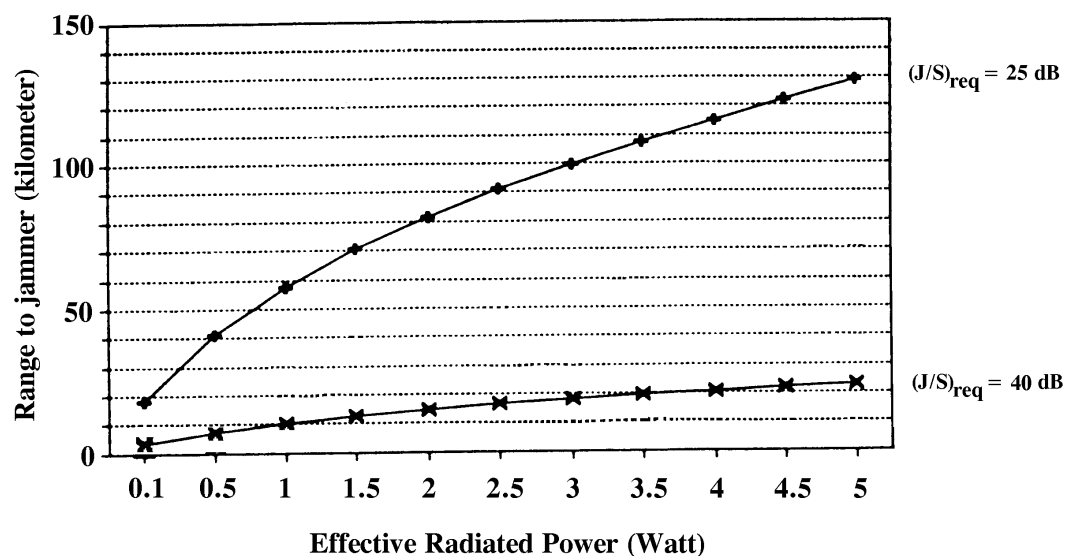
Figure 10: Dependence of the effective jamming range on the radiated power of the jammer
Top: receiver in C/A mode
Bottom: in (military) P mode

It is important to note that the effective jamming range decreases considerably if the required jammer-to-signal ratio can be increased. One way to achieve this is to decrease the electronic bandwidth of certain electronic circuits within the receiver, but this is only permissable if the receiver is aided in some way to acquire and track the satellite's signals. In sophisticated commercial vehicle positioning systems (navigation systems) this is accomplished by feedback of information from other sensors like inertial sensors, odometers, wheel sensors and a (digital) compass. In addition to this feedback, which increases the jamming resistance

of the GPS receiver, the data from the different sensor systems are combined in an intelligent way, using, for example, the Kalman filtering technique, thereby increasing the robustness of the positioning system (Zhao, 1997; Drane & Rizos, 1998). Temporal interruption of the GPS system (e.g. if less than four satellites are visible due to blocking by mountains, buildings or foliage) is less of a problem then. The advantage can be appreciated from figure 11 (Miller et al., 1995).

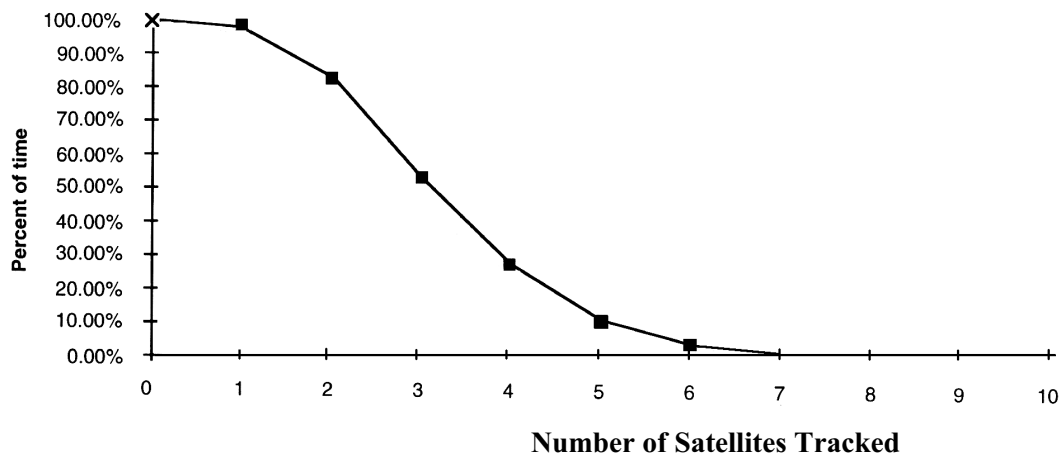**Percent time vs. Number of Satellites Tracked,**

Figure 11: Foliage Scenario 12 Channel GPS Satellite Availability

In this 'foliage scenario' a car equipped with a GPS receiver drove on a tree lined lane along the Hudson River (USA). If, as is normally required, 4 satellites have to be tracked, the GPS system will function properly in 30 % of the time. If sensor data fusion reduces the number of satellites to be tracked to 3, this percentage nearly doubles to 55 %.

The jamming resistance of the GPS system can be increased by the use of adaptive receiver antennas; their purpose is to reduce the received jammer-to-signal ratio. *Beam steering* (e.g. maximum sensitivity in the direction of the satellite) and *adaptive nulling* (e.g. minimum sensitivity in the direction of the jammer or another interfering source) can be achieved by using multi-element array antennas. Protection against jamming for military aircraft –see figure 12- is described in Nordwall (1998).

Vehicle positioning systems are an essential part of (commercial) intelligent transportation systems and (military) battlefield management systems. Complete, accurate and uninterrupted (timeliness!) information about the position of own vehicles is essential for the situational awareness which is the basis for information dominance.

103

This GPS adaptive antenna was designed by Mitre to null out multiple wideband jammers. The design is curved to mount flush on the fuselage of the aircraft with minimum drag. Feed network underneath shows the phase-matched cables used on the 7-element antenna to null unwanted signals.
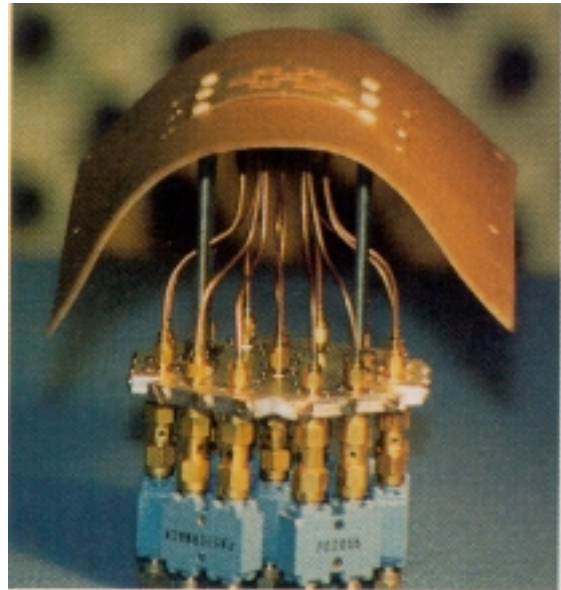

Figure 12: GPS adaptive antenna

4. Conclusions

Sensor systems contribute to a situation of information dominance if the sensors provide information of a higher quality than that which is available to an adversary. Increasingly, however, relevant information is available from commercially operated or government owned public systems almost without any restrictions.

Optical and radar sensors on board of commercial satellites provide high-resolution imagery of nearly all parts of the world, advertised on the Internet. In the forthcoming years the number of satellites will increase significantly, which will reduce the information gaps between the players, military or civil, in the battlespace.

The same holds good for navigation systems relying on the US-owned Global Positioning system (GPS). This system, however, is quite vulnerable, both to natural degradation (e.g. obscuration by buildings, hills and foliage) and to jamming. Advanced commercial automotive navigation systems combine GPS with other sensors, like wheel sensors. Dominant battlespace knowledge requires robust sensor systems, linked to high quality information systems and networks.

References:

Anselmo J.C. (2000), Commercial Space's Sharp New Image
    in: *Aviation Week & Space Technology*, January 31, 2000: 52-54
Aviation Week's Space Business, April 3, 2000
Broek, A.C. van de, et al. (1998), *Geographical information extraction with remote sensing*
    TNO report FEL-98-A077, Den Haag
Drane C, Rizos, C. (1998), *Positioning Systems in Intelligent Transportation Systems*
    Artech House, Boston/London

Foxwell D., Hewish, M. (1998), GPS: is it lulling the military into a false sense of security ?
      in: *Jane's International Defense Review*, 31, 1998 / 9: 32-41

Hewish M. (1999), Military takes a giant leap with commercial space technology
      in: *Jane's International Defense Review,* 32, 1999 / 4: 41-47

http://neonet.nlr.nl/npoc/News/ikonos_amsterdam.html

http://www.neonet.nl/rapids

Journal of Electronic Defense, Editorial, 22, 1999 [August]/ 8: 28

Kaplan, D. Elliot (ed.) (1996), *Understanding GPS*
      Artech House, Boston/London

Miller L.C. et al. (1995), Measurements of GPS and LORAN Performance
      in an Urban Environment, in: *Environmental Factors in Electronic Warfare Related to*
      Aerospace Systems. AGARD Conference Proceedings CP 573, Paper 23
      (Conference Sensor & Propagation Panel [SPP], Rome), Neuilly-sur-Seine, May 1995

Nordwall B.D. (1998), 'NAVWAR' Expands EW Challenge
      in: *Aviation Week & Space Technology*, November 23, 1998 / 11: 57-58

Smith A.J.E. et al. (1999), *Visuele interpretatie van SAR beelden* [Visual interpretation
      of SAR images], TNO-rapport TM-99-A078 / FEL-99-A211, Soesterberg

US Army Field Manual 100-6 on Information Operations (August 1996)

Waltz E. (1998), *Information Warfare, Principles and Operations*
      Artech House, Boston/London

Waltz E., Llinas, J. (1990), *Multisensor Data Fusion*
      Artech House, Boston/London

Wijnhoud J.D. (1995), *Het gebruik van remote sensing en GIS ten behoeve van inventarisatie*
      en analyse van terrein en bodem voor militaire doeleinden [The use of remote sensing
      and GIS for making an inventory and analysis of terrain and ground for military pur-
      poses], TNO-rapport FEL–95-S287 (in Dutch), Den Haag

Zhao, Y. (1997), *Vehicle Location and Navigation System*
      Artech House, Boston/London

The fighting soldier, warrior or informant?

J. Meijer

1.   Introduction

'A great part of the information that reaches us in a war is contradictory, an even larger part is wrong, and by far the most is highly dubious'. In the view of the nineteenth-century Prussian strategist Carl von Clausewitz the value of information is described in a rather pessimistic vein. A full century later the value of information is unquestioned, and there are only luxury problems concerning the way to control the inexhaustible flood of information, the determination of which information at which particular moment is relevant for whom, and how to avoid 'information overload', for instance. In the present, ever-expanding information world, one thing is clear: the advancing information technology will influence the behaviour of the soldier quite drastically. Hitherto unthinkable activities will become reality in the near future, and the role and value of the fighting soldier and his group will acquire a different significance. In this article I want to describe this different role of the soldier. I will begin with a short retrospect, followed by a picture of the soldier at the beginning of the twenty-first century. Subsequently, I will attempt to describe the possible development of the 'soldier as informant', simultaneously pointing out the limitations of this source of information. I conclude by answering my self-imposed question: 'The fighting soldier, warrior or informant?'

The title of the article identifies the fighting soldier as the central person. That is not a coincidence, but it is founded on the fact that there has been a programme in the Royal Netherlands Army for some time now with the appealing name 'Soldier Modernisation Programme' (SMP). Its central theme is the increase of the effectiveness of the fighting soldier, while not forgetting his other non-fighting brothers. In the course of the article I will from time to time refer to the SMP. For the sake of the readability of this article the term 'fighting soldier' will be alternated with others. The article has been written on a personal basis and consequently it does not have the status of a formal army document.

2.   The past

The fighting soldier of the past
Since time immemorial the soldier has been used as an instrument of battle, and there are dramatic examples of commanders who did not worry about a man more or less. The term 'cannon fodder' was not invented for nothing in this respect. In spite of the low esteem of the battle power of the individual soldier, which lasted for centuries, there were some attempts to develop and improve instruments for the soldiers with which to fight and preferably win battles. In this long line of developments the cudgel became a very handy and effective rifle, the harness an effective fragmentation and bullet proof vest, and the banner a radio. Characteristically these developments were often directed at only one aspect of the soldier's equipment and generally there was not too much concern for an integral approach. The result was a literally overweight soldier, slowly sinking away into the mud, unaware of his position, let alone that of his mates.

The fighting soldier as informant in the past
1600, The Battle of Nieuport. Who does not know this famous date, even if at the same time we have hardly an idea where Nieuport is situated or what exactly took place there? Just a

short reminder. In June 1600 the army of the Republic of the Seven Provinces under the command of Prince Maurice marched into Flanders. After an amphibious operation, unique for the Netherlands, a famous battle was fought against the Spanish oppressor on and near the beaches and dunes of Nieuport.

Figure 1: The soldier of the past

The tactics used at the time were based on the employment of cavalry as the surprise element, exploiting initial success, artillery as a support element, and the soldiers, the infantry, as the manoeuvre element. The role of the soldier was primarily that of conducting close battle, his colourful uniform giving information to the commander as to where exactly his unit was locked in battle. Literally flying the banner was, certainly at the time, a matter of life and death. At the time of WWI the role of the soldier was still almost the same as during the Battle of Nieuport, but during and certainly after WWII this began to change greatly, partly because of instruments such as the radio, radars and binoculars becoming available, though slowly at first. It was recognized that the foot soldier was more than mere battle power personified, and that he could be inestimable as supplier of information. In 1960 Lieutenant Colonel US Army Irving Heymont (1960) wrote about this:

> Ground reconnaissance is the best known method of gaining tactical information and is performed by personnel manning observation posts and/or surveillance devices […] Army troops infantry, armor and engineer elements are best suited for patrolling.

It was characteristic that the role of the soldier and certainly his group became more important, but the information flow was in principle only directed vertically and bottom-up. The exchange of information inside the group, the horizontal information flow, was limited to flag and sound signals and, wherever possible, human voice. Top-down provision of information was very much in its infancy at the time. The issue of orders was in practice the only moment when the subordinate got information. The further one was removed from the source of information in hierarchy and distance, the more the information diminished, the victim usually being the ignorant fighting soldier.

3.   The present

The Soldier Modernisation programme
'Lessons learned' of the conflicts fought in the last twenty years of the past century indicated that a drastic change with regard to the fighting soldier was in order. Simultaneously, an ever-increasing pace of technological developments and capabilities fuelled this feeling. The emergence of the computer and positioning devices is a good example of this. In NATO context a number of activities were undertaken with respect to the soldier, mainly focusing on a feasibility study. It was investigated whether the technological developments as foreseen in the nineties could also benefit the fighting soldier. The outcome was extremely positive and the consequence was that in 1994 the idea of increasing the effectiveness of the fighting soldier was laid down in an international programme. The Netherlands too joined the bandwagon and around 1995 the SMP activities were started in the Royal Netherlands Army, at first under the auspices of the Infantry Training Centre and since January 1997 as an independent programme directly controlled by the Army Staff. *The policy framework SMP*, a document agreed upon by the Dutch parliament (Kamerstuk, 1997), outlines the targets of SMP in general terms (Meijer, 1997). A major point is the increase of the effectiveness of the fighting soldier on foot by optimizing his equipment and devices. The optimalization process has to be balanced between five *capability areas*: lethality, mobility, sustainability, survivability, and command and control. The equipment of the Dutch soldier is known for its high quality, but in spite of this the setting up of an integral programme is justified.

Figure 2: The modern soldier

One reason for this is the absence of coherence in the soldier's equipment, many pieces being not very compatible with each other, which results in sub-optimal functioning and a high total weight. In addition, as yet limited use is made of all sorts of modern, recently developed devices already used in the civilian world. An example of this is information technology with its almost unlimited possibilities due to the advancing miniaturization. There are also many possibilities for new fabrics with a very small volume and weight that can give protection as well as comfort. At the beginning of the twenty-first century we see a fighting soldier whose equipment is changing fast and we are facing the need to be constantly on the look out for improvements in ever-returning cycles.

The fighting soldier on the brink of the twenty-first century
In the past few decades spectacular developments have demanded everyone's attention: much improved tanks, helicopters (transport and combat), high-tech frigates, a multifunctional landing and transport vessel, etc. In this turmoil of *developments* attention for the improvement of the equipment of the fighting soldier lagged behind at first. However, the tasks for the armed forces have undergone drastic changes as a result of global developments. The fixed pattern, established over decades, of operational deployment in pre-determined areas went overboard. The North German plains were replaced by, for instance, Cambodia, Bosnia and Eritrea. On a global scale the Gulf War was the first clear indication that the changed tasks and world-wide deployment, accompanied by geographical and climatic aspects, would also have far-reaching consequences for the fighting soldier. A more recent example is the Dutch deployment in Bosnia, where tanks and other armoured vehicles fulfil an important role, but where the real work is mainly done by the foot soldier. It consists, amongst others, of observing and reporting, carrying out foot patrols, searching of houses, villages and areas. Essential elements are showing armed presence, the interaction with the local population, and perhaps most importantly, being an informant.

The fighting soldier in the twenty-first century, a look into the near future
It is very likely that in the very near future drastic changes are going to take place in the way of operating of units. In this context there is already talk of digitalized battalions, mainly consisting of digitalized (fighting) soldiers. To get an impression of the equipment of such a warrior, some pieces of equipment will be surveyed here.

Figure 3: Optimal observation

The infantryman (let us assume that this arm is leading the way) is equipped with a so-called Soldier Digital Assistant (SDA). This device is at the heart of the whole concept of the digitalized soldier and is mainly intended for the determination of his position. Not only his own position is displayed, but also that of his group members, as the SDAs of the individual infantrymen communicate with each other. The SDA is fitted out with integrated navigation modules, based on the long-serving Global Positioning System, and an Inertial Navigation System (INS), which is intended as a back-up for the navigation system. Making use of step counting and the measuring of air pressure differences, INS is capable of indicating the position of the user in case of a breakdown of the navigation modules. Apart from that, SDA is fitted out with a digital compass, which can be used not only for the infantryman himself, but also for his weapon (observation and aiming).

Operating the SDA, the soldier's central computer, is extremely simple and to a large extent takes place through voice recognition. The integrated digital map does not only display the soldier's own position but also that of the group members, the commander and any possible obstacles, like mines, etc.

An opponent's discerned position is automatically displayed as well. Warnings of opponents or other threatening situations are conveyed by vibrations from his battlefield watch. The integrated soldier radio ensures the fully automatic transfer of messages or images by order of the soldier. The radio, as it were, searches the receiver in the digital field and generates just enough energy to guarantee a 100% certain reception of the message. There is automatic switching between the group net, the platoon net and the Battlefield Management System (BMS). This system is a network of automated systems which acquire, process, present and distribute information for the execution of the operational task, from the single platform, e.g. the armoured infantry vehicle, up to battalion size. Another aspect of the new equipment is an all-conditions independence with regard to observation. The rifle is fitted out with sights, capable of always generating an optimal image. They contain a state-of-the-art digital camera, night vision and thermal imaging. Due to this technology it is possible to observe even when there is minimal light (e.g. the light of stars and moon) or through difference in temperature of objects against their environment. There is also a built-in identification module allowing Identification Friend or Foe (IFF).

The relevance of the near future vision
The picture described above could be a Vernean fantasy for some, but I am convinced that within a decade or so such a digitalized infantry group will be active, indeed. That this development will have enormous consequences for the deployment and actions of dismounted units is also evident. Command and control will become much more direct and clear, the decision making process will be fed by *real-time information* and less founded on conjecture. Units of this type will be able to act much more independently, with a guaranteed exchange of information with the higher echelon. Existing tactical procedures at group and platoon level are based on the unit acting without any ICT means. The real challenge therefore is to recognize the consequences of the introduction of these devices at relatively short notice and to anticipate timely on them. Education and training requirements will have to be adapted as well.

Of course it is possible that some of the described devices may break down for some reason or other and in the development process this eventuality is taken into account. The system has a built-in automatic priority that will become active the moment there is a failure. Thus, the radio will receive the remaining energy the longest, and weapons can still be operated purely mechanically. It is extremely important that in their education and training soldiers are still taught and trained how to survive under abominable circumstances and to keep on carrying out their tasks, however more difficult.

4.   The future

The certainties
In the policy formulated by the Army Staff certain ideas about the (fighting) soldier have also been incorporated. As Major General Mammen, Director of the Policy and Planning Department of the Army Staff, once said:

> *The role of the fighting soldier will be and remain of essential importance. Irrespective of how superior our weapon systems and materiel may be, the foundation of our armed*

forces is the soldier, for in the last instance he is the only instrument for really gaining territory, in its general sense (Mammen, 1999).

The saying 'Peacekeeping is not a soldier's job, but only a soldier can do it', leaves no uncertainties about the role of the soldier in the present-day peace support operations.
More aimed at the role of information is a statement from the Army's *Policy Vision Command and Control* (2000):

> With the help of modern technology the individual soldier must acquire a picture of what goes on around him, and this picture will be transmitted to the other individuals in his direct vicinity.

The current doctrine documents stress the concept of sustained battle and, independent of daylight and weather, units must be capable of acting with various degrees of swiftness, as required by moment or place. One condition for this is full 'Night Capability' of the ground component, including that of the fighting soldier.
It is certain that technological development will continue at an ever-increasing pace and result in devices that will lend themselves excellently for application. The name SMP already indicates that it is not an exclusively Dutch programme, but that it has a strong international orientation. It is therefore not a surprise that we, in the Netherlands, will now and in the future make use of the experiences and current developments of our allies. Starting points for this co-operation have been identified among the NATO members, such as the systems approach and the use of the same criteria with regard to lethality, mobility, survivability, sustainability and command and control. The role of the fighting soldier is secure in the future; his value is broadly understood as combat power and as source of information.

The limitations
The *Command and Control Vision* (2000), already quoted above, in the same passage also indicates a limitation:

> In the development of (soldier) systems it has to be taken into account that a soldier will have to be able to fight and that the application of technology must not lead to the soldier being more occupied with his (information) system than with his weapon.

In the drive for more developments, especially those in ICT, there is always the danger of overdoing it. Too much of a good thing, too much information, will lead to uncalled for effects, especially for the fighting soldier. In the SMP these limitations have been recognized and they are incorporated into the realization. The designers are asked to make things as simple as possible; the computer must be operable with three switches; build in filters; make automatic what can be made automatic, etc. When acquiring new materiel, only choose those modules that have proven to yield operational surplus value. Adopt an evolutionary acquisition policy and make maximum use of existing (partial) products available on the commercial market. From the start, involve the future user in the development and testing; he has got to work with it and he will only do so if he has confidence in it.

5.   Conclusion

A statement from Lieutenant General Paul J. Kern, US Army: 'If we are really good, and we are, the soldier of 2025 will be as effective as the tank of 1995'. It is rather forceful language to compare the combat and information power of the future fighting soldier to the

effectiveness of the fire power, observation and information capability of the modern Leopard 2A4 tank. Is this an instance of American bluff or does this general have a realistic view of the future? In this article I have stated that for much of the past the development of the soldier hardly got any attention; there was barely any difference between the foot soldiers in the Battle of Nieuport and the infantry in the Battle of the Marne in 1914. The middle of the twentieth century saw the beginning of a change in thinking and acting for the soldier. This change has continued until today, going faster all the time, and will eventually lead to a fully developed soldier fighting system, which in its turn will be part of a comprehensive information system.

Finally, the answer to the question whether the fighting soldier will be a warrior or informant. Now and doubtless in the future the soldier is and will be a fighting system, deployable in any imaginable scenario and under any circumstance anywhere in the world. The ever-improving image of his surroundings, however, will make his information capability greater. The answer to the question is therefore: the fighting soldier, an informative warrior.

References

Beleidsvisie Commandovoering (2000), [Policy Vision Command and Control] Landmachtstaf [Army Staff], Den Haag

Heymont, I. (1960), *Combat Intelligence in modern Warfare* Stackpole, Harrisburg

Kamerstuk (1997), Document 25 600 X, nr. 22, Tweede Kamer der Staten Generaal [Second Chamber of the States General, Document], Den Haag

Mammen, H.D.(1999), *De gevechtssoldaat, zijn rol in de (nabije) toekomst* [The fighting soldier, his role in the (near) future], Keynote address, MoD, Landmachtstaf [Army Staff], Directie Beleid &Planning, Den Haag

Meijer, J. (1997), *Beleidsraamwerk Soldier Modernisation Programme* [Policy Framework Soldier Modernisation Programme] Landmachtstaf [Army Staff], Directie Beleid & Planning, Den Haag

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 syn-chronisation. 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.
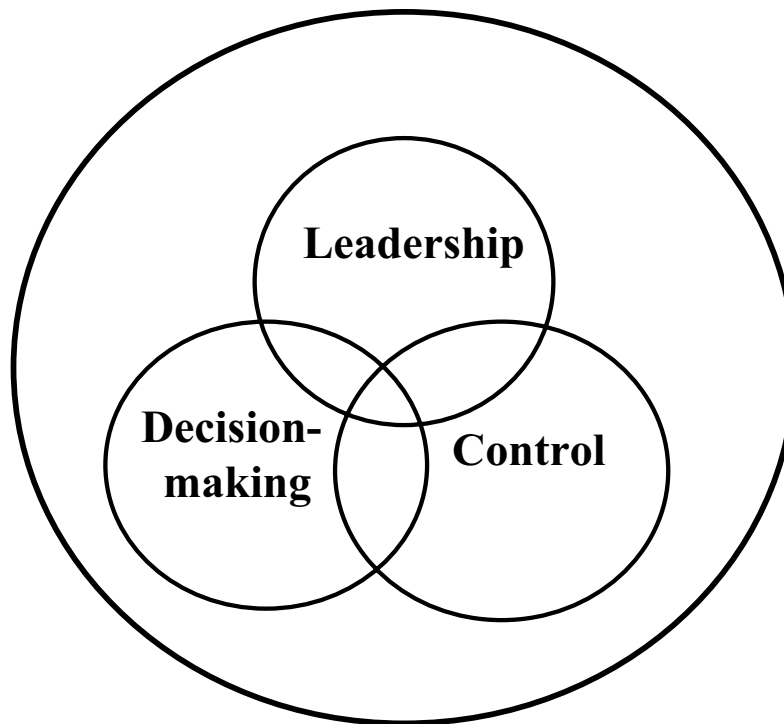

Figure 1: The elements of command

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
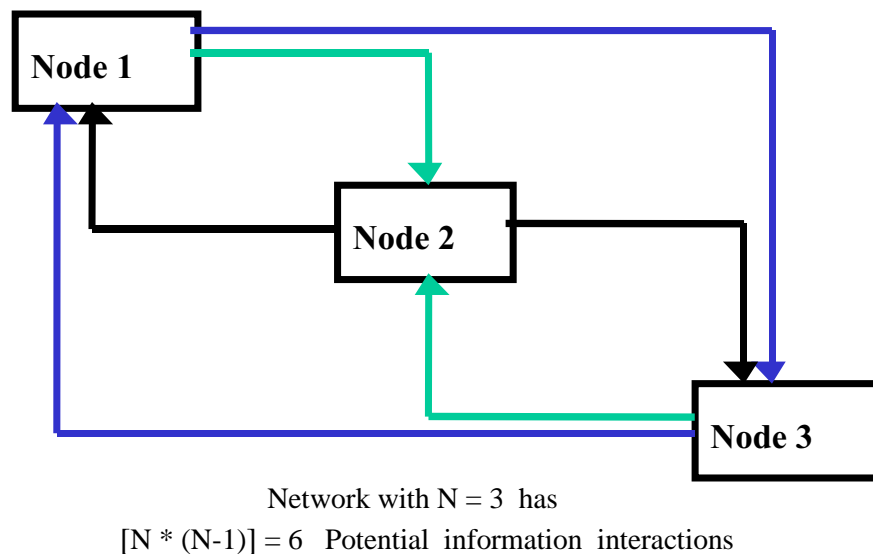[N * (N-1)] = 6   Potential information interactions

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.
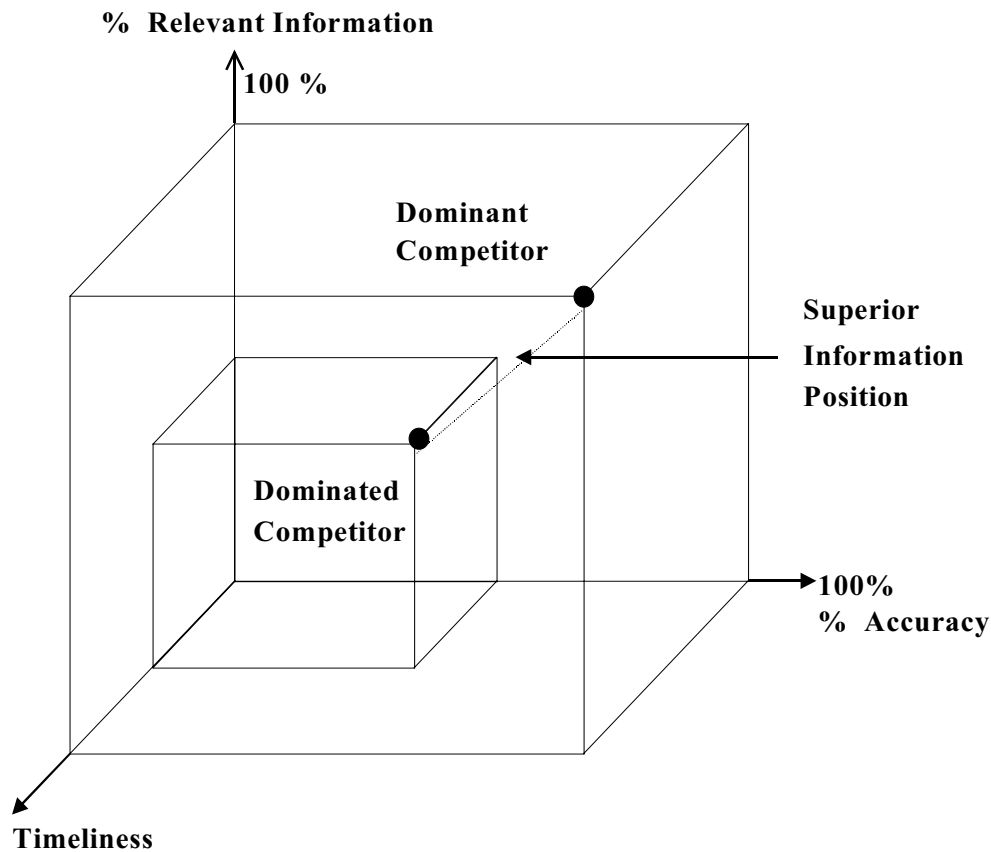

Figure 5: Superior Information Position

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

About the authors

Drs. T. (Tom) Bijlsma has been a part-time lecturer of management sciences since May 1999 at the Royal Netherlands Military Academy [RNLMA] in Breda. After graduating from the RNLMA he worked for ten years as an Army officer. In 1995 he left the armed forces and established himself as a trainer/consultant for several profit and non-profit organizations.

Drs. M.T.I. (Myriame) Bollen read social and organizational psychology at Leyden University. She lectures management sciences at the RNLMA. Presently, she is writing her Ph.D., entitled *Civil-Military Cooperation during Humanitarian Relief Operations.* Besides, she works as a management trainer with PAO/De Baak on topics related to leadership and change management.

Brigadier General Prof. J.M.J. (Hans) Bosch was commissioned into the Cavalry in 1970. He served in various command and staff functions in 103 Reconnaissance Battalion and 43 Tank Battalion. He held functions at the Army Staff, the Army War College and in the Military Intelligence Service. In 1994 he became private secretary of the Commander Royal Netherlands Army. In 1995 he was promoted to Brigadier General and appointed professor at the RNLMA. He lectures on military operational management. Since 1996 he has been the Chief Editor of the periodical *Militaire Spectator*.

Drs. T.P (Tessa) op den Buijs works as a researcher and lecturer at the RNLMA. She graduated from the University of Tilburg with a degree in health and environmental psychology in 1995. She is currently writing her Ph.D. on the functioning of Dutch SFOR and UNFICYP service personnel during their deployment in Bosnia and Cyprus.

Drs. J. (Jan) Heijnsdijk is an associate professor of management sciences at the RNLMA. He is also a member of several national examination boards in his field. His publications include books on 'vital management' (1988) and the practice of organizational management (1997). He has published several articles in military periodicals and written a number of research reports on defence management and result-responsibility in the armed forces.

Drs. H.M. (Henk) van den Hooven studied economics at the Erasmus University Rotterdam. He lectures on management accounting and cost accounting at the RNLMA. Before joining the Military Academy he worked as an assistant researcher at the Netherlands Economic Institute. He is currently doing research into the use of accrual accounting in non-profit organizations.

Prof. Dr. H.P.M. (Hans) Jägers is professor at the RNLMA and at the University of Amsterdam. He studied philosophy and sociology and earned his Ph.D. in economics from the University of Amsterdam. He has published various articles on strategy, organizational design, knowledge management, network organizations, virtual organizations and virtual communities.

Dr. W. (Wendy) Jansen is associate professor information management at the RNLMA. She studied sociology, anthropology and economics and received her Ph.D. from the University of Amsterdam. She has published various articles on ICT, organizational design, knowledge management, network organizations and interorganizational networks.

Drs. H.F.M. (Harry) Kirkels has been a lecturer of English at the RNLMA since 1990. He graduated from Nijmegen University with a degree in modern English literature and modern linguistics. Prior to his appointment at the Academy he worked for an extensive period as a

teacher in secondary education. Apart from his teaching duties he is also involved in co-editing and translating articles written by his colleagues at the Academy.

Lieutenant Colonel A. (Ad) Koppe lectures military operational sciences at the RNLMA. He graduated from the RNLMA and was commissioned in 1981, after which he held several functions in 43 and 11 Tank Battalion. In 1993 he served in central Bosnia as a United Nations Military Observer. In December 1995 he returned as a team leader of a mechanized team in the Implementation Force (IFOR). After having been an analyst for the Middle East and Northern Africa for the Military Intelligence Service he returned to the RNLMA in 1998.

Lieutenant Colonel J. (Koos) Meijer is employed at the Army Staff of the Royal Netherlands Army, Directorate Policy and Planning. He is responsible for the coordination of the Netherlands Soldier Modernisation Programme (SMP), and in coordination with TNO he prepares the research and development SMP-projects. He is deputy-chairman of the NATO Army Armaments Group/Topical Group 1 'On Soldier Systems Interoperability'.

Drs. M.V. (Max) Metselaar lectures on political-military decision making in crisis situations at the RNLMA. He studied political science at the 'Vrije Universiteit' of Amsterdam and at the University of Amsterdam. He has co-edited a book on political decision making, and published various articles on military intelligence and intelligence failures, surprise attacks, crisis decision making and military leadership during peace operations. His Ph.D. research is focused on the question as to what extent dilemmas and cognitive coping responses of political leaders, such as denial and avoidance, explain a lack of governmental preparedness during enemy attacks.

Prof. Dr. N.P. (Nico) Mol is a professor of public financial management at the RNLMA and at the University of Twente in Enschede. His publications include a thesis on the allocation of public budgets (1988), a book on financial planning and control (1997) and a textbook on the application of business economics in government organizations (1998), all in Dutch, and several contributions to English books and journals, among others *Performance indicators in the Dutch Department of defence* (Financial Accountability and Management, 1996).

Prof. Drs. J.A.M. (Jan) Oonincx has been a professor of management information at the RNLMA since 1988. Prior to joining the Military Academy he was an assistant professor of education and research in administrative organization at the Rijksuniversiteit Groningen and a professor of information systems at the University of Tilburg. His research is mainly directed at the application of modern management techniques and the use of information and communication technology in the result-responsible units within the armed forces. He has published several articles on the subject in military periodicals.

Ir. J. (Jaap) Rogge is an associate professor at the RNLMA in Breda. He studied physics at Eindhoven Technical University and was conscripted in 1968. His military duties comprised the teaching of sensor systems at the Military Academy and on termination of his conscription period he was appointed as a lecturer there. He lectured and conducted research on the performance of sensor systems in battlefield environments. Between 1970 and 1995 he has been a member of several NATO Research Groups and AGARD Panels. Since 1990 his responsibility has been extended and has come to comprise sensor systems and technical aspects of information operations (electronic warfare and protection of information).

Prof. Dr. J.L.M. (Joseph) Soeters is professor of social sciences at the RNLMA and at Tilburg University. He is Dean of the Faculty of Military Management Sciences of the Military Academy. His work focuses on the internalization of and intercultural differences relevant for military and civil life. Research projects include studies of the cultural aspects related to bi- or multinational military formations, such as 1 German/Netherlands Corps, SFOR and UNFICYP. He has published numerous articles on these matters in (inter)national professional journals and military periodicals, and is the (co-)author of several books about a variety of sociological issues.

Mr. Drs. G.C.A. (Wilchard) Steenbakkers lectures and is a researcher at the RNLMA. He studied economics and information sciences at the University of Tilburg and Dutch Law at the Open University. He has published various articles on organization design, knowledge management, virtual organizations, network organizations and virtual and knowledge communities. The subject of his Ph.D., which he is currently writing, is the use of information and communication technology in network organizations.

Prof. Dr. A.L.W. (Ad) Vogelaar is professor of military psychology at the RNLMA. He is an expert in the field of military leadership and its correlates, such as stress, coping behaviour and PTSD. He has published articles and books on leadership in stressful circumstances, commander's responsibility, mutual trust, mission oriented command and transformational leadership.

Final editing advice was given by:

Robert J. Smits

Academy Research Centre of the KMA/RNLMA