NLARMS

Netherlands Annual Review of Military Studies 1999

J.M.J. Bosch
H.A.M. Luiijf
A.R. Mollema (eds.)

Information Operations

The Netherlands Annual Review of Military Studies is published under the auspices of the Royal Netherlands Military Academy at Breda.

For more information about NLARMS and/or additional copies contact the editors at the address below:

Royal Netherlands Military Academy
c/o the Academy Research Centre
Kasteelplein 10
P.O. Box 90154
4800 RG Breda
+31 76 527 3319 (phone)
+31 76 527 3322 (fax)

NLARMS

1997: The Bosnian Experience
J.L. Soeters and 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.)

Printed and bound by HAVEKA BV, Alblasserdam

ISSN: 0166-9982

CONTENTS

EDITORIAL PREFACE

INTRODUCTION

Science and technology are the cornerstones of economic and military action. Technology functions as an engine for a broad range of developments. Indeed, technology may create problems, but it is - first of all - determining the chances for prosperity and our position within the modern world. We focus on Information and Communication Technology (ICT) and its effects. In fact ICT brings blessings, mixed blessings and certain vulnerabilities. The blessings are countless; people are able to communicate worldwide within seconds; GPS enables us to know where we are; Internet functions as an enormous databank and links people, organisation, information and ideas, etc. There are also mixed blessings. One has either to adjust to the latest technology, or one is left behind, unable to communicate and act with the same speed. Some see dangers where computers seem to dominate the world we live in. Others question the almost religious belief that computers 'are right'. Again others point at the dangers over information overload and the mismatch between media and governments concerning 'news', as messages, travelling at the speed of light, may be true, partly true or even false. Our scope does include those blessings, mixed or not. But our main topic is about vulnerabilities, as they do count in a world where states, groups, and individuals fight for power, influence, wealth and gain.

These vulnerabilities are - as a concept - not new. Information always was a precious good as it is a means to plan and act on Information always has been one of the instruments to influence others. So there is a very old notion on information as a means, a weapon or a target. New however is the complete dependence of modern organisations on ICT, or - in short - computers and communications. Industry, financial institutions, the military, the state, the media, etc.; they are only functioning because they use ICT to store, send, receive and use information. The underlying information infrastructures are often connected and are based on more or less the same standards. Within the military realm there is 'Command and Control Warfare'. The existing concepts do however not give credit to some new realities. The first has to do with new ways to manipulate, degrade or influence digitised information. The second reality has to do with the growing interconnections of military and civil information infrastructures. This means that these interconnections can be used to influence military and/or civilian Command and Control. The third reality has to do with the sobering observation that an attack on civil information infrastructures might endanger the functioning of modern society. 'Information operations' thus cover a broad range of risks and options. The enemy will probably wear no uniform. The opponent may or may not be a State; there is no warning (time) and we may not know who acted from where. Do the Geneva Conventions apply? And who actually defends those infrastructures?

Many countries are studying this new dimension of conflict. It is not only within the United States that one understands these new realities. It also is a concern in countries like the United Kingdom, Sweden, France, Canada, Russia, China, Israel, Switzerland and Germany. NATO presented early 1999 a Military Committee Document, MC 422 on 'Information Operations'.

In 1998 the Dutch and German Ministries of Defence activated a Working Group to study the meaning and implications of this topic.

This publication informs about these developments. The findings of NATO and the German-Dutch Working Group are among the contributions. But it has a broader scope; it wants to address the broad spectrum of visions on 'Information Operations' as to foster awareness and to start further discussions.

There were many options to present the different contributions. We decided to organise them under five headings: the philosophical dimension; the conceptual approach; the realities of Information Operations; on Information Assurance, and the Legal Perspective.

THE 'PHILOSOPHICAL DIMENSION'

The thesis of **George Stein** is whether the conduct of Information Warfare is like the conduct of war described in the 'Warring States era' in ancient China (c. 403-221 BC) by *Sun-Tzu's Art of War*. Can it provide strategic insight in what he describes as the real asymmetry, the 'metaphysical' or 'epistemological' as it flows from a total different 'model' of how the universe 'works' and how men 'know' to 'work' in the universe. **Szafranski** has another thesis. In his opinion the Armed Forces and their national command authorities in modern Western States have much to learn about effectively integrating information operations into both war and anti-war security operations. Worse, at the present rate of learning, the Western democracies may be surrendering intellectual leadership and ultimately operational leadership to those states, hackers, and criminals who more quickly adapt these new tools. **Tyrrell** examines the nature of information and looks at how it has changed in the 'post information revolution world'. Has it changed the way in which we use it, has it altered the way in which we, as human beings, respond to it? He also examines some potential threats and looks at how information integrity might be better safe guarded. He also raises other questions: where does the responsibility for information rest; what sovereignty can a nation exercise over information and information flow; how should global networks be controlled and what threats to national information integrity can be identified? **Friman** discusses the concept of perception warfare. He questions whether the main object of warfare is the information or the perception. He argues that perception warfare is not something new, but that this concept has mostly been discussed as part of other concepts of war. It is reasonable to believe that we constantly are objects for perception attacks, but what makes it perception warfare?

THE CONCEPTUAL APPROACH

Bosch addresses 'Information Operations' within the broader context of change and continuity. We now face some 'cyberspace', a new dimension where war can be waged. There is a close relationship between 'Information Based Warfare' and 'Information Operations'. The latter do not only influence the military domain, but may well use national, international and even global layers of connectivity to influence those outside the traditional military domain. Given our dependence on information and communication technology and options to manipulate information and the human decision-maker, we face new threats. **Gardeta**

discusses NATO-policy on Information Operations. The global technological evolution in the field of information changed the world. It also resulted in an operational shift of focus towards a systems approach to war fighting. This led to a new policy as contained in the Military Committee document MC 422 of December 15, 1998. The North Atlantic Council approved it on January 22, 1999. Information Operations are actions taken to influence decision-makers in support of political and military objectives, by affecting information as well as the information-based processes. They integrate Command and Control Warfare with the political consultation process, decision making apparatus and combined political-military operations of the Alliance. The German and Dutch Ministries of Defence activated a Working Group to study Information Operations. **Mollema** presents the findings of this study. From spring 1998 till autumn 1999 the Amt für Studien und Übungen der Bundeswehr at Waldbröl, the German IABG, the Royal Netherlands Military Academy at Breda and the Dutch TNO Physics and Electronics Laboratory investigated the meaning and impact of Information Operations. The report has to assist the MOD's in formulating policies, doctrine and requirements. The author is one of the contributors to this report. **Faucon** focuses on the French position. The 1994 French Defence White Paper denoted the presence, if not the confrontation, of two cultures. Firstly, that of the 'realists' to who war is a phenomenon resulting from international relations. Secondly that of 'idealists' for who war is an anachronism as the international society increasingly favours solutions of peaceful compromise. He informs about French-British staff talks on Information Operations, and the resulting view on requirements and constraints in the operational arena.

INFORMATION ASSURANCE

Luiijf focuses on the relevance and broader problems of Information Assurance. He provides an overview of the threats from cyberspace on the Armed Forces and society as a whole. He presents an 'attack taxonomy', ordered both by hacking method and possible reasons of attack. The paper includes a list of internationally unresolved issues. Five years ago, the Canadian Forces (CF) faced decisions on the integration of information-based operations into its military routine. **Romet** describes the elements of the broad conceptual framework that was employed; the specific concept within the CF, and an outline of the resulting structures. He shares lessons learned, and the problems following the holistic approach towards developing the broader program. **Willi Stein** introduces orientations, helpful illustrations as well as definitions and critical factors to open a gate to more co-operation in the area of security. He touches on Information Security (INFOSEC), Information Warfare (IW) and Critical Infrastructure Protection (CIP). The common problem demands a new level of co-operation in science, engineering, and education. **Veltman** and **Parker** clarify the meaning of a 'Red Team'. Such a team, consisting of professionals in ICT, has to identify vulnerabilities within information systems. Experiences learn that Red Teams are instrumental for better security. They also learn that the development of methods and close co-operation with the responsible staff are crucial for building an effective team.

THE REALITIES OF INFORMATION OPERATIONS

A government needs instruments to inform the population. There may be circumstances where this information is endangered. The Swiss government decided to shape an 'Information Regiment' to act if circumstances would disturb the normal activities of press, radio and television. **Hofstetter** describes the history, task and organisation of this regiment. Its Input companies, Radio- and TV companies are a good example of precaution in the field of government control. **Cobb** illustrates that Australia may serve as an example of the vulnerabilities any OECD country is confronted with. The Sydney 2000 Olympics is a case in itself. He presents a risk assessment and stipulates his ideas on possible threats. His main proposals include encryption, a new office culture, the development of contingency plans and the creation of a National Infrastructure Protection Agency. **Metselaar** discusses the impact of the application of new information technologies on warfare and crisis management. His thesis is, that those technologies are a mixed blessing, as they may have a so-called 'Janus head'. On the one hand they will help to acquire and disseminate information. On the other hand there remain dangerous disadvantages and cognitive traps. In his opinion technology might increase and accelerate cognitive, psychological and organisational traps. **Matthee** addresses the specific context of Information Operations in Sub-Saharan Africa. In his opinion, various social divisions and struggles for wealth and power create opportunities for psychological warfare. Linguistic diversity, different frameworks of meaning and the predominance of radio broadcast and popular discussion often determine the parameters. South Africa may be vulnerable to computer warfare; other African countries are not. Present conflicts are likely to be dominated by physical violence and psychological warfare. **Forstner-Billau** represents a vision from Austria. Austria too, is confronted with the increasing dynamics of ICT. He discerns two scenarios: international activities during which Information Operations do not seem to be of real concern as Austria focuses on relief activities, and secondly an attack on Austria. Theoretically the attacker could be an equal or a far superior power. If the latter would occur, he proposes to introduce 'associative communication' as a concept to be studied. **De Caro** stipulates that the Information Age has created forms of war that go beyond conflicts bound by earlier Industrial Age norms. In his opinion the nature of war itself has changed, due to the new dimensions of the 'Information sphere'. Countries should adapt to a world in full view of the global TV instead of trying to evade or hide, as Somalia and Rwanda demonstrated.

THE LEGAL PERSPECTIVE

Governments are faced with the fundamental problem as how to warrant core values of a democracy in the information society. **Muusse** explores the international legal rights for States to conduct Information Operations during peacetime, and discusses whether or not the Law of Armed conflict applies to such Operations during armed conflict. He also questions whether Information Operations can constitute a violation of the UN Charter.

THE FINAL MESSAGE

As stated before, this publication addresses the broad scope of visions on Information Operations. Some years ago these views very much were like the reactions to a painting of Jackson Pollock, Franz Kline or Jean-Paul Riopelle. A seemingly chaotic combination of colours and strokes asked viewers to give an individual interpretation. Present thinking more or less equals a painting by Karel Appel, Henri Matisse or Paul Klee, We agree on what the picture shows; though there is still some personal interpretation. Information Operations will never be defined within the sharp boundaries as presented in the paintings of Piet Mondriaan or Barnett Newman. Conflict and thus our topic has too much to do with emotion and will. There is a basic agreement that ICT brings blessings but also new challenges, options, risks and threats. There is common understanding that information is a strategic asset, as it in the end decides on economic growth, wealth, power and our abilities to organise, act and control. There certainly is no common understanding on where to go from here. This publication demonstrates the different approaches and schools of thought. By doing so it might not only create awareness, but, hopefully, also contribute to further thinking. Without this we will never find answers to questions we cannot ignore. The chips are, so to say, down. We should keep the computer chips working to our advantage. We, the Armed Forces, our modern societies and the world we live in, need them.

The editors wish to express their deep gratitude to the authors for their respective contributions. Contributions came from many countries, even from different continents. It is clear that the subject of Information Operations is a universal issue. Hopefully this third edition of NL ARMS will again serve its purpose, which is to inform the readers on a subject that is ‘high on the agenda’.

In conclusion, we have deliberately chosen to leave the papers and articles in their original form and format as much as possible. Consequently, the readers will notice that there are (minor) differences in the way different authors use different ways of referring to other publications and have different ways of using footnotes, quotes, etc.

Breda, December 1999

The Philosophical Dimension

PERCEPTION WARFARE
A Concept For The Future

Henrik Friman
The Swedish National Defence College, Department of Operational Studies.

ABSTRACT

In the ongoing discussion on information warfare, perception is a central element and a key factor for success. In this text we will discuss if the main object of warfare is the information or the perception. Most literature discusses information warfare and very few references to perception warfare have so far been found. In this text we will assume that something that we could call perception warfare exists and we will make an attempt to describe what a perception warfare concept could look like. We argue that perception warfare is not something new, but has mostly been discussed as part of other concepts of war. By making perception warfare the object and making it visible, we hope to obtain greater attraction to the concept. It is reasonable to believe that we constantly are objects for perception attacks, but what makes it perception warfare? This paper should be seen as a first inventory of the problems in an area in which more research needs to be done.

INTRODUCTION

Traditional warfare is a high-risk business in which human life is sacrificed to achieve the goals by going into combat. In the perspective of humanity, a statesman or commander always has to consider if his goals can be achieved without using the war machine. Clausewitz taught us that the goal of a combat is not always the destruction of the enemy's force; the objective can also be attained without the combat taking place at all.

In most forms of warfare, the illusion of winning and losing is central, and none of the participants wants to be the loser. It is a question of how the participants perceive the occurrence in the context of their situation. Perception warfare is the concept of how to create occurrences that give illusions of all as winners in their own way. It is a combat of the commanders' minds.

We argue in this paper that what combats in the past and in the future have in common, is forcing our will upon the counterpart. In developed countries physical violence is not accepted, and the society will prevent the use of physical violence with all means. In this context it is not trustworthy to prevent violence in society on one hand and on the other hand create forces for high conflicts missions. Still much remains to be done before we see a world without violence, if ever, and we must, therefore, see perception warfare as complement to other forms of combat. The assumption is that a decision-maker, commander, will avoid violence if possible and use other ways and means to achieve similar goals, if such is possible, which is a matter of humanity. This assumption could be questioned by saying that it is unethical to attack other people's minds, i.e. to 'brain wash' and that perception attacks could take place in secrecy without any declaration of war. Both arguments are strong and we cannot deny their relevance. However, in this text we will not take any standpoints on the

ethical questions and remain focused on the attempt to describe the concept of perception warfare.

THE TRADITIONAL VIEW OF WARFARE AND INFORMATION WARFARE

Warfare can be seen as struggles between competing entities or as military operations between enemies. The goal is to weaken or destroy each other. Warfare can be described in many forms, such as war of intervention, war of opinion or national war (Jomini, 1992). The main interest in literature seems to be on different forms for intervention, for example by air, biological, chemical and information warfare. Handel, (1996) argues that the definition of war is a question of the level of analysis. A part of the confusion could be explained by differences in analytical frameworks and definitions. What is common for all descriptions is that we consciously try to achieve goals by using force.

Perception warfare is not the same as information warfare, but there are many similarities. A few years ago we made an attempt to describe different perspectives of the concepts for information warfare (Friman, Sjöstedt and Wik, 1996)[1]. The main conclusion of this study was that the philosophies behind the concept of information warfare are not something new, but still new technology gives new possibilities. One example is to attack the source of information with information as a weapon. In the discussion up until today the main focus of information warfare has been technology, providing solutions to create control of the information flow surrounding the crisis. Concepts or techniques like command and control warfare, intelligence based warfare, electronic warfare, psychological warfare, hacker warfare, economic information warfare and cyber warfare were invented to show different applications of information warfare (Libicki, 1995). Other concepts are propaganda, deception warfare and misinformation. Still, the aim of all these concepts is a combat of controlling information, and using information to create an intentional output.

Experiences in the field and during exercises have shown that it is very difficult to control the actual output from an information warfare activity.[2] Analysis showed that the same individuals acted differently with the same information on different occasions, which indicates that the available information does not itself explain the output and that the problem is more complex than a strict relation between information and output. One explanation of the complexity is that individuals create different ‘pictures’ of situations depending on rational and emotional influences, which in a longer term results in different activities.

The assumptions for effects in information warfare are built on the law of great numbers in statistics, similar to general business marketing approaches. The expected output is measured by a sample, but gives no guarantee that the group in reality will perform the same activities. In statistics the interest is to predict outcomes for large groups and it is hazardous to predict single individuals’ acts. In sociology the acts of some individuals, the so-called ‘leaders’, will influence how others act, so-called ‘followers’. To create an effective information warfare activity, the focus should be on the leaders that (in)directly will affect the followers. We can see this as direct business marketing, which has shown to have a greater impact than general business marketing. In direct marketing, statistics are shown to be of minor importance in relation to quality data of the individual.

We believe that it is the commander, the decision-maker that is the main focus of information activities. The 'picture' of the situation is essential for the group's or organisation's further actions, and that the information 'combat' actually is perception warfare or the creation of this picture. The public will be influenced by the leader's statements and indirectly affected by the commander's beliefs. This perspective is common with propaganda, but differs in terms of objective. In perception warfare the object is a particular 'key' individual while propaganda is directed more to public opinion. Mao Tse Tung (*"On the protracted war*", 1938) once said that *"In order to win victory we must try our best to seal the eyes and the ears of the enemy, making him blind and deaf, and to create confusion in the minds of enemy commanders, driving them insane*". His statement addresses what we can regard as perception warfare.
So far, very few articles have been published openly that explicitly address the issue of perception warfare. One of the first references is Glenn and Peterson's (1995) work, in which perception warfare is explicitly discussed in the context of psychology in information warfare, which seems to be a common way of looking at perception. The question of perception is traditionally seen as part of psychological warfare (PSYWAR), in terms of perception management[3]. We argue that the question of perception is central for success, not only in the context of information or psychological warfare, and that the concept of perception warfare deserves to be a topic in its own merit and not just a part of other concepts. It is quite likely that, like an information war, we could in the future face a perception war. Hence, the concept of perception warfare is highly relevant to further study

The concepts of perception warfare are not something new, but technology to support this type of warfare is of great interest today. We can also assume that the price, risk and effectiveness of using perception warfare can be seen as attractive. We need a deeper insight of the meaning of perception warfare to understand its relevance in terms of warfare.

ESSENTIAL ELEMENTS OF PERCEPTION WARFARE

Pepper (1967) viewed perceptual acts as conscious activity links between received sensory data and the environment. In its simplest form, perception requires a perceived object and an observer. When we say, "I see a chair" the chair is the objective reference, and "I" is the observer. Philosophically, we could argue whether there is an objective reference independent of the sensory data that we perceive. Idealist philosophers have been concerned with the sensory data as their main focus, and realist philosophers concerned with the independence of the observer and the references of the perceptual act. Depending on our philosophical standpoint we will differ in objectives. Pepper, as a cognitive psychologist, advocates a synthesis between idealist and realist perspectives. He does this by focusing on the observer as active participant in a perceptive process, which gives a focus on the nature of perception.

To clarify what we mean with perception warfare we have created a theoretical example of perception attack and defence. Assume that party A has a source that gives A competitive advantage over party B. If B has the interest to limit the advantage, B can destroy the effects of the source or they can try to manipulate A's perception of the source's importance in relation to other objects. The last attempt could be achieved by many means, but with a common ground of manipulating A's logic of how to look at the source. This manipulation can only be achieved by knowledge of the participant's perceptive process. We need to be aware of which patterns create their nature of perception.

Humans seem to have limited abilities to perceive a situation (e.g. Miller, 1956). Simon (1987) has shown that what differentiates a novice from a grandmaster chess player is the ability to see patterns in situations that follow known structures, but if there is no structure, the grand master has no advantage. Similarly to this discovery, an attack on the perception is an attack on the commander's ability to find structures in his view of the situation. By losing the structure the commander cannot see the patterns of logic. Inversely, an attack could create structures that create patterns, which makes the commanders act in certain ways.

The problem is that humans have been shown to be unpredictable, and it is a complex task to predict the actual result of a perception attack. Still, the insight of perception warfare gives us a view of what is important to protect and what can be manipulated in competitive situations. The core questions are: how does the commander create his situational awareness, and which pre-understanding could we assume he has? The processes of the commander's situational awareness and his attitudes will be the main objectives for a potential attack and the key sources to protect. Sun Tzu stated: "*He who understands how to use both large and small forces will be victorious*" (Griffith, 1971, p 82). With this, Sun Tzu probably meant that we must see different levels of issues/components that can lead us to success. Sun Tzu concluded that a confused army leads to another's victory. His concept of confusion can be seen as lost control of the situation or as an uncertain situation.

THE FIRST VICTIM IN WAR IS TRUTH

Reports from recent studies of modern warfare have shown that the ability to create situational awareness is a key factor to control and succeed in warfare. We could describe modern war as the battle of truths. In a battle of trust we search not only for the truth like a journey for the Holy Grail, but instead we attempt to control the truth.

A traditional philosophical question is what is truth, which is a question without a true/strict answer. The discussion often ends in the conclusion that it depends on the situation. Our approach to this topic is that truth is a social construction, based on agreements and belief structures. This view means that what is true for me is not necessarily true for you, but in most cases there is an agreement on what seems to be the general view of reality. The truth then is something related to a norm system.

The traditional concepts of information warfare assume that there is one truth and that the war is about manipulating the ability to see the true picture of the situation. But without just one truth, information warfare will also have to create the information for the general view of reality, in other words what people believe to be true. Influencing the norm system is a process that takes a long time, which is in conflict with the common understanding of information warfare. Information warfare implies clear goals that should be achieved in a relatively short period of time (e.g. Codevilla, 1992).

War is a chaotic situation with high uncertainty. The first thing lost in war is the ability to create a view of what seems to be true. Both the observer and the norm system will be questioned. Rumours and misinformation will make it even harder to value how truthful accessible information is and the decision-maker will be forced to act on incomplete information. In this situation we still will have an opinion about what to believe or not, which is built on how we perceive the situation. What seems to be true or not will be based on

individual belief structures that could change over time. Trustworthiness is a social construct and could be extended, manipulated. Perception warfare is not about damaging the truth; it is about creating the truth. In both perspectives truth is the victim.

THE COMMANDER'S PICTURE OF THE SITUATION

To understand how to influence and interfere with the creation of the commander's picture of the situation, we need to understand what the commander is doing. An abstract description is to see commanders as a cybernetic system in which he/she acts by decisions, which could be explicit in judgements, planning etc, based on his picture of the situation. The result of the action gives new (feed-back) inputs. These change the picture of the situation, which in turn necessitates new acts (e.g. Rosnay, 1979).

The commander's 'picture' of the situation could be described in terms of situational awareness based on his own observations and pre-understanding. His pre-understanding is unique for each commander and is contextual, which explains why the same information inputs can lead to different acts. This situational awareness is built both on rational and emotional factors. The elements of the "picture" are logical in the sense of rationality and structures, but parts seem irrational, being built on emotions. We can describe the logical part in models and thereby make predictions, but about the emotional part we just have intuitive feelings.

The real vulnerability of the commander is his own mind and how he comprehends the situation. *"Capture their minds and their hearts and souls will follow"*[4]. The mode of his mind will create a picture of how he sees the actual situation. This picture is not necessarily true, but still guides the commander how he/she will act. The commander will continue to value how well he believes he has control of the situation in terms of uncertainty and risks. Control is constructed by logical explanations of the situation, with information structured into patterns. By searching for more information he/she will attempt to limit the uncertainty.

In this perspective, perception warfare is the ability to influence the commander's 'picture' of the situation in a controlled way, the art of influencing decisions. It is important that this influencing is a controlled process. Otherwise there is a risk of unfavourable decisions by the commander.

An important note is that no commander wants to be seen as a loser. In a successful perception attack, all participants will have the illusion that they are winners. Thus, the goal is to create a perception that everyone is a winner. It is not a zero sum game: the success of one party is the other party's defeat. Even though in reality one wins more than the others do. The perception of the situation is the key element for how the commander will act.

THE TRUE ENEMY IS YOUR MIND

If individuals are facing perception warfare activities, the mind is the centre of gravity for the attack. The ability for a commander to create a satisfactory picture of the situation is crucial for further activities. The true enemy in perception warfare will be the commander's own mind and not primarily the adversary. The adversary will try in every way to create a 'picture'

for the observer that suits his goals. It is in the commander's mind that the actual picture of the situation is created.

The key question then is how to defend our own mind, which in many aspects has characteristics that resemble the problem with computer viruses and Trojan Horses, but that needs other solutions. In the computer world the best security measure is to physically disconnect the computer from the surrounding world by using stand-alone machines, and access codes. This method is not suitable for individuals who need social interaction with others. Instead, we need to find new ways for verification and authorisation that help us discover perception attacks.

An open mind is the prerequisite for creative problem solving, but at the same time an open mind is vulnerable to external interference. Perception warfare is combat on an individual level with the commander as the 'target'. The key element is to create uncertainty on issues that the commander values as important. Uncertainty is then created in terms of lost control. If we have lost control we have also lost the perspectives of what we are doing in the long run, and risk becoming a follower instead of being a leader. It is becoming a follower that gives the opportunity for the adversary to direct our future behaviour and decisions. The leader is often easier to identify as an object than the followers are. To be able to take control, we need to know what the commander, being the 'observer', finds important and how we can value this factor. For example, if he finds that being in time is important, we can stress him by delaying information. But this is not enough. How late can information be and still be seen as being on time? The question of perception is a question of attitudes, which is the basis of how we value the situation.

The end-state of a perception war is change of mindsets and change of manifestation of the will. Unlike traditional war, all the parties involved in a perception war could have the illusion that they are the winners.

CONCLUDING REMARKS

In this paper, I have tried to clarify the concept of perception warfare. The main purpose has been to define research problems and directions for future research, rather than to discuss any problem in depth. That will have to be done in future work. However, even from this introductory discussion it should be clear that there is a lot that we do not know, and that a lot of work needs to be done before we can create a concept of perception warfare. To conceptualise what is outlined, we will have to work through a series of steps and studies.

REFERENCES

Codavilla, A. (1992) *Informing Statecraft*

de Rosnay, J. (1979) *The Macroscope*, Harper & Row, Publishers, New York (Translated from the French by Robert Edwards)

de Jomini, H. (1992) *The Art of War*, Greenhill Books, London

Friman, H. Sjöstedt, G. and Wik, M. (eds) (1996) *Informationskrigsföring - några perspektiv*, Utrikespolitiska Institutet, Stockholm (in Swedish)

Handel, M. (1996) *Masters of War: Classical Strategic Thought.* 2 ed, Frank Cass, London

Glenn, J. and Peterson, J. (1995) *Information Warfare, Cyber Warfare, Perception Warfare and their Prevention*, World Future Society, Atlanta.

Griffith, S. (1971) *Sun Tzu: The art of war*, Oxford University Press

Libicki, M. (1995) *What Is Information Warfare?*, National Defence University, Washington

Miller G. (1956) 'The Magical Number Seven, Plus or Minus Two', *Psychological Review*, 63 (2)

Pepper, S. (1967). *Concept and Quality: a world hypothesis*. La Salle, Ill, Open Court

Simon, H. (1987) 'Making management decisions: the role of intuition and emotion', *Academy of Management Executive*, Feb, pp 57-64

NOTES

1 In a study at the Swedish Institute of International Affairs.

2 Data mainly collected at the Staff excises at the National Defence College and exercise at the Swedish National Wargaming Centre (1994-1999).

3 US DoD defines perception management as: Actions to convey and/or deny selected information and indicators to foreign audiences to influence their emotions, motives, and objective reasoning, and to intelligence systems and leaders at all levels to influence official estimates, ultimately resulting in foreign behaviours and official actions favourable to the originator's objectives. In various ways, perception management combines truth projection, operations security, cover and deception, and psychological operations. (U.S. Department of Defense *Dictionary of Military Terms*, Greenhill Books, London 1990)

4 Reference unknown.

INFORMATION WARFARE
Learning With Sun Tzu

Prof George J. Stein
USAF Air War College, Montgomery Alabama, USA [1]
Department of Future Conflict Studies

ABSTRACT

The thesis of this essay is that asking whether the conduct of Information Warfare is like the conduct of war described in the Warring States era in ancient China by Sun-Tzu's Art of War can provide strategic insight. It is not asserted, however, that InfoWar equals Sun-Tzu's Art of War. This essay also asserts that the very "otherness" and "oddness" of the Art of War is its great appeal. It is a means to gain the critical distance or perspective to explore the "otherness" and "oddness" of a universe in which InfoWar can be seen as somehow "real." It is, fundamentally, "serious play."

INTRODUCTION

In a science fiction novel by Gordon Dickson, *Tactics of Mistake*, the "*head of the Tactics Department of the Western Alliance Military Academy*" provokes an argument among some field officers by observing that the "*sound strategist, used to dealing with unreal things, is a better manipulator of [men and weapons] than the man used to dealing with the real tools – that are actually only end products.*" He goes on to illustrate from fencing.

> The fencing tactic is to launch a series of attacks, each inviting ripostes, so that there's a pattern of engages and disengages of your blade with your opponent's. Your purpose, however, isn't to strike home with any of these preliminary attacks, but to carry your opponent's blade a little more out of line with each disengage so gradually he doesn't notice you're doing it. Then, following the final engage, when his blade has been drawn completely out of line, you thrust home at an essentially unguarded man.[2]

In his *Introduction to Strategy*, André Beaufre notes that in addition to the historically established strategic factors of time, space and the size and morale of the forces available, it is the fourth factor of *maneuver* which governs "the order and inter-relationship" of the basic three.

> Taking fencing as an analogy, it is clear that there are a number of possible forms of action and reaction: O*ffensively* there are eight postures – 'attack' which may be preceded or followed by 'threat', 'surprise', feint', deceive', thrust', 'wear down', 'follow-up'. *Defensively* there are six postures – 'on guard', 'parry', 'riposte', 'disengage', 'retire', 'breakoff'. As far as the actual forces are concerned there are five possible types of decisions – 'concentrate', 'disperse', 'economize', 'increase', 'reduce'.

> This gives a total of nineteen components to be arranged and combined in the light of the time and space factors. They constitute the keyboard on which the game of strategy is played. …all are aimed ultimately at *freedom of action*, the object being either to gain it, regain it or deprive the enemy of it.[3]

Beaufre goes on with this fencing / strategy analogy by illustrating each of the nineteen components with cases of allied and axis military operations during the Second World War.

Now it is obvious that strategy does not *equal* fencing. And, it is for swordsmen and soldiers to debate whether strategy is *like* fencing. Strategy does not *equal* the Western game of chess or the Eastern game of *Go*. The question for the militarist (used here to mean a person who studies both the theory and practice of strategy) is whether subjecting a particular strategic problem to analysis *as if* the problem were *like* a problem in fencing, chess or *Go* is in any way instructive or useful in learning the Art of War.

If "war" is *sui generis* – a phenomenon in its own class and, in its essence, incomparable with any other human activity, then comprehending it can be done (as is believed by far too many in the US Army) only through *doctrine*. We will employ specialist *military historians* to comb the litter of history to discover "lessons learned" from past war and battle. It has even been said that the military should not conduct information warfare as there is no authoritative doctrine manual based on the lessons learned from past information wars! Any student of the evolution of air power, or more especially, aerospace power understands the leaden drag of "historical lessons learned."

But of course, aerospace power is "like" other forms of power and, equally important, it is "unlike" other forms of power in very distinctive ways. So long as aerospace power is treated by strategists and generals within the "historical" surface-based, two-dimensional territorial campaign, the "distinctive" characteristics of aerospace power can never be realized. To illustrate: what if it were argued that the distinctive characteristics of aerospace power (usually listed as including speed, precision, range, freedom of maneuver [including dispersion and concentration], and discriminate lethality) are the essential characteristics of contemporary and most-likely future "wars." Then, the traditional "principles of war" beloved of doctrinaires would have to be reinterpreted. Would, for example, a huge standing army with mobilizable needing to be trained reserves be appropriate for a world of conflicts requiring speed, precision, range or discriminate lethality?

Clearly, the characteristic conduct of every future war and conflict does not *equal* the characteristic conduct of aerospace warfare. The question for the militarist is whether subjecting a particular strategic problem to analysis *as if* the problem were *like* a problem in aerospace warfare is in any way instructive or useful in learning the Art of War. Is contemporary aerospace campaign thinking a useful *analogy* with which to analyze *other* strategic problems? While not wishing to appear trite, is it not accurate to say that in dealing with the contemporary political, economic and energy environments, what Royal Dutch Shell needs most is the ability to act with speed, precision, range, freedom of maneuver, and discriminate effect?

Now the question facing any discussion of the conduct of Information Warfare (InfoWar) is: how is InfoWar *like* other forms of the exercise of power; how is it *unlike* the "traditional" exercise of power; and what, if any, are its *distinctive* characteristics?

In the last few years, serious and not-so-serious efforts have been made to answer this set of questions. Serious militarists have argued that InfoWar is *the* new means of strategic success and equally serious militarists have argued that it is "nothing but" a "New Age" slogan for the traditional combat service support function of secure and reliable battlefield communications made a bit more complex by computers.[4] Less seriously, but probably more importantly, many people have grasped InfoWar as the Rumplestiltskin Magic Word to open the State's Gold Room and gather vast new missions, resources, personnel and toys for "their" InfoWar capabilities.

Even the normally army-dominated and conservative doctrine writers can catch the InfoWar fever. In the authoritative US Joint Publication 3-13.1, *Joint Doctrine for Command and Control Warfare*, the central goal of C2W -- the Holy Grail of InfoWar is set forth in all its promise. JP 3-13.1 asserts that it "*may even be possible to convince the adversary that the US had 'won' prior to engaging in battle, resulting in deterrence and preempting hostilities.*"[5] Alas, war without blood is fantasy. War is neither chess nor *Go*. Even if war were only *like* fencing, the purpose remains to defeat the enemy, killing him if necessary.

If, however, war and conflict "are aimed ultimately at *freedom of action*, the object being either to gain it, regain it or deprive the enemy of it," then serious *meditation* or *sustained reflection* on "fencing," as Beaufre demonstrated so well, repays the militarist's efforts to understand the Art of War. More broadly, and the point of this essay, the willingness and discipline to explore an *analogy* like war + /- fencing can be very instructive, insight-producing, or, alas, even misleading. Facile analogies can be very misleading and facile analogies in the InfoWar literature are all too common. On the other hand, some of the most creative discussions of InfoWar are also based on analogical reasoning.[6]

It is, then, the thesis of this essay that asking whether the conduct of Information Warfare is *like* the conduct of war described in the Warring States era in ancient China (c. 403-221 BCE) by Sun-Tzu's *Art of War* (Sun-zi ping fa) can provide strategic insight. It is not asserted, however, that InfoWar *equals* Sun-Tzu's *Art of War*. This essay also asserts that the very "otherness" and "oddness" of the *Art of War* is its great appeal. It is a means to gain the critical distance or perspective to, like Dickson's science fiction character "dealing with unreal things," explore the "otherness" and "oddness" of a universe in which InfoWar can be seen as somehow "real." It is, fundamentally, "serious play."[7]

Much current military discussion and thinking in the United States and the West in general are occupied with the question of "asymmetrical" warfare. In general, the concept of potential military "asymmetries" between "modern" *versus* "Third World" nations tends to focus on the likelihood that technologically "weaker" actors will be forced to rely on either asymmetrical methods of "battle," such as urban guerilla warfare, or asymmetrical "weapons," such as chemical / biological terror actions, the purposive generation of refugee flows or humanitarian crises or, in some cases, information warfare. InfoWar is seen as a particularly attractive option for "rising" regional powers as (1) Western militaries, especially the US and NATO, are increasingly dependent on information technologies to conduct "expeditionary" military operations and (2) information technologies are proliferating world-wide, often driven by Western commercial interests.

On the other hand, the true asymmetries which will confront US and Western expeditionary military operations may not be technological. It may not be that they "have" the technologies for InfoWar, but that they may be prepared to "conduct" InfoWar in ways we find difficult to "imagine." Two asymmetries in particular will be unusually challenging. One asymmetry might best be called "contravalent" and will refer to the possibility of conflict and a "way of war" flowing from totally asymmetrical "value systems."[8] Why men fight, what men fight for, and how men fight may be far more "culturally dependent" than the scientific/technological and "rational" Western militaries care to admit.[9] Clearly, the US was totally unprepared for the "fanaticism" of the Japanese *kamikaze* or the "irrational" approach to war (not "battle") of the Vietcong. Equally mysterious is how the Serbian "fanatics" can be so willing to conduct "criminal" attacks, which show a "complete disregard" for "innocent" women and children. Rape, as asymmetric contravalent warfare cannot be addressed simply by labeling adversaries as "war criminals." In the universe of InfoWar, a contravalent notion of "truth" will be a particular challenge.[10] It is not at all clear that we have the vaguest understanding of how "*to convince the adversary that the US had 'won' prior to engaging in battle, resulting in deterrence and preempting hostilities.*"

The second asymmetry, and the focus of this essay, may be even more difficult to comprehend. It might best be called "metaphysical" or "epistemological" as it flows from a totally different "model" of how the universe "works" and how men "know" how to "work" in the universe. This asymmetry strikes at the very heart of the notion of InfoWar. Clearly this was not a problem when "war" involved only the "Clausewitzian" Euro-American nation states.[11] We pretty much understood one another. And, so long as Western technological superiority continued, military actions in the colonial era hardly counted as "real" war. Many fierce "battles," of course, but not "really" war. When, however, something approaching technological parity develops between the Euro-American militaries and "them," the "metaphysical" or "epistemological" asymmetries may become increasingly relevant.

Thinking about "metaphysical" asymmetries in war and warfare might best be approached by the study of the classical military writings of the great civilizations. How many Euro-American strategists are familiar with the Hindu/Indian classic on war the *Mahabharata* or have made any effort to explore several centuries worth of Islamic studies of war and battle? This essay serves as a modest introduction to perhaps the greatest Chinese strategist, Sun-Tzu, to illustrate the importance of the "metaphysical" in military thinking.

LEARNING WITH SUN TZU

Sun Tzu (Wade-Giles rendering of Chinese characters) or Sun Si (current Pinyin system used in China) probably lived during the Chou/Zhou dynasty at the end of the "Spring and Autumn" era (770-476 BCE) or the beginning of the "Warring States" era (475-221 BCE) – thus, +/- 5th century BCE. The absence of any discussion of mounted cavalry argues for the earlier period. The discovery in 1972 of a copy of Sun Tzu's "Art of War" (*Sun-zi ping-fa*) in a Han dynasty tomb (140-118 BCE) essentially identical with the current thirteen chapters argues that the "Art of War" as known today is authentic. Whether Sun Tzu himself wrote it or, like most of the writing we attribute to Aristotle, it was written by his students or disciples remains unknown.[12]

THE "METAPHYSICAL" ASYMMETRY

Let's ask an odd question. "What must the world be like for the theory describing it to be seen as true?" That is, if I have a theory of "magic" and I wave my "magic wand" over the hat, a rabbit better hop out. For the theory of magic to be true, the "world" must contain hats with rabbits in them. My "magic" won't work in a world with no rabbit-filled-hats. Thus, it must be considered that InfoWar will not "work" in a "world" that has had, and arguably still has, a totally "other" metaphysic and, more to the point, a totally "other" epistemological model of "information."

In the Chinese military classic *Questions and Replies Between T'ang T'ai-tsung and Li Wei-kung*, Li Ching observes:

> If one has a state and a family, how could he not discuss attacking and defending? For attacking does not stop with just attacking their cities or attacking their formations. One must have techniques for attacking their minds.

So far, so good. We can appreciate that Li Ching might have been an ancestor of InfoWar. However, he goes on to observe:

> Now attacking their minds is what is referred to [by Sun Tzu] as "knowing them." Preserving one's *qi* is what is meant by "knowing oneself."[13]

Preserving one's *qi* is not usually part of Euro-American strategic thinking. It is, however, central to Chinese and, in general, Asian strategic thinking and reflects a distinctive "metaphysical" asymmetry.

Western metaphysics, that is, what is the primary "bottom line" nature of reality, is essentially "dualistic." Almost every Western philosophical system distinguishes "two" aspects of the world. Permit a brief list of familiar dualisms: Creator-created; Being-becoming; Forms-flux; Essence-accident; Theory-praxis; Natural Law-situation ethics; and Ideal-everyday reality. In essence, we divide the world between a "model" which stands outside (and provides a standard to order and judge everyday life) and the everyday world (Plato's Cave) in which we live. The Chinese or Asian "world" in which Sun Tzu lived and the approach to military strategy he reflects is not "dualistic" in the Western sense but "monistic." [14]

For the Chinese (certainly then and arguably still today) the "universe" is, indeed, a uni-verse, a "one" thing. What "is" is. Neither we humans nor anything else stand "outside" existence. Moreover, everything that "is," is *qi* in constant transformation. While the West might distinguish "matter" from "energy," the Chinese note that "matter" is merely "materialized" or easily observable *qi*, like a stone or military formation, and "energy" is not-yet-materialized *qi*, like Spring and Summer, "spiritual holiness," or the strategic plan in the commander's mind. What "is" is matter/energy (*qi*) in constant, mutually influencing/interacting transformation (*yin/yang)*. Thus, the one book that captures this, and continues to baffle the Western mind, is the thousands-year old *I Ching*, the "Book of Changes."[15]

For the Chinese, and Sun Tzu, this means that we humans do not stand "outside" our universe. In contrast to Western epistemology, there is no possibility of a privileged Archimedean "outside" standard by which to observe, judge or understand "reality." There is no "information realm" in which to conduct InfoWar as a separate "cyber-space." For the Chinese, the "state" or "configuration" of the universe - that is, matter/energy (*qi*) in constant, mutually influencing/interacting transformation (*yin/yang*) at any given moment in time is called *Dao*. "We" "are" in a particular state or condition "now," and "we" "are" in a particular state or condition "then." Thus, "we" "are" best understood as a particular set of relationships at a particular time and place. That the essence of "war" is fundamentally a relationship is, in principle, familiar to any Western strategist. The common Western phrase "system of systems" would probably be translated conceptually into Chinese as "the relationships among the relationships."

The "state" or "configuration" of the universe at any given time or place is *Dao* – the "Way." (*Dao de jing* – The Way and its Power) Everything that is, from Earth to the Heavens, and every being and activity, has its own particular and unique "way" to figure-out, navigate or prosper/decline as part of the "Way."

Sun Tzu opens his *Art of War* with the basic premise: "Warfare is the greatest affair of state, the basis of life and death, the *Dao* to survival or extinction." [16] Unlike our Western or modern prejudice that warfare is the "deviant" condition and only an unfortunate interruption of the "normal" state of peace, for Sun Tzu "warfare" not only "is," but more importantly, is the "Way" of survival and extinction for humans-in-community, the state. As warfare is the basis of life and death, of course it is the greatest affair of state, and of course "it must be thoroughly pondered and analyzed." That is to say, the study of warfare, the basis of life and death, is the study or figuring-out and navigating the "way" of warfare within the study or figuring-out of the "Way."

As the "Way" is a particular set of relationships obtaining at a particular or unique time/space, the "Art of War" or strategy is radically contextual, situational and relational. There are no *a priori* "rules" or "laws" of warfare. This single insight is the key to understanding the asymmetry of Chinese or Asian strategic thinking. If, when, how, where, "this" war is to be fought in "this" manner or with "these" weapons depends, in essence, on the *Dao* of "this" war in relation to the *Dao* itself. There is no way to tell ahead of time whether nuclear attack, InfoWar, deception & denial, or whatever "warfighting" means available might be used.

The "goal" or purpose of warfare is to secure the survival of and, by implication, benefit to the state. It is a fundamentally "conservative" or "order restoring" activity. Expansionism or conquest are concepts that appear very rarely in classical Chinese strategic writing and are totally absent in Sun Tzu. Thus, for Sun Tzu, the priority for military actions is clear. If possible, and in complete opposition to the normal Western approach, "subjugate the enemy army without battle," "capture cities without siege," "destroy the enemy state without prolonged fighting," or, in general, "take the enemy intact." If, however, this is not possible, **win the battles**. Only a strong, well-equipped and well-trained military capable of winning battles can provide ultimate security for the state.

The *Dao* itself is the particular set of relationships obtaining at a particular or unique time/space. Thus, Sun Tzu begins chapter one of the *Art of War,* "Initial Estimations," with the requirement for a careful, rational study of the particular and unique relationships between

"the state" and its adversary at this time and place. We need to examine these "five factors" and answer these "seven questions."[17] In Sun Tzu's universe there were "five elements," "five musical notes," "five grains," "five colors," and "five flavors or tastes" which captured the full range of transformations possible and, yet, were inexhaustible. It should be no surprise that Sun Tzu begins his study of the greatest transformation, life and death, with the requirement to examine the "five factors." And, of course, it is the constant, mutually influencing/interacting transformation among these five strategic factors, which is crucial.

We must retire to a private room in the state temple and "calculate" (the Chinese character implies "grind out") the quantity and quality of our answers to the factors and questions in relationship to the adversary's answers. Why intelligence and spies are essential for Sun Tzu (his last chapter) is obvious, then, in his first chapter. Only when, to borrow a phrase from the Russians, the "correlation of forces" – understood here as *qi* in its particular "incarnation" – is running in our favor can we decide, rationally, for war.

SERIOUS PLAY

How then might we "meditate" or "reflect" with Sun Tzu on InfoWar in these first few paragraphs? How can we think about the *Dao*, *Tien* (the heavens), *Di* (the earth), *Jiang* (leadership), and *Fa* (organization)? The "info-warrior" might begin by asking, "what is the Information component in each of these factors on the adversary side which can be attacked" and "are we able to protect the Information component of these factors on our side?" Hmm? Not very helpful.[18]

Moving to Chapter Two then, "Planning Offensives," the info-warrior might identify the Information component of the adversary's (1) strategy, (2) his "alliances" or support, (3) his military forces, and (4) his "cities." Perhaps an "information warfare" matrix can be developed.

5 Factors ***4 Targets***	**Moral Order (dao)**	**Heaven (tien)**	**Earth (di)**	**Leadership (jiang)**	**Organization (fa)**
Strategy					
Alliances					
Armed Forces					
Cities					

The conduct of warfare recommended by Sun Tzu continues his conservative "preservationist" theme. The "highest" realization of warfare is to attack the enemy's plans or strategy. Failing that, attack his alliances. Failing that, attack his army. Failing that, then and only then, attack his cities.

In the context of 21st century Information Warfare the highest realization of warfare might be to attack, via direct info attack, the information (data, plans, programs, etc.) required for the execution of the adversary's strategy. Each of the five factors must be examined. For example:

(1) What information and information systems maintains the adversary *Dao*? Can the unity between the government and the people required to support the strategy be attacked through the information system? Could a certain "unorthodox" information operation be conducted to cause his media to report that his army has attacked defenseless civilians? In essence, attack the information on which the adversary *Dao* depends. And, of course, take steps to project your own.

(2) If his strategy depends on certain knowledge of weather conditions, then "destroy the tallies" and cease all weather reporting. Conduct military actions during times when his weather information is inadequate and develop weapons to deny the enemy the ability to use weather information. Should, for example, one prepare to conduct operations without the aid of the Global Positioning System (GPS) on which most of the planet's armed forces increasingly rely? Any soldier knows this.

(3) The common reading of what Sun Tzu calls *di* is "terrain" but Sun Tzu provides a full discussion of military or battlefield terrain in chapter ten. Perhaps if we remember that Sun Tzu wrote in a time when *di* or "the earth" was the basis of agriculture and agriculture was the foundation of state power, then in our contemporary fundamental strategic assessment *di* could be read to mean "the conditions which sustain the power of the state to conduct war and maintain the people's support." Thus, the info-warrior would attempt to discover what information and information systems provided the basis of the adversary's state power and his ability to execute his strategy. Is it his banking system? His communication system? His electrical and transportation system? The model of the air campaign developed by Col. John Warden might give us a template with which to start an analysis.[19]

(4) *jiang* in the Zhou era meant the "leadership" in general, not just the military leadership. The info-warrior must discover what information, by what channels, by what processes, through which persons, the adversary *jiang* gets the information required to execute the strategy. Who or what are the mediators through which the adversary leadership gets its information? The five types of spies of chapter 13 come to mind and any contemporary intelligence officer or info-warrior must have been assigned this "mapping" task.

(5) *fa* is the most traditional concept. Normally it is read as the "forces and capabilities" available to execute the strategy. For the info-warrior, however, *fa* might be read as the adversary "command and control" system – electronic or otherwise. How to penetrate, disrupt or influence the *fa* required for troop mobilization, troop deployment, and command & control in battle is the chief task.

Working through the matrix, line by line and column by column for both "knowing ourselves" and "knowing the enemy," evaluating the relationships of each "box" with the adversary box, and then "doing the comparative totals" permits an informed judgement as to whether "this" action, at "this" time, in "this" way, etc. is, as the Chinese might say, "propitious." Is this "strategy by fortune cookie" or "insight provoking?"

After working each box in the top line, and failing to disrupt the adversary plans or strategy, our Sun Tzu inspired infowarrior would attack next the "alliances." In addition to the obvious and clear meaning of "alliances," the contemporary infowarrior might consider alliances as the supporting military *joint* and *coalition* information infrastructure on which the adversary

depends. Reports on the complexity of communications and command & control "alliance" operations in the Kosovo operations will be studied carefully for asymmetric vulnerabilities.

Failing to disrupt either strategy or "alliances," the info-warrior will attack the "army." At the most obvious level, this is command & control warfare (C2W) and the C2W-systems by which the adversary executes his military operations.

All these failing, then and only then, attack his "cities" -- understood by the infowarrior as the entire civilian (political, economic and social) information infrastructure which sustains both popular support for the adversary state and the "base" essential for the adversary to project forces.

If "Information Superiority" in the 21st century is both a major factor of wealth generation and a vital requirement for the ability of the Western Alliance to project power in an expeditionary manner, then attacking the "domestic" and "non-military" information "substructure" on which the execution of our strategy depends is a key factor in Information Warfare.[20]

In each case of war or conflict, the info-warrior must fill-in all the spaces in the matrix. And, as Sun Tzu advised, if you do not have the information you need or if you cannot fill-in the matrix, war is too risky.

Continuing our "serious play:" - while warfare is the "way" to survival or extinction of the state, warfare itself, like pottery, farming, family life, or any human activity, must have its own distinctive "way" if it is to be "congruent" with the "Way." For Sun Tzu, the Chinese, and Asia in general, "Warfare is the *Dao* of deception."[21] Thus, immediately in chapter one Sun Tzu begins his well-known listing the various tactics, techniques and procedures of deception familiar to readers of the *Art of War*, aspirant infowarriors, and any veteran of the Vietnam war: display incapability; feign inactivity; attack where they are unprepared; go where you're not expected; etc. The "way" of warfare is deceit, dishonesty, trickery, ruse, ambush, trap, lies, surprise attack, feigned retreat or surrender, collaboration, treason, and any other way to manipulate the "laws of armed conflict" which attack the adversary's *qi* and cloud his mind.

The "way" of warfare is to attack the adversary's mind – in a word, to conduct Information Warfare.[22]

"These are the ways military strategists are victorious." But, Sun Tzu quickly adds a phrase that puzzles the Western reader, "they cannot be spoken of in advance." Why not? Why cannot we develop "doctrine" to conduct information warfare? The answer is that any warfare conducted by a predetermined set of tactics, techniques and procedures will fail because it is not in conformity with the "Way." That is, the conduct of war and battle is radically contextual, situation-dependent, and relational. Whatever the occasion for *this* war or battle, the objective of war or battle remains life or death for the community. Thus, winning battles is fundamentally secondary in conducting wars. With the exception of a few ambushes, the Vietcong lost every "stand up" battle with US forces. This was asymmetric information warfare – conducted by attacking the adversary's *qi* – and won by the *Dao* of deception.

FOUR KEY CONCEPTS IN SUN TZU'S *ART OF WAR*

Four concepts in the *Art of War* and classical Chinese military writings may be particularly asymmetric from the normal Western assumptions about military operations: (1) the independence of the military, (2) "strategic military power," (3) the disposition of military forces, and (4) the unorthodox and orthodox.[23] All require serious reflection by a contemporary infowarrior as the well-known phenomenon of "mirror imaging" is likely to provoke a serious misunderstanding of observed behaviors.

Perhaps the most asymmetric concept from the contemporary Western idea that "the general" (the armed forces) are always subordinate to the civil authorities, even in wartime, is Sun Tzu's claim that once "war" is declared, "the general" (seen as fielded military forces) cannot be interfered with. Orders from the civil authorities to advance, retreat or engage in battle may be ignored. While this may seem "undemocratic" and a fatal threat to civil-military relations, Sun Tzu's logic is rooted in his "metaphysical" assumptions. That is, if navigating the *Dao* is radically contextual, situational and relational, and this war is radically contextual, situational and relational, then this battle is also radically contextual, situational and relational. Only the commander "on the ground" has the "situational awareness" to judge what needs to be done to "preserve" the state. Improved modern communications do not change the logic. Indeed, President Bush was praised by the US military for his conduct in the Gulf War. That is, he set the grand strategic/political goal and trusted his field commanders to conduct the appropriate military operations. The criticism of President Johnson's hyper-detailed "interference" with the bombing campaigns during the Vietnam War is well known and quiet complaining about "air order tasking by committee in Brussels" is beginning to be heard.

The contemporary implication of this Sun Tzu model may be that the Western infowarrior will not encounter a command & control system which if attacked at the "head" will disrupt the adversary's military operations. Indeed, it might be argued that the "independence of the general" is exactly what is implied by current arguments for a "distributed" decision-making command & control model. Improved communication systems do not invalidate the logic of contextual, situational and relational decision-making. "Centralized control and decentralized execution" may need to be rethought.

The second key concept is "strategic military power." The Chinese character is *shi* and, depending on the requirements of rendering it into English, is also translated as force, strength, authority, influence, power, advantage, etc. As the concept is so central and common in the *Art of War* and other classical Chinese military writings, all good translators will insert (*shi*) next to the English word or phrase used to translate it. In general, *shi* refers to the strategic and operational advantage resulting from a combination of the "mass" and "superior positioning" of military forces.[24] *Shi* is thus always contextual, situational and relational. A standard comparison of "forces and capabilities" is irrelevant as to which side has "strategic military power" at any given time, place or situation.

The third key concept is the "disposition of military forces" (*qiang*) and, like *shi*, can be variously translated. In general, *qiang* is the actual operations or maneuvers conducted by the army which attempt to "shape" the adversary into a "form" which can be exploited. Again, *qiang* is always contextual, situational and relational. The goal is to conduct operations which "shape" the adversary into a mistaken *qiang* which can then be exploited. As Sun Tzu

observed, "One who excels at moving the enemy deploys in a configuration (*qiang*) to which the enemy must respond." Now, to "shape" the enemy will require the most exquisite conduct of InfoWar. Warfare is, after all, the *Dao* of deception and "attacking their minds" is thus a central aspect of *qiang*.

> The T'ai-tsung said: "I observe that the thousand chapters and ten thousand sentences [of the military writings] do not go beyond 'Use many methods to cause them to make errors,' this single statement."[25]

The fourth concept is the pair unorthodox and orthodox. *Qi* (a different Chinese character than *qi* –the "life force/matter/energy") and *zheng*. In general, *qi* and *zheng* are just a way of thinking about how to operate within and exploit the enemy's dispositions (*qiang*) and expectations. It is far too narrow to translate the concept as "regular" and "special operations" forces – although regular and special ops are implied. In general, *qi* and *zheng* reflect the "metaphysics" of "one-world" of constant transformation and mutual interactions (*yin/yang – qiang/shi*). A Sun Tzu adversary will not have a disposition of forces (*qiang*) or "Table of Organization and Equipment" which will permit Markov-like chains of prediction. One must expect the Sun Tzu adversary to conduct a constant, situation dependent and consistently deceptive "shifting" between *qi* and *zheng*.

> The [musical] notes do not exceed five, but the changes of the five notes can never be fully heard. The colors do not exceed five, but the changes of the five colors can never be completely seen. The flavors do not exceed five, but the changes of the five flavors can never be completely tasted. In warfare the strategic configurations of power (*shi*) do not exceed the unorthodox and orthodox, but the changes of the unorthodox and orthodox can never be completely exhausted. The unorthodox and orthodox produce one another, just like an endless cycle. Who can exhaust them?[26]

In essence, Sun Tzu's *Art of War* reflects a "world" called *Dao*: a world of context, situation and relationships which are constantly in transformation through mutual interactions and mutual influences. War is the *Dao* of survival or extinction and thus "war" "is." The *Dao* of warfare is not "outside" the *Dao*. "Warfare is the *Dao* of deception." There is no "ideal" model of strategy and no possibility of military "doctrine" which can be applied apart from context, situation and relationship to the enemy. Although it may be an apocryphal tale designed to criticize the US Air Force for not taking "doctrine" as seriously as the Army, there may be great wisdom in the reply of the USAF general who, when asked "what is Air Force doctrine on …" replied "It depends." The "Art of War" may indeed be adapting to a context, situation or set of relationships through *qiang*, via *qi* and z*heng*, to produce the *shi* which gives "life" and "survival."

CONCLUSION

The thesis of this essay has been that asking whether the conduct of Information Warfare is *like* the conduct of war described in the Warring States era in ancient China (c. 403-221 BCE) by Sun-Tzu's *Art of War* (Sun-zi ping fa) can provide strategic insight. It was not asserted, however, that InfoWar *equals* Sun-Tzu's *Art of War*. This essay also asserted that the very "otherness" and "oddness" of the *Art of War* is its great appeal. That to explore the

"otherness" and "oddness" of a universe in which InfoWar can be seen as somehow "real." is, fundamentally, "serious play."

Earlier we asked an odd question "what must the world be like for the theory describing it to be seen as true?" Perhaps we might rephrase the question to "what kind of world or future operating environment is assumed by the theorists of InfoWar?" In general, the "world" in which InfoWar would be "true" seems very much like the "world" described as *Dao*. The infowarrior is not "outside" but, rather, operates "in" a "world" of context, situation and relationships which are constantly in transformation through mutual interactions and mutual influences. Whether the "world" is described as the "net," the "web," the "mesh" or whatever; and whether the infowarrior is a "node" a "knot" or an "island in the net," the infowarrior is "in" and "of" the *Dao*, not outside. Perhaps the "world" of Sun Tzu is a far more accurate description of the Information Age "world" than we usually suspect. It is not accident, then, that military strategists attempting to deal with war in the Information Age seem to recognize the "contemporary" quality of the *Art of War*.

REFERENCES

Bibliography on Chinese Strategic Thinking

Chinese Strategic Culture

The Seven Military Classics of Ancient China, (Ralph D. Sawyer, translator) (CO: Westview, 1993), ISBN 0-8133-1228-0, (the one book in this entire list you must own. Includes Sun Tzu.)

Art of War, (Ralph D. Sawyer, translation & commentary), (CO: Westview, 1994), ISBN 0-8133-1951-X, (excellent introductory material and footnotes)

Sun Tzu - The Art of War, (Samuel B. Griffith, translator), (NY: Oxford University Press, 1971), ISBN 0-19-501476-6, (version most familiar to military readers. Brig.Gen. Griffith, USMC, forword by B.H. Liddell Hart)

Sun Tzu on the Art of War, (Lionel Giles, translation & commentary), (Singapore: Graham Brash (Pte) Ltd., 1993), ISBN 9971-49-107-9, (first published in 1910 {and thus in the public domain, and thus available on the Internet to download} This is the classic and very scholarly first major translation into English).

Sun-Tzu The Art of Warfare, (Roger T. Ames, translation & commentary), (NY: Ballentine, 1993), ISBN 0-345-36239-X, (first English translation incorporating the recently discovered Yin-ch üeh-shan texts. Full scholarly apparatus*).*

Sun Tzu: The Art of War, (Thomas Cleary, translation & commentary), (Boston: Shambhala Publications, 1988), ISBN 0-87773-452-6, (philosophical translation; locates work in Daost canon).

Sun Tzu's Art of War, (Yuan Shibang, translator; commentary by General Tao Hanshang)

(NY: Sterling Publishing Co., 1990), ISBN 0-8069-6639-4, (commentary by professor at Beijing War College, PRC)

Sun Tzu: The New Translation, (J.H. Huang, translation & commentary), (NY: William Morrow, 1993), ISBN 0-688-12400-3, (especially detailed discussion of alternate meanings of Chinese characters)

Sun Tse: L'Art de la guerre, (Texte traduit par Jean-Jacques Amiot), (Paris: Pocket, 1993) ISBN 2-266-05098-2, (text of the original Père Amiot translation (1772); excellent commentary by contemporary French strategic thinkers, e.g., Gérard Chaliand, Alain Joxe, etc).

Sun Zi – L'Art de la guerre, (Valérie Niquet-Cabestan, traduction et édition critique), (Paris: Economica, 1988), ISBN 2-7178-1377-2, (excellent current French translation with critical apparatus).

Other Suggested Readings on Chinese Strategic Thinking

Sun Pin - Military Methods, (Ralph D. Sawyer, translation & commentary), (CO: Westview, 1995), ISBN 0-8133-8888-0, (elaboration of *Art of War* by Sun Tzu's grandson. Excellent introduction and footnotes).

Sun Pin – The Art of Warfare, (DC. Lau & Roger T. Ames, translation & commentary), (NY: Ballantine Books, 1996), ISBN 0-345-37991-8, (elaboration of *Art of War* by Sun Tzu's grandson. Excellent introduction and footnotes).

Mastering the Art of War: Zhuge Liang & Liu Ji, (Thomas Cleary, translation & commentary) (Boston: Shambhala, 1988), ISBN 0-87773-513-1, (among the Chinese, Zhuge Liang is as well known at Sun Tzu. See the chapter 'The Art of War and the I Ching: Strategy & Change', pp.10-29).

The Wiles of War: 36 Military Strategies from Ancient China, (Sun Haichen, translation & commentary), (Beijing: Foreign Languages Press, 1993), ISBN 0-8351-2795-8, (exactly what the title says – Strategy = wiles or deception).

Les trente-six strategèmes: traité secret de stratégie chinoise, (traduit et commenté par François Kircher), (Paris: Rivages poche, 1995), ISBN 2-86930-905-8, (excellent commentary. The 36 strategies are based on texts taken from the *I Ching*).

***I Ching* or '*Book of Changes*' is central to classic Chinese thinking**

The I Ching or Book of Changes, (Richard Wilhelm translation – rendered into English by C.F. Baynes, forword by C.G. Jung), (Princeton Univ. Press, 1950 {numerous reprintings}), ISBN 0-691-O9750-X

Wilhelm, Helmut & Richard Wilhelm, *Understanding the I Ching*, (Princeton Univ. Press, 1988), ISBN 0-691-00171-5

NOTES

[1] The views expressed in this paper are those of the author and do not represent officially held views of the US Government, the Department of Defense, the USAF, or the Air War College

[2] Dickson, Gordon R., *Tactics of Mistake*, (NY: Ace, 1981), p.12.

[3] Beaufre, André, from: 'An Introduction to Strategy', excerpted in: George E. Thibault (ed.), *The Art and Practice of Military Strategy*, (DC: National Defense University Press, 1984), pp.204-223.

[4] The literature in English on InfoWar is massive. Permit me to at least list some of my own contributions.

US Information Warfare: Jane's Special Report, (London: Jane's Information Group, 1996).

'Information Warfare: Words Matter', in: Stocker, G. & C. Schöpf (eds.), *InfoWar*, (New York & Vienna: Springer, 1998); pp.51-59.

'InfoWar:Worte zählen', in Stocker, G. & C. Schöpf (eds.), *Information.Macht.Krieg*, (New York & Wien: Springer, 1998); pp 57-66. [German edition of previous citation]

'Information Attack: Information Warfare in 2025', *Air University. 2025 Study: Power and Influence*, (Maxwell AFB, AL: Air University Press, 1996; pp. 91-115. (White Papers; v. Vol.3, Book1).

'Information Warfare', in: Campen, Alan D., D.H. Dearth & R.T. Goodden (eds.) *Cyberwar: Security, Strategy and Conflict in the Information Age*, (Fairfax VA: AFCEA International Press, 1996); pp.175-183.

'Information War - Cyberwar – Netwar', in: Schneider, B.A. & L.E. Grinter (eds.), *Battlefield of the Future: 21st Century Warfare Issues*, (AL: Air University Press, 1995); pp.153-170.

'Information Warfare', *Airpower Journal*, 9:1 (Spring 1995): 30-39.

[5] Joint Pub 3-13.1, *Joint Doctrine for Command and Control Warfare (C2W)*, (7 February 1996), p. I-5.

[6] Kelly, Kevin, *Out of Control: The Rise of Neo-Biological Civilization*, (NY: Addison-Wesley, 1994).

[7] The best discussion of 'serious play' remains: Johan Huizinga, *Homo Ludens: A Study of the Play-Element in Culture*, (MA: Beacon Press, 1986).

[8] The admitted neologism 'contravalent' was first applied to information warfare by Air Vice-Marshall R.A. Mason (RAF, ret'd.).

[9] van Creveld, Martin, *The Transformation of War*, (NY: The Free Press, 1991).

[10] Voegelin, Eric, 'Necessary Moral Bases of Communication in a Democracy', in: Marquette University Press, (ed.), *Problems of Communication in a Pluralistic Society*, (WI: Marquette University Press, 1956), pp.53-68.

[11] Pellegrini, Robert P., *The Links between Science and Philosophy and Military Theory*, MA Thesis, (Maxwell AFB, AL: School of Advanced Airpower Studies, 1995).

[12] See the attached bibliography for an introductory guide to Sun Tzu's *Art of War*.

[13] The *Questions and Replies* is one of the 'Seven Military Classics' and, as a later work that the other six, often serves to restate and amplify previous writers, including Sun Tzu. *The Seven Military Classics of Ancient China*, (Ralph D. Sawyer, translator) (CO: Westview, 1993), p.353.

[14] Most contemporary scholars recognize the centrality of this 'epistemological' difference as the chief hindrance to Western appreciation of Asian thought. The author of this essay has relied on three mutually supporting but quite distinctive discussions of the uniqueness and holistic / monistic aspects of Eastern thought. See the introductory commentaries in:
Sun-Tzu – The Art of Warfare, (Roger Ames, translator)
(NY: Ballantine Books, 1993),
Sun-tzu Art of War, (Ralph D. Sawyer, translation & commentary)
(CO: Westview, 1994), and
Sun Tzu: The Art of War, (Thomas Cleary, translation & commentary),
(Boston: Shambhala Publications, 1988).

[15] See: 'The Art of War and the I Ching: Strategy & Change', *Mastering the Art of War: Zhuge Liang & Liu Ji*, (Thomas Cleary, translation & commentary), (Boston: Shambhala, 1988), ," pp.10-29.

[16] *Sun-tzu Art of War*, (Ralph D. Sawyer, translation & commentary), (CO: Westview, 1994), p.167.

[17] Ibid.

[18] although, in the spirit of 'serious play', consulting a Chinese-language dictionary can be 'insight producing'. The Chinese symbol (fâ) translated here as 'organization' has its root in the concept "to flow like water." It should not be surprising then that Sun Tzu will often refer to organizing a maneuver so that it "flows like water." See the on-line dictionary character-by-character analysis of the *Sun-zi ping fa* at: http://www.zhongwen.com

[19] Warden, John A., 'The Enemy as a System', Airpower *Journal*, (Spring 1995), 9:1, p.40.

[20] The literature on this topic is well known. See especially:
Arquilla, John & David Ronfeldt, (eds.), *In Athena's Camp: Preparing for Conflict in the Information Age*, (CA: RAND, 1997), and:
Khalilzad, Zalmay M. & John P. White, (eds.), *The Changing Role of Information in Warfare*, (CA: RAND, 1999).

[21] *Sun-tzu Art of War*, (Ralph D. Sawyer, translation & commentary), (CO: Westview, 1994), p.168.

[22] See also: Sawyer, Ralph D., *The Tao of Spycraft: Intelligence Theory and Practice in Traditional China*, (CO: Westview, 1998).

[23] See the discussions of these distinctive concepts in Sawyer, Ames and Cleary.

[24] See footnote 158 of 'Notes to the Introduction', of *Sun-tzu Art of War*, (Ralph D. Sawyer, translation & commentary), (CO: Westview, 1994), p.292.

[25] *Questions and Replies* in: *The Seven Military Classics of Ancient China*, (Ralph D. Sawyer, translator) (CO: Westview, 1993), p.351.

[26] *Sun-tzu Art of War*, (Ralph D. Sawyer, translation & commentary), (CO: Westview, 1994), p.187.

MARS CHUCKLES AND ATHENA SIGHS IN FRUSTRATION ©[1]

Richard Szafranski
Toffler Associates®

ABSTRACT

The thesis of this article is that armed forces and their national command authorities have much to learn about effectively integrating information operations into both war and anti-war security operations. Worse, at the present rate of learning the Western democracies may be surrendering intellectual leadership and ultimately operational leadership to those States, hackers, and criminals who more quickly adapt these new tools. That said, I do not intend this to be the Third Wave Information Age equivalent of saber-rattling. Rather, it is a call to action. And prerequisite for action is first to appreciate that change is difficult.

INTRODUCTION

Offensive IW, in brief, uses computer intrusion techniques and other capabilities against an adversary's information-based infrastructures. The Commission [US President's Commission on Critical Infrastructure Protection, PCCIP] is aware of *little* in the way of special equipment required to launch IW attacks on our computer systems; the basic attack tools—computer, modem, telephone, and software—are *essentially the same* as those used by hackers and criminals. And compared to the military forces and weapons that in the past threatened our infrastructures, IW tools are *cheap and readily available*.[2]

YES, CHANGE IS DIFFICULT

Moving from the old and familiar to the unfamiliar new is a difficult process for everyone, and especially difficult for soldiers, sailors, and aviators. There is, as Hart observed, nothing harder than displacing old ideas. Just when soldiers, sailors, and aviators and their institutions think they "get it" about the operational art, some new discovery—usually a technology or an application—intrudes to render significant elements of what they know irrelevant, or at least less relevant. When this occurs, Mars chuckles. Think back in time to think forward.

Imagine how difficult it must have been for militaries to accept and accommodate the seemingly unnatural technologies of gunpowder and cannon. Stabbing, slashing, pounding and piercing the enveloped prey seem to mimic the hunt perfectly, and hunting in packs or platoons is an activity that may be natural to our species. Burning some chemical compound to release its energy in a hardened tube must have smacked of necromancy. New competencies in chemistry, metallurgy, casting, and engineering had to develop in tandem with new organizations and employment schemes. Gunpowder and cannon changed the human hunt.

Gunpowder was but one change that transformed navies. Navies saw steam replace sail and internal combustion engines replace steam, only to have steam return in the form of nuclear power for some warships. Navies witnessed the sub-surface become key to the surface and the aircraft carrier displace the battleship as the principal means of power projection. But navies adjusted.

Envision the angst faced by armies and their cavalries when the ratio of horses to motor vehicles shifted from horses to favor motorized vehicles during World War II. The technology of the internal combustion engine and its terrestrial applications for warfare displaced the horse and rendered the sword ceremonial. And then arrived the flying machine in its many incarnations, finally including a rotary-winged form for air cavalry operations. Hot on the heels of flying machines came missiles, pressing the army's artillery with the same assiduousness that flying machines pressed both the cavalry and the artillery. Armies tried to adjust.

But then came rocketry and nuclear weapons and space. German research into vehicles designed to carry conventional weapons gave us cruise missiles and ballistic missiles. Nuclear weapons gave these missiles punch. Long-range precision weapons, both nuclear and non-nuclear, today guided by their own eyes and the artificial moons of electronic navigation, allow armed forces to stand far off and cast death and destruction on enemies that humans only see through the mediating structure of sensing machines. Armies, navies, and air forces all want the non-nuclear ones and get them and use these long-range precision weapons with a profligacy that would stun an accountant.[3]

These very accurate weapons and the rather repetitive thriller impact videos that accompany the successful hits help delude the public into thinking that warfare ought to be casualty-free or at least casualty-limited. Precision long-range weapons now are the *lingua franca* of warfare. Armies, navies, and air forces squabble about what these mean for warfare, for their separate missions, the differentiation of operations in "their" media, and the right and true role of air forces. Armies, navies, and air forces are trying to bend to these changes, but—witness the debates preceding any significant ground operations—armies know that notions of antiseptic Airpower are supplanting public acceptance of the readiness for mud and blood operations. Willingness to engage in these operations formerly put armies closest to the seat of power everywhere. Even armies appreciate that the real risk to homelands in the developed world today is not other invading armies, but Airpower and fifth column terrorism. Does Airpower now become the dominant force?

No. The real risk to the craft of flyers is neither long-range precision weaponry nor unmanned aerial vehicles, but a new discovery. The new discovery, pivoting on potent "new intangibles," does not eliminate the old "things" of fighting past or fighting present, but they now allow it to be augmented, complemented, or in some cases replaced by new things. The Tofflers write

> None of this is to suggest that tangible, material resources and technologies are going to vanish in a puff of dematerialization. Obviously, things matter, and weapons matter more than most things. Software still needs hardware. Soldiers cannot eat data. Nonetheless, the fun-

> damental relations between the tangible and what might be called the "new intangibles" are increasingly crucial to military effectiveness, in both waging war and trying to prevent it.[4]

Information warfare is the great new discovery true acolytes of Mars need to welcome. Mars, after all, gave us computing machines, and computing machines gave us awareness that things in the external world could be reduced to combinations of zeroes and ones. This understanding launched the information age. These combinations could be transmitted electronically as data and recombined upon receipt to form the basis of information. According to the seminal work on control warfare by Arquilla and Ronfeldt, "information" is more than the content or meaning of a message. Rather, information is "any difference that makes a difference."[5] Awareness that almost everything[6] of military significance in the external world could be reduced similarly launched the age of information warfare.

Information warfare is troublesome for the established institutions to "get," because key facets of it are indirect and subtle, not direct and brutish. Information warfare is a form of conflict that attacks information systems—carbon and silicon—as a *means* to attack adversary knowledge or beliefs. Information warfare can be prosecuted as a component of a larger and more comprehensive set of hostile activities—what Arquilla and Ronfeldt call a netwar or cyberwar—or it can be undertaken as the sole form of hostile activity. Information warfare can occur *in* war and it can occur *outside of* war.

Carefully read what US Air Force (USAF) doctrine advances. According to the USAF information warfare (IW) is

> …information operations conducted to defend one's own information and information systems or attacking and affecting an adversary's in-formation and information systems. The defensive aspect, *defensive counterinformation, much like strategic air defense,* is always operative. *Conversely,* the offensive aspect, *offensive counterinformation,* is **primarily** conducted during times of crisis or conflict. Information warfare involves such diverse activities as psychological operations, military deception, electronic warfare, both physical and information ("cyber") attack, and a variety of defensive activities and programs. It is important to stress that *information warfare* is a construct that operates across the spectrum, from peace to war, to allow the effective execution of Air Force responsibilities.[7]

> IW is information operations conducted to defend the Air Force's own information and information systems or conducted to attack and affect an adversary's information and information systems. This warfare is **primarily** conducted during times of crisis or conflict. However, the defensive component, much like air defense, is conducted across the spectrum from peace to war.[8]

This relatively uncomplicated conception, new nonetheless, poorly masks a new admission—repetition reveals it—that this new kind of *warfare* and warlike operation is not restricted to *wartime*. Offensive information warfare, "offensive counter-information" as the USAF calls it, is "primarily," but not necessarily *exclusively* conducted "during times of crisis or conflict."[9] This kind of warfare *is* new, and the new always has been a challenge and vexation to militaries.[10]

And all the while a cacophony of Mars's priests—perhaps aggrieved by accusations (or revelations) that many of their stories slowly are seen as little more than informed speculations, albeit interesting ones—mock Athena. Some cantankerously coo that there is nothing new under the sun and that information warfare is a chimera.[11] Athena sighs in frustration. Both she and Mars know that Mars was the old god of war, and by now even Mars should know that Athena is the new deity of warfare.[12] Change *is* difficult.

BUT DIFFICULT DOES NOT MEAN EITHER UNNECESSARY OR IMPOSSIBLE

It Is Necessary

While there is no need for panic, there is a need to consider the facts. A powerful motivation for change ought to be the awareness that, properly done, information warfare can seriously perturb just by trying to level the playing field. Any serious perturbation in information systems can reduce the effectiveness of operations. Consider the Y2K issue.[13] As US Senator Robert Bennett, discussing the Y2K problem, put it, "The antidote to panic is always accurate information, but some of the accurate information can be pretty scary."[14] Accurate information about hostile information operations can be pretty scary too.

At the lower end of the spectrum of aggravation, small groups and States can use information warfare to disrupt a larger State's efficient functioning. At the higher end, small groups and States can seriously and adversely affect larger States.[15] Limited and tactical uses of information warfare aside, States and groups may now or soon possess "strategic information warfare" or "SIW" capabilities. Strategic capabilities are those that can "seriously harm"[16] another's security or security interests.[17] If offensive counter-information warfare can be done *outside* of war, then strategic information warfare also can be done *without* a declaration of war.[18] And people can do it without the normal military folderol of donning a uniform, wearing a silly hat, being physically fit, leaving their homes, or saluting anyone. All they need is a motive to match the readily available means. The motives could be as simple as curiosity or greed and curiosity and greed are not scarce on our planet.

Thus, we should prepare for such aggravations now, although the Defense Science Board estimated in November 1996 that we have some time: "limited strategic information warfare capabilities" used against us may still be seven to ten years away.[19] Is this so? A study by RAND noted somewhat inconclusively that we don't know.

> A macro assessment of the current state of first-generation SIW in terms of absolute and relative offensive and defensive SIW capabilities of the United States and other nations (or other parties) would be difficult to do, even at a classified level. The current dynamic character of the Information Revolution and the embryonic character of SIW as a potential political-military instrument both argue for caution in making such an assessment, classified or unclassified, at present and for the foreseeable future.[20]

Without putting too fine a point on the "future" almost all[21] agree that

> In the future, the possibility exists that adversaries might exploit the tools and techniques of the Information Revolution to hold at risk (not for destruction, but for large-scale or massive disruption) key national strategic assets such as elements of various key national infrastructure sectors, such as energy, telecommunications, transportation, and finance.[22]

It Is Possible

It would be foolhardy or irresponsible to dismiss the risks of such attacks as impossible. If this is so, we should consider the threat and the risks in order to envision the forms our preparation and response ought to take. RAND analysts saw "a two-pronged threat to U.S. security."[23]

1. **A threat to U.S. national economic security.** Key national infrastructure targets could be at risk to such massive disruption that a successful attack on one or more infrastructures could produce a strategically significant result, including public loss of confidence in the delivery of services from those infrastructures.

2. **A threat against the U.S. national military strategy.** The possibility exists that a regional adversary might use SIW threats or attacks to deter or disrupt U.S. power projection plans in a regional crisis. Targets of concern include infrastructures in the United States vital to overseas force deployment, and comparable targets in allied countries. A key ally or coalition member under such an attack might refuse to join a coalition--or worse, quit a coalition in the middle of a war.[24]

The Economic Attack Test Case

Economies increasingly are dependent on the information infrastructure.[25] Anything that deliberately and adversely affects the capabilities of that infrastructure can be said to constitute an attack. If there are destructive or disruptive information tools intending to affect financial transactions, banking,[26] on-line investment services, billing, electrical power generation or distribution, telephone or data distribution,[27] emergency services, and so forth, then the best time for an attacker to operationally test these is in the wake of Y2K manifestations.[28] If the US, or another larger State, is the intended target of *future* strategic information warfare aimed at disrupting or even crippling commerce and services, then a smaller State, or municipalities within States, ought to be seen as the likely test targets for these Y2K experimental attacks.[29] Cities in Eastern European, Middle Eastern, Southeast Asian, and South American countries might be among those that an earnest adversary considers.[30] Target analysis would reveal particular entities within the candidate State(s) that are especially vulnerable—probably a bank or a telecommunications company.[31] The cyber-attacker would reap at least one tremendous advantage: data.

An attacker would learn much about how municipalities and States respond in the wake of unexplained failures in automated and interdependent critical (often defined as telecommunications, energy, banking and finance, transportation, water systems, and emergency services)

infrastructures. How does a State try to protect its physical and cyber-based systems essential to the operations of its economy? How do attacks on a small State affect the global internetted economy? What separations of power and what seams are observed to exist between the armed forces and the civil authorities? Between Government and commercial actors? What seemed to work and what did not work well? What systems or infrastructure elements were stressed most? How long did recovery take and what were the impediments to rapid recovery? Did trust erode? What small inputs produced the largest outputs? What actions went undetected and what, besides the outcome, was easily detected?[32]

As compounded and cascading failures occurred, human error inevitably would follow. Unrelated equipment failures, weather and other natural causes may provide the opportunity for gathering unexpected data on excursions. An obvious problem for a future attacker is in relating cause and effect. A live test would reveal far more than a simulation or a model would. A live test rendered opaque by Y2K would have obvious advantages to attackers.[33] Hence, if a future adversary intends to develop the capability to produce a "strategically significant result" on a large State's economy, we should be alert for real-world tests conducted in cities in out-of-the way places.[34]

Anti-Access

We still think of power projection in terms of physical means—mass—deployed, and we still think of anti-access as belligerent means aimed at denying the ability to move mass. "Access" may be thought of as the ability to approach a physical place or introduce mass there, but physical access is only *one* form of access. There are electronic "places." There is electronic access to markets. There is access to reality and truth. In the Third Wave Information Age power shifts.[35] Knowledge becomes more potent, using it accumulates wealth, and violence is transformed by taking advantage of it. "Anti-access" in the next century will take many forms: the inability to introduce mass, the inability to sustain mass, the inability to participate in a market, and the inability to know the truth.[36] But some of these will not present themselves as the "anti-access" we expect.

States levy tariffs to deny access to another State's cheaper goods. Trade wars can be very testy, but few think of them as warfare. In the next century they very well may be. Already the Indian Commerce Ministry has stated that "the lack of e- commerce capabilities in the country could become a 'non- tariff trade barrier' against Indian exports" in a better-wired world.[37] Non-belligerent means to deny access already abound and information warfare will make them all the more subtle and elegant. Information warfare aims at the knowledge and belief systems of an adversary and takes advantage of an adversary's weaknesses. We know, for example, that ports and other embarkation points are critical to moving mass. We also know that that the larger developed States are becoming more, rather than less "green." A simple hazardous waste spill in the right place and at the right time likely would not be construed as a chemical attack, but it could hamper a deployment. Is promoting good stewardship of the environment an "information operation"? It could be,[38] as could be promoting ethnic strife, inadequate funding for public education, or "brain drain." These might be longer-term—or shall we say distinctly non-Western—strategies and one would have to take a

long view of competition to engage in them. There are more quickly maturing anti-access strategies also.

Imagine the economic impact of being denied access to a market (or a commodity) outright? Some businesses try to command a market, preserve the dominant share, or capture critical suppliers, all aimed at denying access to, or raising the cost of entry for competitors. In the wake of deregulation, various airlines, telephone companies, and utilities have been accused of executing anti-access or anti-competition strategies. In some cases, courts and regulatory agencies have found such accusations true. Individuals and firms buy functionality or prime real estate to deny others access to it. We should not be surprised that individuals (or the States that sponsor them), criminal syndicates (or the States that sponsor them), or businesses (or the States that sponsor them) aim for real estate or other physical asset ownership to deny access to others. What surprises some is that law and the possession of legitimate ownership, or title, or deed can prevent access. Yes, some big powerful States preserve the delusion that they can fight their way in, seize needed assets or property, or otherwise control access. But the non-belligerent global repertoire of anti-access tools continues to grow and many have security implications.

Worse than not having access is losing it when dependent upon it. What would prevent a cunning future adversary from allowing access only to then use it to advantage? For example, by enlisting a larger State in engineering its own defeat by allowing it to load up International Airport X with military aircraft only to make them easier to destroy or embargo? Or purchasing or owning all the water rights or water in a region? But access is not merely physical: imagine being a multi-national corporation owning all the communications channels serving an area with a multi-national board of directors. Who is to blame if the company refuses to lease a channel? What can be done?

But the highest and best use of anti-access strategies is to deny access to truth.[39] "Denial and deception" viewed in this light are sublime anti-access means: they impede access to the truth. Whether employing active or passive means to "protect their privacy," individuals, groups and States—unless some law or treaty provision is alleged to have been violated—can both impede access to knowledge and mask the meaning of things and actions observed. These are not necessarily belligerent acts.[40]

But how would one test anti-access strategies aimed at deterring or disrupting power projection capabilities in a regional crisis? Information operations, including terror attacks, certainly could be prosecuted easily. Infrastructures vital to force movement are complex logistics nodes. Information warriors can affect the silicon and carbon components in a number of ways: jumble manifests, lock or prevent unlocking electronic locks, terminate or disrupt telephone service, release a series of hitherto unseen computer viruses on the Internet, affix a worm or virus to the popular "anti-virus" software programs that allow real-time updates of virus definitions,[41] jam AM radio nets or cell phones,[42] buyout suppliers, unnecessarily dispatch emergency equipment, shut down child care centers, affect nuclear power plant control systems, have an apparent in-flight medical emergency, start rumors that *Ebola* or *E-coli* is in the water, dump sewage,[43] de-synchronize traffic signals on key arteries, or any number of other disruptive and destructive things.[44]

One needn't test these as an integrated series in advance. Testing each separately would give higher confidence[45] that they would be effective in disrupting operations when employed in concert. Thus the PCCIP recognized that

> …we need the analytic tools to examine information about intrusions, crime, and vulnerabilities and *determine what is actually going on in the nation's infrastructures*. Deciding whether a set of cyber and physical events is coincidence, criminal activity, or a coordinated attack is not a trivial problem. In fact, without a central information repository and analytic capability, it is virtually impossible to make such assessments until after the fact. This is of increasing concern as infrastructure operations become more reliant on information and communications—the very sector about which it is most difficult to make assessments.[46]

Contemplating the list below, one notes that few of the things listed have not occurred in the natural course of events. It is highly unlikely that a power projection or deployment system would perform effectively when faced with a handful of these simultaneously.

- **Jumble manifests**
- **Lock or prevent unlocking electronic locks**
- **Terminate or disrupt telephone service**
- **Jam AM radio nets or cell phones**
- **Buy out suppliers**
- **Unnecessarily dispatch emergency equipment**
- **Shut down the child care center**
- **Start rumors that *Ebola* or *E-Coli* is in the water**
- **Insert computer viruses into telephone-switching stations**
- **Activate logic bombs**
- **Stop the sewage treatment plant from functioning**
- **Cause traffic jams by misrouting public vehicles**
- **Dispatch utility repair crews to rural areas**
- **Jam the TV broadcasts**
- **Crank and prank calls to families**
- **Disable mobile phones**
- **Have several bomb scares**
- **Disrupt the electrical power supply**

Again, an excellent opportunity to test several of these, alone or in concert, will be occur the Y2K confusion. Again, the target likely will be a surrogate for the actual target and proxies may perform the attacks. And yet again, I am not suggesting that anyone do these, merely observing that someone will. What's to be done?

TAKING ACTION

Without awakening all the sleeping dragons of Cold War deterrence theories accept that we now possess doctrine on the use of hostile means with hostile intent before the familiar forms

of hostility erupt. The hostility is the employment of means aimed at subduing the enemy will. The adversary is subdued when the adversary is seen to behave in ways that are coincident with the ways in which we—the aggressor or the defender—intend for the adversary to behave.[47] And this behavior modification can occur before the traditional—read "old"—conceptions of belligerent operations are undertaken. This is not so much "warfare" as it is "peacefare," because warfare is only one side of the challenge of providing security in the 21st Century. Alvin and Heidi Toffler suggest that "…a revolution in warfare requires a revolution in peacefare as well." "Peacefare" must include and embrace active "anti-war" because the other side of warfare is "peacefare" just as the other side of war is "anti-war."[48] Competence in peacefare and anti-war will differentiate those who master the security challenges of the first part of the 21st Century. The Tofflers observe that "Knowledge is what the anti-wars of tomorrow will be about." Thus, the task is to "…accelerate the collection, organization, and generation of new knowledge, channeling it into the pursuit of peace."[49]

An important element of the new knowledge we need is knowledge of how to employ information warfare, or offensive counter-information, to subdue emergent hostile will. Toward that end, let us consider a handful of principles that should guide democracies in the pursuit and eventual employment of this new knowledge. Some are controversial and, I am sure, will provoke debate. Nonetheless, my aim is to generate new knowledge in the pursuit of effective anti-war capabilities to preserve the peace. The principles advocated relate to secrecy, modeling, integration, and agreement on triggering events, preemption, and escalation.

Secrecy

Difficult as it is in democracies to develop new weapons and new capabilities in secret, any research into and experimentation in offensive counter-information capabilities must be highly restricted and heavily compartmented. Certain national capabilities ought not be shared with allies for at least four reasons. First, alliances in the next few decades might be expedient, transient, and highly contingent. One's allies in one moment might well stand on the "wrong" side of an issue the next. The capacity to surprise can be lost if one's former friend is well aware of one's repertoire of capabilities. Second, new knowledge of any kind is valuable intellectual property. To pay the bill for developing new intellectual property and then surrender it is not traditionally[50] good business, or at least not traditionally good national security business.[51] For example, to develop a new cipher or code to protect information, or to develop a new code-breaking capability, and then give it up would be foolhardy. Third, there is a correlation between any new information capability and the economic advantages it can provide to its owners. That is, information weapons, unlike nuclear weapons, may have component elements with high utility for spin-off and spin-on products and for activities unrelated to warfare.[52] Fourth, it would be foolhardy to presume that *other* States and groups are not developing the capacity for knowledge warfare in secret.

On the other hand, sharing certain vulnerability and offensive exploitation techniques could have considerable reward both in the short term and over the long term. First, better-funded players in this game would be foolish not to cooperate in their quest to cover the broad array of attacks that easily could be developed by smaller players ranging wide in the spaces in

which the larger players play. Separate large players attempting to protect themselves everywhere in these spaces would require replication of effort and the dilution of large (but still finite) resources to push power from large organizations down to smaller organizations more focused on mastery of cyber-defense or cyber-aggression. Conversely, recognizing that both defenses *and* offenses have value in this space, information warfare creates opportunity for smaller organizations to generate revenue through cyber-arms research and trade. Third, introduction of threats or offenses into an environment often can increase stability and security by stimulating faster development and more thorough deployment of defensive countermeasures by vendors and customers motivated to immunize their systems. Some might label such a tactic as a "preemptive self-attack."[53] Last, and perhaps most importantly, the best argument for sharing knowledge in this space would be that knowledge in this arena is amplified by the synergies of the network effect, a phenomenon that has helped create the "knowledge explosion" driven by communications technology. Although such exchange may require developing requisite trustable coalitions of parties seeking similar objectives over the long term, the best strategy might be to balance the competitive advantage of secrecy against the benefits of more open exchange.[54]

Anticipating criticisms that the consequences of such secrecy could be an information "arms race," the fracturing of alliances, or random and destabilizing information attacks, I ask that you consider the world as it is already. Competition in computers, software applications, and telecommunications is already rampant on both sides of and across the Atlantic. Each of our companies and nations races to get ahead of the others for the wealth of its stakeholders. We're already there. Admittedly, information arms are a new kind of arms, but I am hard put to distinguish between the anti-virus software of today and the armor of archaic times. To test anti-virus software or to test an agent that inoculates against anthrax, one must have the viruses required. Said another way, to engage in effective *defensive* counter-information one must have a fairly good understanding of the capabilities required for effective *offensive* counter-information.

Because of the world that is, and emotional flag-waving aside, alliances among States are little different than partnerships in business. States have always retained the right and obligation to abrogate even the most solemn treaties in supreme self-interest. The termination clauses in business partnerships preserve similar prerogatives. It is naïve to think that alliances are based on anything except a State's awareness of what constitute its best interests at any given time. States weaker than the United States will, of course, protest that the pursuit of secret and unshared US national capabilities -including information warfare capabilities- is imperialism or isolationism, but the US must get used to such complaints.

Will secrecy expose all of us to an increase in random and destabilizing information attacks? One must ask the hackers and crackers, beholden to no State. Again, perhaps we are there already.[55] Antidotes and retaliatory tools developed in secret by States actually might increase stability and deter random attacks. Hackers that feel some of the weight of a State's legal power or a State's offensive counter-information capability might think twice before provoking any of us. The Net and the Web are the Commons, and all States should feel free to act against anyone misbehaving on the Commons. States will be moderate in their behavior, I believe, if for no other reason than reluctance to expose the existence of information

weapons in their arsenals. Secrecy is the foundation for accelerating the collection, organization, and generation of this new knowledge. And secrecy is key to channeling this new knowledge into the pursuit of anti-war. But secrecy is not enough.

Modeling

Modeling will be an essential step in this process [development of a science-based approach to the challenges of information assurance]. Component and system behavior must be modeled. Complex systems must be modeled. Stochastic systems must be modeled. Human behavior must be modeled. System fault must be modeled. Attack events must be modeled. All of these models, and more, must be able to work together to model entire information systems and quantify the interdependencies the separate models could not address. The models developed should draw upon past work and should span research, including dynamic modeling and agent-based systems.[56]

Today we understand less than we will need to understand to defend ourselves against attack and to enable information warfare and "cyber-warfare" to make significant contributions to war and warfare, anti-war and peacefare. Absent data and models, all the other answers to the questions information warfare poses merely are speculations.

Integration

Once we can model information operations we must find effective ways to integrate information warfare capabilities into diplomacy, anti-war, and warfare. Someone once observed that diplomacy is the art of "saying 'nice doggie' while looking for a big stick." Information is key to knowing which dog is growling, why, what frightens or placates or distracts the dog, what forms the big sticks might take, and where and when to best apply the stick. Applying the correct stick to the correct dog is a more difficult matter, but in order to do any of these, an elusive "someone" must be responsible for integration.

It may be that overall integration is best done by integrating substrates of differentiated capability. For example, give the responsibility for affecting the media to one group[57] and command and control computer networks to another. Integration closes whatever lanes exist between terrestrial forces (armies and navies), space forces, and air forces.[58] Integration also closes the lanes that exist between foreign affairs, defence, trade, and so forth. Ultimately, integration and authority must reside at the seat of power: the head of the State and the commander-in-chief of all the State's armed forces. The more comprehensive and robust the information warfare capabilities of a State, the more urgent the need for integration and centralized execution. Likelier than not, the paradigm of centralized control and decentralized execution will transform into centralized authority for execution and decentralized control of means.[59]

Do such integrating agencies exist today? I do not know.[60] Recent squabbles do not provide overwhelming public evidence of effective information warfare applications. Genocidal broadcasts seemed to have been tolerated in Rwanda and Yugoslavia and, except for conventional strikes against Serbian troop and paramilitary control capabilities, one petty tyrant after

another proclaims hate and pollutes the airways with hate propaganda.[61] Likewise, embargoes remain physical and porous and not electronic and impermeable.

The aim of integrating information operations capabilities is to make anti-war possible. The militaries of the democracies sit in quiet repose waiting for war, bemoaning their lack of resources and training for war. They tell themselves that they exist to "fight and win" their Country's wars. Yet, it is warfare by the anachronistic military definition they await. That their countries are awash in drugs or pressed by criminal syndicates do not rise to the level of an emergency for the armed forces. Or, if these developments do rise to the level of an emergency, they are emergencies for some entity other than the armed forces. The same is true for governments in the democracies on the international scene. A tin pot dictator can engage in the most heinous of crimes by framing the misbehavior as occurring incident to a civil war. Anti-war, actively opposing the emergence of warfare, requires greater insight and sensitivity to the precursor events that erupt in violence. Integration of information operations, and the capacity to conduct secret operations, would allow governments to act swiftly and invisibly at the onset of any renegade behavior. Those "rice bowls" or stovepipes that prevent effective information operations will at some point have to be integrated to allow information operations, both secret and covert, in the coming decades. One thing need not be secret: the categories of misbehavior that invite retaliation.

Agreement on Triggering Events

States recognize some behaviors as misbehavior already. Yet, except for invading a neighboring State, the old Second Wave parameter for misbehavior, States today are largely permissive of one another's bad behavior. Country X can build its export economy on growing opium or on abusive uses of child labor. Country Y can be the world's leading exporter of marijuana. Country Z can imprison all the practitioners of Faith W or V Ethnic Group. And Country T can train all the terrorists required for Countries X, Y, and Z. Our rightful respect for The Law compels us to negotiate with terrorists, war criminals, and democides until the indictments are framed, the trials consummated, and the sentences adjudged. Old murderers die in their beds or idle away at holiday resorts. Few dare speak for those denied speech or robbed of life. The disincentives for misbehavior are not nearly so potent as the apparent incentives.

One can see and quickly assent that our own standards for morality and legality cannot be made universal by violent warfare waged outside our own territories. I cannot, however, see that early information warfare might not provide a good antidote to some of the forms of bad behavior that would not easily rise to the level of a declaration of "War." In other words, there are triggering events that all or most States could recognize as undesirable or "bad" conditions. These are already well recognized by the articles that underpin the *raison d'être* for a United Nations. Groups of states often assert that individual nations deserve reprimand or constraint without desiring to use a high level of violence against them. Moreover, like embargoes and blockades, information operations can provide powerfully effective means of non-lethal constraint. What apparently we lack are the capacity and courage to use information operations in situations where misbehavior ought to be punished. Secrecy will allow the

development of capability and integration will give capacity, but courage is a matter of each State's assessment of risks and consequences. Strong States are more risk-tolerant than weaker ones. Why shouldn't strong States be prepared to preempt with information operations?

Preemption

Preemption is as dirty a word as prevention is a gentle one. The polygraph is not so much designed to catch spies as it is to prevent or preempt deceptive behavior. Even so, it is a primitive tool that requires physical contact with the subject. As computational capability and brain research combine, we may be able to identify miscreants before their misdeeds are serious. David Ronfeldt, the brilliant RAND researcher, suggests that the type of 'netwar' democracies will face in the future—"a new mode of low-intensity, societal-level conflict"—is particularly attractive to a leader with discernible (but unhealthy) psychological traits[62] "who aims to operate slowly and covertly to weaken his chosen enemy." Identifying such characters in advance would be useful. Will our respect for the law allow them to hatch their schemes without our intervention? Probably. But it is equally likely that peace on the planet will spawn homeopathic or antidotal warfare. We may very well have to learn to fight early and preemptively to prevent the spread of fighting.

We should expect that the larger States may engage their adversaries—State and non-state groups—much earlier, more covertly, and more often than in the past. While physical engagements draw attention and pose the risk of loss of life, some information warfare operations do not carry the same risks. Thus, we can expect that information warfare capabilities created in secret and tightly integrated with both non-traditional, non-military attack and interference capabilities and more traditional combatant capabilities will be used as soon as a triggering event occurs.

The attacking force will seek no one's permission except the head of State, friends and allies will not be notified, and responsibility will not be accepted. Unless the average civilian can possess Nation State like defenses, this will necessitate a different approach to civil-military relations than most nations take today. Such necessity would change the relationship between the combatant and the non-combatant, between the military and the civil authority, and, of course, we would call our States "democracies" still.[63]

For these reasons and many others, we should expect new concepts of information operations. Consider what's plausible. In the future the State might require Net users to inoculate their systems against disruptive viruses. Civilian contractors to the Government in the future may have to demonstrate rigorous defensive counter-information capabilities, have a reliable and screened (read "investigated and polygraphed") workforce, and allow the Government access to all their information handling systems. To ensure both compliance and readiness, the Government periodically might unleash viruses on its instrumentalities, its contractors, and almost inescapably, however unintentionally, on us. Preemption may become the norm and only the side with superior analytical capacity will be able to sort out the "who shot John" of an engagement. There is no weapon humankind ever created that has not been employed. Do we

believe that no weapons are emerging from doctrine and from all this talk we hear about information warfare? Would we go so far as to seek and employ whatever is the information analog of the much heralded (and never seen) ultimate weapon?

Escalation

Escalation is as grim a word as preemption is a dirty one. To escalate one must assess that the consequences of getting meaner are less than the consequences of failing to respond to a provocation. One must also have a clear sense of what State or group is the adversary. The Tofflers wonder

> But what if some adversary--State or non-State--employed intangible means to damage or destroy that city's computer networks, including those needed by its police, airport authorities, electrical systems, banks, and the like? Even assuming the source of the attack could be identified and verified, would the situation call for a military response? Whose responsibility would it be to retaliate and how? And what if, at the same time, riots were provoked in the city by televised scenes broadcast from pirate transmitters in Mexico or Mexican airspace, showing false but convincingly gruesome police or military brutality against Latinos in L.A.? If someone were engaging in information warfare against the United States from both inside and outside the United States, would retaliation be the responsibility of the FBI--many of whose computers and systems are outworn relics--or would some of the responsibility fall to the military?[64]

There are no easy answers to these questions. We know that the target sets of information warfare are both carbon and silicon. To subdue increasingly hostile or non-cooperative will, information warfare attacks the mind, that complex of protein and synapses and nerve bundles and electrochemical functions that host the will and determine human behavior. We can envision that the weapons of next generation information warfare could include tools designed to enable entering and affecting the brain: sounds, smells, images, tastes, and tactile sensation. They might include drugs. They might include pheromones. If this is so, what level of attack is just and proportionate and what is unwarranted, disproportionate or unjust? Is any level of response just and proportionate without clearly knowing the attacking State or group?

Perhaps "it depends" appertains?[65] I earlier said I did not wish to awaken the sleeping dragons of Cold War deterrence theories, but it appears this may be unavoidable. Information weapons are new, they blur the distinction between combatants and non-combatants, and the only analogs we have are from the heyday of nuclear weapons. Can we ask the same kinds of questions asked about nuclear force? Would States aim to deter information warfare? How? In the same way nuclear weapons use was deterred: by having enough capability to wipe out millions of people and large potions of the planet?[66] Or should we build our information forces for flexible or selective response? Would it be wise to have some "limited" information warfare response options, but hold "unlimited" ones in reserve? Would States take a counter-force approach, limiting offensive operations to retaliation against the adversary's information systems? Or would attacks take a counter-value perspective and attack the minds of the adversary more directly? Would States opt for "mutual assured information destruction"? Would execution authority reside with the head of State, or would that person delegate

the authority for some attacks against adversary epistemology to military commanders or even to the commercial sector? Would we be prepared for protracted information warfare?

We do not know as much as we need to know for "knowledge warfare." What does precision mean as it applies to information warfare attacks? Are there precision-guided messages (PGM) that could be aimed at single minds? Does the notion of circular error probable become the idea of calculated error probability (CEP) through the statistical technique of Markhov-chaining in information warfare?[67] What are the canons of epistemological damage expectancy or probability of damage? What is information "collateral damage" and how would it be controlled? What is the information equivalent of fallout and what would a fallout shelter look like? Is there any civil defense against strategic level information warfare? What science, technology, or arcane art would provide the machine necessary to assure us that truth or validity had not been corrupted? Is there a truth-dosimeter awaiting discovery? Could attacks against some areas or categories of targets be withheld in a globally-internetted infosphere? What is information warfare termination and how would it be managed and by whom?

One can continue questioning. In the wake of massive information warfare attacks would some earnest scientists warn of an information winter, a global epistemological condition wherein "truth" is largely destroyed?[68] Would some argue for an "information weapons freeze" or "information weapon-free" zones? Would the bishops of one faith group assert that information warfare was only moral if it existed to deter?[69] Would another faith group issue a document entitled In Defense of Truth?[70] These and many other questions come to mind as the future possibility of strategic level information warfare is contemplated. Each is essential to making decisions on development, deterrence, employment, escalation, termination, and recovery from serious information warfare.

But if information warfare is not serious, how do we explain entities in the US like the Army's Land Information Warfare Activity, the Air Force's Information Warfare Center, the Naval Information Warfare Activity and Fleet Information Warfare Center, and their analogs abroad? How do we explain the existence of doctrine?

CONCLUSION

Information warfare represents the use of knowledge to confound knowledge and hamper effective action. The technologies are here, but the techniques await tests and trials. I imagine we will see some of these tests and trials during the period of confusion that will surround the Y2K manifestations. I imagine we will see more at the 2000 Olympics in Sydney, Australia. To protect ourselves and our information systems we must make *huge* strides in modeling, in integration, in securing agreement on triggering events, in understanding preemption, and in understanding escalation. Much or most of this must occur in secret. What will be highly visible, however, is the degree to which we are successful. Knowledge, as the Tofflers said, is what the wars and anti-wars of tomorrow will be about. Mars chuckles at these changes and Athena sighs that we have so far to go. To this point one must wonder whether or not we will succeed.

NOTES

[1] The views expressed are those of the author.

[2] *The President's Commission on Critical Infrastructure Protection*, October 1998, p. 30. Emphasis added.

[3] And will stun their taxpaying constituents, if they knew the real value of some of the targets both as tangible assets and as object residing on a hierarchy of military significance.

[4] Alvin and Heidi Toffler, 'Foreword: The New Intangibles', *In Athena's Camp: Preparing for Conflict in the Information Age* (Santa Monica CA: RAND MR-880-OSD, 1997), p. *xiv*.

[5] John Arquilla and David Ronfeldt, 'Cyberwar is Coming!'*Comparative Strategy* 2 (April-June 1993), pp 141-65.

[6] But not the internal world. There are some things of military significance—intentions and hostile will, for example—that await work undone in chemistry and biochemistry before they can be decomposed into the electrochemical impulses that can be reduced to zeroes and ones. That day will come. See Robert L. Solso, *Mind and Brain Sciences in the 21st Century* (Cambridge MA: The MIT Press, 1997), John Maddox, *What Remains to be Discovered: Mapping the Secrets of the Universe, the Origins of Life, and the Future of the Human Race* (London: The Free Press, 1998), and Steve Connor, "Science finds key to beating fear," *The Times Newspapers Limited*, February 22 1998.

[7] United States Air Force, 'Foreword', *Information Operations*, Air Force Doctrine Document 2–5, 5 August 1998, p. ii. Emphasis added.

[8] Air Force Doctrine Document 2–5, p. 2. Emphasis added.

[9] We must appreciate that careful word choices have been made before doctrine is approved for publication. The choice of the word 'primarily' appears significant to me.

[10] Especially in the alliance context. See Maria Seminerio, 'Infowarfare' part of NATO arsenal?" *Ziff Wire*, March 26, 1999.

[11] R. L. DiNardo and Daniel J. Hughes, 'Some Cautionary Thoughts on Information Warfare', *Airpower Journal*, Vol. IX, No. 4, (Winter 1995), pp. 69-79. Few appreciate the root of the word 'history'.

[12] The outgoing chief of staff of the US Army asserts that the keys to future warfare are 'knowledge and speed'

[13] Andrew Hay, 'Top Y2K problem: Public panic', Reuters, June 22, 1999, URL: http://www.zdnet.com/zdnn/stories/news/0,4586,2280134,00.html.

[14] Jim Abrams, 'Spreading the Y2K word without spreading panic', http://www.nandotimes.com, June 8, 1999.

[15] See *The President's Commission on Critical Infrastructure Protection*, October 1998. On page 30 the authors observe, "Today, however, malefactors are no longer necessarily nation-states, and expensive weapons of war are joined by means that are easier to acquire, harder to detect, and have legitimate peacetime applications. The tools designed to access, manipulate, and manage the information or communications components that control critical infrastructures can also be used to do harm. They are inexpensive, readily available, and easy to use." As to who these "malefactors" might be the authors note on page A-4 that "A broad array of adversaries, including a sizable number of foreign governments, are currently capable of conducting cyber attacks." One must presume—and this is a speculation—that these foreign governments include those of most of the NATO nations, non-NATO Eastern European countries, Russia, Australia, Japan, China, India, Pakistan, some countries in Oceania and South America, South Africa, and others.

[16] 'Executive Summary', *Strategic Information Warfare Rising* (MR-964-OSD), p. 9.

[17] A serious disruption to the Internet, for example, would seriously and increasingly harm commerce in the US. Hackers L0pht, Mudge, Brian Oblivion, Space Rogue, Kingpin, Weld Pond, John Tan, and Stefan Von Neumann testified to a committee of the US Senate that they believed they could (or can), in the words of Space Rogue, "wreck havoc in the country [USA]." See James W. Brosnan, "Hackers testify they can crash Internet service in a half-hour," May 20, 1998, www.washtimes.com, "Stay Out! If you wanna hack here, you've got to be a member," 24 Hours in Cyberspace Inc., http://www.cyber24.com/htm2/6_204.htm, and L0pht's Web site at http://www.l0pht.com.

[18] Adam Hebert, 'Air Force Official Calls Reduced Cycle Times Key To Info Superiority', *Inside The Air Force*, June 21, 1999. According to the article, "Donahue [Lt. Gen. William Donahue, US Air Force director of communications and information] called Allied Force 'the coming of age of cyber warfare,' because of the attempts by Serbian computer operatives to attack U.S. information systems. 'Fortunately, they were about as effective at that as they were at air defense,' he joked."

[19] Defense Science Board, *Task Force on Information Warfare-Defense*, November 1996, Duane P. Andrews, Chairman, Section 2.2. Exhibit 2-6 assesses a major strategic disruption as "Low" by the year 2005.

[20] *Ibid.*

[21] Some disagree, asserting that natural occurrences, manifestations of the Y2K problem, and the slow erosion of our civil liberties are more grave dangers. See *Critical Infrastructure Protection and the Endangerment of Civil Liberties: An Assessment of the President's Commission on Critical Infrastructure Protection (PCCIP)*, (Washington, DC: Electronic Privacy Information Center, 1998) page 2:

> The most recent dangers to civil liberties comes [*sic*] from the new-found threat to our nation's infrastructure. An elaborate report identified a whole series of attacks that terrorists could wage against our communication lines, power grids, and transportation networks. Not surprisingly, perhaps, the report recommended a dramatic expansion of

government authority, new funding to combat the threat, and greater secrecy to conceal potential vulnerabilities as well as the work of the government agencies now tasked with defending us.

But there is another, perhaps more disturbing aspect of the PCCIP report. Almost every solution proposed by the commission represents some new expansion of government authority and some new encroachment into personal liberty. These recommendations follow from the description of a potential problem with barely a moment to consider the consequences for our form of open government.

[22] 'Executive Summary', *Strategic Information Warfare Rising* (MR-964-OSD), p. 1.

[23] Although we will use the United States as an example in many places, do not think that the US is the only 'larger' State that is at risk from information warfare.

[24] 'Executive Summary', *Strategic Information Warfare Rising* (MR-964-OSD), p. 2.

[25] For example, Forrester Research Inc., a Cambridge, MA-based market-research firm reports that last year, U.S. companies spent $43 billion in sales to each other over the Internet, five times the consumer retail total. In four years, the research firm projects business-to-business sales will reach $1.3 trillion and make up 9.4 percent of corporate America's purchases.

[26] Ross Kerber, 'Banks called lacking in Y2K information', *Boston Globe*, June 11, 1999.

[27] Ben Iannotta, 'Ground Stations Could Face Y2K Problems', *Space News*, June 21, 1999, Vol. 10 No. 24, pp. 14, 18.

[28] Let me emphasize most emphatically that this is not a malicious suggestion. It is merely an objective assessment based on the logic of the model for a new kind of warfare.

[29] That attacks against the United States may be deferred is consistent with this model: attack surrogates or proxies to learn. The learning is a precondition and preparation for acquiring the ability to attack larger States later.

[30] There are countries in these regions that may have done insufficient remediation and repair to be largely free of Y2K problems.

[31] Jube Shiver, Jr., 'Phone Firms May Have a Few Y2K Hang-Ups', *Los Angeles Times*, Monday, May 24, 1999.

[32] Some may be inquiring into these issues already. See 'Naval War College Sets Sights on Y2K', *Information Technology Association of America (ITAA) Year 2000 Outlook*, Volume 4, No. 21, June 4, 1999.

[33] These advantages may be compounded if defenders are thoughtless or loose-lipped enough to reveal their plans to potential attackers in advance. See 'DOD May Unplug From Internet Due To Security Worries At Century's End: NIPRNET would be network of choice', *Inside The Army*, June 21, 1999, p. 1. If the aim of this disclosure was to deter attacks, some tactics stronger than dropping-out or pacifism might serve more effectively.

[34] Chris Allbritton 'Cities Preparing for Y2K Problems', *Associated Press*, June 5, 1999. Allbritton writes:

> With about 36,000 local governments in the United States, cities' and counties' preparations for possible Y2K computer bug problems are literally all over the map.
>
> Local governments need computers to operate traffic signals, dispatch police and fire fighters, run jails and maintain sewer systems. Computers are also used to run payrolls, track taxes and manage fleets of city vehicles. So, possible fallouts from the computer problem range from the grievous to the glitchy.
>
> "Our greatest domestic risks for Year-2000 related failures are at the local level", said John A. Koskinen, chairman of the president's council on Y2K. On May 24, he announced a series of "community conversations", town hall-like meetings aimed at sharing information between local businesses and governments, utilities and community groups.
>
> Ultimately, about the only thing localities have in common is uncertainty.

[35] Alvin and Heidi Toffler, *Powershift: Knowledge, Wealth, and Violence at the Edge of the 21st Century* (New York: Bantam Books, 1990).

[36] Although the battlespace of the future may be increasingly transparent, there is little assurance that we will understand the 'meaning' of what we observe. If this is so, 'information superiority', the notion upon which *Joint Vision 2010* rests, is a pipe dream. See Richard Szafranski, Joseph A. Engelbrecht, Jr., and Frank Strickland, 'Meaning and Mystery', a paper presented at *EloKa Lw 2020*, Info Ops Workshop, sponsored by the German Air Force Staff (Fü L. II 1), Bonn, Germany, September 29-30, 1998.

[37] 'Indian Government Concerned Over Lack Of E-Commerce Capabilities', TELECOMWORLDWIRE, May 10, 1999.

[38] For example, the owner of a large timbering concern in the Amazon Basin confided that he believed that a rival timbering consortia from the Pacific region—not Brazil's citizens—funded the anti-timbering Amazon environmental concerns that were making the headlines in Brazil.

[39] Alvin and Heidi Toffler, 'Beyond Future Shock: Conspiracies, The Media And The War For The World's Mind', June 15, 1999, *Los Angeles Times Syndicate.*

[40] A reason we should be opposed to a reduction in intelligence and reconnaissance budgets and increased reliance on "open source" information is because denial and deception are among the most promising tactics of information warfare. For the next decade or so, the best and surest way to get another State's secrets will be to buy or steal them. Of the forms of theft, electronic theft may be the superior form.

[41] An idea suggested by Dr. Alan Stephens in an email discussion of the consequences and timing of the 'Melissa' virus.

[42] Stewart Taggart, 'Shutting Up Cell Phones', *Wired News*, March 26, 1999. The article notes that:

> If you want to neutralize pesky adversaries in wartime, disrupt their communications. If you want to do the same in peacetime, disable their mobile phones. By selling a frequency jammer that prevents mobile-phone communications over a limited area, an Israeli company has taken a classic swords-to-plowshares approach in commercializing a military technology.

[43] See '4 million gallons of sewage spilled during Y2K test', June 17, 1999, *Nando Media* and *Associated Press*, reported in http://www.techserver.com/story/0,1643,60855-96870-691455-0,00.html.

[44] Douglas Waller, 'Onward Cyber Soldiers', *Time Magazine*, Volume 146, No. 8, August 21, 1995. Waller describes a series of physical and cyber-engagements:

> First, a computer virus is inserted into the aggressor's telephone-switching stations, causing widespread failure of the phone system. Next, computer logic bombs, set to activate at predetermined times, destroy the electronic routers that control rail lines and military convoys, thus misrouting boxcars and causing traffic jams. Meanwhile, enemy field officers obey the orders they receive over their radios, unaware the commands are phony. Their troops are rendered ineffective as they scatter through the desert. U.S. planes, specially outfitted for psychological operations, then jam the enemy's TV broadcasts with propaganda messages that turn the populace against its ruler. When the despot boots up his PC, he finds that the millions of dollars he has hoarded in his Swiss bank account have been zeroed out. Zapped. All without firing a shot.

[45] Ultimately the target set of strategic information warfare may be the people's confidence in their leaders or their government. See M.J. Zuckerman, 'Survey: 45% of Y2K experts worried', *USA Today*, June 11, 1999

> The survey, which can be found at www.wdcy2k.org, shows deep differences:
> - **The economy:** 38% expect a 20% loss in stocks and recovery by 2001; 45% expect a mild six-month recession with 6% unemployment.
> - **Business:** 35% predict it will be "jolted a bit" with January "Y2K holidays" to make fixes; 28% see "major manufacturing disruptions."
> - **Utilities and infrastructure:** 40% predict at least "short-lived failures" up to seven days; 42% expect scattered supply and utility problems lasting at least two weeks.
> - **Government:** 19% predict one state government will run into "serious Y2K problems"; 30% expect "at least one major government agency," such as the IRS, will fail.

[46] *The President's Commission on Critical Infrastructure Protection*, October 1998, p. 28.

[47] See my 'Toward a Theory of Neocortical Warfare: Pursuing the Acme of Skill', *Military Review*, November 1994; and idem, 'When Waves Collide: Conflict in the Next Century', *JFQ: Joint Force Quarterly*, Winter 1994-95.

[48] Alvin and Heidi Toffler, *War and Anti-War: Survival at the Dawn of the 21st Century,* (New York: Warner Books, 1993), p. 3.

[49] Alvin and Heidi Toffler, *War and Anti-War*, p. 241.

[50] Brian Witten of the US Defense Advanced Research Projects Agency (DARPA) noted in a conversation that traditional economic metrics and some traditional business behaviors are vestiges of a Second Wave economy emphasizing atoms, not bits.

[51] This point at which we leave 'tradition' is, of course, debatable. See Kevin Kelly, *New Rules for the New Economy: 10 Radical Strategies for a Connected World* (New York: Viking, 1998), Stan Davis and Christopher Meyer, *BLUR: The Speed Of Change In The Connected Economy* (Reading MA: Addison-Wesley, 1998), Carl Shapiro and Hal R. Varian, *Information Rules: A Strategic Guide to the Network Economy* (Boston: Harvard Business School Press, 1998), and Regis McKenna, *Real Time: Preparing for the Age of the Never Satisfied Customer*, (Boston: Harvard Business School Press, 1997).

[52] Brian Witten of DARPA notes: "We've seen this already both in system administrator use of weapons like 'Back Orifice' for the innocuous management of many machines, and in the development JINI integrity enforcement mechanisms to reduce lifecycle costs of integration."

[53] Richard Szafranski, 'Awareness, Adroitness, Audacity', a presentation to the 'Mastery of Information: Technology and Operational Concepts Circa 2030' symposium, Joint Experimentation Futures Workshop, May 4, 1998.

[54] Brian Witten of DARPA calls this "The Network Effect of Knowledge" and notes that "… each new fact has value not only as a fact, but also in its probability of shedding new light on old facts and bringing more new facts to light. In other words, cooperation can let you learn faster – something critical to knowledge warfare."

[55] Paul Festa, **'**Senate, FBI sites down on hack attacks', *CNET News.com*, May 28, 1999, 12:05 p.m. PT, http://www.news.com/News/Item/0,4,37194,00.html.

[56] Michael Skroch, "Development of a Science-Based Approach for Information Assurance," Defense Advanced Research Projects Agency (DARPA), Information Systems Office (ISO), May 10, 1999. Skroch writes of the need to "develop equivalencies, relationships, laws, logic, postulates, proofs, and methods for calculation so that cyberscience and metrics can be used effectively. Just as in other disciplines, complexities of systems will often not allow for closed solutions; therefore, modeling of IA [information assurance] will be needed."

[57] Such a group might be subdivided into print, visual, and voice components.

[58] Perhaps someday this will take separate Information Forces or more robust Air Forces.

[59] See Jeffrey R. Barnett, *Future War: An Assessment of Aerospace Campaigns in 2010* (Maxwell AFB AL: Air University press, 1996), p. xxii-xxiii. For the underpinning logics see Ralph D. Stacey, *Managing the Unknowable: Strategic Boundaries Between Order and Chaos in Organizations* (San Francisco: Jossey-Bass Publishers, 1992, John H. Holland, *Hidden Order: How Adaptation Builds Complexity* (Amsterdam: Addison-Wesley Publishing Company, 1995), T. Irene

Sanders, *Strategic Thinking and the New Science: Planning in the Midst of Chaos, Complexity, and Change* (New York: The Free Press, 1998), Peter F. Drucker *Innovation and Entrepreneurship: Practice and Principles* (New York: Harper and Row Publishers: 1985), Dan Dimancescu and Kemp Dwenger *World-Class Product Development: Benchmarking Best Practices of Agile Manufacturers* (New York: American Manufacturing Association, 1996), David M. Anderson *Agile Product Development for Mass Customization* (Chicago: Irwin Professional Publishing, 1997), Clayton M. Christensen *The Innovator's Dilemma: When Technologies Cause Great Firms to Fail* (Boston: Harvard Business School Press, 1997), Jeremy Hope and Tony Hope *Competing in the Third Wave: The Ten Key Management Issues of the Information Age* (Boston: Harvard Business School Press, 1997).

[60] According to the article 'DOD Creates Office To Battle Cyber terrorism', July 24, 1998, *Newsbytes*:

> The new office, which DOD officials still must name, will be part of the Office of the Assistant Secretary of Defense for Command, Control, Communications and Intelligence and will manage Defense efforts to safeguard the nation's critical infrastructures.
>
> These include telecommunications, banking and finance, energy, transportation and essential government services.
>
> "Because of our constitutional orientation and our history, (DOD) is not going to be the lead in anything, but we will be the backbone of everything, when you get down to it," he said.
>
> The DOD office will work closely with the Justice Department's National Infrastructure Protection Center and the multiagency Critical Infrastructure Assurance Office, Hamre said: "We have committed ourselves and are supporting the National Infrastructure Protection Center," Hamre said: "We provide the deputy, and we'll provide, I believe, three of the five heads of the directorates."
>
> The FBI's new National Infrastructure Protection Center (NIPC), at FBI headquarters and headed by Michael Vatis, will gather threat and vulnerability data and then disseminate analyses and warnings of threats to both the government and private sector.

[61] There were a few late-arriving exceptions. See 'Allies Target Computer, Phone Links', *Washington Post*, May 27, 1999, p. 1. See also 'Yugoslavia Loses Satellite Signals', SkyREPORT.COM E-News for 05/28/99, wherein we read, "Eutelsat has been under pressure from NATO to suspend transmissions. Yugoslav broadcasting facilities, regarded by NATO as part of the country's propaganda machine, have been a target in the NATO bombing campaign."

[62] David Ronfeldt, *'Beware the Hubris-Nemesis Complex: A Concept for Leadership Analysis'*, (Santa Monica CA: RAND MR-461, 1994), p. 31.

[63] One reviewer noted:

> Conversely, although cyber aggression and counter cyber-aggression may be non-lethal in nature, civil or military authorities obviously must take care when considering both attacks and retaliation against cyber-warriors. The arrest of one notorious hacker or an-

other has not slowed the exponential growth of the hacker community. Indeed, over a thousand hackers attended the DEFCON 7 hacker convention. Hackers so far do not appear to be dissuaded by the risks of mucking with the exponentially increasing global value of e-business. On the contrary, they seem to be encouraged by the anonymity afforded by a community growth rate that tracks the growth of the Internet.

[64] Alvin and Heidi Toffler, 'Foreword', *In Athena's Camp*, p. x*viii*.

[65] I do not know to whom strategic information questions should be asked.

[66] Scott D. Sagan, 'SIOP-62: The Nuclear War Plan Briefing to President Kennedy', *International Security*, Vol. 12, No. 1 (Summer 1987), p. 22, and Barbara G. Levi, Frank N. von Hippel and William H. Daugherty, 'Civilian Casualties from 'Limited' Nuclear Attacks on the USSR', *International Security*, Vol. 13, No. 3 (Winter 1987/88), p.169.

[67] Robert J. Wood, 'Information Engineering', An Air War College Research Paper written in fulfillment of the curriculum requirement for graduation from the Air War College, Maxwell AFB AL, 1995.

[68] Dennis M. Drew, *Nuclear Winter and National Security: Implications for Future Policy* (Maxwell AFB AL: Air University Press, 1986).

[69] US National Conference of Catholic Bishops, *The Challenge of Peace: God's Promise and Our Response* (Washington DC: Office of Publishing Services, United States Catholic Congress, 1983). Often referred to as the bishops' "pastoral letter" on the morality of nuclear deterrence and nuclear war.

[70] The United Methodist Church's Council of Bishops, *In Defense of Creation: The Nuclear Crisis and a Just Peace* (Nashville TN: Graded Press, 1986). If there is such a thing as an "information winter", it would be "truth", not "creation", that needed defenders.

THE INFORMATION REVOLUTION

Commodore (Royal Navy) Patrick Tyrrell
Defence Communication Services Agency, United Kingdom

ABSTRACT

This paper is to examine the nature of information and to look at how it has changed in the "post information revolution" world. Has this changed the way in which we use it, has it altered the way in which we, as human beings, respond to it? I shall also examine some potential threats and look at how information integrity might be better safeguarded. A number of other important questions will be raised but, I fear, not answered: where does the responsibility for information rest; what sovereignty can a nation exercise over information and information flow, how might global networks be controlled and what threats to national information integrity can be identified. These are difficult issues, with no clear answers – but that should not stop us venturing down the information road.

> ***"It is only now that we begin to realise the real scale and profundity of the changes in the conditions of human life that are in progress.....The scale of distances has been so altered, the physical power available has become so vast, the separate sovereignty of existing states has become impossible"***[1]
>
> **H. G. Wells**

> ***"The electron, in my judgement, is the ultimate precision guided munition."***
>
> **John Deutch**
> **Director CIA**[2]

INTRODUCTION

In the history of mankind, a phrase often emerges which captures the imagination of the contemporary world. As we approach the end of the twentieth century, journalists, writers, scientists and commentators have vied with each other to achieve some degree of immortality with apposite "sound bites". One such phrase that has lodged itself in the public's consciousness is that of the "information revolution", often with only the vaguest understanding of the concepts involved. Another word that has sprung into our everyday lexicon as a result of this revolution is "cyberspace", initially coined by an American science fiction writer in the early 1980s when observing a number of young boys playing computer games in an arcade and very obviously immersed in some virtual world beyond the monitor screen.

There is a plethora of books, articles, reports and discussion on the implications of the information revolution in every aspect of human endeavour. We cannot envisage modern life without the convenience, speed and universality of modern information systems, from the humble telephone to the ability to be able to join in discussion groups with globally dispersed, but like-minded people, on the Internet. From the cash card to the manipulation of the financial markets on a twenty-four hours, global basis. In these, and many other applications, there is a clear assumption that the information flow is unimpeded, that the information

received is clear, unambiguous, correct and uncorrupted. In many cases, there will be an additional assumption that the information flow is private and that the information is confidential between the initiator and the recipient.

The integrity of information has always been a matter of critical interest but the dramatic changes brought about by the information revolution have made it much more difficult to trace the route by which information passes from one point to another. It is this inability to identify, with any ease, the provenance of information, to understand what might be termed *information opacity*, together with the global connectivity of modern systems, that has allowed, for example, the development of extensive global organised crime, described as the world's fastest growing business, with profits (in 1998) estimated at over $1000 billion. Within a military context, these same conditions have given rise to the concept of ***information warfare*** whereby a potential adversary might attempt to exploit vulnerabilities within a nation's information systems.

DATA, INFORMATION AND KNOWLEDGE

It would be instructive at this point to examine the terms that are often used to describe some of the concepts underlying a modern view of information. The Tofflers[3] include in their broad concept of knowledge: information, data, communication and culture. Schwartau[4] considers data to be individual facts or statistics in a raw or uncorrelated state, which, once organised, become information. It is the application of human insight and intuition that can transform this information into knowledge. A French academic, Philippe Baumard[5], goes further and argues that within a society founded upon Greco-Roman philosophy, the basis for knowledge is confined to "objective knowledge" rather than including broader areas such as "conjectural knowledge". He refers to this as "knowing" as opposed to "knowledge". He considers that many organisations, particularly when operating in periods of considerable change, believe that they have to use more and more knowledge and that this in turn forces organisations to process more and more information. He contends that successful organisations and individuals will place a premium on "sense-making" rather than on simply information-collection. Fukuyama[6] examines the role of the information age in the breakdown of hierarchy and authority within society and stresses the role that trust and the shared ethical norms that underlie it in the conduct of society. It is the human understanding, the ability of men and women to reason, that is the hallmark of human society; our ability so to do will be greatly enhanced by appropriate information.

The value of "knowing" has similarities with the philosophy of Sun Tzu who said that the greatest achievement was to destroy the enemy's strategy before it could be implemented. This had to be done in an unexpected manner with the unconventional use of "divine force" or *ch'i*. The opposite of *ch'i* is ordinary force or *cheng*. On the battlefield, *cheng* is a holding force that puts the enemy on the spot and *ch'i* is the flanking manoeuvre that fatally disrupts the enemy's strategy[7]. This is also the basis behind Edward de Bono's concept of "*lateral* or *parallel thinking*: "in parallel thinking there is as much emphasis on concepts as on information"[8]

Why should we be interested in these differences and how can they help us understand the issues surrounding information integrity? There is a seemingly natural tendency, in the field

of information technology as well as in other technical arena, to allow the technology to drive the development of systems, regardless of the requirements of the society or organisation. Understanding of the human aspects of decision-making is important if we are to be able to focus upon those areas where integrity might be vital and identify other areas where such assurance of integrity is of less importance. The military doctrine of command and control warfare (C2W) focuses on the requirement to influence human behaviour and the definition includes the integrated use of physical destruction, electronic warfare, deception, psychological operations and operations security. It is the use of such techniques as deception and psychological operations that can affect the way that a commander will interpret information, almost certainly by building upon his natural tendency to think inductively rather than laterally. Such *ruses de guerre* have a long and distinguished history from the Trojan Horse to the "Man who never Was". It is instructive to look at work done on expert systems[9] where an essential attribute is the heuristic nature of these systems compared with more conventional programs. It is a knowledge revolution with increasing emphasis being placed upon information flow and knowledge accessibility. The concept of "*intellectual capital*" is now increasingly accepted within the commercial world as one of the most important assets within a company. Developing and enhancing this asset is the key to success as the phenomenal growth of some Internet companies like *Amazon.com* can testify. In attempting to bring these different strands of thought together, it is instructive to look at the *knowledge spectrum* (figure 1). This examines the linkages between a number of concepts and links the processes controlling the translation of data into information with those traditionally human virtues by which information becomes knowledge.

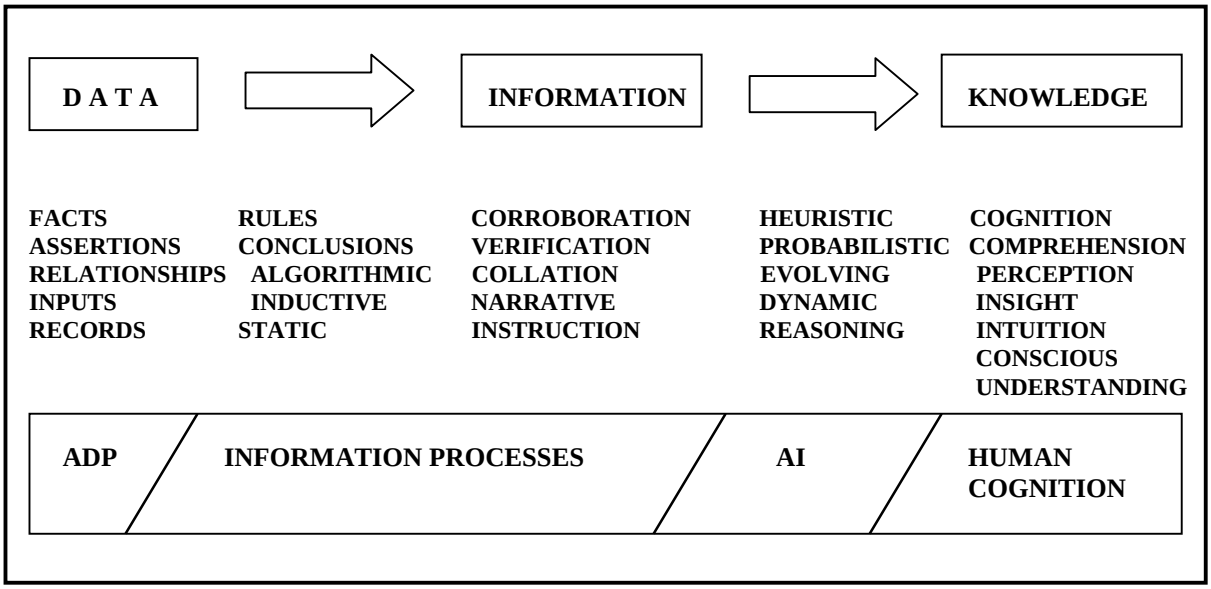

Figure 1: The Knowledge Spectrum

There are also four key stages in the life-cycle of information, its creation, its harvesting, its dissemination and its use:

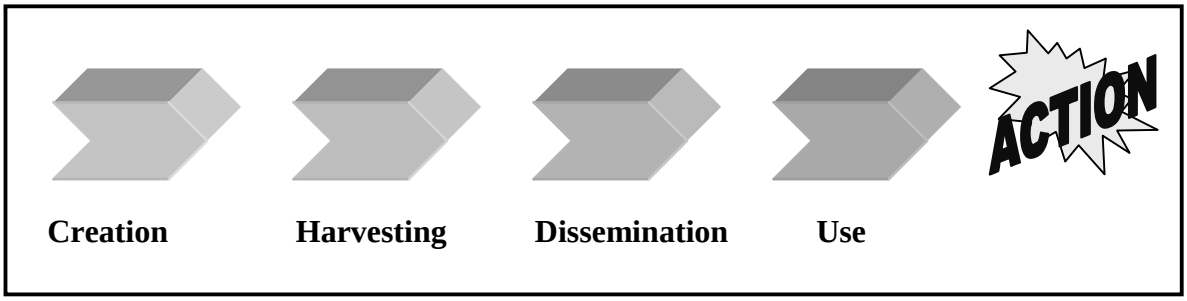

Figure 2: Stages in the life-cycle of Information

These four stages are distinct although share many similar characteristics. The technological developments of the past few years have affected primarily the speed and volume of harvesting and dissemination of information. To be effective, we must be better at the use of information and the ability to lead to better actions.

HISTORICAL PERSPECTIVE OF INFORMATION

Information has always been an important aspect of human society; after all, the ability to communicate and to transfer ideas and concepts is considered to be one of the defining parameters of *homo sapiens*. Until relatively recently in human development, communications were either by word of mouth or, if to be transmitted beyond a small group, written down. The development of printing in Europe by Gutenburg and Caxton in the 15th century had a profound influence on education and the broadening of the intellectual base by providing a relatively cheap, consistent, accurate and available source of knowledge to a wider audience than hitherto. It was not until the latter half of the nineteenth century that further major improvements could be made in the way human beings transferred knowledge. The advent of the telephone and wireless technology removed, for the first time, the requirement for a human intermediary in the transfer of data and permitted the instantaneous transmission of information over large distances. The transfer of information though remained essentially a *linear* and a *transparent* process by which data was assessed, the analysed information was then available to be transferred to the user who could then act upon it as required. The recipient could, if required, follow a clear audit trail to assess the validity of the information. So, for example, if Wellington at the Battle of Waterloo, wished to amend his tactics he would write his new orders and despatch them to the appropriate commander for action. If the body of the messenger was later discovered with his pouch missing there would be a strong presumption that the information contained in the message was now in the hands of the French.

While the first half of the twentieth century saw a number of qualitative improvements to the way in which data might be moved around the world, it was the technological imperatives of the Second World War that provided the impetus for the fulfilment of Babbage's great vision: the computer and the consequential information revolution. As with many technological developments throughout history, the driving forces behind the early innovations in this revolution were almost exclusively military, reflecting the priorities of World War II and the

Cold War. The major change as we approach the twenty-first century is that the factors driving these technologies forward, rely far less upon national defence budgets or other government expenditure than upon commercial priorities, applications and pressures. The reasons for this shift from military to civilian are complex but have much to do with the relative stability and affluence enjoyed by the West within the interstices of the Cold War as well as with the ability of the commercial world to develop a global and competitive market place.

THE INFORMATION REVOLUTION

The term "revolution" has been used extensively to characterise the exponential development of information technology over the past decade. Whereas fifteen years ago, computers tended to automate human activities to achieve speed and accuracy and, in the event of failure, whose functions could be replicated by the manual process, modern systems are extensively inter-linked and interdependent and can no longer be considered to be automated manual systems. Science and technology promises us that, in the near future, artificial intelligence (AI) systems will perform many of those actions now done by the human operator; only limited human 'control' will be required and most operators will be content merely to respond to that which the sophisticated software demands of them. There are already a number of disturbing implications arising from this "key-and-forget" dependence on systems, particularly amongst children where, for example, they display a loss of an instinctive comprehension and appreciation of mathematical problems when keying them into a calculator. They accept the displayed result with no urge to mentally check its veracity. Indeed, many of them may not have the ability to understand the mathematical process behind even the simplest calculation. These young children will be the managers of the future. In a report examining the shooting down of the Iranian Airbus Flight 655 by the *USS VINCENNES* on 3 July 1988, Rochlin[10] draws out some of the perils of increasingly sophisticated, increasingly centralised command and control (C2) systems, becoming larger, more rigid and more saturated with information and responsibility each year but without a concomitant improvement in the capability of the human brain to deal with such demanding concepts.

INFORMATION INTEGRITY

Information as a Strategic Asset

It would be wrong, however, to concentrate exclusively upon the technological advances inherent in the *"information revolution"*; the technology, although highly sophisticated, is merely a tool to manipulate information, to collate, store, sort, refine, and assemble as the user demands. Modern computers and communications can store information, process it and make it accessible in ways never before achieved but that, while conferring great added benefits to a business or organisation, they also enhance the scale and opportunities for mismanagement, theft, loss and abuse, as well as the indiscriminate dissemination of information in a manner inimical to the broad objectives of any organisation. Information as a military strategic asset has long been recognised by commanders with particular emphasis on the requirement for good intelligence on an enemy's intentions and, at the same time, protecting information as to their own plans and operational status. Making this information readily available throughout

the military environment, from the strategic levels of command down to commanders at the front line raises a number of complex problems if commanders at all levels are to be confident of the integrity, relevance and validity of the information presented to them. A latter-day Wellington, therefore, would no longer discover the physical body of his messenger, his digital messenger would have delivered the message, but how do we know that no one else also received it or that the message received by Wellington's commander was the same as that originally sent? The recent destruction of the Chinese Embassy in Belgrade by NATO warplanes is a clear example of the dangers inherent in accepting information without checking its provenance.

The application of the information revolution to organisations, whether civilian or military, has not been uniformly beneficial. Strassmann[11] reports that there appears to be no direct relationship between shareholder returns and the amount a firm spends upon information technology. This view is supported by an Economist study[12] looking at the introduction of electricity into US industry in the early years of the twentieth century where financial benefits only emerged once senior management came to terms with the new technology. In a survey[13] of 70 firms from the Times Top 1000 database, there was a clear discrepancy between CEO's and their IT directors' perceptions. Two interesting facts emerged: first there was a degree of complacency as to the business benefit of IT and, secondly, there was a clear cultural difference between the CEO and his IT-director and CEO's were reluctant to give their IT-director too great a say in the running of the business. These divergent perspectives arise from a lack of understanding, on the part of the CEO, who fails to comprehend the underpinning technologies and, on the part of the IT director, who does not recognise the strategic imperatives of the business. Despite these factors, there is, however, a clear relationship between the catastrophic loss of information systems and the success of a business: in a study on small to medium sized firms, it was reported that some 75% of those firms which suffer a major computer failure, mostly through fire or theft, go out of business within twelve months[14]. It is the unwillingness of an organisation to be able to safeguard strategic information effectively in such eventualities that can lead to their catastrophic collapse. Often, senior management takes little or no interest in the provision, protection and utilisation of this strategic information, frequently to their cost. The role of senior management is obviously key to the success of the above approach: all too often, however, senior management tends to abrogate responsibility to the technical management side of the organisation, leaving them to determine how, why and when modern technology should be employed within the organisation. IT directors, for their part, tend to suffer from a lack of strategic view for information management and an emphasis on what they perceive as their primary role of supporting operations. As a result, the tactical issues tend to take priority over the strategic. Many senior managers, both in the civilian and defence environments are, still afraid of the computer and even more of the cyberworld to which it gives them access.

Military Information Requirements

The very nature of military operations and their exposure to intensive media scrutiny, however, will inevitably place greater demands on the military leadership, with dramatic consequences for failure. In looking at the information needs of military commanders, it is useful to examine the types of military activity in which they are involved. There is considerable difference between the information skills required in a peacekeeping operation,

for example, than in that required during a major conflict. This *"spectrum of conflict"* provides a useful analytical tool and can allow us to distinguish a number of common threads.

Recent operations in Kosovo, for example, have highlighted the requirement for an ability to move from one part of this spectrum to another. The present "peacekeeping" operation could quickly degenerate into a more serious conflict as the ethnic Albanians flex their muscle towards the Serb population.

Military Information Systems in a Civilian World

Even a cursory examination of modern information systems will reveal that the military establishment is no longer at the technological cutting edge; the commercial world is driving research and development in an unprecedented manner. Commercial firms are increasingly considering their information systems to be revenue expenditure, purchased over a short period and replaced at regular intervals. The military and government requirements for long design phases, followed by in-service periods measured in decades rather than four or five years, are inimical to the use of the latest technology. Military systems, at the same time, are becoming increasingly interconnected with those of the civilian world and there is an increasing drive for interoperability between military and civilian systems. As the pressure on the military grows for initiatives such as private finance, creation of agencies and the growing need to rely on civilian firms for much of their deployment and support, there must be an awareness of the increasing interdependence of risk.

Threats to Information Integrity

There are a number of threats that we can identify to the integrity of information. There are three key parameters in assessing the nature of a threat: the first is the identity of the perpetrator, the second is the *modus operandi* and the third is that of motive. One of the distinctive features of threats to digital information is the difficulty associated with the identification of a perpetrator. There are a number of potential sources from which an attack might be launched:

a) The serendipitous hacker (sometimes referred to as a "computer intruder") who considers computer systems to be a challenge waiting to be unlocked and may stumble across opportunities to penetrate information systems fortuitously;
b) A disgruntled employee pursuing a personal grudge;
c) The professional criminal seeking to penetrate the security of a system for his own financial gain;
d) A national, or multi-national, company intent on achieving commercial advantage over its overseas competitors;
e) An international non-governmental organisation wishing to pursue its own agenda;
f) Hostile intelligence services intent on identifying and exploiting points of vulnerability of another nation-state and its military and commercial infrastructure;
g) Terrorist organisations keen to destroy or degrade a target nation's social, commercial or military information infrastructure.

The *modus operandi* adopted by such perpetrators varies widely but one frequently used tool is that of the virus, a piece of software, written in such a way that it can make copies of itself and able to corrupt particular parts of the system at predetermined times. Originally developed at the University of Sofia, Bulgaria, by a disgruntled Professor of Mathematics, they are now a familiar part of the computing landscape. The skill base developed in Eastern Europe was well recognised by the KGB who made considerable use of these and other computing hacking talents[15]. Viruses continue to plague the information world as was seen with *Melissa* and *Chernobyl* during the early part of 1999. It has been estimated that some 200 new viruses are being developed each month[16]and there is evidence to suggest that hackers will try to make the most of the Millennium period to cause mayhem or wreak havoc.

The motive for attack may well determine the level of threat to an organisation and identify some of the necessary actions to be taken to neutralise that threat. In examining motive, we need to look at the types of "*attack*" that might occur and how to counter them. The use of a pejorative term such as "*attack*" is useful in that it conveys the sense of violation of the integrity of the information and, therefore, of the company itself. It also reflects the military pedigree of these particular issues and the initial thinking behind much of the overall philosophy. In addition to intentional attacks, any information infrastructure will be vulnerable to a number of events, protection from many of which could be built into the systems. These events will include natural disasters such as fire or flood, technical breakdown in the system itself or the failure of a supporting system (which may or may not be under the control of the organisation). Supporting systems would include power supplies or the telecommunication service as well as the technical failure of components of the system itself. Once intentional and *force majeure* have been taken into account, there is always human error as employees can, and do, make mistakes, some of which can have major implications to the operation. On 21 November 1985, the Bank of New York suffered a multi-million dollar loss[17] simply as a result of a simple typing error in one line of code, a similar error, in 1991, led to the failure of a major portion of the US telecommunications infrastructure when an AT&T telephone switch in Manhatten failed. The failure of Ariane-5 rocket in 1996 was caused by a similar, simple computer code error. All of these events only serve to highlight the lack of proper checks as well as the failure, over a wide range of business and government, to give serious consideration to potential threats. Such eventualities, however remote, can be factored into the operational doctrine of the organisation and suitable contingency plans made.

A more difficult issue, however, is the response to deliberate and malicious acts: these can range from the unauthorised access into part of the system, the theft of information contained therein, the destruction of data, the insertion of misleading information into a database or the "take-over" of a system by someone for their own ends. An example of this occurred between March and May 1994 when the USAF facility at the Rome Air Development Center, was attacked[18]. Some thirty systems had been compromised, with 'sniffer' technology inserted in order to acquire user IDs and passwords. The hacker used multiple sites and multiple countries as a conduit for his attack in order to frustrate attempts to trace him. The countries were in Europe, South America and Mexico. When finally arrested by Scotland Yard, the hacker was found to be a 16 year-old youth living in London. This ability to obfuscate the source of an attack is one of the distinctive attributes of modern technology, a form of the *information opacity* mentioned earlier, and has a number of implications. If a state or organisation wished to launch an attack upon another state or organisation, this could be conducted through an innocent third party, giving rise to a perception by the target that the

third party was the real perpetrator. We have already considered the intertwining and interconnectivity of systems and a deliberate attack on the supporting infrastructure, including, for example, power or telecommunication bearers, or on information systems external to the organisation, Reuters news reports, stock reports from global based traders or status reports for military logistics from commercial suppliers could have serious implications for the organisation itself. The boundary of any organisation is no longer integral and is permeable to digital information. This is discussed below with particular respect to national sovereignty. Any strategy designed to safeguard an organisation's strategic information must, perforce, examine the external information linkages to the organisation's own systems.

Response to the Threat

Although the evidence for serious attack is limited, it is clear, however, is that few attacks are recognised as such by the users of a system. In the USA, the President set up a study into the "Critical National Infrastructure" and the UK Home Secretary has taken responsibility for the protection of electronic commerce within the UK[19]. How do we attempt to safeguard systems, whether military or civilian, if they are to be interconnected with other systems? To be able to assess the nature of protection required, formal *risk management* techniques will have to be developed to undertake the following:

a) Identify the vulnerabilities to information integrity both within and between systems (the modern tendency to increased networking has raised the potential for vulnerability exponentially);
b) Identify potential threats;
c) Quantify the threats; and,
d) Develop appropriate recovery strategies.

The development of suitable strategies for recovery is particularly important. Evidence from the US Department of Defense shows that there are a large number of attempts to penetrate systems, both military and commercial, and there is an increase in the frequency of attacks in the UK partly as a result of a greater degree of interconnectivity and also from the increasing sophistication of hacker tools. The US defensive IW programme has identified a three-phase approach: *protect*, *detect* and *react*. This approach allows systems to be protected, as far as is practicable, while appropriate systems are in place to detect intruders into the systems, with a suitable organisational framework designed to report intrusions and to be able to react rapidly to any intrusion, prevent further attack, ameliorate damage sustained and restore service as fast as possible. This process concentrates on the systems within an organisation and does not address the vulnerability of those systems outside the organisational boundary. Inevitably, it is not only very costly to protect all systems but also impractical and, in consequence, when looking at those systems which do not demand the highest integrity, the policy is to concentrate upon the "detect" and "react" elements. The determination of the appropriate information integrity is, therefore, of fundamental importance and will, in future, demand routine and rigorous ***"information audits"***. These will be similar to those already conducted within organisations for monitoring such strategic assets as finance and personnel. The audit will examine what information is required by the user, where the information comes from and how is it to be processed. It must address the information imported to an organisation from external systems and how the integrity can be assured. This must, perforce, be a dynamic

process particularly where information requirements change rapidly in the light of operational requirements as, for example, within military structures. Much has been done over the last few years to understand the extent and influence of information systems as a part of the preparations for the Millennium. It will be important to use this data to maintain an understanding of the systems and their dependencies once the Millennium period is past.

Responsibility for Information Integrity

Who then, should take responsibility for ensuring the integrity of information? Should it be a matter of technical competence only, or should it be a senior management function? The implications of either a systems failure or information compromise could be so severe as to affect all members of staff within the organisation and, consequently, it is they, collectively, who should assume responsibility for their own informational integrity. Senior managers should determine the organisation's policy for information assets and identify how compliance with that policy will be measured and reviewed. The list of items to be considered includes the identification of those assets, the quality and quantity of information required and the protection of information from, *inter alia*, unauthorised access, abuse and misuse. Companies will need to examine the question of the increasing inter-twining of systems and the potential for the increasing dependence of one organisation upon the systems of another. A simple example would be the use of commercial telephone capacity to support an organisation's own network. Although the use of service level agreements should ensure the delivery of an acceptable service, there will be increasing scope for the use of such interconnectivity for nefarious purposes. This is already the case where organisations have connected up to, and extensively use, the Internet.

Information Warfare, Sovereignty and the Nation State

It is clear from the preceding discussion that the issue of information integrity is one that affects individual companies, multi-national corporations, governments and, ultimately, the relationships between nations. It is, therefore, instructive to consider the genesis of the concept of *information warfare*, the relationship between military information ethos and its civilian counterpart and to examine the implications for the sovereignty of the nation-state as questioned by H G Wells in the quotation at the head of this paper.

The Concept of Warfare

In any conventional attack upon a nation-state, it is clear as to what constitutes an "*act of war*". Such an act would be followed by the outbreak of hostilities, as happened, for example, after the Argentinean forces invaded the Falkland Islands in April 1982. A broad definition of warfare was given by Malinowski (1968) as an "*armed contest between two independent political units, by means of organised military force, in pursuit of a tribal or national policy.*"[20] Clearly, included in this definition would be the attacks on London by German bombers in World War II. These attacks, designed to destroy London's ability to function as a financial and commercial centre, were conducted by "*organised military force*"; as we have seen above, the capability to achieve that same end now exists without recourse to

such force; would such an *electronic blitzkrieg* be considered to be an act of war and would the answer to this be different if the perpetrators were not a nation-state but a corporate body such as a multinational institution? This is more than an interesting, esoteric intellectual point: if a nation-state cannot determine whether or not it is at war or, indeed, determine who might be conducting a concerted action to damage, destroy or degrade important national assets like, for example, the City of London, the future stability of the nation-state could well be in doubt.

In such circumstances, which part of the nation-state should be charged with ensuring an appropriate defence and, if necessary taking appropriate action to recover the situation? Even within conventional operations, the co-ordination and liaison between those national and international bodies at the forefront of law enforcement has not always been comfortable, with extensive inter-organisation rivalry, lack of consistent communication and incompetent management of joint operations. Over recent years, considerable effort has been made to improve this situation. Within commercial organisations, they, themselves, must assume responsibility for safeguarding commercial secrets and taking any necessary legal action against other firms who infringe their intellectual property rights. Attacks within electronic systems, however, are not as clear-cut as those outlined above and, at present, there is no coherent view as to how both government and commerce should approach the problem.

The Concept of "Information Warfare"

Within the phrase "information warfare", the term *"warfare"* is pejorative and is reminiscent of John Fowles comment[21]:

> ***"Men love war because it allows them to look serious. Because it is the one thing that stops women laughing at them"***

Considerable play has been made over recent years about the idea of information warfare as a new and novel manner of attacking society. I do not believe that it is a new issue, but rather one that has been made more insidious by the ability to harvest large quantities of information and to disseminate it globally. The talk about *cyber-warfare* or *information warfare* centres upon the ability of an attacker to use an attack on a nation's information systems as an alternative to more conventional attacks. These can include those activities which do not normally fall within the purview of the military but reflect the increasing dependency of military systems on commercial and governmental information activities which are essential to the effective functioning of modern military operations. Modern technology is such that a deliberate, unauthorised and systematic attack could be launched against a nation state by another nation, by a commercial organisation or by a group of individuals. This could mean that the identity of the attacker could be unknown, or incorrectly identified (if the attacker is able to deceive the victim as to the true origin of the attack), at least in the early phases of a sustained attack. Such an attack might be launched from a wide variety of dispersed locations, all of which could be easily concealed within civilian society. The extent of the damage could be considerable where, for instance, there was serious degradation of the UK or US financial markets, it is possible that such actions could have unpredictable consequences in a world increasingly connected through global markets and trans-national corporations. This implies that an unknown computer assailant could cause considerable damage to the social, industrial and financial fabric of society, relatively secure in his own anonymity.

Information Infrastructure and the Nation-State

The terms *National Information Infrastructure (NII)* and *Global Information Infrastructure (GII)* have gained considerable currency in the past two or three years and reflect the organic and dynamic nature of the information and communication networks that have developed to support required levels of interconnectivity, integration and dependency. Despite the name, however, neither the NII nor GII exist as coherent or integrated systems. They are not owned by one company or agency, the government has little influence on their overall development and they are driven by consumer demand. They consist of a plethora of different systems, communication bearers, switches and facilities. There is a continual flow of information across international and organisational boundaries, the magnitude of which is increasing exponentially as the "global infrastructure" continues to evolve. The vulnerabilities of such systems are an unknown quantity and are unable to be properly assessed because of the dynamic pace of change and the inability to define the overall system.

Within the western world, London retains its role as one of the major foci for financial and commercial activity. Information flows are key to its success in retaining its primacy: financial markets are now controlled through 'real-time' global operations rooms electronically handling £ trillions per year; the damage to The Baltic Exchange, following the IRA bomb, caused considerable disruption to the UK's trade, shipping and commercial business. The activities of a single trader based in Singapore led to the demise of one of England's most prestigious banking houses and its ultimate take-over by a Dutch bank. The benefits accruing to the UK from the presence of these activities in London are considerable and reflected in our national balance of payments. It is clear that a number of nations, institutions and corporate bodies would like to see this status change and for other cities and nations to assume London's current mantle. It is possible that in the future some may be prepared to attempt to precipitate change by damaging the City's information infrastructure.

Sovereignty

Blackstone defined sovereignty as "*a rule of action prescribed or dictated by some superior, which an inferior was bound to obey.*" Sovereignty is a concept central to the definition of a nation-state and its ability to define and control the way in which the state interacts with other nation-states. Historically, it was considered to be a secularising concept that reflected the decline of universal religious authority and actively encouraged belief in the territorial supremacy of the state[22]. Because there is no state beyond the state, no super state, as it were, each state is "sovereign" in international society, a law unto itself. In the aftermath of the First World War, US President Woodrow Wilson's fourteen points proposed a degree of circumscription on a state's degree of sovereignty[23], a process continued in the UN Charter which, although the UN was an association of sovereign states, reserved the right to intervene in the implementation of measures to enforce peace[24]. This was clearly evident in the actions taken against Iraq after the Gulf War and, more particularly, in the actions against Yugoslavia where the UN and NATO intervened in an internal matter. Elsewhere in Europe, the development of the European Union has, of necessity, required a transfer of sovereignty over certain issues to be transferred from nation-states to Brussels. It appears that what is often termed "national sovereignty" can, in reality, be considered to be made up of a number of

overlapping layers which might include *ethnic sovereignty*, where political power only resides in citizens of a particular ethnic background; *linguistic sovereignty*, where the power resides in those who possess particular linguistic skills and *cultural sovereignty* where the characteristics of a nation-state are defined in terms of its cultural heritage and an assault on that heritage is considered to be an attack on the sovereignty of the state itself. This can be seen, for example, in the case of France were the government has been making considerable efforts to staunch the import of US culture, films, fast-food outlets, etc. Another area of traditional sovereignty has been that of *information sovereignty*, where a nation-state attempts to control the flow of information both within the state itself and across national boundaries. One consequence of the information revolution has been the increasing inability of governments to control the flow of images and ideas that shape human tastes and values. As the concept of *cyberspace* matures, it is clear that the notion of national boundaries will become increasingly irrelevant. How then can nations ensure the integrity of their systems, can governments insist upon minimum standards of ethical behaviour or taste in relation to material freely available to their citizens or will it be a free-for-all? The increasing globalisation of the information infrastructure also calls into question the concept of the nation-state where, for example, a company operating in one country, may well have a political affiliation with another nation or, indeed, increasingly may have no particular national affiliations but seek to fulfil corporate goals, whatever the cost might be to individual states. Paul Kennedy believes that "*the real "logic" of the borderless world is that nobody is in control - except, perhaps, the managers of multinational corporations, whose responsibility is to their shareholders, who, one might argue, have become the new sovereigns, investing in whatever company gives the highest returns*."[25] The concept of sovereignty, therefore, is under increasing pressure and is unsuited to the developing global information infrastructures. It will, however, continue to be used for the foreseeable future in the public discourse of international relations, offering diplomats a hallowed concept by which to carry on political debate, and representing, in a variety of situations, the ongoing struggles of a given people for self-determination and independence.

We have grown used to change, especially over the last decade, and yet, as human beings, we are continually unsettled by it. On whatever criteria one measures revolutionary change, it is clear that it summarises, most effectively, the world of today. The role of information in today's world is not qualitatively different from that of our forebears; we need information to be able to make decisions, to interact socially and to live. What has changed, however, is the quantitative nature of the information and the words of Stanislaw Lem, a Polish philosopher, who remarked that *"the era of great politicians has passed because the flood of information makes it impossible, too complicated, to make decisions."*[26] The issue of information integrity, when faced with such a flood of information, becomes critical and decision makers have to know what information is valid, what is corrupt, what is relevant and what should be ignored. Modern information processes, as we have seen, are vulnerable to an extent and information can be corrupted, degraded, destroyed or otherwise damaged. Although evidence is hard to collect, there have been a number of occasions when systems have been violated and financial or other damage occurred as a result.

The technological pace of change shows no sign of slowing and many of the problems highlighted will need to be addressed in the near future if we are to develop appropriate skills, models and methodologies to be able to quantify the threat to the systems of the future. The implications of doing nothing are so severe that this must be a problem for society in general,

rather than restricted to a relatively narrow and focused group of information technologists. The knowledge spectrum, ranging from data, through information to knowledge, could be useful. We have concentrated upon information, information flows, information integrity and information management, but what we will need to focus our attention on will be the process by which this information is used by the human brain. We may well be assisted in this by the development of artificial intelligence and whatever might follow AI but the human aspect will remain. We must attempt to answer the difficult question as to how we can return to the decision makers, in whatever field they might be, the ability to take decisions with a degree of confidence as to the integrity and relevance of the supporting information.

NOTES

[1] H.G.Wells: *A Short History of the World*, London Penguin 1936.

[2] Deutch, John: 'Oral evidence to US Senate Committee of Government Affairs' - 26 June 1996 - reported in *The Times*, 27 Jun 96.

[3] Toffler Alvin and Heidi: *War and Anti-War - Survival at the Dawn of the 21st Century*, Little, Brown & Co. 1993

[4] Schwartau Winn: *Information Warfare - Chaos on the Electronic Superhighway*, Thunder's Mouth Press, New York 1994

[5] Baumard: *From InfoWar to Knowledge Warfare: Preparing for the Paradigm Shift*, InfoWar Con, Brussels, May 1996.

[6] Fukuyama, Francis: *TRUST: The Social Virtues and the Creation of Prosperity*, London, Hamish Hamilton - 1995 pp 25-26

[7] *The Economist*, Survey of Defence Technology 10 Jun 95 p10.

[8] De Bono, Edward: *Parallel Thinking - From Socratic to de Bono Thinking*, Viking 1994 pp 215-25

[9] Peppard: *IT Strategy for Business*, Pitman Publishing 1993

[10] Rochlin, Gene 'Iran Air Flight 655 and the USS VINCENNES', article in: *Social Responses to Large Technical Systems*, Amsterdam Kluwer Academic Publishers 1991

[11] Strassmann Paul: *The Politics of Information Management - Policy Guidelines*, The Information Economics Press 1995

[12] *Economist* article: 'What Computers are for', 22 January 1994 p 68.

[13] MORI poll conducted for Computer Associates reported in *Management Today* - June 1996 p78.

[14] *Business World*, 20 March 1994

[15] See for example Stoll, Clifford: *The Cuckoo's Egg*, London: Bodley Head 1990 for details of a KGB run hacker activity.

[16] Government Computing - April 1996. p 10

[17] Schwartau, Winn: *Information Warfare* , op.cit. pp 96-98

[18] Reported in several places. See, for example, CSIS Report on Global Organised Crime pp50-52 op cit.

[19] Statement by Home Secretary to Parliament: Monday, 25 Jan. 1999.

[20] The Oxford Companion to Politics of the World Oxford University Press 1993 pp 962-965

[21] Fowles, John: *The Magus*, London Jonathan Cape 1977

[22] See: *Oxford Companion to Politics of the World* op.cit. pp 851-853

[23] Brogan, Hugh: *History of the United States of America*, Longman London 1985 pp495-495.

[24] Calvocoressi, Peter: *World Politics since 1945*, Longman, London 1991. pp122-124.

[25] Kennedy, Paul: *Preparing for the Twenty-First Century*, New York, Vintage Books 1994.

[26] Lem, Stanislaw: reported in *The Times Magazine* 11 May 1996.

INFORMATION OPERATIONS
Some Operational reflections

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

ABSTRACT

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

INTRODUCTION

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

THE BROADER SCOPE

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

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

TECHNOLOGY

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

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

THE MILITARY REALM

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

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

MEANS AND METHODS

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

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

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

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

ABOUT CYBERSPACE

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

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

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

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

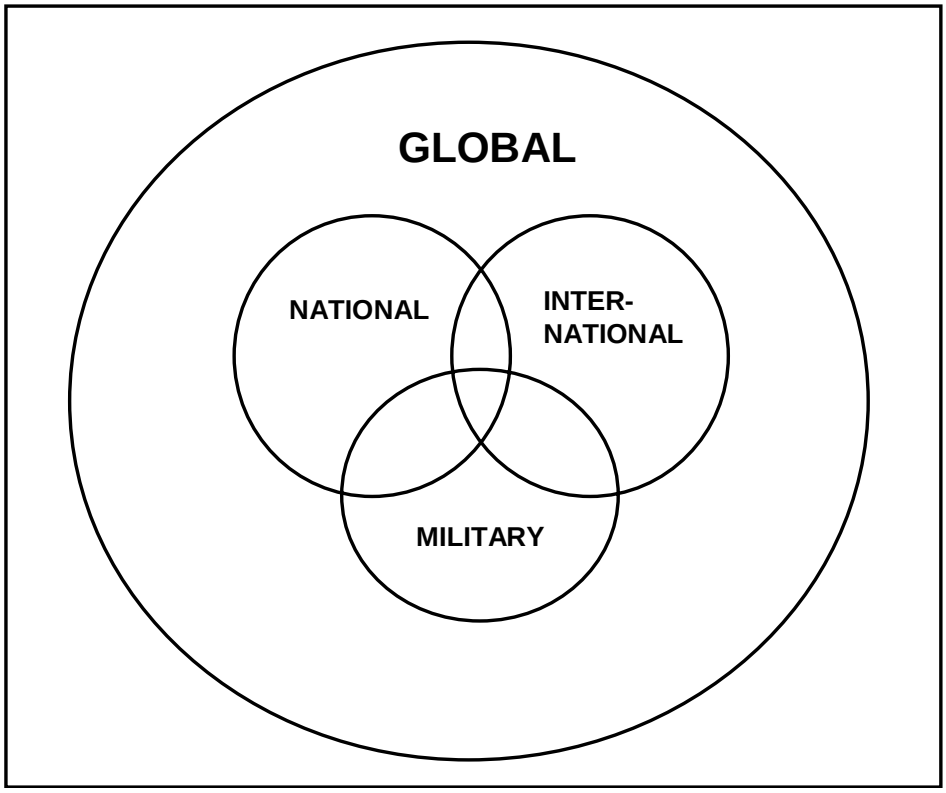

Figure 1: Information Environments

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

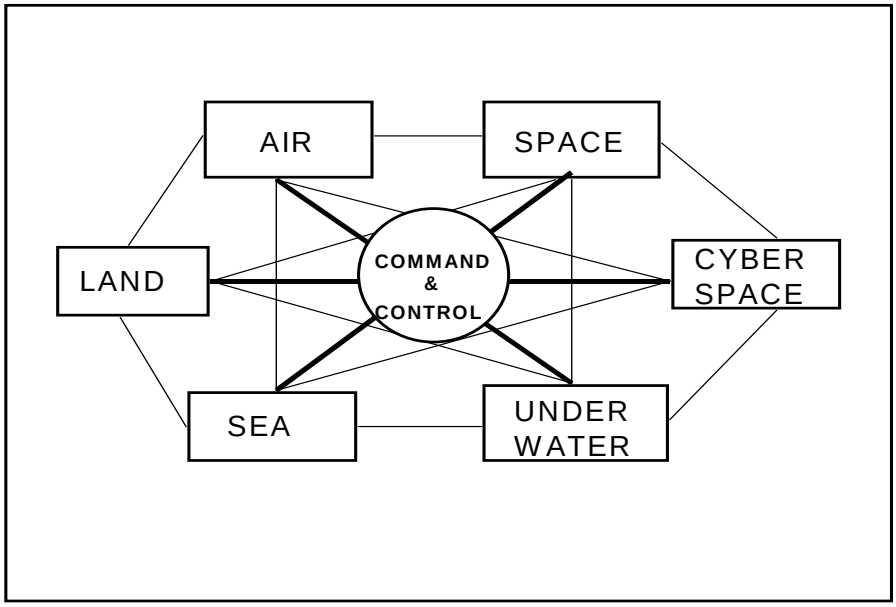

Figure 2: Dimensions of Warfare.

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

INFORMATION BASED WARFARE

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

SOME RESERVATIONS

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

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

THE HUMAN FACTOR

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

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

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

THE SYSTEM OF SYSTEMS

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

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

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

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

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

ON COMMAND AND CONTROL

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

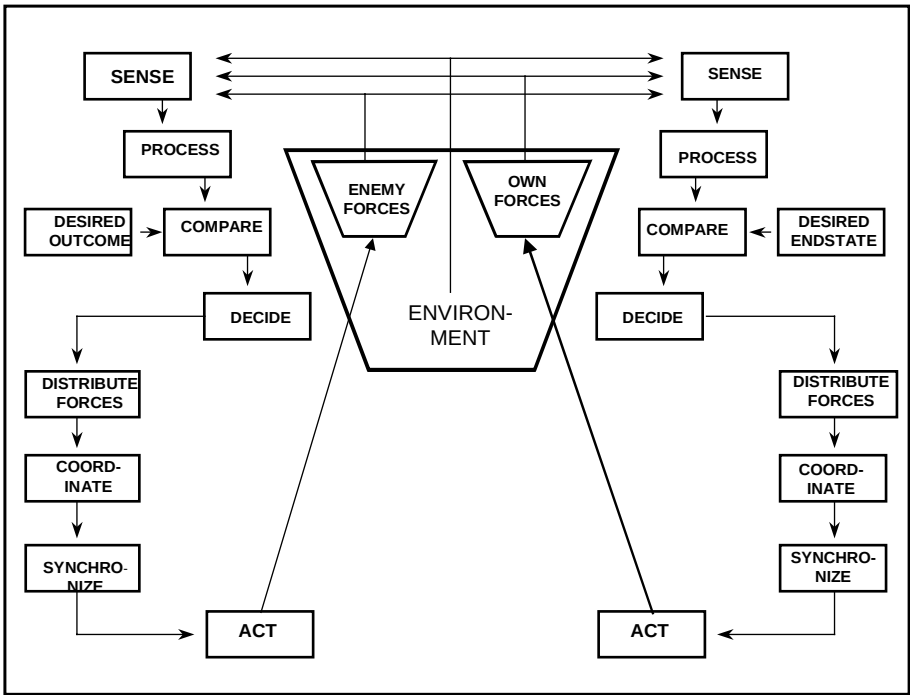

Figure 3:Opposing C2-cycles

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

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

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

THE COMMAND AND CONTROL COMPLEX (C2C)

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

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

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

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

Table 1: Opposing C2-complexes

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

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

COMMAND AND CONTROL WARFARE (C2W)

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

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

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

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

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

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

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

INFORMATION OPERATIONS (INFO OPS)

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

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

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

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

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

- Does the Force effectiveness of the digitised force improve relative to an analogue baseline Force?

- Can the units accomplish their operational tasks better than analogue baseline units?

- Do the battlefield digitisation systems work as expected in an operational environment?[29]

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

OTHER DIMENSIONS

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

SOCIETAL CONNECTIVITY

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

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

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

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

CONTRADICTION?

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

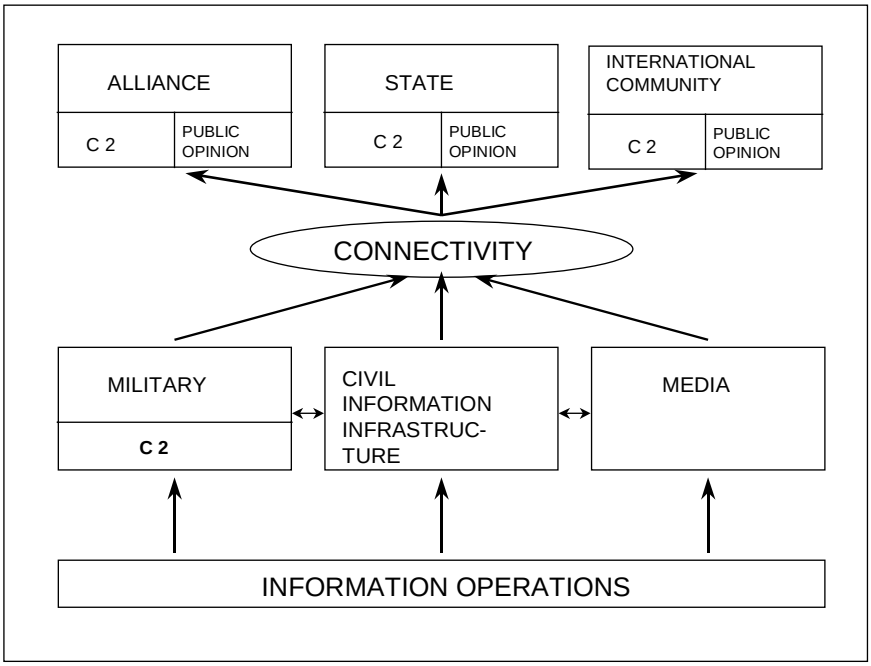

Figure 4: The scope of Information Operations

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

THE PEACE ENFORCEMENT ENVIRONMENT

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

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

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

SMALL WAR

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

ON ASYMMETRY

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

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

CHARACTERISTICS AND EFFECTS OF INFO OPS

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

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

CONCLUSIONS

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

REFERENCES

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

NOTES

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

2 Dupuy, Volume 6, p. 2702

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

[4] Lewin, pp. 129-133

[5] Welsh, p 29

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

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

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

[9] Idenburg, p. 5

[10] *Dying for information*, Executive Summary

[11] Dixon, p. 28

[12] Kam, p. 85-114

[13] Dixon, p. 31

[14] Breakwell and Spacie

[15] Hughes, p. 149

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

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

[18] Crefeld van, pp. 235-249

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

[20] Dixon, p. 28

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

[22] p. 2-35

[23] p 2-36

[24] Alger p. 54

[25] FM 100-6, 1-6

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

[27] AFDD 2-5

[28] Bunker, p. 13, endnote 31

[29] Holcomb, p. 101-104

[30] Forster, pp. 19-22

[31] Grau and Thomas, p. 508

[32] Harcknett, pp. 95-96

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

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

[35] Task Force Eagle.

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

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

[38] Hughes, jr., p. 203

INFORMATION WARFARE OR INFORMATION OPERATIONS?[1]

Lieutenant Colonel Félix Faucon
Centre d'Etudes et de Prospective de l'État-Major de l'Armée de Terre

ABSTRACT.

The careful reading of the 1994 France Defence White Paper denotes the presence, if not the confrontation, of two cultures. Firstly, that of "realists" for whom war is a phenomenon brought on by international relations, a time altered by the bipolar geo-strategic balance. Secondly, that of "idealists" for whom it constitutes an anachronism, or even marginal, manifestation in an international society that increasingly favours the solutions of peaceful compromise under the umbrella of the United Nations.

These two different understandings, confirmed by the political orientations and decisions taken since the White Paper was written, are the principle sources for the diverse capabilities asked of the Armed Forces. At the same time this duality also introduces, in a paradoxical way, new requirements and new constraints in the operational area.

RETHINKING THE TWO-SIDED DOCTRINE

Without questioning the consensus regarding the impossibility of an all-out war (always guaranteed by national defence nuclear weapons), it is the end of the monopolistic principle of non-war. Rather, it is the complement to the non-war principle by the suspension of war through action. In fact, this constitutes the major strategic evolution of the French concept of defence in the past few years.

The strategies of action that now complete the period of stand-off must allow for the increase of the strength or the influence of the country. To re-iterate the classical categories, it encompasses a simultaneous renewal of direct strategies. That is, a strategy where the Armed Forces play a primary role, and indirect strategies where, without being totally absent, the Armed Forces have a secondary role. As a matter of fact, it becomes necessary to be able to take control of the events of which we allow resurgence (i.e. war). At the same time, the use of force must be proportional to the strict limits of the objective sought: mastering the will of the adversary. Within this context, the process leading to the definition of the Armed Forces required capacities begins with an analysis of the operation arena in which the Armed Forces must be able to act effectively. Therein lies the starting point of any observation regarding, in particular, the land-operations strategy. This is examined in a study currently being undertaken at the Centre for Strategic Studies (Centre d'Etudes et Prospective) of the French National Army.

Two important events have stimulated the observation concerning the confrontation of the two opposing schools of thought and the role(s) which the French Army must play. Firstly, the necessity to foresee military action of a certain magnitude while conflicts start at the regional level. Secondly, the appearance of new operations which goal is not necessarily decision-

making by arms or physical confrontation, but which are based on strategies of influencing the adversary. These two aspects lead to a diversity of the *'operational space or -field'* in which the engagements must take place. Note that the meaning of the term *'operational space or -field'* here corresponds with (*Dictionnaire Robert*): "*a limited space (concrete or abstract) reserved for certain operations or with particular characteristic*".

From the viewpoint of an almost complete revision of the land operation strategy, it is wise to define potential operating fields in all their diversities, and to find a typology in order to provide a modern definition.

The typology of the operational space or -field as defined in the France Defence White Paper is subdivided in conceptual, psycho-sociological, geopolitical, geographical, physical, command-and-control and information systems. A field is active the moment that at least one of the following situations arises: the players involved are susceptible to engaging in actions contrary to those of the ground forces, or the field represents an occasion for action by the ground forces, their partners, or for the other players which are part of the conflict.

This new definition serves well the effort not to limit the two-sided doctrine to direct conflicts only. This definition allows for the broadening of the classical concept of "operations" well beyond the geographical limits imposed by its traditional meaning: the "theatre". The time limits are also questioned: we can clearly see that the battle of doctrines, for example, is an operation that must be undertaken without interruption. The strategic continuum, in the past ensured through dissuasion, is now ensured through the search for influence by means of either covert or open action.

A field of operation is defined as a material or immaterial space in which the ground forces must be able to reach an objective defined by the operational strategy, independent of the current school of thought. The Army must be able to conduct actions of surveillance, acquisition, maintenance of contact, and intervention (neutralisation, destruction, support), under the widely varying circumstances of different fields of operation. Consequently, regarding the means, it must be possible to act in all the fields, including immaterial fields, and, within the operational concepts, to exploit influence, synergies or constraints created by this diversity. The idea of the 'multi-field manoeuvre' for example, ensures the convergence of various efforts aiming to reach a military objective or a strategic goal.

Moreover, within the 'strategies of influence' so far desired by the nation, the Army must evaluate the consequences for its organic roles, taking into account confrontations and rivalries that permanently influence the strategic realm and that do not always take into consideration operations by using physical force. It is from this conceptual approach that we must consider the concepts of recent publications regarding information warfare.

Information warfare: journalistic headline or an operational concept? To shed more light on this topic, the Centre for Strategic Studies has attempted to deal with the topic during a symposium which it organises every second year with its British counterparts and the Delegation for Armament, named AFLOS: Anglo-French Land Operations Symposium. The seminar of AFLOS 97 was held in May of 1997, and it is interesting to reveal the main results.

INFORMATION WARFARE AND INFORMATION OPERATIONS: A FRENCH-BRITISH APPROACH

It is difficult to know exactly how to begin discussing the topic of the information warfare. It should be noted that there is no simple approach to an area of such complexity. In fact, it is more influenced by the interactions between its components than by the inherent nature of each one of them. A systematic approach should define the concept of information warfare and attempt to define its scope.

In the preparatory phase of the AFLOS 97 seminar, the British views on the topic and the terminology used by the French Army were combined. Basically, before attempting to define the different terms to be used, we must order them by their contents, by linking the logic, the grammar and the different terms. This 'dynamic shaping of the language' was of great help to the interpreters, as the symposium was held bilingually, each representative used his mother tongue. It was indispensable to the proper comprehension by the experts who, for the duration of four days, strove to determine the role of the information warfare.

The definition of the role is of utmost importance. As a matter of fact, this concept presents itself as a system of concepts. It is therefore advisable to clarify the primary principle of any system: the goals it wishes to reach, in other words the role that it hopes to play in a given space or field. That is the only way to take operational concerns into consideration.

The working group answered the following two questions.

> What effects could result from the use of information warfare techniques in the given scenarios? (There were two scenarios describing an operational situation in 2020).
>
> What are the objectives the Allies wish to attain through the use of the information war? '(This latter question was done by a systematic method established by a working group 'laboratory' organised by a company from Champs-sur-Marne: creativity, reformulation, typology, axiology, and finally, modelling).

The result of this undertaking consisted of a dynamic articulation of the objectives of information warfare. Its role, updated by AFLOS 97, can be represented in a model, which includes 51 objectives, classified at 6 levels and in 4 dimensions. Table 1 takes this the results, but it is impossible, reproduce the objectives defined by the British and French experts entirely. An important note: it is necessary to first reach objectives at a lower level if we wish to achieve objectives at the higher level.

In shows to the ultimate goal of the information war. First of all one can say that it contributes to the overall performance of ground troops, and it therefore belongs to the area of operational functions. Secondly, there are three major goals for the information war, written in the sixth level. One must: (1) reinforce the coherence of the effects of the forces, and increase the pace of their action; (2) drain the morale and the will of the enemy in order to dissuade him from all physical confrontation; (3) mould the field of operations so as to establish the conditions for success.

Level	Level description	Dimensions			
		A- Knowledge	B- Influencing power (dominance)	C- Manoeuvre	D- C3
6	Contribute to the global performance of Forces				
5	Lessen the effects of the enemy's actions				
4	Guarantee the effects of our actions				
3	Master one's own abilities to act				
2	Ensure timely information availability				
1	Prepare themselves at length				

Table 1: The model of AFLOS 97 Information Operations states 51 objectives

How to reach these goals? That is done by a process of 'double relaxation' that comprises one of the principle characteristics of the model. Firstly, it is based on the guaranteed effects of our own action, and secondly by the reduction of same effects of the adversary on us. To do this one needs a solid base of knowledge of the environment, and the handling of the information needed to ensure own abilities to act.

The initial results of the symposium also allowed determining the objectives of information warfare, either from an organisational point of view (how to intervene?) or from an operational point of view (how and in what order to react?). The model produced by the working group demonstrated that the concept of information warfare is not a 'total'one in terms of an overall operational concept. This for the following reasons: the activities are concerned with the whole spectrum of operations; are certainly permanent, while others address neutral categories (populations for example), for which we cannot even use the terms "offensive" or "defensive".

The model prepared by AFLOS 97 is therefore more related to information operations (Info Ops) rather than exclusively to information warfare. As a result we can say that the purpose of these operations is to ensure the coherence and effectiveness of own actions, whatever the nature, in both the physical and immaterial operational realms. Ultimately, it is a vision that may completely renew the classic concepts of operational command. The Pilot Committee of AFLOS must now use this 'raw material' and submit technical and operational recommendations to both Armed Forces.

After that formal presentation of the results of the French-British AFLOS 97 seminar, it is possible to come to some additional comments. First of all; this study on Info Ops clearly shows that the most important elements are not the technical changes, but rather the strategic

changes. In fact, the four principle dimensions of these operations (see Table 1) correspond in general with the four most important fields of operation mentioned above. The "knowledge" relates to the conceptual fields (i.e. the battle of ideas, concepts, doctrines), the "influence power" to the psychological fields, the "manoeuvre" to the physical fields, and "C3" to the command & control systems as well as the information systems. This illustrates the evolution that was experienced in recent years: basically a 'direct action' strategy during the Cold War and the present-day strategy of primarily 'indirect action'.

Hence, the importance placed on the neutralisation of the adversary's capabilities, (level 5), in order to push back the chance of direct confrontation, (level 6), must be absolutely effective. This requirement is extreme, if we look the past dogma written in the 1972 France Defence White Paper which prescribed classical forces to win the necessary time for the initiation of the nuclear consultation, and in no way to win it by their own means. This relationship between Information Operations and the means of the operational superiority to be consolidated on the physical fields must be kept in mind. That is also the reason why the information, which in the past was only concerned with 'physical fields', no longer satisfies the needs of Information Operations. Consequently, we see that with another strategy, we seek information of a different nature, relative to other fields. A different strategic evolution would certainly have lead to another structure of the conclusions written in the AFLOS model. The French and the British share this strategic vision.

The second remark, which stems from the former, is that our problem does not end at mastering the information systems and their techniques. The supply of technology abounds today, but which operational needs must it satisfy? That is the basic question. Therefore, the true problem is to know how to specify which information we need. However, this specification is very difficult as the areas are fairly unfamiliar, beginning with the psychological fields. However, this effort is indispensable, and we have just seen why.

All of this brings to light the central role of the ground forces in the new strategic situation. The best contributors to psychological action are the ground troops, those that are in contact with the inhabitants and the belligerents. This contradicts certain visions of future confrontations, marked both by an excess of technological confidence and by strategic error. They pretend to solve everything at a distance and marginalize the ground forces, where as, to the contrary, the latter play an important strategic role, confirmed by all of the on-going operations. In an open conflict, the outcome is 'written on maps', by means of the land gained or lost, and the control of the crisis is only possible through the presence of contact for a longer period of time. This final point explains why the effort, by the French Army, to repossess the psychological weapon cannot be limited to Special Forces only.

The third comment is that the objectives found in the C3-dimension essentially regard the "speed", that is controlling the pace of the engagements. The improvement of decision-making will certainly be achieved by a global plan of computerisation, given the very nature of necessary information, as already indicated. However, beyond the 'culture of contact', it would be wise to preserve that of the decision itself, in other words: know how to make *"tough decisions with weak information"*, to borrow the words by Michel Godet.

In other words, we cannot expect everything in operations from an information system. The education of commanders remains indispensable, and they cannot become slaves of the

electronic systems, a tendency that is already noticeable within the American Army Training and Doctrine command (TRADOC). The network must not become an alibi to indecision but, quite to the contrary, must ease decision-making at all levels, which concretely translate the reactivity of the whole and the mastering of the pace of operations.

From this description of the problem of Information Operations, it would be interesting to see what, in this respect, is the position of the US Army.

WHERE STANDS THE US ARMY?

The Americans are of the opinion that information has top strategic priority for at least the next four years. They have allocated extensive resources and have taken a considerable lead over the Europeans.

In August 1996, the Field Manual 100-6 appeared. It deals with Information Operations for the US Army. What does it say? Firstly, it is a global concept. The US Army started from the following conclusion: *the concept of Information Warfare, as confirmed by the (US) Department of Defense and the (US) Joint Chiefs of Staff, is not sufficient to realise the entirety of activities linked to information, and that concerns the entire array of Operations.*

For the US Army, Information Operations is an on-going activity, whereas the Information Warfare is like adding the information dimension to a conflict or a war. Its goal is to achieve dynamic coherence among three interactive components: 'operations', relevance of information and intelligence, and 'information systems'.

'Operations' encompasses C2-warfare operations, civil affairs operations and public affairs operations. The relevance of information and intelligence aims to improve the decision cycles. Firstly, by broadening the needs for information. For example, logistics staff is only interested in one type of information, civil affairs in another, and so on.
It therefore makes sense to expand the limits of information accessible to everyone. Secondly, by enlarging the field of information research whose main objectives are: the update of knowledge of information and decision structures of the adversary (a pre-condition to the effectiveness of C2 in battle, i.e. of command); and the search for information critical to the command of the operation (this last notion being pertinent, including non-warfare operations). The information systems" or C4 (comprising personnel, equipment, and procedures) must satisfy the harsh requirements, regarding the growing quantity of information that needs to be treated, as well as the shorter deadlines to integrate them and present them in a format useful for decision-making. The ultimate goal is to control the speed of operations. Horizontal and vertical systems integration is thus a prime necessity.

Based on this concept, the US Army comes to concrete conclusions at the level of doctrine by coming to the practical use of ground forces: the information systems (C4) must give all the players all the "useful" information to win the C2 battle.

Improving the effectiveness of the 'command systems battle' therefore constitutes the goal of the American process. Nevertheless, this battle does not limit itself to information systems themselves. It also includes protection (operations security), in other words the capability to

protect one's own C2 from attack (counter-information, security of transmissions and so on); military deception; psychological operations (Psy Ops); electronic warfare (EW); and physical destruction. That is why the US Army advocates give responsibility of the information operations co-ordination, either to an ad-hoc task-group (similar to what is being practised in the determination of targets or attacks in depth, and headed by the operations officer, the preferred solution for operations of low intensity), or, in conflicts, to a designated Info Ops unit, possibly at division level, and in any case, at the Army corps level.

From this quick summary, we can attempt to evaluate the interest and the limits of the American process. Regarding the concept, the emphasis on "Information Operations" for all the operations and the information warfare reserved for conflicts, seems very pertinent within the new strategic context.

However, the presentation of the American Information Operations concept, this time at the Joint Forces level, only presents two activities: defensive and offensive. This binary concept – which undoubtedly unconsciously refers to the single Armed Forces' homogeneous centre of operation – downplays the pertinence of the position taken by the US Army. It would seem more appropriate to use the categories of "action-protection" for Information Operations and reserve the "offensive-defensive" for the Information Warfare. If the systems put into place could be classified in the latter fashion, it would certainly be appropriate to use a politico-strategic approach of the more detailed activities, to include neutral and civil aspects in the concept.

The process of the U.S. Army in fact covers two aspects. First, it is a technologically important challenge, linked to their ambition of integrating all information systems. This, in turn, leads to a certain number of risks (for them in case of failure, and for the Europeans in case of success…). Secondly, it is an operational necessity (improve the coherence of actions in all dimensions of operations, material and immaterial). This latter requirement consequently meets certain of the important conclusions reached in the study regarding land operational strategy as stated earlier.

Information Operations cannot be limited to the battle of information systems. This result of AFLOS 97 is confirmed by the overall American approach. Yet, the required dimension of joint Forces poses a difficult problem. This relates to the fact that both the Navy and Air Force often act 'at a distance'. It is only because of logistics, intelligence, and fire support that they have left the building of an incomplete concept, which they give little value, to the support that ground troops can bring to indirect strategies. It would seem that this is the obstacle that the US Army faces in extending the concept beyond the sole strategies of direct action, the area of preference of the other Forces.

It is therefore suitable, in France, to identify all the interests of a global concept, largely exceeding the mere domain of information technologies. We have seen that the approach taken by the US Army seems acceptable; it provides a way to work into that direction. Again it is essential that our contribution be a conscious one and not incidental. In summary, it is better to work on the convergence of these points of view on the basis of their possible synergism and not, as is too often the case, on the narrow basis of the highest common denominator.

CONCLUSION

To conclude, it is appropriate to resolve some issues. First of all, it is high time, in our country, to 'de-demonise' the psychological weapon immediately upon its conception or its initiation by the military. Therefore, the mastery of Information Operations, among others, of action and Psychological Warfare, becomes even more crucial in open or latent conflicts when the use of physical force is more compelling. The need for coherence between all the forms of action, as we have seen, points into that direction.

Let us also be conscious of the extreme external pressure applied by the Americans and by the interoperability to develop a common strategy with them and with other countries, such as Germany or the UK, which are progressing in the same direction. They progress and, already during the Gulf War, but still today in former Yugoslavia, Armed Forces units destined for psychological activities are put into place. As a result of insufficiently preparing ourselves, would our only role be simply to follow, or even be hostage, to our allies? Certain taboos linked to the national history should remain as such and leave the everyday news. In fact, we do not lack arms. Hence, the national Defence Centre for Social Sciences Studies, but also certain researchers such as Mr. François Géré to cite only him and his summation regarding "Psychological Warfare"[2], has kept the French opinions on these topics alive. And we ensure that the Armed Forces, the strategic affairs committee, the interservice Defence College, the State's Superior Court, but also the doctrine and training command, have studied this field that demonstrate the necessity of a new approach by the Armed Forces in this area and all other aspects that touch on Information Operations.

Secondly, one should definitely not neglect the effort of protection that has yet to be accomplished in the psychological area, since the actual context of employment of ground forces constraints us. In fact, the value system allowing for the legitimisation of action in the eyes of the combatant, and thus to strengthen his morale, cannot be the same according to his fighting as a civilian for the Vosges blue line, or as a professional soldier in a distant action with stakes less clear. Today, in certain operations, the psychological losses can represent up to 50% of total losses. The operational stake consequently is to increase that ratio for one's possible adversary, while at the same time reducing one's own loss.

This need for protection must be extended to the civil population, beginning with our own national public opinion, support upon which is dependent, as in all democracy, the legitimacy of the action taken, and which must be protected from disinformation operations. As a matter of fact, the US Army has made sure to differentiate Public Affairs from Psychological Operations. This is wisely, because we can clearly sense that the role of politics in these two activities must exercise itself according to different objectives: persuasion and conviction in the former, and strict control in the latter.

Finally, one should not, after reading this paper on Information Operations, be left with the impression that a choice would be possible between action in immaterial fields or in material fields. On the contrary, it is actually the complementary relationship between these different modes that must be researched and expanded: the classical methods having to guarantee, once deemed necessary, the indispensable physical operational superiority of the military's

credibility, mostly political however, of the action undertaken, hence the liberty of action and the certainty of the Armed Forces.

We are in the heart of the indirect approach voiced once by Liddle Hart. Namely, when he explained that "one must not seek out battle, but rather an advantageous situation which, if it does not produce a decision itself, its pursuit through battle would definitely allow for its realisation".

NOTES

[1] This paper was earlier published in: Défense Nationale, March 1988 and translated by permission of the author. Assistance for the translation was provided by Dominique Reverin and Peter Hupkens of TNO-FEL, The Hague

[2] La guerre psychologique ; Editions Economica, 1997

INFORMATION OPERATIONS, THE NATO PERSPECTIVE

Major General (Spanish Army) Jose Gardeta,
International Military Staff, Operations Division, NATO Headquarters, Brussels

ABSTRACT

The global technological evolution in the field of information has changed the world. Information now not only integrates most elements of modern life, including the civil community and the military world, but also accelerates all processes. An operational shift of focus towards a systems approach to war fighting is evident. This shift of focus led to the necessity for NATO to closely examine all systems involved with respect to the possible impact of information. This in turn led to the development of the NATO policy for Information Operations (Info Ops), contained in the Military Committee document MC-422 (15 Dec 1998), that was approved by North Atlantic Council on 22 January 1999. In summary, Info Ops are actions taken to influence decision-makers in support of political and military objectives, by affecting information as well as the information-based processes. Info Ops integrate Command and Control Warfare with the political consultation process, decision making apparatus and combined political-military operations of the Alliance. It provides the Commander with a vehicle for implementing this new view/approach into the military planning processes. Similarly it provides a defensive focus. The important operational change is the shift of focus towards the role of information. This includes the semantic, or perceptions aspects, as well as the technical ones, (physical and logical). Military planning, therefore, not only requires the direct involvement of the political decision making apparatus, but also the involvement and integration of a wide range of staff elements.

INTRODUCTION[1]

The subject of Information Operations (Info Ops) is becoming more critical to our nations with each passing day. Please note that I say, *"a subject critical to our nations"*. I do not specify our military or our political institutions because the implications of Information Operations go well beyond any single aspect of a nation. Information Operations have the capability to reach the core of a nation, to impact the infrastructure, to damage the very things which allow a nation to function as such.

One of the greatest benefits gained through the employment of Info Ops is the ability to prevent a crisis developing into a conflict through means and methods which demonstrate to a potential adversary that escalation of the crisis is not in his best interest. Activities in this regard must be conducted during peacetime, and should be balanced both politically and militarily, based on identified weaknesses and strengths, and to focus on those areas where they can be most effective towards reaching a final objective.

Perhaps the most disquieting facet of Info Ops developments is the fact that there is a general misunderstanding of what exactly they are. Most are familiar with various bits and pieces of the concept, and unfortunately identify the individual pieces as the whole. This is a very dangerous practice, because by focusing on one piece of the puzzle we lose sight of the complete picture which we are attempting to develop, leading to neglect of the others pieces, which in turn provides potential adversaries with options to attack us. It is quite obvious that

The Netherlands recognise the importance of Info Ops as well as its implications. An important indication of this understanding is the bilateral study between the Netherlands and Germany, a summary of the results of which you find in this same publication.

How did we arrive at this point in time with yet another new strategy proclaiming to be the way forward for the future? Did this strategy ‘’du jour’’ spring forth fully developed? Permit me to answer the second question first. Information Operations is not a new concept, it is the result of the evolution of our efforts in the military to develop a systematic approach to warfare. This evolution has been ongoing from the first engagement when one group of men organised to fight another. More modern manifestations of the evolution are found in the concepts espoused by Von Clausewitz in his book, “On War’ where he discusses the principles of warfare. Even more recent is the US concept of Joint Vision 2010, in which a new approach to defining and implementing joint operational requirements is advocated. These, and numerous other attempts to effectively organise the military for maximum effect, plus today’s technology, have led us to our current position.

Before we delve too deeply into Information Operations, I would be remiss if I did not mention the strategy that led to the development of Information Operations, a strategy which was executed to near perfection by the Allies in the Gulf War. That strategy is Command and Control Warfare (C2W). Please indulge my use of the next few definitions to help understand the relationship between Info Ops and C2W.

DEFINITION OF C2W

C2W is defined in MC-348, ‘NATO Command and Control Warfare Policy’ as:
“The integrated use of all military capabilities including Operations Security (OPSEC), Deception, Psychological Operations (PSYOPS), Electronic Warfare (EW) and Physical Destruction supported by all source intelligence and CIS, to deny information to, influence, degrade or destroy an adversary’s C2 capability while protecting against similar actions.”
In other words, C2W means exactly what its name implies, executing actions to prevent an adversary’s leadership obtaining the information needed to make accurate assessments and decisions regarding the control and use of his assets.

C2W Pillars and supporting structure

Figure 1 illustrates how the main five ‘pillars of C2W’ are individual disciplines, yet when co-ordinated and firmly supported by Intelligence and communications, the whole which they produce, C2W, is far greater than the sum of all its parts.

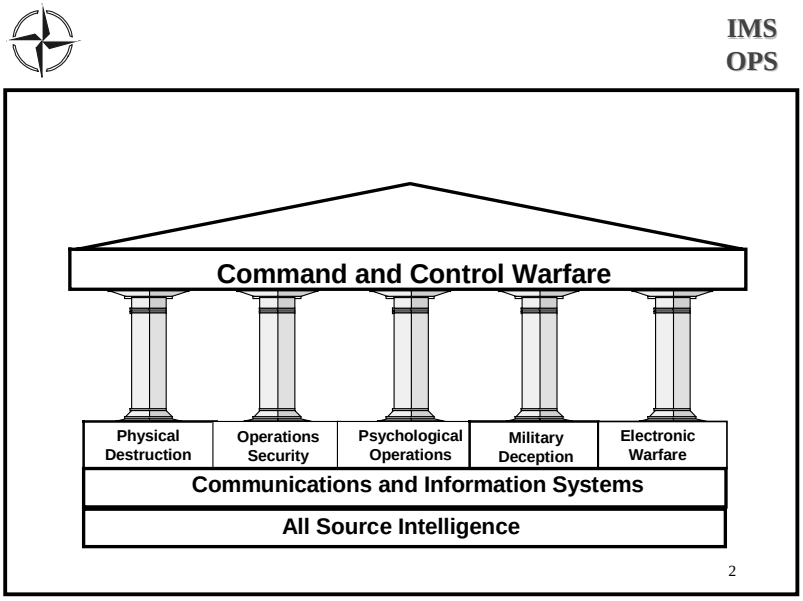

Figure 1: The five 'Pillars' of Command and Control Warfare

Spectrum of conflict

C2W is all about co-ordination. By employing the five pillars, and other military capabilities in a co-ordinated fashion, we achieve a synergy which allows us to operate extremely effectively within the crisis/conflict part of the spectrum of conflict.

Info Ops does not replace C2W, but integrates this military strategy with the political consultation process, decision making apparatus and combined political-military operations of the Alliance. In other words, C2W is a military application of Information Operations. NATO has considerable experience with C2W and executes it quite well. We have had approved policy in MC-348 since 1995, and almost every OPLAN developed since then has contained a C2W Annex.

While the Gulf War is generally recognised as the first Information War, it was not the first employment of C2W in combat. Commanders across the ages have known that depriving their adversary of information is an excellent means to stymie his campaign, while enhancing their own.

How then in this melange of information can we on the one hand prevent critical information getting to our opponent, whilst on the other, stop the opposite effect, information overload, happening to us? A large part of the answer lies in planning at all strategic, operational and tactical levels. But, in today's environment, planning must not be strictly relegated to military planning, and this applies particularly to NATO. Recall how I began this paper, with a brief snippet highlighting the fact that Info Ops has the potential to impact on practically every component of a Nations infrastructure. When you consider the fact that all of NATO's military capability is derived from all 19 Nations, the effect that Info Ops can have on NATO Operations becomes clear. We witnessed, first hand, the effects of a well-directed and

executed Info Ops campaign during Operation Allied Force, …accomplished by our adversary.
Info Ops are concerned with information objectives, which a commander seeks to achieve by his actions. It is therefore a strategy, which is both fundamental and central to a commander's planning of military activities. Info Ops have different impacts at the different levels of war, since the focus of each level is different. At the Strategic level Info Ops are employed in support of NATO objectives. This support is achieved by influencing or affecting all elements (political, military, economic or informational) of an adversary's national power, while protecting those of NATO. The focus of Info Ops at the Operational level is on supporting the campaign or major operational objectives. The major impact at this level is felt by adversary lines of communication, logistics, and command and control. Info Ops at the tactical level supports achieving specific tactical objectives.

At this point it is appropriate to provide a definition of Information Operations. MC-422, which is titled *'NATO INFORMATION OPERATIONS POLICY'*, was approved by the Military Committee on 15 Dec 98 and by the Council on 22 Jan 99. In this document Info Ops is defined as*:"actions taken to influence decision makers in support of political and military objectives by affecting other's information, information based processes, C2 Systems, and CIS while exploiting and protecting one's own information and/or information systems."*
There are two main categories of Info Ops: defensive Info Ops and offensive Info Ops, depending on the nature of the actions involved.

Some of the capabilities used in defensive Info Ops include: information assurance, OPSEC, physical security, counter deception, counter propaganda, counter intelligence, and EW. Offensive Info Ops can also support defensive Info Ops. Information systems serve as enablers and enhance war-fighting capabilities; however, NATO's increased reliance on these systems creates vulnerabilities. It is impossible to completely protect all systems 100% of the time. Therefore we must protect assets relative to the value of the information they contain and the risks associated with the loss, or degradation, of that information. This value will of course vary over time. There are several interrelated processes involved with defensive Info Ops which include, inter alia, protection of the information environment; the capability to detect attacks on systems; the capability to restore systems to use following attack and ability to respond to that attack.

Offensive Info Ops involve the integrated use of assigned and supporting capabilities and activities, mutually supported by intelligence, in order to affect opposing decision-makers and achieve, or promote, specific objectives. Capabilities used to this end include, but are not limited to, OPSEC, military deception, PSYOPS, EW, Physical attack/destruction and computer network attack.

In my opinion, NATO will perform, in particular in crisis response operations, minimal Offensive Info Ops because of the nature of the Alliance itself, which requires the consensus of 19 sovereign nations to approve and implement actions. The different national legal systems of NATO's members complicate this issue, since in some cases, certain Info Ops activities are considered illegal.

WHAT DOES ALL THIS REALLY MEAN?

I believe it means using all the capabilities at your disposal to protect your information, information systems and information-based processes, while you attempt to impact those of your adversary. Some of the capabilities we possess are more adept for use in Info Ops than others, but that in no way diminishes the possibilities that creativity can devise with regards to the employment of assets. When analysing these capabilities there is no more appropriate place to start than those found in C2W: Electronic Warfare, Operations Security (OPSEC), Deception, Physical Destruction and Psychological Operations (PSYOPS). Make no mistake; Info Ops is comprised of much, much more than the five elements of C2W. I would like to highlight one, which is likely to be the most useful during the time when Info Ops will have its most profound effects, i.e. in peacetime. That pillar is PSYOPS.

PSYCHOLOGICAL OPERATIONS.

Our discussion of PSYOPS requires a moment of digression in order to set the stage. As C2W was being exploited by the military, it became apparent that the C2W target set, adversary leadership, presented different opportunities when considered for prosecution at different levels within the adversary's chain of command. That chain of command extends all the way back to the adversary's capital and his civilian leadership. Clearly, the ramifications of employing the majority of the C2W capabilities against a nation at that level, or any level for that matter, could constitute an act of war. But just as clearly, if the adversary's leadership can be affected at that level, i.e. political leadership, an impending conflict might be averted. But, during peacetime, Political Leadership is not a legitimate military target. You can see the dilemma faced by military planners as they continued to develop the C2W process. These farsighted individuals concluded that operating at that level, with all the possible legal ramifications, was beyond the remit of the military and required direction from a level at least as high as the one being attacked. They also realised that this was perhaps a battle for another day, but sewed the seeds of a concept called Information Warfare by defining it in terms of C2W and continued to pursue C2W.

PSYOPS has a special place in C2W and Information Operations for several reasons. Tantamount among them is the fact that it provides the military with the means to influence the adversary's leadership, body of troops, and even the civilian population during peacetime. In spite of this capability, which I view as the bridge between C2W and Info Ops, PSYOPS is so maligned that the mere mention of it in some circles elicits most unfavourable responses. This is especially true within political quarters. This is priority due to a broad based misunderstanding of PSYOPS by both the military and civilian arms of government, and its association with the Special Operations community. Members of these institutions must understand three very important points about the relationship between PSYOPS and the normal release of information to the public**.** First, PSYOPS techniques are used to plan and execute truth projection activities intended to inform Target groups and populations persuasively. (*The targeting is a conscious deliberate and important part of the process.)* The intent of PSYOPS is not to propagandise or lie, but to provide the truthful information or statements at a time which best suit our operational needs. As a matter of fact, lying would be counterproductive, because if discovered all credibility would be lost, making mission accomplishment impossible.

When properly employed, PSYOPS techniques can lower morale and reduce the efficiency of enemy forces and could create dissidence and disaffection within their ranks. Second, PSYOPS and Public Information (PI) releases must be co-ordinated. This is the one major impact which PSYOPS will exert on the flow of information. Timing of the release of information to the public could be adjusted to reinforce the perceptions which PSYOPS seek to establish. Finally, PSYOPS executed in peacetime will have a different focus than when executed during crisis or conflict. Peacetime efforts support typical military operations other than war, such as Peace Support Operations (PSO), humanitarian assistance and disaster relief. During a conflict PSYOPS are used as any other capability to support achievement of the commander's objectives.
The political side of the Alliance should view PSYOPS as a partner with PI activities, not as a competitor, and certainly not as a propaganda machine. PSYOPS is a purely military capability and as such can neither replace nor suborn PI. As I said earlier, the planned and co-ordinated use of PSYOPS and PI, has the potential to prevent the out-break of open hostilities. This fact alone makes it well worth the effort which the political community must expend in understanding PSYOPS and the opportunities produced by it.

Our digression into the PSYOPS discussion was not all in vain. It subtlety brought out another fact, which, in my view, is the most important aspect of Info Ops, that is its potential to prevent competition developing into conflict. Thus, rather than detracting, it provides a perfect transition of our discussion from C2W back to Info Ops.

IMPLEMENTATION

Now as we have seen where the NATO Info Ops concept came from and how we have defined it, I would like to take some of your time to think aloud as to how we might be able to implement Info Ops into NATO's existence. I think it is essential to highlight some fundamental changes which have occurred over the last 10 years, and have significantly affected the way that NATO's military enters and handles a crisis or conflict. These environmental scene setters include technology; the level of political involvement in a conflict; national sensitivities and their impact on resources, and finally, intelligence.

The global technological evolution in the field of information has changed the world. Information not only integrates most elements of modern life, including the civil and military worlds, but also accelerates all processes. The speed, with which we can transmit information, and the volume of that information, was unprecedented just 10 years ago. Today we have the means and ability to pass almost unlimited information to a point of our choosing in a matter of seconds. The miniaturisation of the computer has made it standard equipment, even on the battlefield. Work is already well underway on the development of systems, using real time targeting, where data required is transferred directly to the weapon being employed, sensor to shooter.

Technology is only one of the information operations regimes. Another we touched on briefly in our discussion of PSYOPS. That is the semantics or cognitive regime. The technical portion (that is the physical and logical) is probably understood better than the semantic, because it involves what we are used to, equipment and its employment. While Info Ops focuses on non-kinetic solutions, we must keep in mind that physical destruction, one of

C2W's main five elements, is also an element of Info Ops. The cognitive includes the capabilities found in PI, PSYOPS, and Media Operations

The cold war provided the Alliance with an 'ideal planning situation ': relatively long periods of tension build-up prior to hostilities, known areas of engagement, and known and understood adversaries and their capabilities. The main function of the political apparatus with regards to a conflict was to decide if NATO was to be involved, and if so, declare that involvement. There was comparatively little political interchange with the military once the conflict was fully developed.

Today, as you all know, circumstances differ considerably. But have we, the military, also changed to keep pace with this New World? As demonstrated in Operation Allied Force, the NATO world of today is rife with political involvement throughout the crisis. This means what political involvement has always meant in democratic societies; political authorities control the military. The military must function in the reality created by the politicians. A perfect example of this was the situation arising from the statement, which advised the world that NATO would not employ ground forces in Kosovo. Obviously, this was a purely political move on the part of NATO. The use of ground troops was so contentious that consensus, at the political level, could not be reached and this statement was made to retain Alliance unity. However, I believe that the impact which the statement had on our military operations was profound. The impact of military action on political sensitivities and the implications of political imperatives for the conduct of military operations must be fully understood by both the political structure and the military.

Another variable, which we must bear in mind, are national sensitivities. National sensitivities have always been a major NATO consideration and this is as it should be in an Alliance where all decisions taken are based on consensus. However, in the Cold War days these sensitivities did not impact on the business of Article V type situations, or the allocation of national resources to NATO as much as they do in this, the information age. What this implies is evident. As mentioned before, many of our resources were tailored to meet the requirements of Article V type scenarios, which NATO has been planning for years**.**

Two examples of the more important resources to which I am referring are offensive Info Ops capabilities and intelligence. These capabilities are very carefully guarded by the nations, meaning that they will be hesitant to allocate them for NATO employment.

Another important factor pertaining to national sensitivities and their relationship to the allocation of resources is public opinion. Today combat scenes enter our homes almost without delay; war as seen by CNN is the norm. Obviously public opinion is extremely important to the politicians and will certainly affect their decisions concerning resources.

INTELLIGENCE

The next, and final, environmental change which I will discuss is a bit easier for us in the military to understand and relate too, because we deal with it on a daily basis, that is Intelligence. The planning, execution and assessment of effective Info Ops activities is virtually impossible without the proper intelligence. This presents NATO with a particularly difficult problem to solve, as the Alliance does not possess organic capability to collect and

process the data required for developing intelligence. Additionally, there is no joint Military/Political intelligence apparatus in place in NATO. And to top it all off, the intelligence requirements for Info Ops are different from those traditionally found in the military.

Intelligence must be timely, accurate, usable, complete, relevant, objective and sufficiently detailed to support an array of NATO requirements. In many instances intelligence preparation of the battle space, which is absolutely essential to effective Info Ops, will entail answering a question which we the operations community have never posed to intelligence, the question of why. In the past we needed ‘’just the facts’’, i.e. target identity, defences protecting it, etc. In the Info Ops world this information is not sufficient to get the job done. Let me offer a short hypothetical vignette to clarify what I mean.

Let’s suppose that NATO anticipates a peace support operation in country X. In preparation for the operations an analysis of country X’s infrastructure is completed in search of vulnerabilities and strengths. During the analysis it is discovered that an extremely large and old well providing ground water is the meeting place for hundreds of people each day in country X’s capital. If this well was to be a target in the past, the intelligence required was, ‘just the facts’: location, dimensions, defences etc. Now, if it were to be an Info Ops target, then we would need in addition to these: information such as, why do hundreds of people gather at this well each day. Are they there for cultural or religious reasons or are they just in search of potable drinking water? The answer to this question could provide opportunities for the employment of several Info Ops capabilities and will most definitely impact any operations against this well. So you can see the additional burden which Info Ops places on the Intelligence Community. The resources necessary to answer ‘why’ could be substantial.

Intelligence also contributes to the attack detection process by providing warning and assessment of potential adversary activity and cueing collection to specific activity indicators.

In addition to all this, the operational community must be very precise in describing its requirements to the Intelligence community. They can’t satisfy the new needs if they don’t know what they are and how they are to be used. The first step in developing Intelligence requirements is to determine from where military threats to NATO will come. It is then necessary to determine if that specific nation or group possesses the capability to pose an Info Ops threat.

In short the scene setters for NATO have changed dramatically as opposed to just ten years ago. The military world will not only have to accept this, but will have to adapt as well.

Clearly the situation as described above has a great impact on all military operations including Info Ops. This is especially true at the strategic political/military level. As mentioned before NATO Info Ops should not be considered a new strategy. As they say, old wine in new sacks! But the speed and volume at which we can transmit information and the area of applicability have totally changed information’s overall impact on the political/military interface.

WAY AHEAD

What does all this mean to NATO and how can we take full advantage of the new opportunities offered by Info Ops? Obviously the first step is to develop a plan, a way ahead. For the way ahead it is important to keep in mind all the new conditions under which we must live and operate. Let's summarise some of the highpoints of our discussion to this point.

First we must train our leaders and key personnel to think differently.

We must understand that documentation (policy and doctrine) will not always provide us with the certainties we are accustomed to or are looking for. The current situation and political guidance will dictate how the military acts and reacts in a conflict, and all this will occur within very short time constraints.

One of the strongest lessons taught us by Kosovo Operations is that the military must live in the environment created by politicians. However, politicians must also realise the military consequences of the decisions they take. It is crucial that the political leadership and the military form an integrated front to address Info Ops issues. A military steering mechanism will be needed to fulfil this requirement.

Turning now to the way ahead for NATO Info Ops. The working level structure for day-to-day activity is in place. We now need to develop the appropriate steering mechanism to direct and guide the programme to obtain maximum benefit for the Alliance. To this end we have established the NATO Information Operations Working Group. This Committee is chaired by a Flag Officer (Assistant Director Operations of the International Military Staff, or his deputy), and has permanent members from: the Nations, Strategic Commands (SCs), Legal, Chairmen from functional areas which comprise the elements of C2W, i.e. PSYOPS, International Staff/Political Affairs and The NATO Information Security (INFOSEC) Subcommittee.

During our participation in the development of the Info Ops Campaign for Kosovo, it became apparent that there is no common NATO understanding of Info Ops or the requirements for establishing a campaign. Our Info Ops actions during the conflict aptly displayed this. Developing awareness is extremely important at this juncture. First of all, at the top level, awareness allows Info Ops to enter the thought process of Decision-Makers as they consider approaches to Alliance military and political issues. The earlier this occurs, the more likely it becomes that Info Ops will be successfully woven into the resulting operations. At all levels, awareness enables a broader perspective when approaching day-to-day duties.

We have also accomplished quite a bit on the defensive side of the house, which is managed by the NHQC3S.

The NATO C3 Board (NC3B) has begun addressing many aspects of Info Ops. This focus has been primarily in Defensive Info Ops. It has tasked the INFOSEC Sub-Committee to develop the NATO vision of Assurance of Information. Discussions in this area have focused on the roles of the Military Committee and the NC3B via the INFOSEC SC. Efforts are underway to identify the scope of the work to be accomplished to achieve Information Assurance, and to ensure these efforts are well co-ordinated, especially in the security area, with the Military Committee activities. A paper is in its second revision to address the issues

raised in Assurance of Information, with recommendations as to the Way Ahead. Upon SC approval, this paper will be forwarded to the NC3B for its approval, with the recommendation that the NC3B co-ordinate and advise its sister committees of the actions underway.

In addition, the NC3B has tasked the INFOSEC Sub Committee to develop the implementation plan for a NATO Computer Emergency Response Team (CERT). The NATO CERT will provide relevant CIS users with timely security alerts and advice. The INFOSEC Branch Staff has visited a US operated Regional CERT located in Germany for implementation and operational input. From this visit, and after co-ordination with the SCs and various NATO agencies, the staff began drafting a working paper to identify to the NC3B the scope and resources (costs/manpower) of a NATO CERT. It is expected to provide this Working Paper initially to the Sub Committee and eventually to the NC3B for its approval. The establishment of a NATO CERT will be far reaching, and will impact both military and civilian elements of the NATO organisation.

Again, developing awareness is extremely important. The primary means by which we are attempting to develop awareness is through lectures at the NATO-School SHAPE, Participation in National forums, Professional Seminars, and NATO bodies/agencies/working groups. Our participation in a Symposium at the Royal Netherlands Military Academy, December 3rd 1999, is an example.

Info Ops must become ingrained in the Operational Planning Process. Info Ops are applicable across the entire spectrum of conflict from peace through crisis and war and back to peace. They are given clear political guidance by the Council, and will play a key role when implementing all aspects of the Concept. The production of OPLANS related to the crisis in KOSOVO indicated that this was occurring in the response planning process. We will ensure that this process is codified in the appropriate documents.

Let me touch NATO's obvious dependency upon nations for important capabilities such as intelligence, which are vital to the planning and conduct of Info Ops, as we have seen. Some of the offensive Info Ops capabilities developed by NATO nations is very sensitive and quite expensive, therefore, it appears likely that some Info Ops capabilities, -particularly of the offensive variety-, will not be provided to NATO by the nations. It is therefore prudent for NATO to develop some organic offensive Info Ops capability. It is essential that in the event of a NATO Info Ops campaign, the multinational balance characteristic of the Alliance's composition be reflected. Where possible, therefore, various nations with the necessary expertise should contribute Info Ops resources at all levels.

Info Ops 'peacetime' activities, if discovered by the intended target, may very well be construed as provocative or even hostile, and could therefore require clear political authorization from the Council to amplify specific Rules Of Engagement or planning guidance.

Two of the most important components of Info Ops, the Intelligence and CIS communities, will be heavily involved in determining and addressing the issues of threats to our systems and the vulnerability of our systems to those threats. As a minimum we must determine the critical systems which must be protected in order for NATO to continue functioning.

In order to verify and practice procedures it will be necessary to include Info Ops in NATO Exercises.

The development of Info Ops Doctrine must be initiated soon. Doctrine is a compendium of lessons learned. Operations in the Balkans will certainly provide excellent material for this document. However we should be prudent when developing Info Ops doctrine. Yes we may describe lessons learned, organizational structures, and management tools, etc. but we should not go far beyond that. Remember Info Ops is a way of thinking and not something that can be easily quantified.

CONCLUSION

In conclusion let me reiterate that Info Ops is not new. What is new is the thought process, which Info Ops mandates. Our goal is to develop Information Operations to the point where it is pervasive in NATO Operations.

---

[1] The text of this paper is a slightly modified version of the text of the Keynote Address spoken by Major General Gardeta at the Information Operations Symposium at the Royal Military Academy of The Netherlands, 3 December 1999.

THE GERMAN-NETHERLANDS STUDY ON INFORMATION WARFARE

Lieutenant Colonel (RNLAF) Albert.R. Mollema
Royal Military Academy, The Netherlands

ABSTRACT

From Spring 1998 till Autumn 1999 the German and the Netherlands Ministries of Defence tasked the Amt für Studien und Übungen der Bundeswehr at Waldbröl, GE, assisted by the IABG (GE), the Royal Military Academy of The Netherlands and the TNO Physics and Electronics Laboratory of The Netherlands, to conduct a study which would form the nucleus paper as to assist the MOD's of both nations to identify the problems and possibilities of Information Operations (Info Ops). The study was conducted to define the basic elements of Info Ops and what its implications would be. This article is mainly an excerpt from the chapters of the full study report, to which the author was one of the contributors.

INTRODUCTION

The study's initial chapters mainly lay down the aim of the study, definitions and references and quoting from other studies or Policy Papers as generated by Germany, The Netherlands, USA, and NATO.[1] The study continues to focus on the perceived nature of future conflicts and what this could mean to both nations, focussing on bi-national operations. It further highlights threat aspects, the relationship between military and civil Information Infrastructures (II), and status and trends of Information and Communications Technologies (ICT). Separate chapters deal with the human and legal aspects of Info Ops. The study concludes with a series of recommendations. This article is an unclassified shortened version of the official study.

CHARACTERISTICS OF FUTURE CONFLICTS

The level of modern day Information Technology dictates the need to protect and use one's own information, information-based processes, Command and Control (C2) systems and command information systems (CIS), including public infrastructures. Info Ops capabilities, as may be required in future conflicts, will vary according to the technological advancement of the different parties involved. A typology of future conflict parties, based on their level of technological advancement, is made in this study. For the technological ability to execute defensive or offensive Info Ops, it is important to take into account the degree at which the conflict parties rely on and depend upon information, information-based processes, C2 systems and CIS.

During the past 50 years, the number of conflicts in the world has increased from approximately 4 per year in 1945 to over 40 per year in 1995. This increase is largely due to the growing average duration of conflicts that went up from an average of 2 months in 1945 to 14,5 years in 1995. Approximately 80% of all conflicts were of an intrastate nature, and the

number of victims was generally low. (With the exception of the Iran – Iraq War, which counted many victims).

Since the end of the Cold War, causes for conflicts have changed. Interstate- or even inter-block (potential) conflicts dictated force structures of most western nations. Territorial disputes and ideological and economical competition were understood as main causes for conflict. In the last decade, ethnicity, nationalism and religious fundamentalism have played an increasingly important role in intrastate conflicts. Because of the wide range of issues involved, a multi-dimensional approach to conflicts is required. Urbanisation in developing countries will increasingly cause conflicts to be fought in urban environments. Each intrastate conflict creates streams of refugees, which mostly settle down as close to their native land as possible. Such areas are typically struck with violence and/or large-scale medical problems. Finally, the repatriation of refugees after conflicts have ended, have the potential to cause new conflicts in the future.

REGULAR AND IRREGULAR CONFLICTS

The intrastate conflict typically has the characteristics of an irregular conflict, as opposed to a regular conflict. Irregular conflicts have the following characteristics: They are about freedom, identity, nationality and power of certain population groups against others or against a (legitimate) government. It may translate into a struggle for (part of) the State territory (autonomy or independence) or for power within the State. Anarchy and chaos characterise the irregular conflict. Largely disorderly groups instead of regular troops do the fighting, with only limited or even no central authority while often using guerrilla-like tactics. The warring factions are prepared to fight for a long duration and accept large losses in order to achieve their goal. Every citizen may be a warrior. In many cases this simply means civil war. Agreements among conflict parties are laboriously made and often violated. This is also applicable for the law of war and cease-fires. The fighting is often done from a position of military weakness, which leads to unorthodox means of combat, with mobility and lack of co-ordination as main characteristics. There are no fixed operating lines and the notions of ”in front” and ”behind” are gone. Armed actions are aimed to create confusion, and vary strongly in scale. The level of violence varies. In many instances, the fighting is done with light, less advanced arms. However, heavier armaments and even very advanced weapons, including weapons of mass destruction, may be employed.

TYPOLOGY OF TECHNOLOGICAL ADVANCEMENT

Technology has always played an important role. Conceptual thinkers like Van Creveld and the Tofflers have done some considerable work on identifying the relationship between conflict and technology. Without falling into the trap of the ‘chicken and egg’ discussion, both argue that technology has and will play a decisive role. For Van Creveld, future conflict will be decisively dominated by automation. He argues that mankind has developed from the ‘age of tools’ via the ‘age of machines’ and the ‘age of systems’ into the ‘age of automation’. The need for information and the requirement to control and command makes the effectiveness of the Armed Forces dependent on automation. Technological developments become part of military thinking and cause change of concepts, doctrine, organisations, and operations.

For the Tofflers, information is the critical factor. To them conflict mirrors the changes in labour and welfare. Mankind has gone through three waves of change. After the agricultural revolution and the industrial revolution, we are now witnessing the information revolution. Since (civil) society is increasingly relying on knowledge, future conflict, by consequence, will be about knowledge. It is important to note that different societies probably have reached different levels of technological development. This in itself may cause conflict, but it certainly will influence the way in which conflict is conducted.

TYPES OF ARMED FORCES

Using the level of technological advancement four different types of forces can be identified. These are:

Armed Forces of the industrial age being on the threshold of the information age.
These forces have all the capabilities of the industrial age and can typically rely on a broad (national) arms industry. They are basically in a position to develop information age capabilities, if they have not already done so. This is the case for the US, followed by most of the Western European Nations that are member of NATO.

Less developed Armed Forces of the industrial age
These forces are characterised by a limited arms industry, although they may have a strong industrial base. Their armaments requirements are mainly met through the purchase of equipment. In principle, they are able to operate weapons of mass destruction, in particular biological and chemical weapons, and possess simple means of delivery. They can utilise dual use technologies, especially in the field of communications, navigation, and reconnaissance.

Poorly developed Armed Forces of the industrial age
These forces lack not only the industrial base but to a large extent also the economic prerequisites for the development of industrial age capabilities. They usually have proliferated capabilities and use weapons and systems which operation and maintenance do not require much effort and training. These forces can acquire certain Info Ops capabilities, e.g. by purchase on the free market.

Non-governmental adversaries
These ‘forces’ comprise groups such as partisans, guerrilla fighters, insurgents, terrorists, organised crime groups as well as mercenaries. Their capabilities will primarily depend on their objectives, as well as on resources which are either available to them or which are made available by third parties. The technological capabilities will usually be those of the poorly developed Armed Forces of the industrial age, although some may be more sophisticated.

ASSESSMENT

The more advanced industrial age nations will be able to implement, already in the short term, selected capabilities of the information age in certain sectors of some key areas. In the coming 20 years, mixed forms can be expected, ranging from Armed Forces, which have not yet reached the comprehensive capabilities of the industrial age to those, which have made some

progress on the way to the capabilities of the information age. Additionally, there will be an increasing number of non-governmental adversaries that may have a mix of low and high tech capabilities.

Armed Forces of the industrial age are characterised by mass employment of troops, weapons and ammunition. The main shortcomings of this type of Armed Forces - as compared to the Armed Forces of the information age - are the insufficient reconnaissance and target identification capabilities, information processing limitations, which only allow for rough co-ordination of activities of different Armed Forces elements, as well as quantitatively and qualitatively insufficient precision weapons.

In order to gain or maintain the initiative, parties to a conflict need to make better and faster decisions than their adversary. Information age forces do heavily rely on the developments in ICT that will speed up decision-making, enabling forces to respond faster. Generally it is thought that information age commanders will have (the means for) full operational awareness. However, seeing everything does not mean understanding everything. Especially in a-symmetric conflict, intentions of an opponent may be difficult to comprehend

It may be considered that German and Netherlands Armed Forces are on the threshold of the information age and do belong to the group 'third wave countries'. Nations that form part of this group are the relatively most prosperous and must be prepared to be engaged in a-symmetric conflicts. Less developed opponents may believe that changing the status quo can only be in their favour. Since knowledge is not only controlled by the State, the likelihood of non-governmental adversaries taking part in conflict increases. Hence, intra-state conflict will become more likely.

Although technological advancement may fascinate us, one should not forget that conflicts are determined by human behaviour that is complex and often unpredictable and irrational. ICT knowledge is widely spread and may be a "poor mans" weapon against more sophisticated opponents. Defensive Info Ops capabilities are therefore a necessity

TRENDS AND TENDENCIES

In general, there seems to be a tendency towards a-symmetric intrastate irregular types of conflict. In order to resolve this these types of conflicts, a multi-dimensional long-term commitment seems to be required. Military means do not by itself provide a lasting solution but are required to create a situation in which other institutions and agencies can work towards a political solution. The different nature of defensive and offensive Info Ops capabilities may be characterised as follows:

Offensive Info Ops capabilities focus on the adversary's information, information-based processes, C2 systems and CIS, and must therefore be tailored to the adversary-specific technological advancement as well as the conflict-specific characteristics.

Defensive Info Ops focus on the protection of one's own information, information-based processes, C2 systems and CIS. One needs to take into consideration that this protection should be of concern with every type of adversary and within every type of conflict, and that one's own Armed Forces must be ready to fight any adversary in any conflict at any time.

In conclusion, there is a tendency towards a-symmetric and irregular conflicts, where the use of Offensive Info Ops as well as Defensive Info Ops capabilities will be very much situation dependent. This means that if we want to be prepared to: *"(….) be ready to fight any adversary in any conflict at any time….., it follows that…., from an Info Ops point of view the most demanding option is (to be) selected (…) with regard to equipment, doctrine, and operational concepts (…...)."*[2]

ASPECTS OF INFO OPS IN THE MILITARY AND THE CIVIL ENVIRONMENT

One needs to have a clear understanding about the role and impact of information and information technology in modern military C2 systems and C2 processes. It is equally important to realise the degree as to which the modern military C2 infrastructures are dependent upon civil communication networks and technology, in other words, the interdependencies. This includes the role of the media, which play an important role of psychological warfare. Finally, this must result in some kind of 'risk analysis'.

Information Operations and supporting technologies provide new opportunities for military planners and commanders. Information processing systems and networks are much faster and can process much more information than was possible in recent past. At the same time, military and civil systems have become increasingly vulnerable to deliberate and accidental loss, and/or alteration of data. From the military point of view, it is important to consider the risks of data being lost, deliberately manipulated, passively collected, or (maybe worst of all) of data overload.

Only when there is a certain level of 'confidence' in the mind of the decision-maker, one does not need to refer to (dangerous) 'intuitive' decision-making. The overall purpose of any C2 system is essentially to **reduce 'fog and friction'** as much as possible, while at the same time providing the commander with the means to properly **retain command.** Military information functions are there to 'cycle' faster through one's own decision cycles than the opponent does, in other words the well-known Observe-Orientate-Decide-Act loop ('OODA'-loop).

Apart from all aspects above, the military, as a human being, is in and of itself 'part of the problem'. The study calls this **'the human factor'**. It requires a new 'mindset' in terms of adapting to rapidly changing circumstances. The quality of information is directly dependent upon integrity, accuracy and timeliness. The interrelationship, convergence and interdependence of civil and military networks in the widest sense of the word are growing, both in terms of information and management. 'Cyberspace' is not a military sanctuary. It is this 'space' where the military share the 'info sphere' with the civil realm. This means that threats and risks can no longer be defined in purely military terms. The distinction between military and civil targets is rapidly disappearing. What are the risks? How can we assess those risks? Figure 1 provides some examples of the existing interrelationships; it also indicates the risks to be assessed.

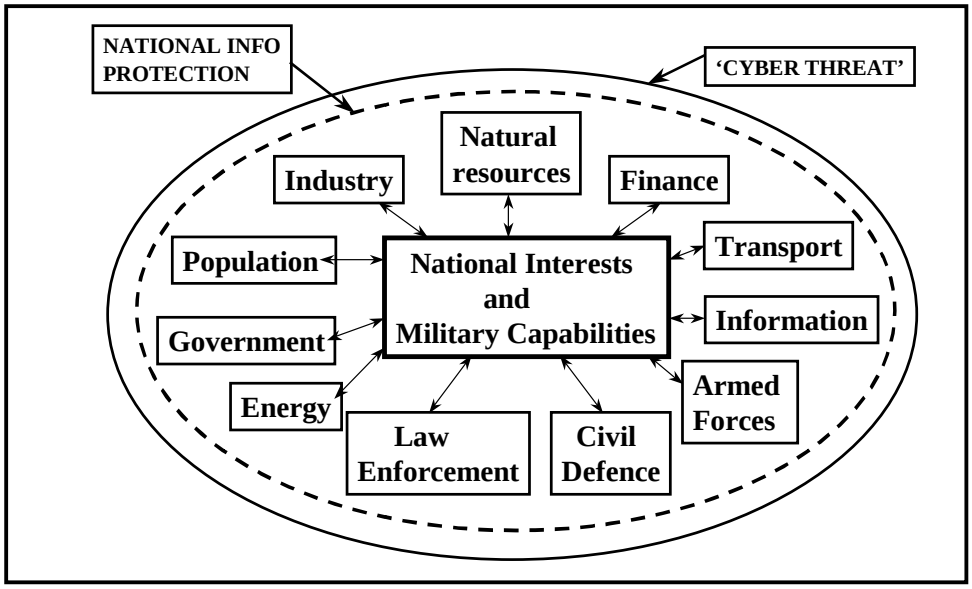

Figure 1: Risks in a Civil / Military environment

The military, being part of society, is under threat of 'cyber attack' just as any other segment of society. It essentially depends on what the 'cyber attacker' decides to be his target or '**cyber centre of gravity'**. Protection is obviously needed. This means that detailed analysis and assessment needs to be made as to what are perceived to be the most attractive targets. The study finds that the task of assessing the risks is extremely critical in terms of the overall dependency on the respective global-, national-, and defence information infrastructures (GII, NII, DII). At the same time the operational and technical aspects are extremely complex as well.

During all phases, from conception to fielding and throughout the **operational lifetime of a system, a thorough assessment has to be made as to what the purpose of information and communication related technology is;** for example:

- What level of security is required?
- What is the sensitivity of the information to be handled?
- Does it require or justify 'stand-alone', dedicated military networks or systems?
- To which level do we integrate with civil systems?

This risk management process needs to be done on a continuous basis. Various studies show that this process either does not take place, or that one refrains from taking the measures as a consequence of the risk assessment. Once a system is fielded, it should also be checked and verified for unauthorised use. In conclusion; Info Ops systems security risks are a clear and present danger. Security has the potential of being the weakest link. Above all, we need to realise that risk assessment is a critical and indispensable phase in the process of defining Info Ops requirements, as it is a continuous process while operating Info Ops systems. Assessing the risks is a never-ending business!

THE TECHNOLOGICAL DIMENSION

One chapter of the bilateral German-Netherlands Info Ops study deals primarily with the technological aspects of Info Ops, both from its offensive as well as from the defensive aspects. The result is a form of (technical) 'risk assessment' that eventually leads to security requirements for systems, interfaces and tasks. The more complex systems are, the more difficult or even impossible it is to prepare integrated ICT security concepts. Some critical elements are discussed here.

Interoperability

In joint and combined coalition forces (e.g. a Combined and Joint Task Force), interoperability plays a major role. Interoperability is important and takes place at different 'levels': means, organisation, tactics and doctrine. Technological interoperability levels (means) that can be distinguished are: component interoperability, format interoperability, content interoperability and usage interoperability. At all these 'levels' of interoperability between joint and combined coalition forces, the resulting information flows are of great interest to an Info Ops adversary.

Vulnerability Analysis

Vulnerability analysis aims at identifying existing vulnerabilities of potential targets, at assessing the potential impact of an attack and at defining required countermeasures. To assure timely availability and reliability, it is crucial to investigate the vulnerabilities to Info Ops attacks along the four phases of the C2 cycle ('OODA-loop'). All elements of the intelligence collection and reconnaissance processes as part of the situational assessment phase will be essential targets for offensive Info Ops. They permit the influencing of the command and control and decision-making process. The same is true for all those elements that are associated with the (further) processing of the information. While interfering with data digitally transferred via fixed networks requires the capability to penetrate those networks, information transfer via radio and microwave may be selectively disrupted, jammed or, in case of inadequate cryptographic protection, manipulated by feeding in false information (e.g. using Electronic Warfare means).

Apart from these types of attack, there are attacks possible that are launched either in support of the just-mentioned types or directly on the information processing capabilities itself. This requires precise knowledge of the architecture, the hardware and software in use, and the capability to intrude the adversary's CISs, and supporting information infrastructure. Such attacks result in an impairment of the information situation. Decisions may be delayed, owing to delayed or unavailable information. Decisions may also be led in a particular direction by using deception to produce a false situation picture. To ensure own command capabilities, particular attention is paid to the protection of one's own (Joint/Combined) information collection and reconnaissance capacities. At the same time, a capability should be developed to suppress hostile reconnaissance. The combination of these capabilities results in an information advantage over the adversary in terms of both time and quality.

The study provides an in-depth analysis of such aspects as processes, basic structure, the acquisition of ICT-systems (commercial-off-the-shelf or not), interoperability aspects and of course vulnerability analyses.

THE HUMAN FACTOR

Apart from information gathering operations, the main target of an offensive Information Operations campaign is not the specific systems that are actually attacked, but rather the adversary's decision-making process. **Ultimately, the target is the human "system" as decision-making unit**. The offensive Info Ops primary goal is to influence the decision-maker's knowledge, beliefs, mind and will in order to reduce their will and ability to decide and fight, and to disturb the decision-making process in order to create incorrect decisions

The Human Element In The Command And Control Process

Defensive Info Ops not only deals with pro-active training & instruction and other protective measures to counter offensive Info Ops aimed at the human as part of the decision-making system. It also deals with issues of making effective use of the new information means while avoiding human factor pitfalls like micro-management, fixation on the current battle, information overload, and transfer of intent in a much stronger way than ever before. Finally, the human element plays a role in communicating the decisions. Whereas ICT may provide an important means of communication one should not ignore the aspect of credibility, which may require a face-to-face situation. Defensive Info Ops also deals with issues of making effective use of the new information means while avoiding human factor pitfalls like micro-management, fixation on the current battle, information overload, and transfer of intent in a much stronger way than ever before.

Offensive Info Ops is primarily aimed at influencing the decision-making, beliefs, mind and will of the opponent, in order to reduce his will and ability to decide and fight, and to disturb the decision-making process so incorrect decisions are made. To influence the adversary's information flow, means as for instance deception, disturbance and/or delay of information flows, information overload, increased uncertainty (e.g. by affecting integrity) and Psychological Operations (Psy Ops) can be used. The Info Ops targeting can be directly aimed at the politico/military decision-making unit and/or indirectly to the public opinion (the 'society') behind the decision-making unit.

Four different groups of people are involved in the politico/military decision-making processes: analysts to collect and process information, politico/military decision makers, the military chain of command to communicate decisions and act, and society as a whole which influences the mind-set of the humans within the decision loop.

Human intuition plays an important role in the process of information gathering, analysing, sorting / prioritising and processing. It is a role that cannot be automated. Furthermore, human intelligence (HUMINT) has a major role in addition to the more technical sources of intelligence. The brain activity and decision making process of the politico/military decision-makers involves, apart from information (facts, knowledge, state and objectives), many psychological influences. Decisions in western societies are based on legislation, generally

accepted ethics and public backing (state of mind, beliefs, will). The outcome of an adversary's decision-making process in another culture (e.g. non-democratic or fundamentalist) might result in a completely different decision when faced with a similar situation.Finally, the human element plays a role in communicating the decisions. Whereas ICT may provide an important means of communication one must not ignore the aspect of credibility that may require a face-to-face situation.

Bottom line is: Which information, which processes and which systems are critical for any particular operation?

THE LEGAL ASPECT OF INFORMATION OPERATIONS

The study devotes one chapter to the legal aspects of Info Ops. From a legal point of view, there is a very close relationship between the active performance of offensive Info Ops and the reacting part of the 'victim', who is using defensive Info Ops, or is verbally accusing his opponent of being the aggressor. These generally contrary positions are 'two sides of the same coin'. State 'A'does not have a legally based position to accuse State 'B' of violating its rights of sovereignty by Offensive Info Ops activities, if State 'A' itself wants to use Offensive Info Ops as the first user. This case has to be clearly distinguished from the generally admissible right of reacting by self-defence.

Info Ops And Domestic Law

Questions of domestic security and the protection of internal legal positions are the responsibility of the respective State itself, i.e. the State's own domestic (and mostly private) ICT infrastructure. If this domestic ICT infrastructure should become an object of legal protection, every State may carry out all legislative procedures to create a legally protected position. The scope of legislative measures concerns especially the fields of penal law and civil law. The German Penal Code, for example, contains a number of protected positions, respective forbidden activities, referring to criminal acts, committed by the use of computers. Nevertheless, the greatest disadvantage of domestic law regulations is - if there are no additional international regulations - the geographical limitations of the State. International crime - and the possible misuse of Info Ops may be a part of it -, its detection, prosecution and final defeat are an increasing legal problem in the ever-globalising world, where boundaries in their conventional understanding loose importance more and more.

Info Ops And International Law

Info Ops as a new, but integral part of modern have to be integrated into the well-established system of the existing and applicable international law. A new and 'uncommon' and non-physical (military) means does not automatically require new international regulations. In other words: No provision of international law explicitly prohibits what is known as Info Ops. Referring to international law, there are three qualitative legal steps by which the own legal position may be violated by Info Ops: Aggression (armed attack), intervention and the 'ability of States to hurt each other'. The quality and intensity of the Info Ops 'disturbance' determines the respective level and sets the scale for the possible reaction. In general terms it

may be stated: The more intensive the Info Ops disturbance is and the worse the damages are, the more a State has the rightful justification to react accordingly. **The fundamental legal rules of necessity and proportionality also have to be respected, as the distinction between civil objects and military targets should be respected**. Finally the Info Ops aggressor needs to be identified clearly.

Info Ops And The Link Between Domestic And International Law

A limitation for the intensity of reaction is always to be seen in the respective domestic constitutional law. What may be advisable in the international relation does not automatically need to be permitted under domestic constitutional law and requires. For example, an additional domestic legislative act (like the Deutsche Bundestag, the GE Parliament, constitutionally needs to vote separately for each mission of the Armed Forces well ahead of force employment). Domestic law and international law often are linked together; they don't exist completely independently from each other.

Implications

ICT infrastructures are partly protected by clearly defined domestic legal positions. International conventions in the field of telecommunications, satellites etc. also protect private and government-driven public ICT infrastructures. The observance of the written law and a certain number of regulations do apply. This enables to act on the basis of repression, after an incident has happened (civil law, partly penal law). Averting dangers, a classical police task, is not their regulation. There is no specific responsibility and competence of any national ICT agency to act on the basis of prevention. This gap of responsibility should be closed by an agency like the ICT emergency/incident response organisation. The existing protection is very selective, hence limited. Previously, it was designed to meet the needs of then existing technology. The 'more and faster' developments and evolution of ICT-related technology and systems show the need for new laws and regulations.There is a need for international regulations to simplify the identification of a potential aggressor on the other side of the 'border'. An international penal competency and responsibility, which allows prosecution and punishment of respective suspects would be helpful. The non-physical parts of the IT infrastructure are very difficult to classify in a legal way. If the whole 'cyberspace' could be declared to be an international legally protected entity (with legal responsibilities and validity for everybody), like the High Sea or the Outer Space, the protection could be handled much easier, free of national peculiarities. It is obvious that, for the time being there are more questions than answers around 'cyberspace'.

THE CONSEQUENCES

One of the most difficult things to do is to describe and assess future trends concerning the Info Ops threat. In the short term, these trends can probably be best described in terms of 'more and faster' of the information, knowledge, technology and systems that are currently available. One can expect that some of the major areas of future interest to the military are the growing need for more data collection, information handling, and smart filtering and storage

capabilities. This includes an increasing use of “internet” and “intranet” capabilities, combining both military and non-military information sources and means.

STATUS OF INFO OPS CONCEPTS

With a few exceptions, most nations did (not yet) develop substantial conceptual thinking in the area of Info Ops. Issues such as Electronic Warfare (EW), Psychological Operations (PSYOPS), Civil-Military Interface and Co-operation (CIMIC) were mostly dealt with on a case-by-case basis as individual needs developed over the time. It was the NATO Command and Control Warfare (C2W) concept (MC 348) in 1995 which triggered the first activities in some NATO nations to develop a basic national C2W-policy and to establish requirements along the lines of the C2W-concept. It now appears that only after NATO started the developments which led to the publication of the Info Ops Policy (MC 422) in early 1999, the necessary attention was drawn to the Info Ops threats, vulnerabilities, defences and opportunities in most NATO nations.

CURRENT TECHNOLOGY AND FUTURE TRENDS

The reluctance to think about Info Ops conceptually is most likely driven by fear of this ‘unknown world’. At first sight, it seems to be an area with no clear boundaries in terms of concepts, technology, civil-military co-operation, or rivalry. The C2 technologies are developing so rapidly, that the best technology of today seems to be obsolete tomorrow. On top of this, a general lack of knowledge and awareness, as well as a certain degree of conservatism in military organisations are factors of influence. Even in the civil environment, where competition is a stronger driver for ICT than usually in military and other governmental organisations, it appears to be extremely difficult to keep pace with changes in and threats to the ‘ICT-world’. It is a fair conclusion that government agencies, including the military, are at best able to ‘follow’ the commercial market rather than setting the pace.

THE CIVIL-MILITARY ENVIRONMENT

Military Info Ops measures cannot be studied isolated from political necessities and sensibilities. Therefore, they need to be imbedded into existing national laws and regulations on the one hand, and in those of allied or associated countries on the other hand. The task-spectrum may require additional measures for example in the field of Civil Military Co-operation (CIMIC). A national legal environment must be created in a manner, which allows the preparation of defensive Info Ops already in peacetime while avoiding undermining the freedom of civil data-traffic (economy / individual) and its protection. To grasp this problem, one requires extensive discussion involving every ‘connected’ part of society such as political, diplomatic, economic, military, commercial and technical representatives, to name a few.

The term ‘defence’ can no longer be understood being limited to lethal-weapon activities. As a matter of fact, Info Ops developments have brought in a new quality of warfare. The above-mentioned interdependency between the civil and the military segments of society will have to lead to a new basic (and legal) understanding and definition of the terms ‘crisis’ and

'war'. By keeping bi- or multi-nationality in mind these definitions are to be developed accordingly, incorporating all affected institutions.

READINESS EVALUATION

In order to assess the readiness of own Forces against Info Ops attacks, two basic measures should be taken. The first is risk analysis and auditing of military information infrastructure. Secondly, the Armed Forces should have an Info Ops capability, able to either covertly ('Red Team') or openly ('Green Team') attack one's own Info Ops defences in order to assess preparedness. Experience and knowledge of these 'attack cells' can be used for both obtaining intelligence data and for taking counter-measures in so called 'Blue-Team-Operations' by assisting the incident response team during an adversary's Info Ops attack.

ORGANISATIONAL STRUCTURES

The complete range of existing C2- and Information systems as well as specialised Information Systems needs to be ascertained and secured. Examining those systems in terms of operational tasks, design and effectiveness (quantitatively as well as qualitatively) will be the next step. An additional subject of examination will be the possible existence of similarities of information systems on respective levels of command. As a result, unnecessary redundancies are to be identified and eliminated. A new basic infrastructure has to be defined While maintaining necessary flexibility, this infrastructure should be able to accommodate future extensions. Vulnerabilities need to be limited and the expediency of systems to be enhanced. Allocation of functions and personnel to military organisational areas and elements must occur on a mission-oriented basis, and be reflected in all sub-systems and respective levels of command. Info Ops need to be understood as an integral part of the combined military planning and –execution cycle. Hence, the establishment of organisational elements like an Info Ops Cell (IOC) needs to be performed as a joint effort, organised under a Joint Forces Commander (JFC) to assure unity of command.
These structures are complementary to the static organisational build-up and comprise all measures that deal with the information flow inside C2- and Information Systems and between the systems. The aim is to provide timely information that meets appropriate standards in 'quality and quantity'of protection against adversary's Info Ops. Continuous risk management must take into account the growing degree of inter-linkages and data-flow between military and civil users. The leadership-principle (i.e. mission-type tactics or detailed order-tactics) has an impact on both static as well as dynamic/process- driven organisational structures. Effective Info Ops planning and execution require an understanding of 'Information Situation Awareness', including such aspect as a 'Recognised Information Picture' (RIP), which encompasses a 'Recognised Intrusion Picture', similar to recognised, air-, land-, or maritime pictures.

DOCTRINAL ASPECTS

The combination of modern C2 means with harmonised procedures and command structures (alignment of the C2 process) provides the opportunity of gaining a good quality of information on all levels of command. The organisational availability of this information as

well as its use can be positioned either centralised or decentralised. Centralised availability of information is related to highly automated C2 processes. **The aim is to maintain an extensive political and military control of the events in the area of operations**. The basically positive character of appropriate control may lead to the phenomenon of micro-management by passing down commands, disregarding existing levels of command. This might endanger the leadership principle of mission-type tactics. Successful leadership will largely depend upon the degree of technical readiness.
Decentralised processes do appreciate creativity and leadership ability. Decision-making processes are based upon a high degree of autonomy and reduce in their consistent application the system-vulnerability through limitation of command-levels and flow of information. This however does not automatically exclude direct influence in (preferably clearly) defined cases of absolute necessity. However, it must be kept in mind that the successful application of this concept is highly depending upon the abilities of both leader and the personnel led; this aspect must be reflected in respective training-concepts.

TRAINING, EDUCATION AND EXERCISES

The numerous threats, the desired offensive Info Ops capabilities, as well as mission-type tactics require a high standard of training and education. Hence, the aim of all related measures must be to achieve:

- Individual willingness and ability to accept responsibility,
- The ability to delegate,
- The generation of a high degree of sensibility concerning the potential adversary's Info Ops capabilities,
- An acceptance for the necessary information security (Info Sec) measures,
- Willingness to acquire an adequate degree of capabilities in technical handling of ICT-equipment,
- A basic education and training towards ones individual psychological stability to counter the adversary's doctrines and procedures.

The latter deserves particular interest in cases of Peacekeeping and/or Peace-enhancing measures within UN-missions. In addition to this, nationally performed exercises must whenever possible incorporate CIMIC-elements.

INFO OPS ASPECTS IN COALITIONS

There are several aspects of Info Ops (opportunities as well as vulnerabilities) that go well beyond the national level and are unique to Armed Forces in coalitions.
The benefits of coalitions lie in the combination of the Info Ops capabilities of the different partners, thus giving a wider variety of options and tools into the hand of the military commander. On the other hand, new vulnerabilities may arise; existing vulnerabilities might be multiplied in the coalition environment.

Info Ops -Threats in Coalitions

Even if each participating nation has successfully adapted itself to the Info Ops-challenges, frictions still exist (or new ones can arise), when Forces join in a coalition. These frictions, which are inherent to coalitions, stem from various sources:

- **human aspects**: There may be tensions between participating nations, originating from historical, cultural, religious or ethnic backgrounds or language problems.
- **technical aspects**: Interconnections of the various ICT-systems may cause possible weak points.
- **organisational aspects:** Differing Force structures, C2-structures or principles of leadership (mission -type vs. order-type tactics) may hamper effective Info Ops of the coalition.

An opponent will try to detect and to exploit these weak points by aiming his Info Ops-measures at them. Target is the coalition decision-making structure in the military/technical sense and the cohesion of the coalition in the psychological sense.

RECOMMENDATIONS FOR THE WAY AHEAD

Defensive Info Ops

Threats and vulnerabilities related to the use of ICT were discussed. In order to counter these threats and vulnerabilities, and to meet the foreseeable future developments, effective defensive Info Ops capabilities are to be acquired. These include the survivability of large-scale systems like the recognised intrusion picture, recognised information picture, adaptive systems and high confidence systems. One major prerequisite for an adequate Information Assurance is the establishment of an ICT emergency/incident response organisation that is available on a 24 hour, 7 days a week basis. Apart from the respective national role, such an incident response organisation should link into NATO’s Computer Emergency Response Team (NCERT) as well as defend the security posture of multinational collaborations. Nationally, it is advisable that all military Services establish organisational structures or have at least Info Ops billets within operational units.

Information Assurance is to become a natural ‘state-of-mind’ within the Armed Forces. In order to maintain the Information Assurance posture of the nation and/or multinational coalition, a timely and accurate recognisance of asymmetric Info Ops threats is required. This gives the Services time to take appropriate Info Ops precautions and be able to prepare counter-measures in case of an attack. Adversary's Info Ops reconnaissance efforts should be detected, analysed, and understood. This requires an effective combined Intelligence - Info

Ops knowledge cell. Information Assurance should therefore be considered as a common interest to all NATO countries.

Offensive Info Ops

Active offensive Info Ops capabilities should be developed in the case the Netherlands and/or Germany come to a decision regarding their requirement. When deciding to develop such a capability, the spectrum of offensive Info Ops capabilities already acquired by the other NATO partners must be taken into account. Additionally, the (inter)national legal offensive Info Ops operating-space is to be clearly defined. Existing legal restrictions should be examined in order to gain a solid judicial foundation for the employment of effective Info Ops whenever required by the respective government.

ORGANISATIONAL RECOMMENDATIONS

Concepts and Doctrines:

Info Ops policy documents to cover defensive-, as well as offensive Operations are to be published to aid in clarifying terms, definitions, and responsibilities. A Joint Info Ops doctrine should be published and kept current. This doctrine should include a clear view as well as predefined structures for Joint/Combined Info Ops. All services should implement the Joint Ops policy and doctrine at the same pace and intensity.

Use of Commercial-off-the-shelf (COTS) Systems:

The use of **commercial-off-the-shelf** systems as well as interoperability should be driven by an operational necessity, balancing Information Assurance, survivability, flexibility, availability, performance, costs and residual risks.

Military Organisational Elements

As Info Ops should be an integral part of all joint and combined military operations it requires extensive planning and co-ordination among many elements of the joint headquarters, component staffs and other agencies. One organisational element able to combine all these activities and to develop guidance and plans for Info Ops might be an Info Ops Cell (IOC), formed by representatives from each staff element, component, and supporting agencies responsible for integrating capabilities and related activities. The IOC merges capabilities and related activities into a synergistic plan. The IOC co-ordinates staff elements and/or components represented in the IOC to facilitate the detailed support necessary to plan and co-ordinate Info Ops. Figure 2 provides an overview of a possible joint IOC.

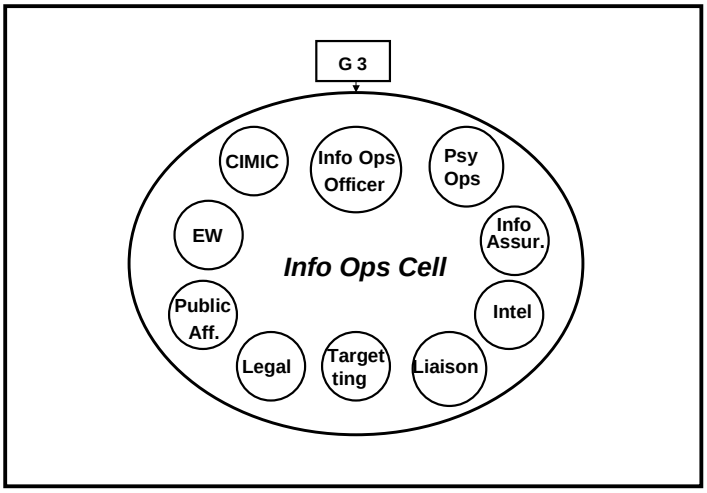

Figure 2: Composition of an Info Ops Cell (IOC)

Co-operation of Civil/Military Info Ops related institutions

The Ministries of Defence directing the Armed Forces do have the opportunity to play an important role in increasing the Information Assurance awareness of other governmental and public authorities. Defensive Info Ops knowledge should be shared among Armed Forces, civil defence organisations, national command structures and the critical industries (energy, transport, communication, etc.) as long as the military security necessities can be preserved.

The increasing convergence and entanglement of military and civil information infrastructures and the requirements for a national defensive posture in order to protect society against adversary's Info Ops, require Information Assurance efforts with respect to a Minimum Essential (Defence) Information Infrastructure (ME(D)II). The risks of information flows in coalitions being dependent on the availability and integrity of civil information infrastructures should be well understood and wherever possible reduced. Critical functionality should be recognised and safeguarded. The Defence component of the MEII should be regarded as a support element to civil authorities and critical economic functions, both in interest of one's nation and in support of NATO and the European Union).

RECOMMENDED LIST OF ACTIONS

The Study Group produced the following action list:

- Establishment of a centrally controlled Information Assurance capability
- Provision of adequate manning/billets.
- Exploitation of existing Info Ops knowledge.
- Creation of a pool of reserve personnel having Info Ops knowledge and experience, or having ethnic, religious and cultural backgrounds (PSYOPS, CIMIC).

- Development and maintenance of a National Info Ops policy (based upon NATO MC 422) and a Joint Info Ops doctrine.

- Simultaneous Implementation of the Joint Info Ops Policy by all Services.

- Acceptance of the permanent requirement for national and international research in the areas of Info Ops, Information Assurance and critical infrastructure protection.

- Achievement of Info Ops awareness-building through integration into existing command structures,through education, study and further research.

- National definition of the desired offensive Info Ops capabilities taking other NATO nations' capabilities into account.

- Definition and harmonisation of existing national and international laws and restrictions.

- Consideration of operational necessity, balancing Information Assurance, survivability, flexibility, availability, performance, costs and residual risks concerning necessary COTS procurement.

- Establishment of Info Ops cells on Joint and Combined levels.

- Definition of a Minimum Essential Information Infrastructure, national-, bi-, and multinational. Due to the fast changes, this requires re-examinations at regular intervals.

- Installation of interagency working groups including all relevant sectors of the societies.

NOTES

[1] NATO documents:

MC 422 *NATO Information Operations (Info Ops Policy)*, 18 Dec 1998

MC 348 *NATO Command and Control Warfare (C2W) Policy*, 12 Oct

MC 402 *NATO Psychological Operations (PSYOPS) Policy*, 7 Apr 1997

MC 411 *NATO Civil-Military Co-operation (CIMIC) Policy,* latest edition

MC 64 *Electronic Warfare (EW) in NATO,* latest edition

AStudÜbBw, Study Report *"Armed Forces Employment 2020"*. BMVg GenInspBw, FüH III 3 - Az-31-60-05/VS-NfD dated 16 March 1998, Teilkonzeption bereichsübergreifender Aufgaben - Operative Information (TKBA OpInfo).

[2] Study Report: '*Possibilities, Prerequisites and Implications of Information Operations (Info Ops) within Multinational Operations of Armed Forces'*, (German – Netherlands Bilateral Study Information Operations), September 1999, para.3.4

INFORMATION ASSURANCE, A LONG WAY TO GO

Eric (H.A.M.) Luiijf M.Sc.Eng.
TNO Physics and Electronics Laboratory (TNO-FEL), The Netherlands

ABSTRACT

Information and Communication Technology (ICT) has an immense impact on the Military Mode of Operation. Modern Armed Forces are increasingly using commercial-off-the-shelf (COTS) hardware and software. Military and government decision-making units, critical industries, and society as a whole, are becoming more and more inter-networked. They rely heavily on essential, global, converged and entangled infrastructures. Most of these infrastructures are controlled by complex ICT. Both military command and control systems and society as a whole have become very dependent on the information infrastructures.
Information Assurance, as part of defensive Information Operations, aims to safeguard both the security posture of one's own Armed Forces and the essential information infrastructures.
This paper discusses both military and civil aspects of Information Assurance. It provides the reader with an overview of the clear and present threats from Cyberspace on the Armed Forces and society as a whole. A Cyber attack taxonomy ordered both by hacking method and reason of attack is presented. The paper discusses the strong need for Information Assurance and concludes with a list of internationally unresolved issues.

INTRODUCTION

Not so long ago, Cyberspace based warfare, automated shooters, smart ammunition and high-energy power guns existed only in science fiction literature and movies like Star Wars. Nowadays, Information Operations (Info Ops) changed from conceptual thinking into reality and has become a hot topic, both for the military and for governments.
During the last two decades, Information and Communication Technology (ICT) gained a large impact on the Military Mode of Operation. At the same time, Defence is no longer the main driver in ICT-developments. The modern Armed Forces increasingly use commercial-off-the-shelf (COTS) hardware and software. Also, military and government decision-making units, organisations, society and critical industries increasingly become inter-networked. For essential functions they rely heavily upon global, converged, entangled and often public infrastructures. Most of these infrastructures are controlled by complex ICT systems. Both military command & control systems and society as a whole - and "western society" in particular - have become very dependent on the information infrastructure and need to look carefully at the related threats.

Almost daily, hackers explore vulnerabilities in our global ICT infrastructures and in computer systems. Until now, ideological and cultural adversaries, such as individuals, guerrilla and terrorist groups, have not yet fully discovered "Information War" as a major means to disrupt military operations as well as society. Physical destruction by means of bombs and killing people by means of terror actions are still preferred above Cyberspace actions. However, some activists already have discovered the simple poor man's means to do so. While hidden in the fourth dimension, the info sphere, they attain a secure physical distance in time and place.

Armed Forces, governments and society as a whole need to be prepared in order to counter these new information-infrastructure threats. However, the current lack of awareness about information security and information infrastructure vulnerabilities, give rise to the fear that the clear and present Cyber threat danger is not yet taken seriously.

Information Assurance, as part of defensive Info Ops, aims to safeguard both the security posture of one's own Armed Forces information and the essential information infrastructures. This paper discusses both military and civil aspects of Information Assurance. A Cyber attack and attackers taxonomy and an introductory overview on hacking tools and techniques is presented. The paper concludes with a list of internationally unresolved issues.

INFORMATION ASSURANCE

The NATO MC422 'Information Operations Policy' [1] defines Information Operations as: "Actions taken to influence decision makers in support of political and military objectives by affecting other's information, information based processes, C2 systems and CIS, while exploiting and protecting one's own information and/or information systems. There are two main categories of Info Ops: defensive Info Ops and Offensive Info Ops, depending upon the nature of the actions involved".

For the information protection of one's own assets, the term 'Information Assurance' was introduced by the US Forces [2]/ [3]/ [4]. They defined Information Assurance: "Information Operations that protect and defend information and information systems by ensuring their: availability, integrity, authentication, confidentiality and non-repudiation. This includes providing for restoration of information systems by incorporating protection, detection, and reaction capabilities".
I regard this definition inadequate for several reasons. First of all, the US definition states an incomplete list of information security aspects, it neglects for instance security aspects as reliability, survivability, safety, and audit to name a few. Secondly, this definition largely neglects the protection of the critical and essential infrastructures, which is required for the politico-military freedom to act and decide. The infrastructures are nowadays global, intertwined and most often in control by commercial companies.

To cover all these aspects, I propose the following high-level definition for Information Assurance: "Information Assurance are actions taken to protect the State/Union, its society, its international allies, its economical national and international interests against the effects of attacks on, and disturbances of, information, information systems, information infrastructures, information-based processes, and essential information infrastructures and services."

This definition takes into account all civil information assets and infrastructures that are critical to a nation or to an economic entity like the European Union and its allies. Of course, Information Assurance cannot and should not stop at the countries' border. At large, Information Assurance should be based upon mutually agreed support between countries and unions. One can argue that the aforementioned definition of Information Assurance should be "Stateless" as the information highway crosses many countries' borders. Currently, however, the State or Union is the highest organisation structure that can nationally and internationally address the vulnerability of the information society to its broadest extent, from disruption of information highway-based services to psychological information operations (Psy Ops).

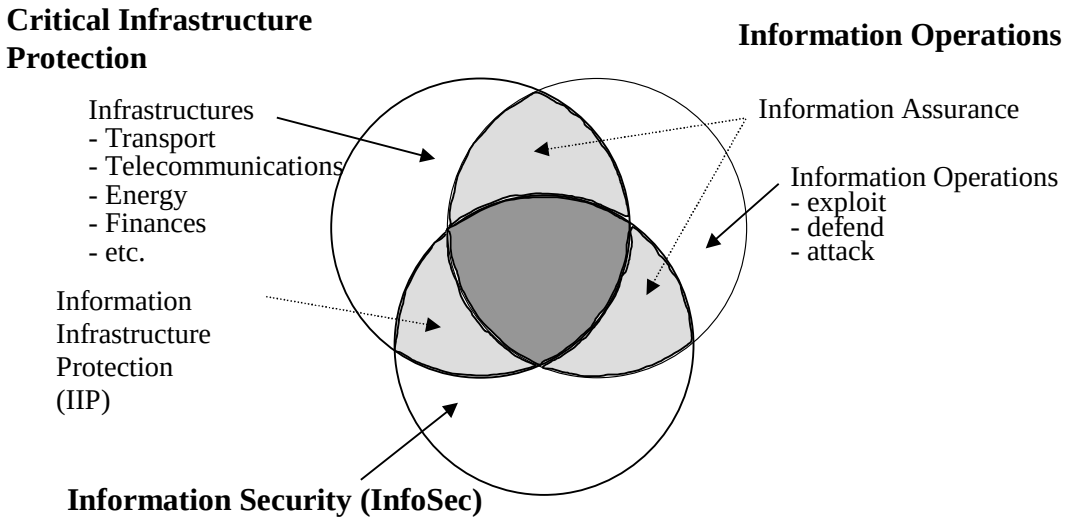

Figure 1: Relationship Information Assurance with Info Ops, Info Sec and Infrastructure Protection (from note [5])

Figure 1 shows the interrelationship of Information Assurance with Information Infrastructure Protection, Information Security and Information Operations.

Currently, the Armed Forces, government decision-making units, and critical industries become increasingly inter-networked and rely heavily upon global, intertwined and converged infrastructures. As an example, over 95% of the communication by the US Armed Forces during Operation Desert Storm went over commercial leased lines and satellites [6].
Most of these information infrastructures are controlled by complex information and communication technology. The basic building blocks for these infrastructures, however, are the same commercial-off-the-shelf (COTS) hardware and software that is used all over the globe. Knowledge about, and programs to exploit vulnerabilities in, commercial hardware and software can be acquired easily. A vulnerability found by a hacker in the early evening in Australia could become common knowledge in other parts of the world almost at the speed of light. In other words, systems in Europe and the US can already be under attack at daybreak or even during the night, at local time.

One of the tasks of a nations' Armed Forces is to prevent that attacks on the nation occur, and to defend the nation in case of an adversary's attack. The question is what role the Armed Forces will have to fulfil in defending the nations' Cyberspace. Especially when it needs to be taken into account that the Cyberspace extends over traditional international legal borders and far outstretches the "normal" military battle-space dimensions of land, sea and air.
Moreover, when looking at possible future conflicts, there is an increasingly growing probability for asymmetrical and low intensity type conflicts in which Information Operations will play a fundamental role. Thereby, it should be taken into account that the threats are not local to an operation "theatre", but can originate from an adversary anywhere out of the global society at any time in "Cyberspace". The Cyber terrorist - a premeditated, politically motivated non-military organisation (NMO), sub national group, clandestine agent or action group – [7] or their supporters poses unconventional threats to a wide range of military and non-

military targets, including the economical base. In a short period of time, they can raise attacks against the new information age societies. Crippling of the information infrastructure of a single nation, for instance, that takes part in an alliance could blunt, or even stop, the deployment of the Armed Forces of the whole alliance.

When looking at the defence side, it can be concluded that the Armed Forces and the ICT-based society are largely unprepared for dealing with the new global threats. Although high-tech information and communication technology is required, success in attacking critical information bases and infrastructures does **not** require major investments and thus are easily affordable for potential adversaries. Many quite helpful and sophisticated tools and documentation can be downloaded for free from the Internet [8]. The chances of being detected are quite low as research by the US General Accounting Office indicates. The chances of being caught are even lower [9]. It can thus be concluded that a heavily increased level of Information Assurance is essential to counter these threats.

VULNERABILITY AWARENESS REVIEW

Despite the many warning signals by hackers, Trojan Horses (e.g. Back Orifici and Netbus) and virii, power outages and broken fibres, as well as the Y2K-problem awareness, both the Armed Forces and the information age society seem to be unwilling to investigate and research its vulnerability and to take appropriate action.
Although the Armed Forces in a number of nations deal with Information Operations, the protection of the government's emergency management assets and infrastructures, to be used by government agencies and supporting Armed Forces, is often overlooked. With exception of a small number of nations [10], the continuity and protection of essential information infrastructures and information systems is not taken seriously. Those nations that undertook some action, understand that they are faced with a large task that should be dealt with in co-operation of Defence, government agencies, and public-private collaboration[11]. Also, legal issues and conflicting regulations prohibit a 'ready-for-battle' course of action.

As an example, the US President's Commission on Critical Infrastructure Protection (PCCIP) [12]/ [13]/ [14] looked at vulnerabilities in the following areas: information and communications, energy (electrical power systems, gas and oil transportation and storage), banking and finance, physical transportation (including air traffic control), and vital human services. The PCCIP reported that there is an increasing dependence on critical infrastructures. The developments of computer technology and astonishingly rapid improvements thereof have ushered the information age and affect almost all aspects of commerce and society. Our security, economy, way of life, and perhaps even survival, are now dependent on the interrelated trio of electrical energy, communications, and computers. The inter-relationships of infrastructures are, to say the least, worrisome. Everyone foresees the worst if more than a single infrastructure is disturbed, either deliberately or just by 'acts of God'. "The capabilities to launch an attack against the nation's information infrastructures are now quite widespread, and an attack is probably not that far away," warned Philip LaCombe, the director of the PCCIP. Disruption of the services on which the economy and our well being depend could have significant effects, and, if occurring frequently, could seriously harm public confidence.

The PCCIP concluded that the increasing vulnerability comprises the classical threats to infrastructure, and the new Cyber threats. The right command sent over a network to a power

generating station's control computer could be just as effective as a backpack full of explosives. The perpetrator would be harder to identify and apprehend, to boot. Moreover, infrastructures are growing in complexity and are operating close to their designed capacity. This increases the likelihood of cascading effects that begin with a rather minor and routine disturbance and end only after a large regional outage. Because of their technical complexity, some of these dependencies may be unrecognised until a major failure occurs. This failure can either be introduced by a ('stimulated') operational mistake, a technical failure, and an act of sabotage or – new – by an act of 'cybortage'.

Although infrastructures have always been attractive targets, borders and friendly neighbouring nations provided some protection in the past. Today, this situation has changed dramatically as national borders are no longer relevant in Cyberspace. Potentially serious Cyberspace attacks can be conceived and planned without detectable logistic preparation. They can be invisibly reconnoitred, clandestinely rehearsed, and then mounted in a matter of minutes or even seconds without revealing the identity and location of the attacker. As the Armed Forces increasingly use the same infrastructures, it becomes more and more difficult to distinguish between attacks on Armed Forces and attacks on society as a whole.

Almost daily one can read in the newspaper examples of ICT-vulnerabilities in our so-called "western" society (at large) and how the Armed Forces and society deal with them. People seem to smile about the incidents and forget about the impact that may occur when information systems and infrastructure are deliberately targeted on a larger scale.
Seen in this light, it is worthwhile to revisit some examples:

The lessons learned from disruptions by natural disasters, e.g. the Hansin Dai-Shinsai earthquake on January 17, 1995 with its epicentre near Kobe. The vulnerability of our ICT-based society was demonstrated in many ways. Although there was sufficient food available, it could not be sold as the ATM system was disrupted causing a lack of cash. Emergency backup communication via satellite was disrupted as the earthquake offset the satellite dishes and nobody in the disaster area knew how to realign them. The last major earthquake in 1995 in the San Francisco Bay area showed the same kind of ICT-vulnerabilities [15].

After learning from the financial market chaos caused by the London Square Mile bomb explosion on November 4, 1992, the Provisional IRA used hoax calls to disrupt infrastructure services (e.g. underground; the London financial district). They also planned to place either real or realistic-looking dummy bombs at six electricity substations at the outside of the London (security) "ring of steel". If the plan had been successful, the utility companies involved would have switched off *themselves* all power in a controlled way. This to reduce chances of cascading downed circuits throughout the whole UK. It was estimated that it would have disrupted all power services in London for at least 1, probably 1.5 days. The chaos and psychological effects would have been tremendous. The PIRA did not understand (yet) that transmitting the right commands on the right remote control lines causes the same effect.

Soccer fans, trying to obtain tickets for the 1998 World Cup soccer games, caused the telephone networks in several European countries to collapse on April 22, 1998. In the Netherlands alone, 30 central office switches went down for several hours. This included the four major cities and the emergency numbers. After Rinus Michels, former Netherlands soccer coach, I concluded that 'Soccer is infrastructure warfare'.

Vending machines supposedly dial the distributing company when they are near empty. However, some of the incorrectly installed machines in Australia dialled the default number 000, which is the emergency number in Australia. As there were thousands of machines installed, about 1 million 'mistake' calls per year were made to the emergency service, blocking access for those who really required help. This kind of widespread irregular 'attacks' turned out to be hard to tackle.

On March 10, 1997, a young hacker took down the Bell Atlantic central office switch in Worcester near Boston, USA. As a result, the airport lacked telephone and data services for over 6.5 hours. On January 4, 1999, five people broke into a Las Vegas Sprint telephone office and made off with telephone switching equipment. It caused a 7-hour interruption of phone service to 75.000 customers [16].

On May 19, 1998, a PanAmSat Galaxy IV satellite spun out of control, disrupting pager service to 80-90% of the 40 million pagers used in the US for over 3 days. Doctors were among the first affected as hospitals page them in emergencies as well as police officers. The Amsterdam Internet Exchange went down the December 26, 1998 due to a defective power transformer. Effectively, the Netherlands was largely cut off from the Internet for a number of hours. On June 16, 1999, 4 fibres were cut in Groningen causing a grinding halt of mobile and fixed telephone services as well as loss of data services in the northern Netherlands provinces.

On March 26, 1999 the Melissa macro worm spread very quickly over the Internet. Many US government sites, including a military base that supported the Kosovo Operation, turned out to be vulnerable. The worm luckily had no destructive 'payload' [17].

From these and many other, almost daily occurring big incidents, it should be clear that the Armed Forces, government, society, organisations and critical industries need to prepare jointly for defending their assets in the information age.

CYBER ATTACKS: FACT OR FICTION?

Cyber attacks and Cyber terrorism can be found on the Information Operations road map. The question is whether one should regard this as a future, a futuristic or an actual today threat. Is it real or is it fiction?

Studying this question, open information bases do not give very substantial facts. For instance, computer crime is not recorded as a separate item by most Bureaus of Statistics. It probably will be categorised under crimes like fraud, falsification or another category. Thus, no sociological breakdown of Cyber attackers is at hand. The ones caught range from schoolboys, students, a brain damaged man living on social security, to real terrorists. Some hacker groups, e.g. Master of Downloading (MOD) have multinational membership [18]. On the other hand, terrorism itself will remain a major trans-national problem, driven by continued ethnic, religious, nationalist, separatist, political, and economic motivations. Cyber terrorism is likely to come out of its infancy soon. Thus, in order to address the question "Cyber attacks: fact or fiction?" we have to make an assessment to categorise the different Cyber attack aspects, look for indications, look for our vulnerabilities, evaluate reports and draw

some conclusions.

CYBERWAR – THREAT ASSESSMENT

When looking at the different types of conflicts that might occur, one should look at the type and the driving intent of potential adversaries. Table 1, based on Waltz [19], provides such a breakdown.

Guerrilla Wars

		High-tech	**Low-tech**	
Economic Based Wars	**Physical conflict**	1. Military C2W . high intensity battle space . economic pressure & power . precision targeting . stealth: physical . C4I technology	3. Guerrilla warfare . low intensity battlespace . ruthlessness . random targeting . stealth: natural environment . human networks (as technology)	**Terrorism**
	Abstract conflict	2. NetWar, CyberWar . Cyberspace conflict . knowledge as power . information base targeting . stealth: using ICT . global networks (as technology)	4. Ideological warfare, conflict and power . mass/society targeting . stealth: ideological . ideological human networks	

Cultural Wars

Table 1: Typology of four conflict types (Waltz, note19)

It is clear that the major emphasis in box 1 lies with the military (information operations; command and control warfare). The high-tech Cyber terrorist (box 2 in figure 1) - a premeditated, politically motivated non-military organisation (NMO), sub national group, clandestine agent or action group –(see note 7) or their supporters poses unconventional threats to a wide range of military and non-military targets, including the economical base.

A major advantage for the virtual protagonist (boxes 3 & 4) is that he/she does not need to be around, in time or place, when attacking a system or infrastructure. Mounting a delayed attack is easy, as the modem dial-up for an attack launch can easily be automated. The global infrastructures make it easy to choose the country from which an attack is mounted, and by the way, it is easy to stealthily use international phone lines to reach a modem in another country. For security services, governments and organisations under attack, it will be hard to have indications of which targets might be selected. Lacking this intelligence, there is hardly

time for some warning. Tracking and identifying virtual terrorist groups may be even more difficult, if not impossible.
The possibility to use these aspects as a tactical means using new and combined technologies makes it quite different from earlier warfare means. The relatively low cost, high potential success rate and low probability of own losses makes "Offensive Information Operations" in principle quite attractive for individuals, economic adversaries, as well as protest and terrorist groups.

THE TAXONOMY OF CYBER ATTACKERS

Type of the trade

The first breakdown is to look at the type of hacking trades within the hacking underground:

- **Hackers**, who try to break in to demonstrate the vulnerability of computer systems and networks by exploiting "less well" managed systems and/or known bugs. Their intention is most often not a malicious one, but mere a kind of wondering what will happen if…. These include sniffers and snoopers, who listen on the networks for plain passwords.

- **Crackers**, who break into computer systems, try to destroy or modify information or exploit these systems e.g. to distribute software illegally. Software crackers are specialists in this group who like to break software security/self checks. Software with broken self-checks or valid licence numbers is placed on web servers (‘warez’).

- **Phreakers** (phone freaks), exploit phone exchanges, the cellular phone system and use phone signalling for fraud. They also may be involved with smart cards and credit card fraud. The phreaker group “Phone masters” broke into switches of AT&T, Southern Bell, BT, had access to portions of the US power grid and air traffic control systems. They forwarded FBI phone lines to phone-sex chat lines in Germany and other countries and got access to lists of tapped phone lines (in the end, their lines as monitored by the FBI showed up as well).

- **Social engineers**, who are deceptive collectors of information that allow them to collect passwords or other vital information to access systems and networks. **Thrashers** are social engineers, who use physical collecting methods. So called **dumpster-divers** like going through the company’s garbage to find valuable information that can be helpful to prepare a social engineering attack or to attack directly.

- **Satcom, CATV cable modems and pay-TV** hackers crack the scrambling of signals in order to view the transmissions for free. Their actions currently have only economical impact. With the offerings of Internet access over CATV cable modems, confidentiality, integrity and privacy threats become an issue. However, these fall under the other categories.

- **VX** - Virii Creators, people who write viruses and the like. The so-called ‘lamers’ are of a lower class: "they use virus construction kits, makes small useless modifications or just infect others' computers".

- **Screen** (‘eaves’) **droppers** stealthily monitor distant computer screens using the electro-magnetic radiation of screens. These ‘(Wim) van Eck systems’ might pick up screens from a distance of 1 km. Transient Electro-Magnetic Pulse Emanation STandard (TEMPEST) measures largely take away this risk.

- **The insider**: can be any of the above and can have ‘unlimited’ access to internal information and systems.

Reason of attacks

Secondly, we can order Cyber-attacks by the reason of the attacks and who is behind it (attribution):

- **Incompetence, negligence**. *Who:* the insider. *Goal:* obviously no goal.
  Note that everything being said about the external hacker threat should be balanced with the results of many studies that show that the insider is responsible for 60%-80% of the information security breaches. Lack of defences due to negligence and lack of security awareness is the main cause of successful attacks. The outsider can often attack by making use of the doors left unlocked by the system and network administrators. Moreover, hardly any organisation takes measures to detect unauthorised insider activities.

- **Internal denial of service**. *Who:* the disgruntled employee.who wants to hurt his employer *Goal:* burned grounds (deleted or damaged information) or locked information (key known only to employee).

- **Recreational / amateur hacking**. *Who:* any single or small group of teenager(s), student(s) and technology interested person(s), sometimes working in peer-groups. *Goal:* trying to understand ICT and the way security sometimes (often) does not work (curiosity). *Edge risk:* the person might become a 'small criminal' by obtaining financial gains (e.g. phreaking, smart card fraud).

- **Electronic disobedience**. *Who:* activist group; supporters of a cause. *Goal:* obtaining media attention and temporary service interruptions by denial-of-service attacks. *Edge risk:* become more violent when actions have no impact. Example: Electronic Disturbance Theatre (EDT) in support of the Mexican Zapatista fighters flooded web servers of the Mexican President, the Frankfurt Stock Exchange and the US Department of Defense with web page requests. Result was a denial-of-service.

- **Publicity seeking hacking/bragger**. *Who:* any single or small group of teenager(s), student(s) and technology interested person(s) as well as (semi) professional hacker group. *Goal:* the intent is to obtain a large media attention by breaking into a high valued ICT system and bragging about it. *Edge risk:* become involved / hired by criminals or sub national group.

- **Legal support seeker**. *Who:* hired semi-professional hacking person or group; disgruntled “former” employee. *Goal:* try to discredit an ICT-service and/or service provider to prove his/hers own innocence. *Edge risk:* becoming 'violent' trying to make his/her point.

- **Obtaining intelligence**. *Who:* National intelligence communities, economic information collectors (business intelligence firms), economic and industrial espionage and hired professional hacking persons/groups.
  Goal: national and business intelligence to obtain advantage over other nation(s) and organisation(s).

- **Action group cause; criminal protagonists ('hacktivists')**. *Who:* any motivated group with technological knowledge or support. *Goals:* seeks publicity and tries to annoy the objected organisation or government department or agency. *Means:* looks for denial-of-service attacks, e.g. by overloading, as well as loss of integrity of systems. *Edge risk:* becoming 'violent' trying to make their point and move to terrorism.
  As an example, in August 1999, the 1996 Nobel Peace Price winner José Ramos-Horta threatened the Indonesian government. A group of over 100 hackers all over the world sympathises with the East Timor struggle for independence and is willing to attack Indonesia's main economic assets (banks, telecom operators, airliners) in case the Indonesian government does not accept the outcome of the referendum held in East Timor.

- **Economic gain**. *Who:* unscrupulous business party or "ethical flexible" employee. *Goal:* obtain benefits by crippling competitors' ICT-business.

- **Vandalism**. *Who:* mainly disgruntled employee or individual. *Goal:* hit the economic values of an organisation.

- **Criminal activities**. *Who:* professional hacking persons/groups either with criminal goals themselves or hired by criminals or criminal groups. *Goal:* operation (if possible stealthy) to obtain intelligence, counter-intelligence (e.g. obtain, destroy, discredit or destroy police information), to disrupt security infrastructures during a planned action or to obtain a financial gain.

- **Cyber terrorism**. Who: premeditated, politically motivated sub national group, clandestine agent, organised crime groups or unscrupulous economic competitors. Might make use of paid professional hacking group or person(s). Whether the attack is foreign or domestic does not make any difference. Goals: a wide range of military and non-military targets, including the economical base.

Note that apart from the Cyber attackers, the new ICT means in general and the Internet in particular, are used as a communications means for sub-nation, terrorist and criminal information dissemination (e.g. bomb recipes, lock picking courses, offers for illegal passports) and secret communication. These categories are not treated in this paper.

METHODS OF CYBER ATTACK

Apart from the insider misuse, most of the Cyber attack trades have their own underground information circles with sometimes even quite open web information bases (see note 8). Combinations occur, e.g. phreaker tool and knowledge is used to open a free circuit to a telephone exchange. Hackers might pass through multiple computer systems and exchanges

before they get to their target that could mean going through multiple states or countries. Some hacking groups are well established and have their own regular publications (e.g. 2600 in the US, which has been around for over 10 years; Chaos Computer Club (CCC) in Germany). Many E-zines on this topic can be found on the World Wide Web as well. The hacker/phreaker circles document their knowledge, findings and even hardware designs quite well. Even knowledgeable UNIX and Windows/NT systems managers use these sources for obtaining more insight. Most of these documents and databases with information related to system weaknesses can be found on the Web.

Apart from physical attacks, the different types of information attack means vary from a strict software mode of attack to electro-magnetic spectrum means. An example list of these means follows below:

- **Computer virii**: code that self-replicates when executed and stealthily infects executable code, including macrocode. Apart from the replication code, a virus contains a payload that might be friendly or malicious. Virii are unguided pieces of software. Their infecting speed is depending on the type of infection mechanism used. Although sometimes destructive and annoying, virii are a less obvious Information Operation means

- **Trojan Horse**: code that has hidden side effects. Goodies and nice websites with active code (Java, ActiveX) pose a danger for those downloading code or visiting such sites.

- **Worm**: self-replicating code that uses network functionality, e.g. Email distribution mechanisms, to spread. The Melissa 'virus', which swiftly spread through the Internet in 1999, was such a worm.

- **Logic bomb** and **time bomb**: a stealthily piece of code that executes when a certain – externally triggered – condition, e.g. time, removal of a file, change on an external website, occurs.

- **Logic torpedo**: a virus type that tries to advance towards a certain set goal, being a system or program to deliver its payload there.

- **Data manipulation**: ranges from discrediting information integrity by changing data bits to **video morphing** in which video or still picture information is manipulated in such a way that for instance a President shaking hands with someone he never met in his whole life.

- **Backdoor** or **trapdoor**: an opening in the system left by a programmer or system administrator allowing unauthorised users to gain access to part of or the full system.

- **System design** and **coding flaws**: for each operating system, network software, network switching elements, and boundary protection devices (firewalls, guards), lists with vulnerabilities and patches are published by the vendors and Computer Emergency Response Teams. Usually, the system administrators have no or limited time to install patches as soon as this information gets out. This results in well-known open doors in many production systems.

- **Overloading**: bombarding a system with so many requests that the system cannot cope with the influx resulting in a denial-of-service for authorised users. A tool that was designed for flooding is Floodnet by the Electronic Disturbance Theatre.

- **Chipping**: modifying chips in such a way that the chip contains a backdoor or logic bomb.

- **Blue boxes**: tapping into phone lines and 'playing' with the signalling.

- **War dialler**: a software and modem set-up that allows fast sequential dialling of list(s) of telephone numbers in order to detect active modems or telephone lines that allow 'after-dial'.

- **Electro-magnetic spectrum** means, some examples:

    - Tapping information using the radiation of screens and soft tempest (software stimulated emissions)

    - Tapping other EM-spectrum signals,

    - Interfering with radio signals, e.g. a GSM-suppresser, as well as high-peak power ultra-wide band spectrum transmitters,

    - Electro-magnetic pulses, overloading and even destroying system circuits,

    - High-power microwave tools.

EVALUATION OF CYBER ATTACKS

To estimate the threats of Cyber attacks, the table below gives an estimate of the target likelihood by target and by motive. At the same time, the table shows whether validated attacks were reported by open sources.

CYBER ATTACKS	Validated Attacks (Status September 1999)	Targets				
		Infor-mation	Systems & Small Networks	Organi-sation & Industry	Govern-ment	Infra-structure & Society
Incompetence, negligence	Widespread	Main target	Main target			
Internal denial-of-service	Widespread	Main target	Limited	Main target		
Recreational hacking	Widespread	Limited	Main target			
Electronic disobedience	Limited		Target	Main Target		
Publicity seeking hacking	Widespread	Main target	Limited			
Legal support seeker	Limited	Main target	Limited			
Obtain economic intelligence	Limited, fast growing	Main target				
Economic attack / gain	Limited, fast growing	Main target	Main target	Main target		Limited
Obtain national intelligence	Known to occur	Main target		Limited?	Target?	
Action group / hacktivists	Limited, growing	Limited	Main target	Main target	Main target	Limited
Vandalism	Limited		Main target	Target	Target	Limited
Criminals: simple crime	Limited	Main target		Target		
Criminals: financial crime	High, fast growing	Main target	Phreak-ing	Target		
Organised crime	Unknown	Main target		Main target	Target	
Cyber terrorism	PIRA: limited				Target	Main target
	Limited	Main target	Target	Target	Target	Main target

Recently, network support personnel of the US Space and Naval Systems Warfare Center (SPA WAR) in San Diego were asked to investigate user complaints about a slow printer. Hackers had diverted the printer stream to a server in Russia, which in turn finally sent the output to the printer in question [20]. One can only guess what happened with the printer output. During the Kosovo crisis, attacks were reported from sources in Serbia and Russia, as well as from sympathisers in other countries, on NATO systems, US government systems, and defence systems of coalition partners. Apart from denial-of-service attacks and defacing of web sites, attempts were made to intrude defence networks.

So, when discussing the question: “Cyber attacks: fact of fiction”, it can be concluded that all types of Cyber threats have been realised in one way or another. Daily, one can find articles in

the news about hacked systems, credit cards and affected infrastructures. However, full-scale attacks with a major impact on Armed Forces and/or society have not (yet!!) been realised.

OPEN ISSUES

The information infrastructures are ICT-dependent, intertwined and inter-networked. They are highly vulnerable. Around 80% to 90% of the information needed to defend one's nation is nowadays in the private sector, in other words: is beyond government control. Fundamental changes in the approach to information assurance in the 21st century society are required. In the following some of the open issues are highlighted.

Organisations in general are not paying enough attention to information security, neglect warnings, cannot keep up to date with significant changes in the network environment and are unprepared for the things that may happen. I am quite convinced that many government agencies have sensitive systems and networks that have unlocked doors waiting to be opened unauthorised. The economic electronic intelligence gathering industry, both ethical and non-ethical, is mushrooming. There are indications that obtaining financial advantages by using non-ethical economical attacks is growing, given the low chance of detection. How long will society accept these risks?

Most governments lack awareness on the vulnerability of their own society. The outcry on international Cyber terrorism can be expected sooner or later. Studies like the US PCCIP study are either not realized in most countries or are hampered by lack of co-operation by other government agencies and industry. In Cyberspace, one can be attacked either from across the street or from somewhere in Timbuktu, which makes it rather difficult to go after Cyber attackers. The only solution is to keep the gates closed at all times, meaning one has to be continuously vigilant.[21] Organisations using information and communication means at large, as for instance the Armed Forces, have very limited resources both in terms of quality (knowledge) and quantity (number of system managers). It is already a burden to keep the information infrastructure working on a day-to-day basis. Resources to maintain the security posture are scarce. Organisations should become aware that Information Assurance should be high on their priority list in order to survive adversaries' Information Operations. The question is whether actions will be taken in time or that we will experience some electronic Pearl Harbor.

To address these issues, a fundamental international legal effort is required to address Cyberspace, the international legal fundaments, international police co-operation, the legal definition of Cyber attack and what kind of defences against Info Ops are allowed. Currently, international legal support is ineffective due to complex procedures. The adversary on the other hand requires only small bit streams that are measured in seconds. Secondly, the current preparedness of police involves criminals, not terrorists. Who will defend countries against Cyber terrorism? What will be the role of the security services in the 21st century given the threats of Cyber and infrastructure terrorism? How should inter-State information exchange be organised to fight cross-border threats?

Emergency preparedness requires training and rehearsals. Information Assurance requires the Armed Forces, governments and critical information infrastructure suppliers to be prepared for managing protective actions in case of an attack. The question is how to develop realistic

rehearsal scenarios, particularly when considering the cross-border aspects of Cyberspace.

Increasingly, Armed Forces and governments agencies actively use ‘Tiger’ or infiltration teams that try to break-in into their own sensitive systems. There are a number of legal issues when deploying these so-called ‘Red Team’ capabilities that need to be solved. Proper Information Assurance requires actively seeking holes in one's defences in combination with intrusion detection and trained counter-teams. When looking at the international aspects, the question is whether countries should co-operate with Red Team activities at a technical level? Is a continuous assessment of international information infrastructures required?

There is currently a lack of management attention on information security awareness. The question is how to start Information Assurance awareness at the right level in the Armed Forces and in government organisations.

A simple solution by some to the Information Assurance problem is to deny all electronic communication and information exchange. On the other hand, there is the pressure for sharing of international information and intelligence between coalition partners and governments. How to maintain the confidentiality, integrity and availability of one's own information if a certain degree of exchange is required before obtaining information from other parties. To deal with this dilemma, further Information Assurance developments are required.

And last but by no means least, hacking and phreaking are a reality. However, most of them are recreational hackers. The question, however, then is which alerting tools should be developed to recognise the 'probing' spies, criminals and terrorists in the haystack of background noise?

CONCLUSION

To survive possible Cyber attacks, e.g., from virtual terrorists, for whatever ideological or other reasons, requires countries, governments and organisations to be prepared. The Cyber attacker has the advantage of being place and time independent from the target, whilst the technology required is relative cheap to acquire. Information Assurance is supposed to be the answer to the asymmetrical threat. For that reason, Information Assurance, which includes aspects of information security, information infrastructure protection and defensive Information Operations, requires much more attention than currently is the case. The lack of awareness, security management and proper risk analysis causes a potential of high, unmanaged risks. The use of commercial-off-the-shelf (COTS) hardware and software increases the potential vulnerabilities of systems and infrastructures in case known exploitable vulnerabilities are not countered as soon as possible. COTS producers are reluctant to add mechanisms that support Information Assurance and trustworthiness. The question is how to maintain trustworthiness while predominantly using COTS components [22]. And, as the (virtual) ICT world, the global connectivity, converged infrastructures and inter-networking cross many international borders, effective international co-operation will be essential to counter attacks to the national or defence information infrastructure.

The fact that Armed Forces and emergency management communications rely partly, or sometimes even largely, upon third party-owned civil infrastructures is of great concern. International co-operation is still based on antiquated mail-coach technology and lengthy

administrative, if not bureaucratic, procedures. The Cyber attacker, on the other hand, uses the light-speed electronic highway, and is informally organised. There is still a long way to go to close the Information Assurance gap. This requires both raising the awareness at the highest decision-making levels, major technological developments, and global co-operation on harmonised legal systems and criminal investigative support.

To summarise, the current status of Information Assurance in the Armed Forces and in society as a whole, makes us fear for the worst.

NOTES

[1] NATO (1999), *NATO MC422 Information Operations Policy* (January 12, 1999)

[2] US Army. (1996). *Field Manual No. 100-6, Information Operations* (FM 100-6). [On-line] Available: http://www.jya.com/fm100/fm100-6.htm

[3] Department of Defense Directive (1996). (DoDD) S-3600.1.*Information Operations (IO)* (December 9, 1996)

[4] US Joint Staff (1996). *Information Assurance. Legal, Regulatory, Policy and Organizational Considerations*. J-6A 009773-97. 3rd edition (1997)

[5] Stein, Dr. W., *Information Warfare in Umfeld von IT-Sicherheit und Schutz der kritischer Infrastrukturen.* Seminar CCG. June 22-24, 1999.

[6] Hamre, Dr. J.J. (1998). DoD Speech to Fortune 500 Chief Information Officers Forum on July 21. US DoD. Aspen, Colorado. [On-line] Available: http://www.defenselink.mil/news/Aug1998/t08121998_t072198.html

[7] Pollitt, M.M. (1998), *Cyber terrorism, fact or fancy?* Computer Fraud & Security, (2) pp 8-10. Elsevier Science Ltd.

[8] Luiijf, H.A.M. (1998). TNO-FEL's URLography on Information Warfare. [On-line] Available: http://www.tno.nl/instit/fel/infoops

[9] US GAO (1996*). Information Security: Computer Attacks at Department of Defense Pose Increasing Risks*, GAO Executive report B-266140. [On-line] Available: http://www.infowar.com/CIVIL_DE/gaosum.html-ssi

[10] Publicly known infrastructure assurance activities are on-going in: Australia (note 11), Canada, Egypt, Germany (BSI/AG KritIS), Sweden, Taiwan, the United Kingdom and the USA (note 12-14).

[11] Cobb, Dr. A. (1997). *Australia's Vulnerability to Information Attacks*. Australian Strategic and Defence Studies Centre, Australia. ISBN 07315 27232. [On-line] Available: http://coombs.anu.edu.au/~acobb/X0016_Australias_Vulnerabi.html and http://www.infowar.com/CIVIL_DE/civil_100497a.html-ss*l*

[12] PCCIP (1997). *Research and Development: Recommendations for Protecting and Assuring Critical National Infrastructures*. Washington, D.C., USA. . [On-line] Available:

http://www.pccip.gov

[13] PDD63 (1998), *Presidential Directive 1998, number 63: Critical Infrastructure Protection Directive*. Washington, D.C., USA. [On-line] Available: http://www.ciaoorg

[14] (US) President's Commission on Critical Infrastructure Protection by Executive order #13010 of July 15, 1996. PCCIP (1997). *Critical Foundations: Protecting America's Infrastructures*. Report 040-000-00699-1, United States Government Printing Office (GPO), Washington, D.C., USA. [On-line] Available: http://www.pccip.gov

[15] Noam, E.M., Sato, H. (1995). *Kobe's lesson: Dial 711 for 'open' emergency communications*. Columbia Institute for Tele-Information, USA. [On-line] Available: http://jisp.cs.nyu.edu/RWC/rwcp/people/yk/shinsai/comm-proposal.txt

[16] Oakes, C. (1999). *Thieves hit phone center*. Wirednews. January 4, 1999.

[17] US GAO (1999). *The Melissa computer virus demonstrates urgent need for stronger protection over systems and sensitive data.* Report GAO/T-AIMD-99-146, April 15, 1999. [On-line] Available: http:///www.gao.gov

[18] AntiOnline (1998). Coverage of a chat with the Masters of Downloading (MoD) hackers group that attacked US DoD and NASA systems and claimed more attacks.

[19] Waltz, E. (1998). *Information Warfare principles and operations*. Artech House, Inc., Norwood, MA, USA. ISBN 0-89006-511-X.

[20] Bruno, L., Gareiss, R. (1999). *Cloak-and-Printer*. Data Communications. July 1999, p.14.

[21] A detailed discussion on vulnerability assessment and some of the tools used by vulnerability assessment teams can be found in Chapter IV, the article by Parker and Veltman .

[22] US National Research Council. (1999). *Trust in Cyberspace*. Washington DC, USA.

RED TEAM OPERATIONS TO ASSESS INFORMATION TECHNOLOGY VULNERABILITIES

Maarten Veltman
TNO Physics and Electronics Laboratory (TNO-FEL), The Netherlands
Richard L. Parker
NATO C3 Agency (NC3A), The Hague, The Netherlands

ABSTRACT

All Information and Communication Technology (ICT) systems have vulnerabilities. Weaknesses in these systems are introduced either during the specification, implementation or operational phase. Leaving aside these introduced vulnerabilities are intentional or unintentional, the fact remains that these factors make information security as strong as its weakest link. A team of professionals - a red team - whose aim is to combine the required technical skills into practice - pinpoints and tracks these vulnerabilities. The first step in a red team analysis is the collection of information, followed by an on-site analysis, resulting in a complete and accessible report. The tools and techniques used by the highly skilled red teams are the same hackers use on today's computer and network environments supplemented with their own developed tools and techniques. Experiences learn that the development of methods and the maintenance of a cooperative relationship with the responsible staff are crucial in the raising of a professional coherent red team.

WHAT IS THE PROBLEM THAT WE'RE TRYING TO SOLVE?

All Information and Communication Technology (ICT) systems have vulnerabilities. Once a computer or network component is inserted into a system, that component's vulnerabilities put the rest of the system at risk. There are nominally three sources of security weaknesses in ICT systems – specification, implementation and operation. Weaknesses in specification and implementation are usually found through experience or lab-base analysis and result in patches or upgrades. But even the most secure system can have vulnerabilities introduced through poor operation/configuration practices.

Most modern ICT systems have communication and application capabilities based on the TCP/IP[1] suite of protocols. At the time of their specification, these protocols did not really address security concerns as we know them today; they were designed for use in a small, liberally connected community where all of the members trusted one another to behave well. Consequently, there are some aspects of these protocols that are a bit troublesome now. The File Transfer Protocol (FTP) for example not only supports remote file retrieval, but also allows a remote user to delete and replace files on a server. In today's, environment, measures need to be taken to ensure that only trusted remote users have these capabilities, otherwise, for example, web site modification would be even more common than it already is.

Implementation vulnerabilities can be either unintentional or intentional. Unintentional vulnerabilities are common enough – software bugs. Sometimes, these bugs lead to potential security breaches (e.g., a buffer overflow crashing out of a program into a privileged shell

resulting in privilege escalation) and sometimes they result in mere annoyance (e.g., screen lockups). In either case, the developers did not intend the result that manifests itself and when such a bug is discovered, a patch or modification to the program to correct the problem usually follows quickly.

Intentional implementation vulnerabilities are an altogether different matter. In some cases, these can be 'backdoors' or 'Trojan Horses' left behind to allow the programmer (or someone the programmer told) to exploit a hidden function in a particular piece of equipment. A common example of this type of code is the ubiquitous 'Easter Egg'. Easter eggs are nominally harmless code left behind by developers and are invoked by some obscure trigger input or event; the functionality they represent has nothing to do with the stated function of the program.

Given careful identification of the location of the egg within the executable module, though, modification or replacement of the code could be achieved with no perceivable difference in the operation of the program and without changing the size of the file. It is conceivable that one could remove the Easter egg code and replace it with something more malignant, say a module to modify or redirect data on file saves.

Part of the problem lies in the standard practice of providing default configurations for systems that make them as easy as possible to get up and running. In order to increase the likelihood that system components will work "right out of the box", default configurations are designed to be as 'forgiving' as possible – allowing for the widest variation in conditions in which the component will work. For example, a Sun SparcStation is typically configured to support a wide range of network services (e.g., SMTP Email and Network File System).

Sometimes configurations support security functions that are not sufficiently integrated into the overall system operation. For example, it is of no use if security features like logging and auditing are installed but the output is never checked or used by authorised personnel or automated functions. Another all-too-common example is use of weak (or nonexistent) passwords during the identification and authentication (i.e., login) process. Examples like these make operators wonder why the 'security' feature was installed in the first place.

Even when a system component is initially configured to reduce the number of vulnerabilities, that component's configuration changes over time. New software packages and system upgrades are installed; users and operators change parameters to accommodate changes in operational requirements. Furthermore a lot of these parameters are not independent and thus changes may introduce unforeseen side-effects. All of these aspects combine to make it nearly impossible to gauge the overall security posture of a system that comprises a large number of servers, workstations and communications components.

HOW DO WE PROPOSE TO ADDRESS THIS PROBLEM?

In the last few years, information security (Infosec) specialists have come to rely increasingly on an analysis technique referred to as "red-teaming". The name is borrowed from military exercise vernacular where the home forces are assigned the tag "blue team" and the opposition forces are assigned the tag "red team'. By playing out a scenario against a live "enemy", tactics and strategies can be reviewed and refined. In the ICT world, operational systems are

reviewed for security vulnerabilities by a team of Information security specialists, using tools and techniques specially developed for the task and some borrowed from potential adversaries – *hackers*.

The rest of this article details the nature of Infosec red-teaming, the sorts of tools and techniques involved, the kind of results that can be obtained and some observations based on red team experience.

WHAT EXACTLY IS RED TEAMING AND WHERE DOES IT COME FROM?

In late 1993, Dan Farmer and Wietse Venema released a paper entitled "Improving the Security of Your Site by Breaking into It" [2]. The paper exhorted operators to start analysing the security of their systems by looking at them from the hackers' point of view. This paper also announced the forthcoming release of the Security Administrator's Tool for Analyzing Networks, a.k.a. SATAN. SATAN automated a series of checks for vulnerabilities commonly found in Unix systems. It was based on earlier work done by Farmer at COAST and CERT (COPS – Computer Oracle and Password System) and Venema's prior work, including TCPwrappers. "There Be Dragons" [3] and "Packets Found on an Internet" [4] written earlier by Steve Bellovin detailed network traffic associated with hacking attempts and would eventually lead to Bellovin and Cheswick's book "Firewalls and Internet Security: Repelling the Wily Hacker". [5] These papers and numerous contemporary efforts led to the current state of practice in the area of network/system vulnerability analysis, based on probing systems for known or suspected vulnerabilities 'from the outside', using exploit techniques to determine the target systems' security posture.

These documents and the activities that they represented formed the basis of ICT system security analysis based on active scanning for exploitable vulnerabilities – red teaming. Teams of specialists, equipped with purpose-built hardware and software tools can provide an independent analysis of a system's security posture in this fashion. Over time, the staff, tools and techniques for performing this sort of vulnerability analysis have become more specialised, migrating from systems operation to dedicated roles in vulnerability analysis. Again, borrowing terminology from the military arena and owing, in part, to the adoption of these techniques by military organisations like the Defense Information Systems Agency (DISA) and Air Force Information Warfare Center (AFWIC) in the US, this process has become known as "red teaming".

Setting up and running a red team is no simple matter, however. Team members with the right technical capabilities can be difficult to find. The tools needed for this type of activity can be expensive and don't always meet expectations. The staff responsible for setting up the security for systems may not appreciate having a team come in and explain where the system is deficient. Any number of things can go wrong during an analysis effort; personality conflicts; misinterpretation of results; component crashes attributable to the effects of the analysis tools, etc.

Setting up a team can be the first real challenge. To date, the staff involved in this sort of activity are typically highly technically skilled, with a broad range of knowledge comprising the hardware, software and protocols that are found in IT servers, clients and communications components. Most have had experience in development and/or operation of several of these

components. One telling skill is the tendency to "need to know" how the system works, down to the level of understanding the data structures and exchange sequences that make up IT processes.

These characteristics (and the diversity and strength of the personalities that usually accompany them) have made it difficult to assemble many groups of analysts capable of performing red team analyses. Fortunately, the tools and techniques are becoming more structured, making it possible to train less technically-focused personnel in what used to be something of an arcane art rather than a well-defined practice. While a fair degree of technical ability is still required to competently apply the tools and techniques and to properly interpret the results, intimate understanding of the inner workings of IT components is no longer necessary. Infosec specialists with the detailed understanding of the internals of IT systems are still required for analysis and countermeasures of new and complex vulnerabilities as well as providing advice to operational red teams, however.

Selection and familiarisation with the 'tools of the trade' becomes the next major challenge. For the most part, these tools collect together known vulnerabilities and exploits, automating the job of checking a system and requiring less understanding of all of the details of all of the vulnerabilities on the part of the user. Some of these tools are commercial developments (e.g., Kane Security Analyst), some are 'freeware' (e.g., Scotty/Tkined, NTCrack) and some are a bit of both (e.g., ISS Internet Scanner offers both a limited freeware version and a full-capability commercial version). However, programs used by system managers / security inspection teams can also be used by anyone else.

Table 1 lists a short subset of tools used to detect and correct (or exploit) vulnerabilities in operating systems and applications commonly found in today's communications components, workstations and servers. The tools have been loosely grouped here for the sake of simplifying discussion of their general capabilities; emphasis should not be placed on categorising them, rather one should focus on understanding their capabilities and application.

Vulnerability Analysis
ISS Internet Scanner, Kane Security Analyst, Trident IP Toolbox / L3 Expert, Security Profile Inspector (SPI), NAI CyberCop, SATAN
Network Monitors and Sniffers
Ethload, Sniffer, Etherpeek, TCPDump, Snoop, IPWatcher, T-sight, Scotty/Tkined
Intrusion Detection
RealSecure, NetRanger, Stalker, Intruder Alert, Network Flight Recorder
Exploitation
GetAdmin/Crack4, Offline NT Password Utility, NTCrack, CDC Back Orifice
Other Notables
TCPwrappers, Tripwire, COPS, crack, ScanNT, Nmap port scanner

Table 1: Red team tools

Once a team has been assembled and tools selected, the really difficult part begins – gaining community acceptance and field experience. While laboratory activity is essential, it is no substitute for operational experience. Learning how to run an analysis with minimal disruption and maximum effect is not an abstract exercise; it is knowledge gained through experience.

WHAT SORTS OF VULNERABILITIES CAN BE FOUND AND CORRECTED BY RED TEAMING?

The sorts of vulnerabilities which can be found by red teaming are quite diverse. They diverge from technical, organisational to social matters and in some cases they overlap.

Starting with a technical perspective a common network structure can be recognised. Most networks which are looked at by red teams (from a 10.000 foot height) consist of the same network structure and network elements. At the physical layer there will be network cables and wiring making communication possible between the network elements. Routers and switches provide a means to route the traffic from one place to another. Furthermore there will be systems offering services to workstations or clients.

Acting as the average user one couldn't care less about all these elements unless it's not working. From a user's perspective, the most common services would be electronic mail, file access, web browsing and the ability to participate in (corporate) news discussions.

Taking these generalised services as a base, one can easily forget that there are a lot of underlying protocols facilitating these services. For example protocols facilitating electronic mail are the Simple Mail Transfer Protocol (SMTP), Post Office Protocol (POP) and Internet Message Access Protocol (IMAP). Let alone the standards and protocols affiliated with the application of electronic mail. The point to be taken is that all these protocols have their own quirks, either related to specification, implementation or operation.
A red team will try to pinpoint problems related to security weaknesses regarding integrity, authenticity, confidentiality and availability.

Looking at the vulnerabilities a red team from a technical perspective would try to exploit, the following classification can be made:

Information gathering.

Collecting information about the structure of the target network, systems and users using it, is a good starting point. Almost all information which can be gathered can be useful either directly or in a later stadium. This information, even meaningless at first sight, can support in identifying the weak spots. Information in this category is the sort and type of operating system and the sort and type of services offered. Let alone, (public) user directory services containing a wealth of information, in some cases including users private home addresses and telephone numbers.

Example: A way of getting an overview of services offered by a server is to determine what services are listening for connections on that server. In a TCP/IP based environment the normal use of well-known services are limited to certain fixed TCP/IP port numbers. For example the FTP-service listens on port 21, e-mail (SMTP) is offered at port 25 and WWW is offered at port 80. By sending connection requests to all port numbers and registering what response gets back it is easy to tell what services are listening and therefore offered. This popular technique is known as *portscanning*. Once all information is collected a search can be done for known vulnerabilities matching the detected operating system, services and version.

Exploiting a trust relationship.

A very common technique to elevate a privilege is to exploit a trust relationship between two trusted parties. A well-known implementation of this technique is called *spoofing* (impersonation). Most protocols and services lack good mechanisms for the authentication of the sending party. Spoofing makes use of this shortcoming by forging the source of a packet. When the receiving party receives this forged packet it assumes its communicating with the genuine trusted host whereas actually it's talking with the attacker.

Another method to exploit a trust relationship is to hijack an existing connection between the two trusted parties. Without adequate measures only the setup of a connection is authenticated. The most common use for authentication is by typing in a username and password. Once the session is setup it is possible to take over the session without having to re-authenticate. Obviously this technique is called *connection hijacking*.

A real world example of the trust relationship exploitation is the way the r-utilities can be mislaid. The Computer Emergency Response Team (CERT) warns for this attack in their CERT advisory 95-01 [1]

Backdoor attacks.

"A Backdoor is a family name for Trojan Horse programs which open (new) security vulnerabilities to the system when executed."[2] A backdoor can be introduced either during the development phase by the programmer or in a later stadium by an attacker. The presence and applications of backdoors can be very powerful. A red team can make use of documented/known backdoors or introduce their own.

An example for Unix environments is RootKit. RootKit consists of a set of modified system tools (e.g. login) equipped with backdoors. Once a hacker gains control over the Unix operating system he or she replaces the genuine system tools with the ones from RootKit. The modified system tools offer the ability to retain access to the system by making use of the installed backdoor.

In Microsoft Windows environments a popular example is the hacker program "Back Orifice". The crux of the exploitation resides in the fact that the Trojan horse has to be installed and activated on the target system at some time. The most common way to achieve this is by sending an email attachment to the ignorant target user. By hiding the Trojan horse in a small game, picture or greeting card the Trojan horse will install itself once the target user opens the message. Once installed complete control over the target machine is granted, including the remote control over the mouse and keyboard. A demonstration of this attack makes users aware of the risks which are introduced by executing non-verified e-mail attachments.

Denial of Service (DoS).

The term Denial of Service sounds malicious and in some way it is. However controlled Denial of Service attacks can be supportive for other attacks, for example the earlier explained trust relationship exploitation. Denial of service attacks exists on many layers. An example given here refers to the protocol which is used across the Internet, called TCP/IP. Part of the protocol is the connection-oriented Transmission Control Protocol (TCP). One of the most well known

Denial-of-Service examples with TCP is called *SYN-flooding*. We'll go into some technical detail here.

The setup of a TCP-session consists of a process called the three-way-handshake. This process is depicted in figure 1.

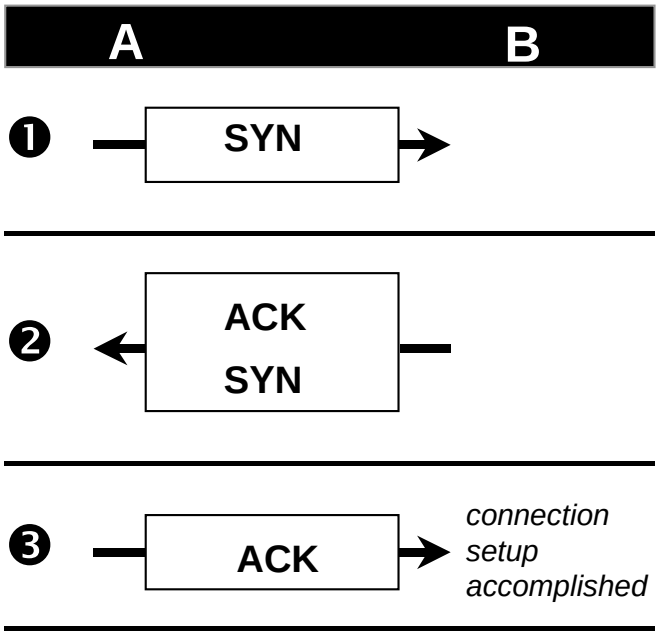

Figure 1: TCP/IP three-way handshake.

Imagine client A wants to setup a connection with server B. To start the connection the client will send a packet indicating its willing to setup (synchronise) a connection (SYN). The server B will confirm it received this packet by sending a confirmation (acknowledge) packet (SYN+ACK). At this time the state of the connection is half-open. To finish the three-way-handshake client A will acknowledge the received package from server B (ACK). Now client A can exchange data with server B.[3]

One of the problems with the above setup is the limited number of sessions which can be in a half-open state on server B. This number of sessions is called the backlog and depends on the type of operating system, but normally this would be about 4-6 sessions. If the client does not acknowledge the server's packets, the server will time-out this session, retry it a couple of times and finally remove the details from its backlog. The total duration of this process can take up to 10 minutes. Now just imagine the scenario as depicted in figure 2.

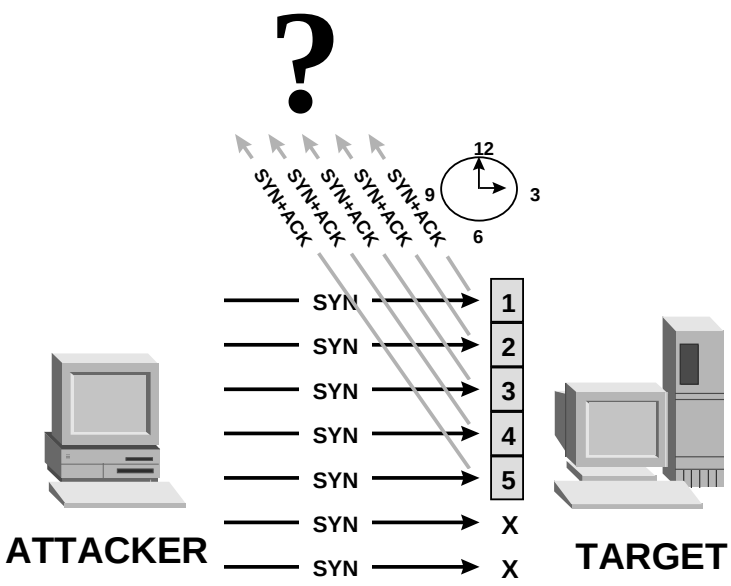

Figure 2: A Denial of service example: SYN-flooding.

In combination with the spoofing technique as explained earlier, the attacker will forge a couple of connection setup-requests (enough to fill up the backlog on the server). The target thinks its communicating with a host other than the attacker. This host however is not able to respond (either too busy or non-existing). At this time the target will not accept new connections (its backlog is filled anyway) and wait till it either receives the acknowledgements for the connections or it reaches its time out. This technique, called *SYN-flooding*, is a very effective Denial-of-Service. The attacker only needs to send a couple forged packets every 5-10 minutes to effectively put the target out of business. This type of attack is seen less frequently today, but two years ago, it was a very common exploited vulnerability.

Passive attacks.

A passive attack is an attack without the target noticing it is under attack. An example of a passive attack is the ability to read all packets on the wire, also known as *sniffing* or *snooping*. During normal operation a Network Interface Card (NIC) only processes packets destined for its own card and forwards it to higher layers. By putting the card into a special mode (promiscuous mode) all packets arriving at the NIC will be processed. Legitimate use for this feature would be network management and troubleshooting. However, the misuse potential for this feature is much higher. Specialised programs float around on the Internet which will grab unencrypted authentication sessions (which can include passwords) or other sensitive data. In general all non-encrypted traffic is at stake, this includes e-mail and Web sessions.
A red team can use this technique for a diversity of reasons. Sometimes the grabbed information proofs that the target is working with sensitive or classified material, in an inappropriate manner on a non-classified network. In other cases the information can be used to launch new attacks to systems or to extract passwords for unauthorised access to target systems.

Exploiting known system and service vulnerabilities.

The majority of attacks can be placed into this category. Most commercial vulnerability scanning software like Internet Security Scanner (ISS) and Network Associates CyberCop scanner identify holes in software or an operating system. Because of its diversity no generic description can be given. A good example explaining the possible impact is discussed below.

The most common services people actually deal with are presented at the application level. Services like Electronic mail (SMTP), File Transfer Protocol (FTP) and the World Wide Web (HTTP) are best known. One of the vulnerabilities the implementations of these protocols have in common is called a *buffer overflow*.

Buffer overflows arise when placing an object in a, for that purpose reserved, too small buffer. A more practical example is the password login prompt. Normally a password will not exceed 16 or so characters. What will happen when one inserts 300 or even more characters at this password prompt? A graphical interpretation is depicted in figure 3.

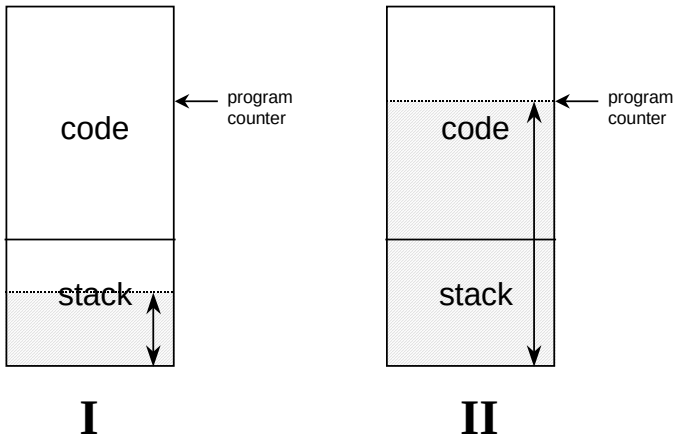

Figure 3: Principle behind buffer overflows.

The normal (simplified) situation is portrayed in situation I. The actual position of the running program code is kept by a counter called the program counter. The input values are stored at the stack, which is dynamic. The program will read the input information, put it in the stack (e.g. password) and remove it after its done using it. When no boundary checks are done these input values can, if exceeding the buffer, overwrite other parts of the program, including the program code (see situation II). Normal behavior when experimenting with buffer overflows will be a denial-of-service.

However if the input data is crafted in a special way, one can overwrite the program code with new program instructions.
The effect of all this would be that for example the authentication process (in case of the password example) executes arbitrary code inserted by the attacker. This code will run in the security context of the process in question, the authentication process. If the security context is high enough total control of the operating system can be accomplished.

Putting this theory into practice an attacker needs to know the precise position (offset) for the code to be inserted. But as with all vulnerabilities once people find one, automated exploit scripts and tools are released to the public shortly after the announcement. Most buffer overflow exploits insert shell code by which a rootshell arises, giving total control to the attacker.

When looking at security advisories from the Computer Emergency Response Team (CERT) and Computer Incident Advisory Capability (CIAC) one will find a lot of warnings for these buffer overflow vulnerabilities. An example is CERT advisory 07 (June 16th 1999). [1]

Having a firewall in place can, if configured and maintained correctly, prevent many attacks. But what happens if users use workstations equipped with modems to create their own connections to the Internet or other networks. The corporate firewall will be of little use. A way for red teams to identify these and alike systems is by using equipment for scanning the telephone range for listening modems. In some cases the found modems are installed by administrators to facilitate remote management. A noble idea, but deadly if used by other people.

Besides the technical vulnerabilities a lot of shortcomings result from the lack of a (good) security policy and organisational measures, which include procedures for operational management, change management, acceptable use policy etc.

In practice red teams often find operating systems or services running versions, which have known vulnerabilities. Although updates, patches or fixes of the vendor are available, administrators choose not to install these fixes for a variety of reasons. The consequences can be disastrous. Exploiting a known vulnerability in an identified system takes less then a second to complete and days or weeks of work can be at stake.
Due to the growing interconnection the spreading of information related to vulnerabilities is extremely fast. When for example someone in the United States finds a vulnerability and publishes details about it, tools for exploiting it will see daylight shortly after that and your systems on the other end of the world will get attacked the same day. Administrators have no choice other then acting firmly and keep up with security information of their vendors and/or CERT's when it comes available.

In other cases security functions are implemented but not actively deployed. Administrators are more then happy they succeeded in installing the software, the last thing on their mind is putting effort in enabling the security features.
This reflects to the history and ongoing process of putting the emphasis for network and system design mainly on the desired functionality and ease of use. Security requirements are (if lucky) secondary in this design. As mentioned before, the 1970 technology (TCP/IP) on which the Internet is based has no standard measures for offering confidentiality, authenticity and integrity.

And even if security functions are implemented, the strength of a system stands by its weakest link. A situation red teams run into quite frequently is the use of weak (or no) passwords during the identification and authentication process, which makes you wonder why this 'security' feature was installed in the first place.

And even outwardly difficult passwords are cracked within hours and even minutes. The principle behind most password crackers is not about the ability of decrypting passwords, but by comparing the encrypted password with the encrypted result of a set of characters used as input. Password crackers therefore use two approaches:

> **Dictionary attack**. By encrypting words from a dictionary and comparing the results with the encrypted password. If the chosen password is listed in a dictionary it's merely a matter of minutes before the password is found. One would be surprised how many people use common words or names of their relatives. Just as a "nice try but no go" note: Most password crackers automatically check for variations of the dictionary word by adding digits or spelling it backwards.
>
> **Brute force.** All possible character combinations are encrypted and compared with the encrypted password. Eventually leading to the password. As the popular Microsoft Windows NT password cracker program L0phtcrack states: "All alphanumeric passwords can be found in under 24 hours on a Pentium II/450."[4]

SOCIAL VULNERABILITIES

Besides technical means for information gathering, the traditional way of gathering information can be quite fruitful as well. When doing an inside penetration test a physical observation of the rooms where targets are situated can be a possibility. A fact of life is that people tend to write down things they need to remember. Needless to say, login names, passwords, system names and even personal information like credit cards and social security numbers are written down and stored at a place accessible by members of a red team.
The gathered information can also help in guessing your way into a system. Many times people use common names or names of their relatives as the basis of their password. This technique is called *password guessing*, some call it simple luck.

Besides information stored for re-use, also things casually thrown away in a dustbin can be useful. There is even a name associated with this technique, which is *trashing*.

A level often forgotten but nevertheless very powerful is the mindlevel. This level refers to psychological means to influence people. A technique employed by some hackers is called *social engineering*.

Imagine the behavior of users of a corporate network when somebody calls, telling them he or she is the administrator of the network. "*Sir, we have a problem with our user database, your record has accidentally been deleted. Can you supply me your password, so I can fix the record*". You would be surprised how many people will help out by giving their password.
Or what will happen when people from the system management department receive a falsified letter from the vendor of their equipment, telling them they really need to install the enclosed patch. When installed the 'patch' will introduce a backdoor for the attacker. Guaranteed it will work when the system management department receives the letter a couple of days before Christmas.
Striking enough not to many red teams actually use these techniques, which, if they are used in the right manner, can be very supportive to emphasis on programmes related to the education of users.

Preventing the exploitation of social vulnerabilities is very difficult. Part of it has to be suppressed by acceptable use policies and the education of the users. At the bottom line, a great deal of maintaining the level of security is all between the ears and the associated behavior of the users.

WHAT ACTUALLY OCCURS DURING AN ANALYSIS EFFORT?

Each analysis effort is different from every other effort and it is not possible to describe a 'cookbook' approach to red-teaming. However, it is possible to provide a glimpse of how such a group goes about their business. The process described here is applicable to systems that have external network connections (e.g., the Internet). For systems that do have external connectivity, part or all of a vulnerability analysis can be performed from a remote location.

A red team effort usually begins with a request or suggestion that a particular system be subjected to analysis. Once the pertinent authorities have agreed to the analysis activity, the red team begins to collect any available information on the structure of the system to be analysed. Before doing so potential legal aspects have to be covered. This requires the red team having a clear understanding what the limits are of the 'cyberspace' network area to be analysed. Legal aspects should be well understood and be discussed beforehand. Risks of unintentional accessing networks outside the intended boundary should be considered as well. For example when an assessment is made of vulnerabilities of networks in the Netherlands, the computer crime law (Wet Computercriminaliteit), the European Directive on Privacy (Wet Bescherming Persoonsgegevens, a privacy law, successor of the Wet Persoonregistraties) and the telecommunications law (Wet op de telecommunicatie) restrict red teams in the allowed ways of operation. Obviously the owner of the network(s) to be analysed should take responsibility, given a professional and legal-compliant approach by the red team.
After all hurdles have been taken, the red team can begin its work.

Phase 1 – Information collection

First, the physical network topology is detailed - whether the network is coaxial, twisted-wire or fiber Ethernet; the location, make and model of routers, bridges and hubs. Next is the logical network topology – the location of key servers (e.g., DNS, Web); the IP address space and any subnetting that is implemented. Frequently, it is very helpful to develop a diagram or drawing depicting the key components of the system under analysis. Both high-level and detail views are useful, but invariably, it becomes necessary to produce a single diagram that shows all of the significant components on a single page, regardless of how large or small that page needs to be to make the drawing legible. The team can then analyse the flow of information in the system – identifying key servers and the protocols and applications used to provide those services. As much as possible, this information needs to be collected in advance of the active portion of the vulnerability analysis. It is slow, painstaking work, but understanding the entire system under analysis is crucial to the success of the overall effort.

Phase 2 – On-site analysis

Having collected as much advance information as is possible, the red team moves to the more visible phase of on-site analysis. This is where the vulnerability analysis tools, sniffers, mappers, drawing packages and other tools are brought to bear to validate the documented

representation of a system with the reality of that system as it is implemented. While it is important to have local support and coordination for this phase of the analysis, it is also important to avoid turning the on-site visit into a special event, making it impossible to get an unbiased view of the system's normal operation. While nobody likes surprises, it is important to limit advance knowledge of the red team visit to as few personnel as is practical. To avoid conflicts, cognizant local personnel need to be available to handle any concerns or misgivings on the part of staff that are not given advance notice of the analysis effort.

Typically, a red team will carry portable systems loaded with the software they need to perform the vulnerability analysis – the previously mentioned tools. The red team should also be equipped with a broad variety of network components to facilitate access to the system under analysis. Cables, network hubs, cable testers, power distribution strips, connectors, adapters, multimeters, raw cable, crimping tools, soldering irons, hand tools, a portable printer and more will all be useful at some time or another. Over time, each team will collect the set of tools that they find they need, but it is always better for a red team to be completely self-sufficient than for them to impose upon the staff whose system is being analysed.

Team members will usually spend some time verifying the information collected in advance and collecting any information that is missing from the initial data. In particular, verifying that the actual topology of a system matches the documentation is important. Seemingly minor discrepancies can significantly change the overall result. For example, a network connection provided for remote configuration capability when a system is first put up might be forgotten and left in place after a system is put into full operation. Verification of the documented set of information services is also important, since each information service brings its own set of vulnerabilities in the servers and clients involved. Once the system's topology and information have been verified, the team can identify key elements (i.e., primary servers, typical clients, key network elements) for detailed vulnerability analysis.

Phase 3 – Reporting the results

After the vulnerabilities have been identified, the red team starts the process of developing a report for the authority that authorized the analysis. There are three key aspects to how this phase of the process works. First, **the report from the analysis must be complete and accessible**. The report is of little value if it does not explain both vulnerabilities and suggested remedies in a manner that can be understood and acted upon by the staff responsible for the subject system. Some of the tools employed in an analysis effort generate documentation as part of their operation; combining the output of such tools with other information (e.g., network topology diagrams) to produce a succinct, complete report is just another part of the red team activity.

Second, **nobody, but nobody, likes to be embarrassed**. To put this into context, it is essential that the results of an analysis effort be discussed with the staff affected by those results, with the participation or sanction of the authorizing authority, prior to the results be fully disclosed to the management / command structure involved. This allows the affected staff to understand the results and the implications without being put on the defensive and increases the likelihood of positive reception of the results.

Finally, the red team has to remember that **the results of the analysis belong to the authorising authority**. The network topology analysis results, vulnerability data collected and

the report itself are privileged information and should not be shared with others without the express permission of the entity that authorised the analysis in the first place. In fact, it is not uncommon for red teams to use notebook computers with removable disk drives so the team can leave all residual data with the authorising authority.

Again while this isn't a complete description of all of the considerations and activities that occur during a red team analysis, it does provide some insight into the operation of such an activity. To understand red teaming more fully, it is probably best to actually spend some time performing vulnerability analyses in a lab environment, then pursuing field exercises.

WHAT OBSERVATIONS CAN WE DRAW FROM OUR EXPERIENCES?

Over time, each team finds the combinations and variations of tools, techniques and personnel that best suit the systems that they analyse. Frequently, multiple similar tools will be used separately or in combination. For example, the NATO C3 Agency (NC3A) red team staff typically carry two different LAN analysis tools (i.e., sniffers), owing in part to the different capabilities of the two products and in part to the preferences of individual team members. Different team members will apply different techniques to acquiring the same information, as well. Someone adept with Unix will probably elect to use the program *snoop* rather than an external LAN analyser. One group will prefer ISS for vulnerability scanning, while another uses CyberCop and yet another group will employ both tools. Familiarity with a broad range of tools and several implementations of each type of tool is more important than "selecting the best tool". And the team's 'toolbox' will change over time.

Development of a team's method of work is probably more important than selection of tools. Staff will need to spend time working with their tools in a laboratory environment in order to familiarise themselves with the correct operation of the tools and interpretation of the results. They also need to spend time working with each other, getting used to the way each team member operates and his/her strengths and weaknesses. This aspect has proven to be crucial, since capable team members are frequently used to being lead contributors in prior professional activities.

Red teams also have to develop a method of working with the staff responsible for the systems that the team will analyse. Here it is very important to maintain a cooperative relationship rather than an adversarial one. Frequently red teams will be employed as a step in the process of accrediting operational systems as well as reviewing the security posture of existing systems. In both cases, it is important to have close coordination with the system operators and approval from their management/command structure. It is also important to put at least two or three analysts into each effort, both to share the workload and to provide "a second pair of eyes" for difficult problems. When possible, it is also helpful to have a designated senior member of the team to deal with any issues that arise between the red team and the local operations staff.

SUMMARY AND CONCLUSIONS

The mentioned key aspects of red team activities and their application in the preceding sections probably lack a minor, though not to be forgotten aspect - the costs of setting up and maintaining a red team. In short these costs are substantial. As mentioned before specialised tools and software is needed, let alone the availability of highly skilled and trusted trained professionals.
In addition the complete process of information collection, on-site analysis and reporting takes time. Finally effort has to be made in the ongoing process of optimizing the red teams methods and techniques to ensure instant knowledge about new developments and technology as it comes available.

A red team plays a modest, though effective role in the bigger picture of the information security and information assurance fields. However, the sorts of vulnerabilities which can be found during red team activities are supportive in the process of developing and maintaining the basis of information security - a security policy. A security policy describes organisational procedures and technical measures to reduce and contain the risks. Without such policy, an occurring incident can result in a much higher non-predictable financial loss. A red team will offer part of the solution by pinpointing and reporting weak spots in an information technology infrastructure resulting in the taking of adequate measures. At the end it's better to prevent and stay ahead of trouble instead of waiting for things to happen.

REFERENCES

Computer Emergency Response Team (CERT). http://www.cert.org

Dan Farmer and Wietse Venema. "Improving the security of your site by breaking into it"
http://www.deter.com/unix/papers/improve_by_breakin.html

Steven M. Bellovin. "There be Dragons". AT&T Bell Laboratories. August 15, 1992.
http://www.research.att.com/~smb/papers/dragon.pdf

Steven M. Bellovin. "Packets found on an Internet". August 23, 1993.
http://www.research.att.com/~smb/papers/packets.pdf

William R. Cheswick and Steven M. Bellovin. "Firewalls and Internet Security : Repelling the Wily Hacker". Addison-Wesley, 1994. ISBN: 0-201-63357-4.

TNO-FEL's URLography on Information Security.
http://www.tno.nl/instit/fel/infosec

NOTES

[1] TCP/IP stands for Transmission Control Protocol/Internet Protocol. TCP/IP is the protocol on which most of the modern Internet is based.

[2] Taken from Datafellows Anti-Virus.

[3] To simplify we'll omit the technical discussion about sequence numbers.

[4] The standard Microsoft Windows NT password is 14 characters maximum.

AN HOLISTIC APPROACH TO INFORMATION OPERATIONS: The Canadian Experience

Tiit T. Romet
Ibis Research Inc. and Private Consultant,
Formerly Defence Scientist, DND, Canada

ABSTRACT

This paper will initially describe the elements of the broad conceptual framework that was employed. It will then describe the specific concept developed within the CF and an outline of the structures that have been put into place. The paper will conclude with observations on lessons learned, and the difficulties experienced in following the holistic approach towards developing the Information Operations program, both within the military and the government at large.

BACKGROUND

Five years ago, the Canadian Forces (CF) were faced with decisions on how to integrate information based operations into its military routine. With the rapid evolution of computer and communication technologies, information was recognized at the outset as a strategic resource that must be effectively managed. Canada was already integrally networked with the United States in numerous related areas such as telecommunications and banking. Coupled with the overall global growth of commerce and information exchange via ever expanding communications networks, it was necessary to understand that the traditional view of borders no longer existed.

The expectations were being created not only in the military, but also in government and private sectors that information can be instantaneously gathered, analyzed and exchanged. The Internet had become the network by which personal (private), business and even (sensitive) military information could be exchanged. Both our economic and military effectiveness was increasingly dependent upon automated information systems and networks. Furthermore, as cost cutting and the creating of new efficiencies emerged, the military was integrating more and more civilian technologies into their military systems. We described these phenomena as the “civilianization of the military.”

With the United States military moving forward rapidly in this new domain, which they initially called “Information Warfare”, Canada needed to address the many issues that faced them. The CF understood that it did not have the human or fiscal resources to take the US approach and needed to develop a conceptual framework within which its own requirements could be analyzed and implemented.

DEVELOPING THE FRAMEWORK

The Advancement and Employment of Technology

It is generally accepted that the emergence of information based activity is directly linked to the technological advances occurring over the past decades and their application. The key technology areas, which are the underlying elements, include **communications, sensors** and **computers.**

The breadth and variety of **communications** that have developed vastly improves the options, complexity and criticality of the information that it carries. With the means of transmission offering greater choices, ranging from wireless, to wideband copper cables to optical fibers, the progressively increased availability of the number of channels, bandwidths and types of circuits (eg. satellite relay, cable television etc.) has extended the range, and shortened the time over which information can be exchanged.

Information is now available through a greater number of sources, and in particular from the military perspective, non-human **sensors.** The whole electro-magnetic spectra can be exploited passively or actively through the various collection means such as radio, radar, infrared/electro-optics, and synthetic aperture radar. In parallel though, the countermeasures have also evolved to better mask, deceive or hide objects of interest.

The constant evolution of **computer** hardware and software through increasing size, power and applicability while decreasing in size and cost is a daily reminder of the difficulty in staying at the lead-edge of information technology.

Not only has the technological basis for the information-based society evolved, so have the systems and organizations which utilize the technology increased in number and complexity. **News media** now cover global activity on a 24-hour, 7-day a week basis and increasingly, it is being made equally available to greater numbers of the world's population.

The **Internet** has become underlying conduit for much of the exchange of information and communication. It has evolved dramatically from its beginnings, a proposal by the RAND Corporation as nuclear-survival network using individually unreliable or vulnerable elements interconnected so that system capability and functionality would be survivable. Today, the demand for information via the Internet overrides the concerns for security and integrity of the information, or the reliability of the source. Consequently, even today, information can be exposed to interception, distortion or theft.

Electronic commerce is the most rapidly growing economic area. Legal tender in the form of money, stocks and bonds, and many other transactions now occur electronically or are only an electronic entry in a databank. The commerce of Canada (and thus that of the CF) is heavily dependent on the privacy and accuracy of the Internet and its commercial equivalents.

Information Environments and Infrastructures

While the United States began its exploration and activity in Information Operations from within the military, Canada chose its starting point the **global information environment (GIE).** The GIE was defined as individuals, organizations or systems outside the sphere of military control, and while separate and distinct, encompasses the **military information environment (MIE).** It was considered that all "operations" take place within the GIE and because of the technological advances, military operations can be viewed, analyzed and disseminated to a global audience in near-real time. In fact, in can be shown that information could be distributed quicker via commercial linkages than by government or military means.

To support the GIE, there exists a **global information infrastructure (GII)** that is an interconnection of communication networks, computers, data bases and consumer electronics that allows for the access of information to a wide audience. It is linked globally and characterized by a merging of civilian and military information networks and technologies. There exists within the GII, **national information infrastructure (NII),** which consists of a series of components that include public (governmental) and private information networks and support national visions, activities and organizations. There are no discreet boundaries between the GII and NII; in fact, global access to information becomes increasingly critical with the globalization of markets, resources and economies. The **defence information infrastructure** is embedded within the above two infrastructures provides mission support, command and control and intelligence networks to the military.

Information and Decision Architecture Overview

Within the broad conceptual framework, an architectural framework was established which could address such concerns as privacy, confidentiality and the decision making process. While many different models and systems have been developed to describe decision making, they all have the same basic common elements:

a. acquisition of data
b. processing of raw data into useful information which leads to understanding
c. comparison with the existing or current state
d. decision on implementation, direction etc.

It was important to understand that within the decision making cycle there were two distinct yet interrelated entities that ultimately contribute to a final decision. There exists an *information domain* that is comprised of three elements:

i. a specific set of information assets
ii. authorized uses of the information
iii. a security policy governing the use of the information assets.

As an example, the information assets could include all the medical records and information on an individual within a government health plan. The authorized users would be the selected government employees, the medical doctors and the patient. The security policy would specify how information is protected, who has access, how the information is stored, processed etc.

The other entity is the actual *information systems*, which comprises of the processing and communication components that must incorporate the security features and policies outlined in the information domain.
Layers of Vulnerability

The actual structure of the information system can be separated into three layers which overlay each other and are based on their function: physical, logical and semantic. This categorization has been useful in understanding the vulnerabilities of information within any information infrastructure. At the base is the **physical layer** that can be described as the hardware elements of the information system. These would include buildings, computers, communication equipment and even personnel. This view naturally leads to the concept of carrying out "links and nodes" analysis. The middle strata is the **logical layer** which consists of how the structure is operated, the software, the systems, the processing of data into information and ultimately knowledge, and the distribution of the information and the operating procedures. The third and highest level we called the **semantic level** and represent the content and interpretation of the information contained within the information system.

The **physical layer** is vulnerable to physical destruction and the object of traditional military weapon systems. As civilian and military infrastructures become more and more integrated, greater emphasis must be put into links and nodes analysis to ensure effective targeting. The goal of disrupting the **logical layer** is to interfere with system functions. Attacks could include delaying of the execution of procedures, misdirecting information or infection by software viruses. In the ideal disruption, the attacker does not need to destroy the information or system but rather control it. At the highest echelon, the **semantic level**, the objective of the attack is to affect and/or exploit the trust users have in the information system, the network and in their ability to interpret and make decisions about the information. Our broad framework emphasizes that what the military had called Psychological Operations may have a much broader context if describing global or national information infrastructures.

Implications to the Military

The broad framework that was being outlined was attempting to show that a society's ability to wage war depends on every component of the technological infrastructure that now exists. The ever increasing interdependencies between civilian and military infrastructures demands changes in how conflict is to be carried out, challenges the design of traditional institutions and hierarchies and redraws our concept of borders and national security. As stated by the Tofflers, societies wage war by their means of producing wealth, and we are, or have moved, into the information era.

THE CANADIAN FORCES CONCEPT

Based on the initial broad concept development, and then through follow-up visits, meetings, and discussions, the Canadian Forces formulated their vision of Information Operations. For the CF, IO went beyond simply information systems and processes, but rather, **IO should be viewed as a STRATEGY, NOT a capability unto itself.** If viewed as a strategy, then the objective of IO became the decision-maker, whether they be a president, prime minister,

commander or individual service member, sailor, soldier or airman. Therefore, IO became a strategy that integrates various capabilities to achieve political or military objectives. It followed then that IO includes a wide range of capabilities that could encompass traditional military activities such as destruction, deception, OPSEC, EW, PSYOPS (C2W) to technologically based activities such as computer network attacks, or civil affairs, public affairs and even legal affairs.

Definition

For the CF, the definition became:
"Actions taken in support of political and military objectives which influence decision makers by affecting other's information and/or information systems while exploiting and protecting one's own information and/or information systems."

The CF definition for IO shows that information is the means, and the decision maker is the end. The definition intentionally downplayed the technical aspects of IO and focuses on all measures that could be used to influence the decision maker. While many debates have gone on in Canada, as well as throughout the world on defining IO, the CF definition was intended to be broad. As such, it could be applied to national, international, civil or military activities and applies equally to peace, crisis or war.

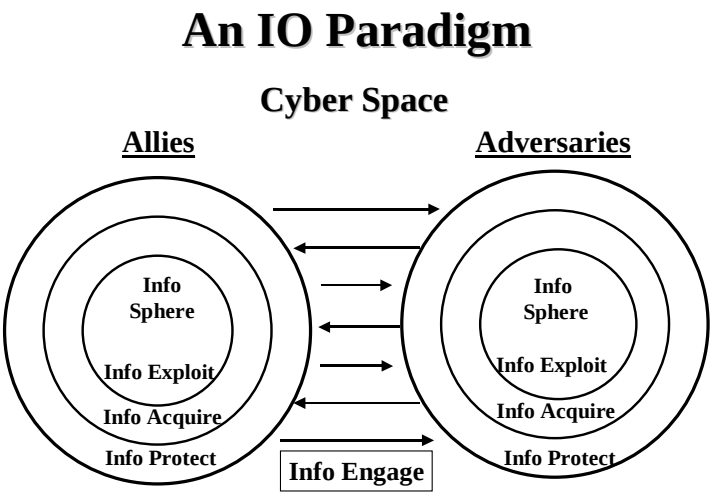

Figure 1: The IO Paradigm

The IO paradigm that was developed to portray the CF message and that became the basis for the development of the CF structure was a series of information "spheres" as shown in the above figure.
This environment, that was called for lack of any better words **cyber space,** contains the sum total of all information, both adversarial and friendly. There are four basic processes that can be carried out in this cyberspace: information exploitation, acquisition, protection and engagement with the understanding that the same activities will be carried out simultaneously by any adversary.

The CF wants to be able to **exploit** the information it possesses. This implies having a system established that will provide the appropriate information to the appropriate user at the appropriate time. The CF will need to **acquire** information, both that pertaining to our potential adversaries through various intelligence and other means, and that of our allies and friends to ensure compatibility. Whenever one collects or exploits information, it also needs to **protect** the information and the processes by which it collects and exploits. This process will include both protection from our adversaries through computer/system intrusion detection and reaction; and from ourselves, such as the disgruntled employee or viruses. The protection aspect also includes the ability to recover and operate after intrusions or disruptions. Finally, the CF needs to **engage** our adversaries (or our own internal "enemies") by trying to prevent or blind their ability to acquire information, break through their protective mechanisms and acquire or gain control of their information and/or processes.

IMPLEMENTATION INTO THE CANADIAN FORCES

It was from these four basic processes and functions, exploit, acquire, protect and engage, that the CF evolved its IO Group structure and activities to be able to carry out its responsibilities and mandates. Parallel to this effort, the Defence Department was also engaging the other government departments and Privy Council Office (central government activities) both at the Executive and Staff Working levels, to establish a co-ordinated government response to the threats and vulnerabilities. DND saw itself has having an important role to play but one as a partner in the larger Government of Canada process. This view integrated well with the overall concept of Global and National Information Infrastructures, their protection and Canada's role within these processes.

IO Working Group

Initially, the CF established an IO Working Group to address many of the issues that needed to be investigated for the military to become proficient in IO, including concepts, doctrine, policy, R&D requirements and training. The Group encompassed all the major components of DND including J3 Operations, intelligence, the three services, legal, policy, Chief Information Officer, R&D community and public affairs.

Since its inception, the CF has re-structured to form the CF Information Operations Group (CFIOG). This effort integrated and consolidated many functions that relate to IO activities to form a single voice to represent IO activities. New activities were established based on the IO paradigm that was described earlier. A National Vulnerability Assessment Team (NVAT) was initially established to begin the role of protection of the CF's information resources. This activity has now been joined by a Computer Incident Response Team (CIRT) and is currently establishing the mechanisms to detect, report and investigate intrusion attempts of military information systems.

Parallel to these efforts, CF Doctrine has been written, approved and disseminated. Individual service doctrines have been prepared and integrate with the broader CF Doctrine. While this aspect was completed without major delays, the CF Policy development was more difficult. Among the largest issues included concerns about the role and activity of PSYOPS, its relationship with Public Affairs, and legal aspects of offensive and defensive IO activities.

Some of the key features that the recently approved policy contains include:

a) IO is an integrating strategy that focuses on all aspects of influencing decision makers
b) IO is not simply a technical issue, but includes things such as publics affairs, PSYOPS, government infrastructure vulnerability
c) Commanders are responsible to implement defensive IO at all times
d) Co-ordination of IO will be carried out by an Information Operations Co-ordination Cell (IOCC)

Information Operations Coordination Cell

The IOCC concept has been designed to provide IO inputs to operational plans developed by the National military staff. The composition is seen to be flexible, customized to meet the needs of specific requirements. While the concept has been accepted, it has yet to be activated consistently for exercises or operations. The inclusion of IO requires major re-thinking by staff and re-alignment of planning processes by all concerned. It will undoubtedly be some time before consideration of IO becomes second nature to our planners and staff.

Role of Research and Development

From the earliest stages of IO concept development, it was clearly stated that the R&D community needs to be engaged in supporting the CF IO process. Each of the IO processes defined in the IO paradigm, protection, exploitation, acquisition and engagement need a significant R&D contribution for the CF to fully carry out its role. This role becomes a particular challenge with the evolving relationship between civilian and military technologies and requirements.

J6 Coordination Role

Within the CF, the J6 have been given the role of coordinating the IO development. A small IO staff forms the permanent nucleus of the IO coordination role and provides the constant IO visibility required to implement the change. This role includes not only CF and Government of Canada functions but our international relationships as well. They have the advantage of having implemented the IO concepts and establishing the structures to accommodate the requirements.

LESSONS LEARNED, BEING LEARNED, TO BE LEARNED

With the National Government

The basic concept that was initially established and maintained throughout the IO developmental process was that IO was a strategy and that it encompasses an information environment that exceeds that of the military alone. This holistic approach therefore requires contributions from the whole to function effectively, otherwise the Department of National

Defence (DND) would operate in a vacuum. The greatest difficulty DND has encountered is probably the reluctance of the Government of Canada to accept the leading role that is necessary in the holistic approach; and a role that all participants engaged in the area have expressed as necessary. National Defence sees itself as a significant but wholly cooperative member integrated into a larger national role.

Another difficulty that arises in Canada's situation has been its reliance on incorporating IO developments and studies originating abroad into a Canadian position. This will diminish Canada's role as an innovator in IO, both in civilian and military fields. However, it can argued that by taking the cautious approach, Canada will avoid repeating earlier mistakes; but at the cost of losing its uniqueness which it could have established. In this process however, DND is left to forge ahead in the IO arena without the benefit of strong central leadership.

It is therefore not surprising, that Canada remains the only Western/technologically advanced nation without a government sponsored computer incident response team. With the holistic approach taken by DND, the concept of information as a national asset is a fundamental premise, and as a result requires appropriate national security to be considered as well.

With the Department of National Defence

Certainly an advantage of the holistic approach has been the relatively smooth development of DND policy and doctrine. In particular, the integration of individual service policy and doctrine has been made easier. Trying to achieve a departmental consensus, let alone a national consensus, is much more difficult if it is being driven from the bottom up.

The introduction of IO into the Department has created the opportunity for new roles to be established, especially in some traditional areas. For example, the J6 that has traditionally been responsible for communications and electronic support finds itself potentially controlling "operational weapons" in the form of computers and networks. While the J6 in Canada has firmly believed in the lead role of the operational elements of the department when it comes to IO, it has been given greater responsibilities in areas that have not been traditionally within their mandate.

As the slow transition to the IO Group took place, it was obvious that a number of traditional roles and structures were going to be changed. It has been a characteristic of many organizations, not only within DND but elsewhere as well, that there is the tendency to consolidate and protect the existing structures and functions. Yet with a holistic approach to IO, and in organizational development in general, rather than becoming more inward and protective, it is far more beneficial to leverage skills and functions. This is a difficult lesson to learn.

With the new IO concept, it is also necessary to develop personnel with new skill sets, and to be placed into new, non-traditional roles. It follows that new opportunities have to be made for training, and within the personnel system, recognition for the new roles and responsibilities that are associated with carrying out IO related functions. The holistic approach has made these opportunities slower in evolving as traditional roles and training still receive the greatest attention and support. No longer can military personnel be expected to be posted into a new position for three years and then move on. The training and demands of

working within IO requires a longer commitment and ongoing training to remain at the lead edge. These issues still need further refinement within the CF to fully benefit from an IO program.

Research and Development

The military R&D community finds itself in a particularly difficult position. First, it must compete forever diminishing resources within government. Second, and more importantly, it must compete against the civilian/commercial competitors that have been at the technological lead edge for a number of years. This also means that the traditional R&D role needs to change or adapt to one of being a leading edge integrator rather than innovator. This is particularly relevant in the Canadian situation where Canada seldom produces complete systems, but rather provides components or produces hybrid systems that have integrated numerous technologies and concepts. As well, to maintain pace with the civilian and commercial sectors, the former concepts of long, medium and short-term research need to be re-thought. Because of the increased integration required, it is almost a necessity for the R&D scientist to work hand-in-hand with the operator to be fully integrated into the IO operational strategy.

General Comment

From the initial IO working groups, it was made abundantly clear that no new financial allocations could be expected for IO activities. It was expected that existing funds be re-allocated to meet the needs. In a holistic approach, the opportunities to find re-allocated funds are much fewer since every organization and manager will be trying to protect their limited resources. Even the US approach of working up from the individual service elements eventually reaches a point where there is no further opportunity to re-allocate or adjust funding. Since IO has been introduced as a new concept with its own set of threats and vulnerabilities, it does become necessary to inject new funding and personnel into the area.

ACKNOWLEDGEMENTS

There have been many individuals that have contributed to the IO development within the Department of National Defence and without which, I would not have had the opportunity to prepare the accompanying paper. Among the many individuals that need mentioning are: Robert Garigue, currently Chief of IT Security/CIO office for the Province of Manitoba; Dr. Leroy Pearce, Scientific Technical Advisor to the CIO, DND; Col Randy Alward, Commander IO Group, DND; LCol Alan Smith, J6 IO, SqLeader Barry Horne, Majors Alan McGreer and Randy Colmar, exchange officers in J6IO; Maj Doug Smith; Dr. Brian Harrison; Capt Luc Dandurand and WO Bruce Fraser of the IO NVAT team; Dr. Brian Eatock H/IO and Mr. Gordon Marwood, Chief Scientist, Defence Research Establishment Ottawa.

INFORMATION WARFARE IN THE CONTEXT OF SECURITY-RELATED ISSUES
Where could we go from here?

Dr W. Stein
Forschungsgesellschaft für Angewandte Naturwisschenschaften, Germany

ABSTRACT

The goal of this paper is to find orientations, helpful illustrations as well as definitions, and perhaps critical factors that can help to open a gate for more cooperation in research, development, and education in the area of today's information security-related issues. This area includes Information Security (INFOSEC), Information Warfare (IW) and Critical Infrastructure Protection (CIP). One can find many traditional factors impeding understanding and cooperation that may include different term s and definitions, economic competition, and interests of national security. It turns out that there exists a common problem area in the context of information warfare, with challenges for a new level of cooperation in science, engineering, and education.

INTRODUCTION

It has been well accepted meanwhile that the information and communications sector with its information systems and infrastructures is central to all other sectors of modern societies, indeed to essentially every aspect of national and international functioning. Attacks on information systems are already a fact of life in the information age. Almost daily, hackers explore vulnerabilities in our global information infrastructures and in computer systems. Various ideological and cultural adversaries - individuals, guerrilla and terrorist groups - are on the way to discover 'Information War' as a major means to disrupt operations in government, military, and corporate sectors. As a consequence, information operations (Info Ops) have changed from conceptual thinking into reality and are on the way to become a hot topic, in military areas, in government areas, and in corporate areas. Governments, armed forces, and society as a whole need to be prepared, in order to counter these information threats and attacks. But currently there seems to exist a lack of awareness about information security and infrastructure vulnerabilities.

Although a small portion of these attacks result in significant loss or damage, the vast majority of them result in little or no damage - the crime equivalents of trespassing, public nuisance, minor vandalism, and petty theft. It has been estimated that more than 90 percent of these attacks are perpetrated using available tools and techniques (based upon incidents reported to CERT), that only 1 attack in 20 is noticed by the victim, and that only 1 in 20 gets reported (these last two statistics were a result of a Defense Information Systems Agency (DISA) study and similar rates have been reported by others). However, it appears that reporting rates may be on the increase. As we can see, there is (nearly) nothing new in this area. As a consequence, the interest in securing information, computers, and networks arose early and the first report dates back to 1970 [24]. After the emergence of the Critical Infrastructure Protection (CIP) program during the last five to ten years, we are faced now with three security-related areas with interrelated challenges: Information Security (INFOSEC), Information

Warfare (IW) and Critical Infrastructure Protection (CIP) [1/ 18/ 23/ 24]. While screening the security-related issues, we can find various terms, sometimes redundant definitions, and overlapping areas (different between communities, nations etc.), e.g. security, assurance, and protection of information and/or infrastructures; as well as information warfare and information operations [23]. These heterogeneous and diverse components can make cooperation difficult or even impossible. Figure 1 shows the areas of Information Warfare (IW), Information Security (INFOSEC), and Critical Infrastructure Protection (CIP) as well as their potentially interrelated sub-areas. Although the three areas have many common subjects (e.g., in problem areas, methods, tools; partly using the same infrastructures, having similar research and development goals, using similar analysis frameworks etc.) the degree of cooperation in research and development seems to be very limited.

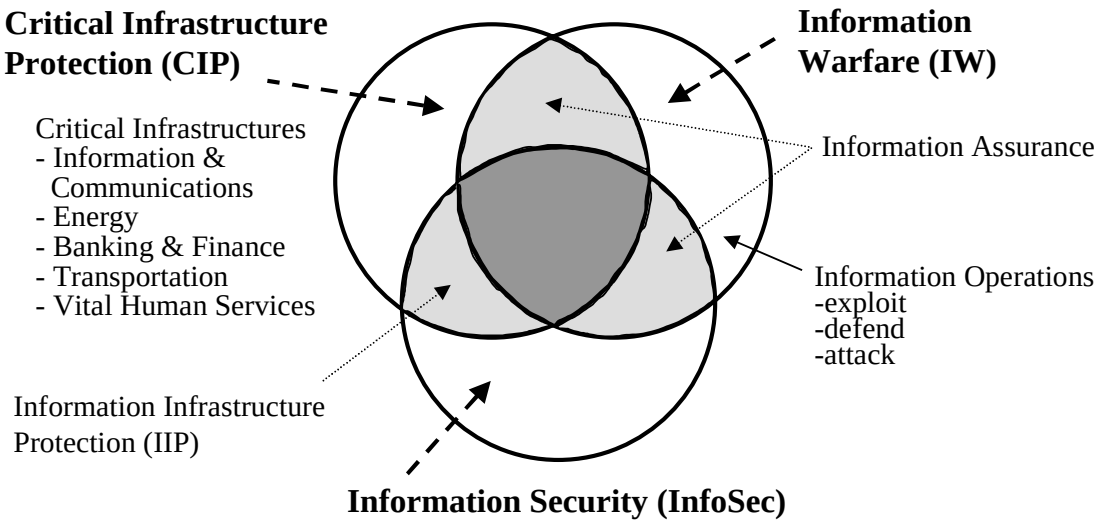

Figure 1: Areas and interrelated Sub-Areas of Information Warfare, Information Security, and Critical Infrastructure Protection.

The term 'information security' (INFOSEC) has been around for at least two or three decades. A US federal standard defines it as "The protection of information against unauthorized disclosure, transfer, modification, or distraction, whether accidental or intentional." By contrast, the term 'information assurance' is relatively new [4]. A 1996 US Department of Defense directive defines it as "Information operations that protect and defend information and information systems by ensuring their availability, integrity, authentication, confidentiality, and nonrepudiation. This includes providing for restoration of information systems by incorporating protection, detection, and reaction capabilities." Defensive information warfare is closely related to both concepts but is concerned only with intentional attacks. Information security and information assurance also address unintentional threats, e.g., errors, accidents, and natural disasters [4].

Thus information assurance is based on an Info Ops definition and has a somewhat broader meaning than information security. The term information assurance can be found meanwhile in various government areas, e.g., Department of Defense, Critical Infrastructure Protection, and National Security Agency [14]. Various definitions of information operations (Info Ops) are

presented in [23]. NATO defines Information Operations as [10]: “Actions taken to influence decision makers in support of political and military objectives by affecting other's information, information based processes, command and control (C2) systems, while exploiting and protecting one's own information and/or information systems. There are two main categories of Info Ops: defensive Info Ops and offensive Info Ops, depending upon the nature of the actions involved”.

SECURING NETWORKED INFORMATION SYSTEMS

As figure 2 indicates, today's challenge is on securing networked information systems, in civil as well as in military environments. Consequently the NSA Information Systems Security Organization (NSA/ISSO) has defined an information system (IS) as: “The entire infrastructure, organization, personnel, and components, for the collection, processing, storage, transmission, display, dissemination, and disposition of information”, and information systems security (ISS) as: “Protection of information systems against unauthorized access to or modification of information whether in storage, processing or transit, and against the denial of service to authorized users, including those measures necessary to detect, document, and counter such threats.” Securing networked information systems requires an overall system perspective. Security is tightly coupled with safety and reliability, and must not be ignored or relegated to incidental concerns. We take a broad view here of the problems of attaining security and safety, and consider these problems as a unified global system/network/agency problem. The securing procedure indicated in figure 2 can be applied to a single computer platform as well as to the IT systems and infrastructures of a national-scale level [1].

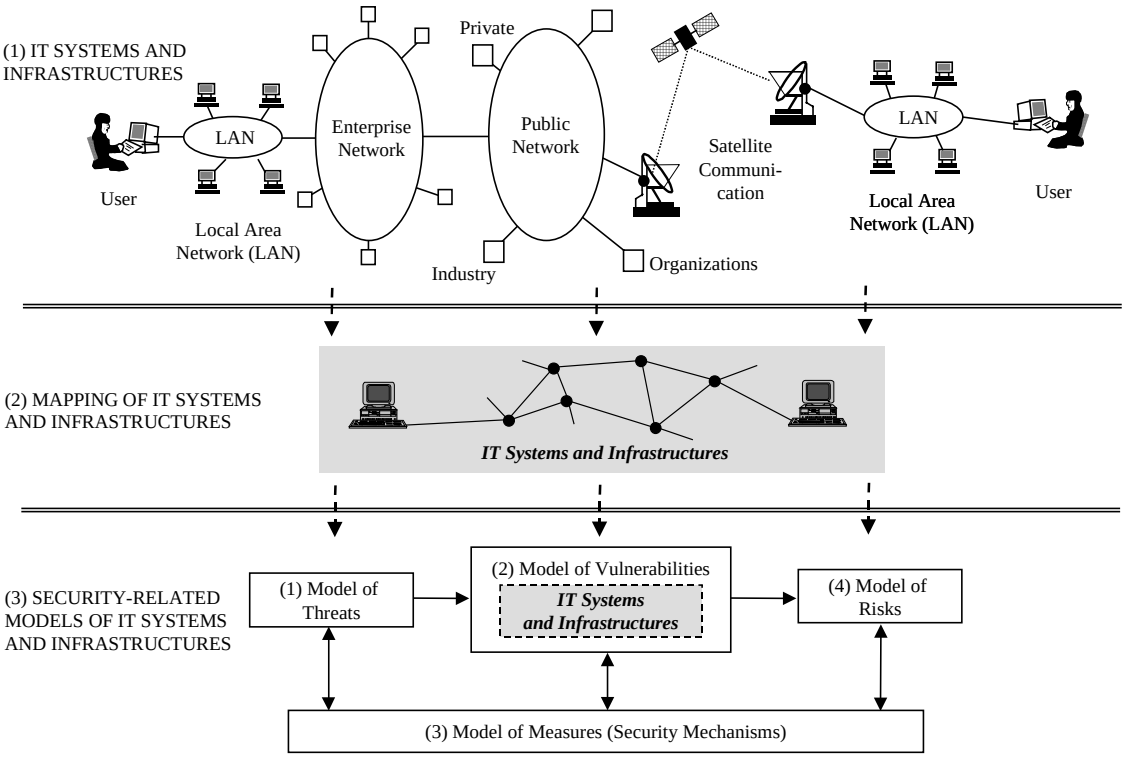

Figure 2: Steps in Securing Networked Information Systems: Analyzing Vulnerabilities, Threats, and Risks.

Security vulnerabilities (figure 2) are ubiquitous. Most computer operating systems have weak authentication and are relatively easy to penetrate. Most such systems have weak access controls and tend to be poorly configured, and are as a result relatively easy to misuse once initial access is attained. These systems often have monitoring facilities that are ill adapted to determining when threats are mounting and what damage may have occurred. Consequently, misuse by outsiders and insiders is potentially easy to achieve and sometimes very difficult to detect.

Threats to security (figure 2) are ubiquitous. The range of threats that can exploit these vulnerabilities is enormous, stemming from possible terrorist activities, sabotage, espionage, industrial or national competition, copycat crimes, mechanical malfunctions, and human error. Attacks may involve Trojan-horse insertion and physical tampering, including retributive acts by disgruntled employees or former employees or harassment. Denial of service attacks are particularly insidious, because they are so difficult to defend against and because their effects can be devastating. Systems connected to the Internet or available by dial-up lines are potential victims of external penetrations. Even systems that appear to be completely isolated are subject to internal misuse. In addition, many of those seemingly isolated systems can be compromised remotely because of their facilities for remote diagnostics and remote maintenance.

Risks are ubiquitous (figure 2). The consequences of these vulnerabilities and associated threats imply that the risks can be very considerable. Computer-related misuse may (for example) result in loss of confidentiality, loss of system integrity when systems are corrupted, loss of data integrity when data is altered, denials of service that render resources unavailable, or seemingly innocuous thefts of service.

INFORMATION SECURITY-RELATED ISSUES

Information security (INFOSEC) is the fundamental and in some respect already classical part of the three security-related issues. Information security (or computer security, as it was initially called) was first definitively characterized in a Defense Science Board report in 1970, but practical and operational experience, in particular incorporation of security safeguards into systems, commenced much later [24]. Computer security as a discipline was first studied in the early 1970s, although the issues had influenced the development of many earlier systems. The decade of the 1970s was devoted largely to research funded by the Department of Defense, notably the US Air Force and DARPA. According to [24], real-world experience did not begin until the publication of "Department of Defense Trusted Computer System Evaluation Criteria" commonly known as "The Orange Book" or the TCSEC. Throughout the 1970s and 1980s, INFOSEC efforts were focused on non-networked, trusted computing security evaluation criteria (TCSEC) and communications security (COMSEC) for national and military communications. Even then, systems incorporating security safeguards were not installed until the late 1980s. The subject of information operations was developed in experiments by US forces, mainly in the years between 1985 and 1995 [5/ 8/ 10/ 13/ 19/ 21/ 22/ 23/ 25]. Beginning in the late 1980s, there has been increased interest in protecting the critical infrastructures upon which society depends against physical and information attacks. The Critical Technologies Institute (managed by RAND) was created in 1991 by an act of Congress and studied and defined the issue of Critical Infrastructure Protection (CIP) [1/ 18/ 23/ 24.]

INFORMATION SECURITY

Intuitively, the natural-language meaning of security implies protection against undesirable events. System security and data security are two types of security. INFOSEC can be defined at two levels [23:] At the policy level, INFOSEC is the system of policies, procedures, and requirements to protect information; at the technical level, INFOSEC includes measures and control that protect the information infrastructure against denial of service, unauthorized disclosure, and modification or destruction of information infrastructure components (including data). INFOSEC includes the totality of security safeguards needed to provide an acceptable protection level for an infrastructure and for data handled by an infrastructure. More recently, the aspect of survivability (the capacity to withstand attacks and functionally endure at some defined level of performance) has been recognized as a critical component of defenses.

A comprehensive system- and network-wide set of realistic requirements is desired, encompassing security, reliability, fault tolerance, performance, and any other attributes necessary for attaining adequate system and network survivability. The most general topic of system requirements is dependability (in [11] survivability is discussed instead). Dependability (or survivability) includes the component requirements (A) security, (B) reliability, and (C) performance. The primary properties of security are (1) confidentiality, (2) integrity, and (3) availability. Survivability is the ability of a networked information system to satisfy and to continue to satisfy certain critical requirements (e.g., requirements for security, reliability, real-time responsiveness, and correctness) in the face of adverse conditions. Survivability must be defined with respect to the set of adversities that are supposed to be withstood. Types of adversities might typically include hardware faults, software flaws, attacks on systems and networks perpetrated by malicious users, and electromagnetic interference. As is often done for reliability, survivability could alternatively be defined as a probabilistic measure of how well the given requirements are satisfied. But mostly a non-quantified definition is preferred. There are clear links between the concept of system survivability and dependability. The three primary attributes of security are (1-3), whereas additional three attributes (4-6) in common use too:

(1) Confidentiality protects the existence of a connection, traffic flow, and information from disclosure.

(2) Integrity assures that information and processes are secure from unauthorized via methods such as encryption, digital signatures, and intrusion detection.

(3) Availability provides assurance that information and services will be accessible and usable when needed.

(4) Authentication assures that only authorized users have access to information and services.

(5) Non-repudiation assures that transactions are immune from false denial of sending or receiving information by providing reliable evidence that can be independently verified to establish proof of origin and delivery.

(6) Restoration assures information and systems can survive an attack and that availability can be resumed after the impact of an attack.

Security includes both system security and information security. It must anticipate all realistic threats, including misuse by insiders, penetrations by outsiders, accidental and intentional interference (e.g., electromagnetic), emanations, covert channels, inference, and aggregations. There is much more to security than merely providing confidentiality, integrity, and availability. Reliability is generally defined as a measure of how well a system operates within its specifications. For, example, fault tolerance can enable a variety of alternatives, including real-time, fail-safe, fail-soft, fail-fast, and fail-secure modes of operation. Performance is a critical requirement. In some cases, adequate performance may be critical to the survivability of an enterprise or an application. On the other hand, in most cases, performance is itself dependent on survivability and availability. If a system is not survivable, adequate performance cannot be achieved. What is immediately obvious is that close interrelationships exist among the various requirements.

Here we resume the steps of securing networked information systems (figure 2) as they are described by Waltz [23]. Security analysis must be applied to determine the degree of risk to the system, to identify design, configuration, or other faults and vulnerabilities, and to verify compliance with the requirements of the security policy and model. The analysis can range from an informal evaluation to a comprehensive and exhaustive analysis.

The first step in the analysis process includes an assessment of the threats to the system, based on intelligence and extrapolations of technology capabilities. The vulnerability assessment hypothesizes the areas of likely access (internal and external) and assesses the relative vulnerability (or security weaknesses) to attack. Vulnerabilities can be attributed to failures in analysis, design, implementation, or operation of the network or system.

The result of the threat and vulnerability assessment is a threat matrix that categorizes threats (by attack category) and vulnerabilities (by functions). The matrix provides a relative ranking of the likelihood of threats and the potential adverse impact of attacks to each area of vulnerability. These data form the basis for the risk assessment.

The risk management process begins by assessing the risks to the system that are posed by the risk matrix. Risks are quantified in terms of likelihood of occurrence and degree of adverse impact if they occur. On the basis of this ranking of risks, a risk management approach that meets the security requirement of the system is developed. Security can be quantified in terms of risk, including four components: (1) percent of attacks detected; (2) percent detected and contained; (3) percent detected, contained, and recovered; and (4) percent of residual risk. This phase introduces three risk management alternatives:

> (1) Accept risk: If the threat is unlikely and the adverse impact is marginal, the risk may be accepted and no further security requirements imposed.
>
> (2) Mitigate (or manage) risk: If the risk is moderate, measures may be taken to minimize the likelihood of occurrence or the adverse impact, or both. These measures may include a combination of OPSEC, TCSEC, INFOSEC, or internal design requirements, but the combined effect must be analyzed to achieve the desired reduction in risk to meet the top-level system requirements.

(3) Avoid risk: For the most severe risks, characterized by high attack likelihood or severe adverse impact, or both, a risk avoidance approach may be chosen. Here, the highest levels of mitigation processes are applied (high level of security measures) to achieve a sufficiently low probability that the risk will occur in operation of the system.

When the threats and vulnerabilities are understood, the risks are quantified and measures are applied to control the balance of risk to utility to meet top-level security requirements, and overall system risk is managed. The design stage then implements the design, which must undergo design analysis and security verification testing. In addition, an independent red team may also be chosen to conduct the security verification testing, which implements the threat model in an attack engine to conduct simulated attacks on the system to evaluate actual security performance. Red team attacks (also called “penetration testing”) target the physical and operational security as well as the technical aspects of the system. The results of the red team verification may result in design changes to assure compliance with the system security requirements.

INFORMATION WARFARE

As with security and assurance of information, we have to think about definitions and meaning first, since information warfare has come to mean a number of different things - perhaps a combination of them all; and what it means really depends upon someone's particular bias. (1) The pure information warrior sees information warfare as a war without bombs or bullets; a conflict of any magnitude waged anywhere, motivation independent. (2) The next group to come along believes in ‘Information in Warfare’. Many of these people feel that conventional war fighting capability can be increased through the advent of better information technologies. (3) Knowledge-Based Warfare is a nascent smart-extrapolation of the last concept and makes a distinction between information and the subjective increased value of knowledge. Ultimately, Information Warfare is about the convergence of military and civilian security issues and how people deal with them in a rapidly changing world.

The objective of information-based warfare is ultimately to achieve military goals with the most efficient application of information resources [23]. Offensive information operations are malevolent acts conducted to meet the strategic, operational, or tactical objectives of authorized government bodies; legal, criminal, or terrorist organizations; corporations; or individuals. Offensive information attacks have two basic functions: to capture or affect information. Information superiority is the capability to collect, process, and disseminate an uninterrupted flow of information while exploiting or denying an adversary's ability to do the same. If information operations are performed in the context of a strategy, they have a desired objective (or end state) that may be achieved by influencing a target (the object of influence).

Information operations are defined by the U.S. Army as Continuous military operations within the Military Information Environment (MIE) that enable, enhance and protect the friendly force’s ability to collect, process, and act on information to achieve an advantage across the full range of military operations; information operations include interacting with the Global Information Environment (GIE) and exploiting or denying an adversary’s information and decision capabilities.

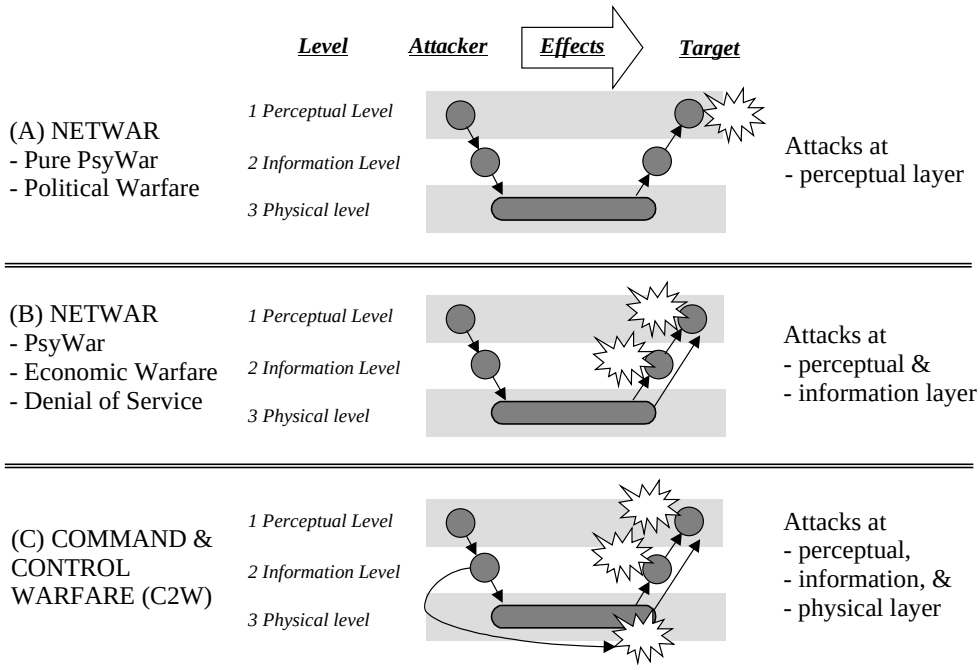

Figure 3: Three-Level Model of Information Operations [23] .

A simple functional model is presented (figure 3) to form the basis for future discussions of operations and the techniques employed [23]. The model is an extension of the basic conflict model and includes concepts that recognize three conceptual domains of information operations activity. The model recognizes that targets exist in (1) physical space, (2) cyberspace, and (3) the minds of humans. The highest level target of information operations is the human perception of decision makers, policymakers, military commanders, and even entire populations. The ultimate targets and the operational objective are to influence their perception to affect their decisions and resulting activities.

The information operations model (figure 3) distinguishes three levels or layers of functions on both the attacker and the target sides. The layers are hierarchical, with influence flowing downward on the attacker side and upward on the target side. The objective of the attacker is to influence the target at the perceptual level by actions that may occur at all levels of the hierarchy. The three layers follow the cognitive model, dealing with knowledge at the highest level, information at the intermediate level, and data at the lowest level.

The first layer is at the perceptual or psychological level, which is abstract in nature and is aimed at management of the perception of a target audience. At this level, the strategic objective defines the desired actions of the target and the perception(s) that will most likely cause those actions. If the desired action is termination of aggression, for example, the objective perception for targeted leaders may be "overwhelming loss of control, disarray, and loss of support from the populace". If the desired action is disengagement from a military action, the objective perception for targeted military commanders may be “lack of logistic support to sustain operations.” These perception objectives may be achieved by a variety of physical or

abstract (information) means, but the ultimate target and objective is at the purely abstract perceptual level, and the effects influence operational behavior.

The second layer is the information infrastructure layer, which includes the abstract information infrastructure that accepts, processes, manages, and stores the information. This is the layer that is most often considered to be the 'cyberspace' dimension at which malicious software and infrastructure exploitation (hacking) attacks occur. Attacks on this intermediate layer can have specific or cascading effects in both the perceptual and physical layers.

The third layer is the physical system level, which includes the computers, physical networks, telecommunications, and supporting structural components (e.g., power, facilities, environmental control) that implement the information system. Also at this level are the human administrators of the systems, whose physical influence on the systems is paramount. Attacks at this layer are also physical in nature.

Attacks may occur directly across the perceptual layer (e.g., a direct meeting between leaders in which human discourse is used to influence the perception of a target, or to collect intelligence), or they may target lower layers with the intent of having consequent influences on other layers.

The model illustrates how operational elements must consider each level of the model. Consider, for example, how intelligence collection for indications and warning, targeting, and battle dam-age assessment must consider all three levels.

In figure 3, the attack threads through the information warfare model for three categories of information warfare are illustrated. Exploitation of the physical and information layers purely for purposes of perception management, or psychological warfare (PSYWAR), is illustrated at the top of the figure. Command and control warfare (C2W), in which attacks occur at all three layers, is depicted at the bottom of the figure. These distinctions are representative only, recognizing that in real-world conflict, attacks will occur at all levels to varying degrees. Large-scale netwar, for example, may be supported by small-scale but crucial physical attacks on infrastructure or personnel to accomplish overall objectives.

CRITICAL INFRASTRUCTURE PROTECTION

Within the last five to ten years there has been increased interest in protecting the critical infrastructures upon which society depends against physical and information attacks. The NSA Information Systems Security Organization (NSA/ISSO) defines: "Critical infrastructures are those physical and IT-based systems essential to the minimum operations of the economy and the government." We have to consider different types of infrastructures: (1) the critical national infrastructures, (2) information infrastructures such as the Internet, or whatever may replace it - a National Information Infrastructure (NII), or a Global Information Infrastructure (GII) - and (3) underlying computer systems and networking software. Important from the present perspective is the recognition that very serious vulnerabilities and threats exist in these critical infrastructures. Perhaps equally important is the recognition that these critical infrastructures are closely interdependent and that they all depend on underlying computer-communication infrastructures.

For a particular country, a characteristic set of critical infrastructure sectors may be found by identifying the attributes of the country, its structure, its institutions and organizations that inherently contribute to resilience, and derive an estimate of the present level of resilience. According to US views [11], these infrastructures initially subsumed eight major sectors: information and communications, electric power, finance and banking, water and sewage, transportation, oil and gas, emergency services (e.g., police, fire, medical), and essential government services. As the commission proceeded, it revised, slightly modified, and aggregated these sectors into five: (1) Information and Communications; (2) Energy; (3) Banking and Finance; (4) Transportation; and (5) Vital Human Services. Many of these critical infrastructures are becoming increasingly more international. This is a logical consequence of the increasing globalization.

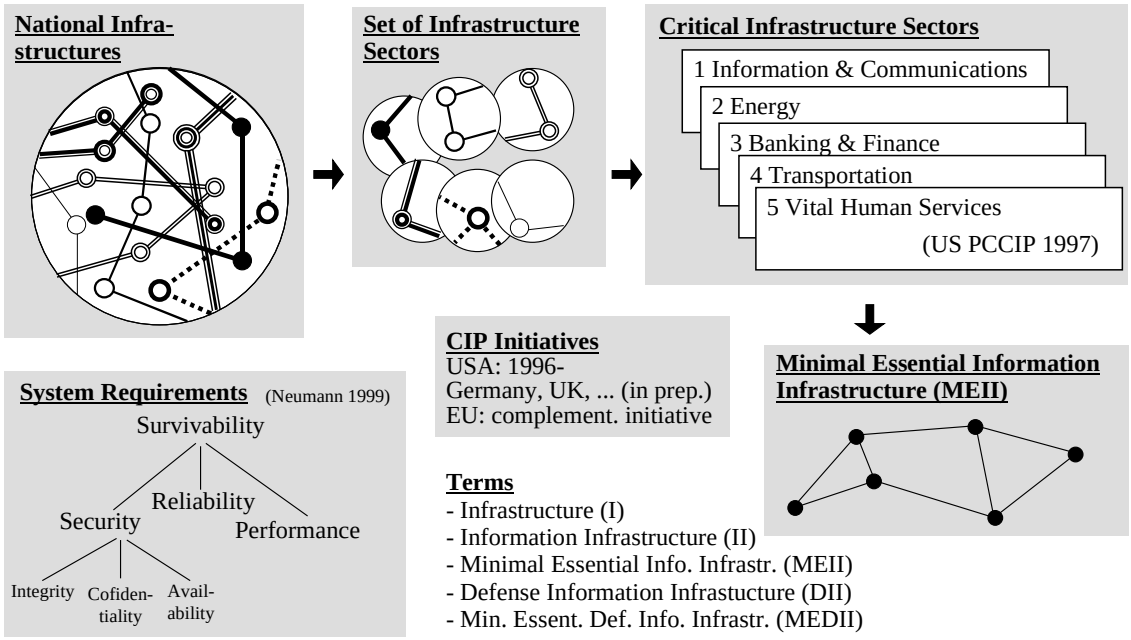

Figure 4: Approach to Critical Infrastructure Protection (CIP).

The concept of a minimum essential information infrastructure (MEII) addresses the survivability and assured availability of essential information infrastructures, particularly in the face of various forms of information warfare attack [1]. The concept has been proposed in the critical infrastructures community to ensure that some essential functionality would continue to exist despite a reasonable range of survivability threats - attacks, outages, failures, environmental disturbances, and so on. Up to now, there is a considerable debate over the definitions of minimal and essential - as well as recognition of the problems inherent in trying to focus on a single universal MEII. Nevertheless, the concept is valuable as a guiding architectural concept. Based on extensive interviews, detailed studies of the architectures of several pervasive and important systems, and analysis of the literature on vulnerabilities and risks in information systems, a methodology to assist in developing MEII-like characteristics in future information systems has been developed. The methodology consists of (1) identifying the information functions that are essential to the unit's mission; (2) determining the information systems that are essential to accomplish those functions; (3) searching for vulnerabilities within those systems components; (4) applying appropriate protection techniques for vulnerabilities found at varying system levels; and (5) testing the protections against a set of threat scenarios

to check their robustness. Application of this methodology will result in a form of MEII that is a set of systems in nested enclaves of increasing security.

The goal of infrastructure assurance research and development (R&D) is to support the development of technologies that will counter threats and reduce vulnerabilities in those areas having the potential for causing significant national security, economic, and/or social impacts. Physical and information threats are addressed. Specific technologies considered are those that protect infrastructure and thereby reduce vulnerability, detect intrusions and provide warnings, mitigate the effects of disruptions (incidents), assist in the management of incidents, and facilitate recovery. Focal points of the program are to: (1) develop technologies that support rapid recognition of large-scale attacks and (2) develop systems that exhibit inherent survivability properties, i.e., the ability to continue operation in the face of attacks that are partially successful. Particular objectives are to: (a) recognize national-scale attacks and distinguish them from events of only local significance; (b) limit the impact of an attack by ensuring the integrity of data and programs; and (c) impede denial-of-service attacks by limiting the resource consumption that can be attained by the attacker. Finally, we have to realize that many of the critical infrastructures are becoming increasingly more international. This is a logical consequence of the increasing globalization.

Meanwhile, several critical infrastructure protection initiatives are in preparation in Europe (e.g., European Union, Germany, UK). Complementary to national initiatives in Europe, the European Commission is exploring the establishment of a European Dependability Initiative of the Information Society Technologies Program. This work is carried out with the support of the Joint Research Center, Institute for Systems, Informatics, and Safety. The studies initiated by the European Commission introduce and explore the concept of survivability. It highlights the distinction between the traditional dependability perspective and the viewpoint currently explored in the survivability approach.

INFORMATION ASSURANCE AGENDA

Reporting And Analyzing Security Incidents

Reporting and analyzing security incidents will for a long time remain an unsolved problem, if only one attack in 20 is noticed by the victim and only one attack in 20 gets reported. In an unusually broad and stringent study, Howard [6] analyzed trends in Internet security through an investigation of 4,299 security-related incidents on the Internet reported to the CERT Coordination Center (CERT/CC) from 1989 to 1995. Prior to this research, our knowledge of security problems on the Internet was limited and primarily anecdotal. Howard's research accomplished the following: (1) development of a taxonomy for the classification of Internet attacks and incidents, (2) organization, classification, and analysis of incident records available at the CERT/CC, and (3) development of recommendations to improve Internet security, and to gather and distribute information about Internet security.

With the exception of denial-of-service attacks, security incidents were generally found to be decreasing relative to the size of the Internet. Estimates based on this research indicated that a typical Internet domain was involved in no more than around one incident per year, and a typical Internet host in around one incident every 45 years. The taxonomy of computer and network attacks developed for this research was used to present a summary of the relative fre-

quency of various methods of operation and corrective actions. This was followed by an analysis of three subgroups: (1) a case study of one site that reported all incidents, (2) 22 incidents that were identified by various measures as being the most severe in the records, and (3) denial-of-service incidents. Data from all incidents and these three subgroups were used to estimate the total Internet incident activity during the period of the research. This was followed by a critical evaluation of the utility of the taxonomy developed for this research. The analysis concludes with recommendations for Internet users, Internet suppliers, response teams, and the U.S. government. Howard's study presents only a preliminary analysis of the data derived from the incident records during 1989 to 1995. It was recommended that the data set should be made available on-line for use by other researchers. In addition, useful information concerning incident analysis, the related methodical problems, and the use of taxonomies, is given by Cohen [3].

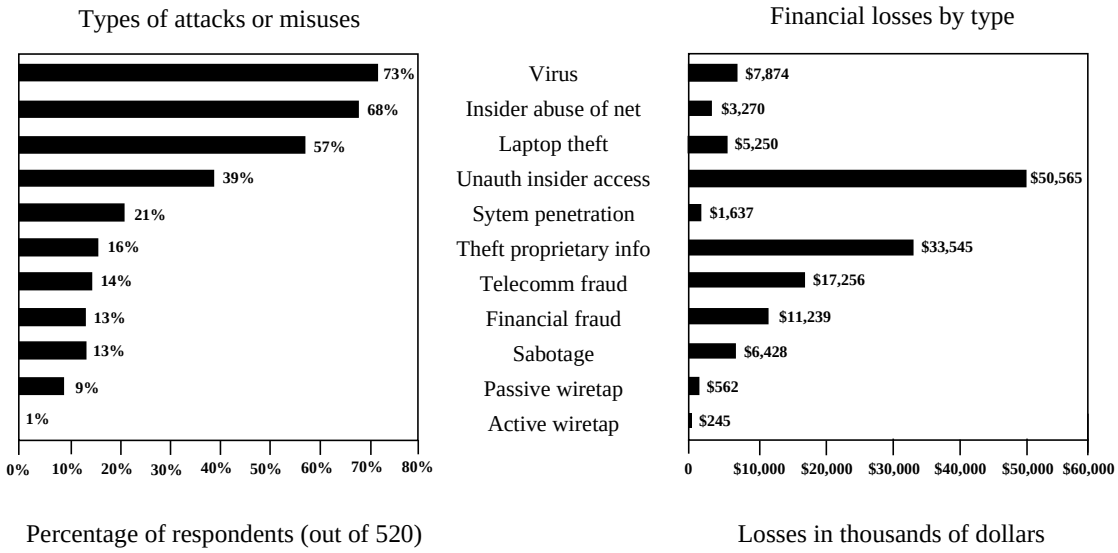

Figure 5: Computer Crime: Type of Attack and Financial Losses [4].

As correlated with increasing security incidents, computer crime and misuse have been on the rise, no doubt owing to the proliferation of computing technologies and growth of the Internet. The left side of figure 5 shows the number of respondents reporting different types of attacks or misuse against their computing and telecommunications resources, ordered from most prevalent to least prevalent type. The right side of figure 5 shows the losses in thousands of dollars for incidents of those types with quantifiable losses. The figures show that whereas computer viruses were encountered by the greatest number of companies, with 73% of respondents saying they detected incidents of that type, they did not account for the largest losses, which were attributed to unauthorized access by insiders and theft of proprietary information. The two least reported threats, active and passive wiretaps, however, also accounted for the smallest losses. The respondents said that likely sources of attack are disgruntled employees (89%), independent hackers (72%), domestic corporations (48%), foreign corporations (29%), and foreign governments (21%).

Assurance Mechanisms

Information assurance includes the totality of security safeguards needed to provide an acceptable protection level for an infrastructure and for data handled by an infrastructure. More recently, the aspect of survivability has been recognized as a critical component. Survivable systems include the properties of: fault tolerance; robust, adaptive response; distribution and variability; and recovery and restoration [23].
The emphasis of this chapter is on technical security measures, but physical and personnel security measures are essential complementary protection. Physical-level security includes controls for physical access to facilities, protection from local capture of information via unintentional electromagnetic radiation, protection from failure of supporting utilities and natural disasters, and many other threats.

A formal security policy model is the core of the concept of trust [23]. It mathematically defines a trusted computing base (TCB) as an abstract model. The model includes the notion of a secure state of the TCB, subjects (users that access the TCB), objects (data sets in the TCB), and actions that the TCB performs. The model describes these fundamental actions and the state transitions of the TCB. The model permits analysis and provides a means of proof that any given TCB architecture implementation always remains in secure states.

The control of access to authentic users is the fundamental security mechanism of single or networked systems. The process of authentication requires the user to verify identity to establish access, and access controls restrict the processes that may be performed by the authenticated user or users attempting to gain authentication. Authentication of a user in a secure manner requires a mechanism that verifies the identity of the requesting user to a stated degree of assurance.

Cryptography provides the mathematical processes for transforming data (by encryption and decryption) between an open format and a secure cipher text format to provide the privacy property. The strength of the encryption algorithm is a measure of the degree to which the cipher text endures attacks. The ultimate strength and generality of cryptographic processes lies in the mathematical formulation of the underlying transform algorithms. The general cryptosystem includes the cryptographic message path that includes the encryption, transmission, and decryption process, and a supporting method of distributing a numerical variable, or key, that controls the encryption transformation. The generation, storage, distribution, and overall protection of keys are critical to the security of all cryptosystems. Compromised keys provide the most direct means of unauthorized access. For this reason, physical, information, and perceptual layers of security must protect the key management functions, including those summarized below. In addition to providing privacy, the encryption process provides a means of authentication of a message by an encrypted data item called a digital signature. The digital signature permits proof of identity of the sender, and proof that an attacker has not modified the message.

Firewalls are trusted systems that integrate authentication, connection control, incident-response, encryption, network structure security, and content security into a single secure unit. Located between two networks, all traffic passing between the networks must pass through the firewall, which restricts passage to only authorized traffic allowed by the security policy. The firewall effectively creates a security “domain” or “enclave” by providing a perimeter de-

fense to a network (the secured domain). The four basic types of firewalls are (1) packet filters, (2) circuit relays, (3) application gateways, and (4) dynamic packet filters.

Systems for intrusion detection and response (IDS) are needed to protect computer systems and networks from internal or external intrusions. Traditional computer security distinguishes auditing from alarm reporting. Security auditing reviews the records of activities to detect security incidents (including changes in operational configuration), to verify compliance with security policy, and to test security controls. Security alarm reporting monitors security-related events that may indicate misuse of security controls or configurations, hostile activities against security controls, or behaviors inconsistent with security policy. Automated detection of incidents and immediate alarm reporting and response is required to respond to structured information warfare attacks on networks. As in all alarm systems, false alarm and detection failure rates measure overall detection performance. Automatic detection and reporting is required for a wide range of threatening actions, e.g., external intrusions, internal security intrusions, system failures, and anomalous behavior.

SCIENCE AND ENGINEERING ISSUES

Citizenry, industry, government, and the military have become vulnerable due to the reliance on technology, particularly information technologies. Even more frightening, but less understood, is that this vulnerability is increased due to reliance on the world economy and coalition arrangements in the military. As the immensity of the information assurance (IA) problem before the information society has been uncovered, growing attention is being given to this topic by the press, industry, and the government. The field of information assurance focuses on designing systems that can enforce security policies even in the presence of malicious code. The challenge is to design, develop, and deploy complex systems with confidence in their ability to satisfy security requirements. A theory of computer security is on the way that offers a formal method for security engineering, so that we can expect to get affordable, verifiable, scalable technologies for a robust and secure defense infrastructure. This theory will have three components: policy, mechanism, and assurance.

Attempts have been made to address the growing information assurance problem. Some of these attempts were typically ‘reactionary’, at a shallow level, and with narrow focus. For instance, firewalls were introduced to protect local area networks from the Internet; however, they were developed at a superficial level to control the known protocols and threats that were plainly evident. Many authors have shown that there are inherent problems in the existing design and assessment processes that create our information systems [3/ 11/ 17/ 18].

According to DARPA [20], these problems can only be addressed by a fundamental change in information assurance philosophy. It is evident that existing methods are inconsistent, inefficient, do not approach problems with a truly “system-level” viewpoint, and have goals and results limited by the currently abstract and immature nature of the discipline. These limitations cannot be overcome with additional evolutionary research in the same core concepts such as vulnerabilities, threats, and countermeasures. According to DARPA [20], a new information assurance paradigm is required – one that enables the designer and analyst to capture and probe the causality, relationships, and objectives of an entire system. A step in the basic science of information assurance should be to develop equivalencies, relationships, laws, logic, postulates, proofs, and methods for calculation so that metrics can be used effectively.

Just as in other disciplines, complexities of systems will often not allow for closed solutions; therefore, modeling of information assurance will be needed. The overall goal of the new DARPA approach is to provide a science-based environment for design and assessment that will yield improved information assurance and allow for faster design and assessment at less cost. This environment will consist of methods and automated tools to provide consistent results and metrics to specify information assurance. This work is being performed because current designers and assessors have no way to consistently measure the many aspects of information assurance. They also work without an integrated environment and automated tool support that could vastly improve their performance and the assurance of their information systems.

Some analyses of methods and tools needed by the information warfare (IW) community have resulted in a set of major findings and recommendations. The assessment of the nature of the problem has led to the appreciation that information warfare methods must be able to cope with complex, dynamic, interactive, adaptive processes; teams of humans, under stress, across cultures; and uncertainty as an inherent property. It is anticipated that a diverse mix of methods and techniques will be needed to attack the problems in the IW areas. These tool-based methods should include, but are not limited to, the following: (1) Expert elicitation (e.g., use of structured means to elicit judgments from experts); (2) Constructive Modeling and Simulation (e.g., simulated people operating simulated systems); (3) Virtual Modeling and Simulation (e.g., real people operating simulated systems); and (4) Live Modeling and Simulation (e.g., real people operating real systems).

EDUCATION

Advancing the professional education in Information Warfare (IW), Information Assurance (IA), and Critical Infrastructure Protection (CIP) is an urgent need, in all civil and military organizations of all countries, since the most important aspect of these three areas is people. To meet these challenges, we must improve both the quality and delivery of assurance-related education. According to [7], the number of skilled practitioners of computer security who are able to address the complexities of modern technology and are familiar with successful approaches to system security is very small.

People want security but are faced with two difficulties. First, they do not know how to achieve it in the context of their enterprises. They may not even know of a way to translate organizational procedures into policies, much less implement a set of mechanisms to enforce those policies. Second, they have no way of knowing whether their chosen mechanisms are effective. Modern educational approaches emphasize information assurance not simply as a separate discipline, but as a multi-disciplinary science which includes elements of operating systems, networking, databases, the theory of computation, programming languages, architecture, and human-computer interaction [7/ 11/ 12/ 13/ 14]. The body of knowledge must be incorporated as appropriate into this set of disciplines.

In 1999 the NSA Information Systems Security Organization (NSA/ISSO) has founded a National INFOSEC Education & Training Program (NIETP) with seven subprograms [14]: (1) Seven Centers of Academic Excellence in Information Assurance Education; (2) National Colloquium for Information Systems Security Education; (3) University Outreach Program;

(4) Electronic Develop-A-Curriculum Program; (5) "Blue Box" Initiative; (6) Service Academy Visiting Professorship Program; and (7) Information Assurance Courseware Evaluation Process. The goals of the National Colloquium are to create an environment for exchange and dialog among leaders in government, industry and academia concerning the need for and utility of information security and information assurance education. Given the scope and fluid state of knowledge of information security, the Colloquium will strive to foster the development of academic curricula which recognizes the need expressed by government and industry, and is based on the recognized 'best practices' available in the field. The Colloquium will assist educational institutions by fostering the continued development and sharing of information security education resources.

The information warfare (IW) course of the Naval Postgraduate School (NPS), Monterey [13], is designed to provide students with an opportunity to apply fundamental systems engineering analysis and theory to an IW system problem encountered in an operational environment. Students can model a generic information system, applying systems engineering design theory, and processes to develop a relevant IW system. They could learn to choose sound engineering approaches to both defend the system under study, and conversely to attack the system if one were to assume its possession by an adversary. The class can be coordinated using a step-by-step decision analysis process. For example, nodal and critical path analyses will be reviewed for vulnerability, with emphasis on technology trends in the fields of communications and computers. Organizational decision systems (command & control) and human factors engineering will be studied in order to permit modeling of adversaries military and civil command structure as part of the project. There can be a class project (with two teams competing) devoted to the formulation and presentation of an organized systems approach to solving the operational application of an Information Warfare challenge using the communications equipment selected.

CONCLUSIONS

Twenty years ago, corporate and military information infrastructures were separate and distinct, and the term 'information warfare' did not exist. Today they are on the way to become one and the same, and the resulting networked information systems open many doors for information warfare. The military community depends upon (nearly) the same computer networks and networking equipment to fight wars as industry depends upon to conduct business. In this respect, it is worth noticing that over 95% of US military communication links make use of commercially leased lines and satellites, and during the operation Desert Storm this percentage was even higher [9]. The government has three roles with respect to the nation's information infrastructure: to be forthcoming about the genuine threat, to stimulate adequate regulations, and to foster public confidence. This paper could help to open a dialogue among academia, industry, and government toward assuring information infrastructures and information systems. The security community needs a common vocabulary to discuss threats and countermeasures, and a common methodology to discover weaknesses in systems, to prioritize weaknesses in terms of relative dangers to the system, and to determine cost-effective countermeasures. Indeed, there exists a common problem area in the context of information warfare, with challenges for a new level of cooperation in science, engineering, and education - but many of these problems still have to be uncovered for cooperation. As expressed in figure 1, the areas of Information Warfare (IW), Information Security (INFOSEC), and Critical

Infrastructure Protection (CIP) belong together, and we should work out the interrelationships between their sub-areas.

NOTES

[1] Anderson, R., Feldman, P., et al. (1999): *Securing the U.S. Defense Information Infrastructure: A Proposed Approach (MR-993)*, Santa Monica, CA: RAND. <www.rand.org/publications/>

[2] Cobb, A. C. (1997): *Australia's Vulnerability to Information Attack: Towards a National Information Policy*, Strategic and Defence Studies Centre, Australian National University, Canberra. <coombs.anu.edu.au/~acobb/X0016_Australias_Vulnerabi.html>

[3] Cohen, F. (1999): *Simulating Cyber Attacks, Defenses, and Consequences*, Fred Cohen & Associates (Information Security Services). <all.net>

[4] Denning, D. E. (1999): *Information Warfare and Security*. Reading, MA: Addison-Wesley.

[5] Gray, J. V., Barlow, W. J., Barnett, J. W., Gerrity, J. L., & Turner, R. D. (1997): *Information Operations*, A Research Aid (IDA Document D-2082). Alexandria, VA: Institute for Defense Analysis (IDA).

[6] Howard, J. D. (1997): *An Analysis Of Security Incidents On The Internet 1989-1995*, Pittsburgh, PA: Carnegie-Mellon University. <www.cert.org/research/JHThesis/Start.html>

[7] Irvine, C. E., Chin, S. -K., & Frincke, D. (1998):' Integrating Security into the Curriculum', *IEEE Computer*, Dec. 1998, p. 25-30.

[8] JP3-13 (1998): *Joint Doctrine for Information Operations*, (Joint Publication JP3-13, 9 October 1998). <www.dtic.mil/doctrine/jel/c_pubs2.html>

[9] Luiijf, E. A. M. (1999): 'Information Assurance and the Information Society', In: Gattiker, U., Pederson, R., & Peterson, K. (Eds.): *EICAR Proceedings 1999*. Aalborg, DK: TIM-World ApS (ISBN 87-987271-0-9).

[10] NATO (1998): *NATO Information Operations (Info Ops) Concept*, (NATO MCM-0969-98). Brussels, Belgium: NATO Headquarters.

[11] Neumann, P. G. (1999): *Practical Architectures for Survivable Systems and Networks*, (Report). Computer Science Laboratory, SRI International, Menlo Park, California. <http://www.csl.sri.com/~neumann/arl-one.html>

[12] NPS/CISR (1998): Naval Postgraduate School Center for Information Security Studies and Research. The Naval Postgraduate School, Monterey, CA. <cisr.nps.navy.mil>

[13] NPS/IW (1998): Information Warfare Academic Group. The Naval Postgraduate School, Monterey, CA. <web.nps.navy.mil/~iwag/matrix.html>

[14] NSA/ISSO (1999): National Security Agency (NSA). Information Systems Security Organization (ISSO). <www.nsa.gov:8080/isso/>

[15] OSD (1998): Information Operations Planning Tools. <www.acq.osd.mil/at/iopt.htm>

[16] Pfleeger, C. P. (1997): *Security in Computing*, Englewood Cliffs, NJ: Prentice Hall.

[17] Salter, C., Saydjari, O. S., Schneier, B., & Wallner, J. (1999): *Toward A Secure System Engineering Methodology,* Proceedings, ACM New Security Paradigms Workshop, Sept. 22-25, 1998, Charlottsville, VA. New York: ACM.

[18] Schneider, F. B: (Ed.) (1998): *Trust in Cyberspace,* (NRC Report). Washington, DC: National Academy Press. <www.nap.edu/readingroom/books/trust/>

[19] Schwartau, W. (1998): Bibliography of W. Schwartau (Chez Winn). www.infowar.com/

[20] Skroch, M. (1999): *Development of a Science-Based Approach for Information Assurance,* (White Paper, DARPA/ISO, 10 May 1999). Alexandria, VA: Defense Advanced Research Projects Agency (DARPA). <www.darpa.mil/iso/iaset/iaset.htm>

[21] Theuerkauf, T. (1998): *Erste Ueberlegungen zu den konzeptionellen Ableitungen des Phaenomens Information Operation / Information Warfare*. In: CCG (1998): Information Warfare (Seminar, 30.6.-2.7.1998). Wessling-Oberpfaffenhofen: Carl-Crantz-Gesellschaft (CCG). www.ccg.dlr.de

[22] TNO/FEL (1999): WWW-resources related to Information Security and Information Operations / Information Warfare. Instituut TNO/FEL (Physics and Electronics Laboratory), Den Haag. <www.tno.nl/instit/fel/intern/work.html>

[23] Waltz, E. (1998): *Information Warfare Principles and Operations*, Norwood, MA: Artech House. <www.artech-house.com/links/pdfbooks.html>

[24] Ware, W. H. (1998): *The Cyber-Posture of the National Information Infrastructure,* (MR-976-OSTP). Santa Monica, California: RAND Corporation. <www.rand.org/publications/>

[25] Whitaker, R. (1998): *Information Warfare. Questing Power via Cyberspace*. <www.informatik.umu.se/~rwhit/IW.html>

The Reality

CRITICAL INFRASTRUCTURE ATTACK
An Investigation of the Vulnerability of an OECD Country[1]

Dr Adam Cobb
Australian Parliamentary Fellow, Information and Research Services, Department of the Australian Parliamentary Library, Canberra, Australia

ABSTRACT

This paper takes Australia as a case study and asks specifically where, how, and why Australia's critical infrastructure might be at risk. By examining the core elements of the National Information Infrastructure (NII), such as power distributions systems, telecommunications and financial networks, it is possible to gauge whether the system is vulnerable. The evident vulnerabilities are then juxtaposed against a selection of threats, thereby creating a risk assessment. The paper will end with suggestions as to future policy options available to the Australian Government. It should be noted however that this paper does not claim to provide an exhaustive survey of either vulnerabilities or threats. The criteria for selection were focused on the most serious threats and vulnerabilities that were evident in the open source literature at the time.

INTRODUCTION

There are risks as well as benefits associated with information technology. For example, the use of networked computers for criminal purposes is a significant and growing phenomena which is already costing Australia millions of dollars. A 1997 Australian Government law enforcement survey reported significant increases in both the sophistication and number of external attacks on Australian companies in the past 18 months financial systems and confidential corporate data were the two most frequently attacked information types (....) a number of respondents (...) expressed concern as to the vulnerability of their financial systems to attack (OSCA, 1997, para. 4.09)

Regrettably, the risks are not limited to crime. They span the spectrum from accidents to malicious attacks. Accidents include natural disaster, unanticipated problems (such as the Year 2000 Bug or Y2K problem), technical faults, and user error. Threats include, dis-information, hate/revenge (personal or work-related), crime, commercial or military espionage, state and non-state based terrorism, and information warfare.
In early 1998, both Queensland and Auckland, New Zealand, were afflicted with severe blackouts as key choke-points (or nodes) in the electricity distribution networks collapsed. As the Auckland crisis proved, contemporary cities quickly grind to a halt when electricity, telecommunications and financial networks are out of action. But think of the consequences of nation-wide computer breakdowns that could happen on 1 January 2000. Everything from your family video and microwave, the world wide Global Positioning Satellite (GPS) system, and nuclear power plants in the former Soviet Union are at risk. The Australian Government Minister responsible for fixing the Year 2000 bug estimates the cost of fixing government mission-critical systems alone at $600 million (Fahey, 1998). Being an advanced economy, with a well-educated workforce, extensive infrastructure, a strong and growing service sector, and high levels of overseas trade and finance, Australia provides a good example of the opportunities and problems faced by a typical OECD

country in the information age. This paper takes Australia as a case study and asks specifically where, how, and why Australia's critical infrastructure might be at risk. By examining the core elements of the National Information Infrastructure (NII), such as power distributions systems, telecommunications and financial networks, it is possible to gauge whether the system is vulnerable. The evident vulnerabilities are then juxtaposed against a selection of threats, thereby creating a risk assessment. The paper will end with suggestions as to future policy options available to the Australian Government.
It should be noted however that this paper does not claim to provide an exhaustive survey of either vulnerabilities or threats. The criteria for selection were focused on the most serious threats and vulnerabilities that were evident in the open source literature at the time.

The potential for critical information infrastructure systems failure is a matter for a ***joint*** private sector and whole-of-government approach—as it spans all those aspects of national life that depend upon interlinked information systems. It would therefore be prudent to attempt to anticipate the risks of both accidental and malicious system failures and plan for protecting the National Information Infrastructure.

INFORMATION WARFARE AND NATIONAL SECURITY

Much of the literature on information infrastructure vulnerabilities arises out of a new subject area in strategic studies—'information warfare'. It is a new and highly contested field of enquiry and in one variant refers to the ability of a military force to protect its own knowledge and information systems while at the same time attacking those of an adversary. While a concern with infrastructure is nothing new to the military strategist, new technologies have changed the way infrastructures operate, thereby demanding their re-examination in the strategic context. The same can be said of traditional approaches to military technology.

Information warfare has also been associated with the so-called 'Revolution in Military Affairs' (RMA). While the RMA is a highly contested concept, its supporters argue that new military applications of very high technology provide modern defence forces with a revolutionary tactical and strategic advance on past means of using military force[2]. In this new world, stealth technology, surgical precision, long range and stand-off platforms are integrated by networks of sensors, computers and command and control systems that give a 'God's eye view' of the battle space[3]. No longer a three dimensional world of land, air and sea, the battle space integrates these with two 'new' dimensions - space and cyberspace - where the conduct of war depends on compressing time and distance. The RMA is also concerned with developing new organisational structures to assist in optimising new technologies, and in this respect has been referred to as a Revolution in Management Affairs[4].

This development comes at a time when three other trends are converging. First, organised violence increasingly concentrates on civilian targets. The focus of war since the last century has shifted from being the preserve of governments and the armed forces to involve entire civilian populations. Likewise, the spectre of terrorism concentrates on 'soft' targets. Second, out of desperation, revolutionary powers have often used new technologies in innovative ways that have given them, initially at least, a decisive advantage in war.

This century has observed incredible changes in technology for war-fighting purposes, from horse-drawn artillery to nuclear intercontinental ballistic missiles. As a rule, revolutionary powers have been much more imaginative than *status quo* powers in their development of doctrine and organisational structures coupled with new technologies. Prior to the outbreak of WWII, General Douglas Haig, the British architect of trench-warfare in WWI, stated emphatically that the coming war would be quickly won at its outset by a decisive cavalry charge. In 1939, there was rough parity between Allied and Nazi tanks, radios and aircraft. It was the combination of these technologies with new tactics that enabled the Germans to achieve stunning victories in 1939-40. 'Blitzkrieg' combined the tank with radio, airpower, and mobile infantry, in military formations (Panzer Divisions) using new doctrine unthought of by Haig and his contemporaries.

Third, the end of the Cold War, like the end of WWI, has created a period of strategic uncertainty. With high levels of unemployment, disillusionment with traditional forms of politics and deepening divisions along racial and ethnic lines, growth of anti-immigration movements, widespread job insecurity, high levels of financial speculation and an inability of conventional policy prescriptions to address any of these issues, the international political economy in some mature economies is beginning to demonstrate parallels with the inter-war years. As E.H. Carr convincingly argued of the period 1919–1939, the failure of the democracies to understand and overcome the destructive excesses of the policies that led to the Great Depression, left a policy vacuum that the totalitarian powers eagerly filled (E. H. Carr 1939, 1942, 1945). There are also parallels in the military–strategic context. As in the inter-war period, new technologies currently exist in the form of 'information weapons' but, as yet, no one has formulated the comprehensive doctrine or organisational structure necessary to bring 'info-blitzkrieg' into being. As the economic outlook continues to decline for many mature economies, which also happen to be *status quo* powers, the chances are that revolutionary powers will seek to champion their alternative either by demonstration, or worse, by force.

There is a Revolution in Military Affairs (RMA) in so much as traditional military weapons, platforms and sensors will become much less important in proportion to the growing centrality of the information dependence of civil society. This development is ushering in a new era where protection of critical infrastructure will be the key to economic success and national security. History shows that at turning points in the past, unsatisfied powers have seized the initiative—commercial, military or ideological. In the turbulence of contemporary global politics and economics, those that seek new alternatives to old dilemmas will gain a decisive advantage. The RMA's of the past have involved new weapons, strategies and organizations. The revolutionary concept of the 21st century will bypass traditional weapons and focus conflict on the heart of civil life—the information systems upon which societies depend.

National security involves much more than military defence. At a minimum, it is fundamentally about the survival of society. Pushing the definition a little further, it is concerned with the creation of the necessary political, economic, social, and environmental conditions within which society might flourish (Cobb, 1996). Clearly, an attack on the non-military NII, upon which economically developed societies so heavily depend, will be an attack on the security of that society. Indeed, in some respects, such an attack could be far more harmful to the stability and capacity of a society to function than an attack on the armed forces of the state, because it disrupts or destroys the most fundamental

infrastructural elements upon which modern society depend. It is the electronic equivalent of total war.
Consequently, the spectre of information-based conflict is the most significant threat to national security since the development of nuclear weapons over fifty years ago. Like nuclear weapons, information-based weapons relocate the strategic centre of gravity from military forces to direct attacks on civilian targets. While the use of nuclear weapons post-1945 came to be considered unthinkable, it is conceivable that information-based weapons will be used to target and destroy information dependent nations.

Information-based conflict foreshadows a new kind of conflict, where the overt, physical assault is replaced by ubiquitous, anonymous, and ambiguous subversion of society. No longer a matter of clearly defined spatial limits where an 'enemy' is clearly an outsider, such subversion can come from within or without. An information assault on the diverse and complex roots of society cannot simply be addressed by a compartmentalised bureaucracy designed to address the nineteenth century problems of gunboats and cavalry-divisions. A holistic, integrated approach is required. While few ever realised it in the past, security has always been indivisible. It will be ever more so in the future, especially in the context of securing the information and infrastructure systems upon which society, domestic and international, depend.

While a new concern for infrastructure security may have been born out of the RMA, it is not and should not be the preserve of the military strategist. As this paper seeks to demonstrate, warfare is just one of a number of potential risks Australia faces in the early 21st Century.

THE NATIONAL INFORMATION INFRASTRUCTURE (NII)

What is the National Information Infrastructure?[5] For the purposes of this paper, the NII is comprised of systems whose incapacity or destruction would have a debilitating impact on the defence or economic security of the nation. They include, but are not limited to, telecommunications, energy, banking and finance, transportation, water systems and emergency services, both governmental and private. According to function, they can be arranged thus:

- *Core state functions:* executive government, and essential agencies such as defence, intelligence, foreign affairs and trade, finance, social security, national and state emergency services.

- *Core utility functions:* power grids, telecommunications, petrol refineries, gas and oil storage and transportation systems, transportation and traffic systems (air traffic control, GPS systems, meteorological support), and water supply.

- *Core commercial functions:* banking and financial services, mass media, business systems and communication networks.

The NII runs on the telecommunications network, and is linked to the Global Information Infrastructure (GII) via submarine cable and satellite. It is also dependent on a constant supply of energy and thus elements of the NII dependent on one another. In the next

section a detailed examination of vulnerabilities in select NII systems is presented before examining the potential threats against these systems.
Computers cannot operate without power; nor can telecommunications, the financial network, or defence communications—all areas prone to information attack and discussed below. Moreover, the interdependency of these parts of the NII complicates efforts to defend them. Growing complexity and interdependence, especially in the energy and communications infrastructures, create an increased possibility that a rather minor and routine disturbance could cascade into a regional outage. Technical complexity may also permit interdependencies and vulnerabilities to go unrecognised until a major failure occurs.

VULNERABILITIES IN THE NATIONAL INFORMATION INFRASTRUCTURE

Energy

Energy distribution in the state of New South Wales (NSW) is the responsibility of TransGrid. According to TransGrid's annual general report, the company's 'high voltage electricity transmission network is large by world standards, involving approximately 11 500 km of transmission lines and 73 substations... [and six area headquarters at] Tamworth, Newcastle, Orange, Metropolitan Sydney, Yass and Wagga' (TransGrid, 1996):

> Information systems and communication links [are] also required to enable TransGrid to manage its market operation responsibilities. The real time nature of electricity delivery involves continuous changes to achieve balance between supply and demand. Accordingly, prices, generation dispatch instructions, market information and other matters are determined each half hour leading to the need to frequently update and communicate a large amount of data. **In short, the market in its present form could not operate without computerised information systems and communication links** (TransGrid, 1996: p. 20, emphasis added).

The entire NSW power grid including generators, distribution and the six area headquarters are controlled from the System Control Centre at Carlingford, a Sydney suburb. There are two central power sources feeding the state. One is the coal-powered Hunter Valley system, situated north of Sydney. The other is the Snowy Mountains Hydro Scheme, situated just outside Canberra and south to the border with Victoria, and comprising six main power stations located at dams in the region. The power generated from this region is channelled through one key point, Yass, before it can reach Sydney. The Hunter system does, however, provide an alternative supply, with additional diversity of routes into Sydney. Nevertheless, with the Snowy Scheme out of action, the subsequent pressures on the Hunter would probably overwhelm the system.

The National Capital, Canberra, is serviced by one main substation. That station is in turn connected to only two other substations, located at Yass and Cooma. Within Canberra, most major government agencies depend on two smaller substations located in the city (City East zone and Kingston zone) and there are precious few transformers available in reserve to service the city. The computers operating the power grid can be accessed via a number of routes, including the direct dial-in diagnostic system used by technicians to monitor, detect and fix problems across the breadth of the grid. From the point of view of security, these are serious vulnerabilities. Few sections within even the Department of

Defence, for example, have an alternative energy supply to the city grids. Similarly, the joint force commanders are all located in Sydney and rely on the city's power supply as well as public communication links between themselves and ADHQ in Canberra.
As the explosion at the Longford gas refinery in Victoria in 1998 vividly demonstrated, energy distributions systems are vital to the national economy. Recent estimates suggest Australia lost up to 1% of GDP as a consequence of the Longford incident. Australia's major cities are serviced by two or three natural gas fields via extremely long pipelines that are computer controlled. Two key pipelines feeding both Sydney and Adelaide originate from the Moomba (SA) oil and gas fields. Similarly, Perth is fed from the far north west of WA by two lines, Brisbane is dependent on one line, while Melbourne relies on lines emanating from the Bass Strait platforms. In all cases, the pipelines span thousands of kilometres over uninhabited sections of the outback or under the ocean. The lines are policed in terms of physical protection. For example, one of the roles of the RAN's patrol boat flotilla is to very publicly patrol the Bass Strait oil rigs. Yet the line and the computer systems that operate them are not policed at all. The accident at Longford could have been just as easily triggered by accessing the SCADA system (Supervisory Control and Data Acquisition) running the plant.

Telecommunications

There are two major telecommunication service providers in Australia, Optus and Telstra. Telstra operates an extensive network of coaxial cable, microwave radio, optical fibre, digital radio concentrators, mobile phone cells, submarine cables and submarine fibre cables (Telstra, 1996). There are dedicated trunk switches in every capital city in a static hierarchy configuration. Routes are tested in a routine order, with the most direct route selected first. It is possible for calls between cities to bypass major hubs only if all lines through the hub are in use. Each hub is linked with other capital cities by two geographical routes and each capital city trunk switching centre should have access to the other capital cities without physically routing via a common building in the city.
While there is some redundancy on the eastern seaboard, there are also a number of important choke-points. For example, the exchanges in Katherine (NT), Woomera (SA), and Ceduna (SA), link central and western Australia to the east. Both microwave and fibre lines pass through these exchanges. If these critical nodes were attacked all terrestrial communications between the west and east would be severed. Add the exchange at Camooweal (QLD), and the entire centre of the continent would be severed from the outside except for direct satellite links and HF radio. With the exchanges gone, these remaining systems would be overwhelmed by the demands of regular telephonic and data traffic that daily cross the continent.

Australia is also a critical node in the international fibre network. Calls in and out of Australia via submarine cable and satellite are all processed through two buildings in Sydney: the Paddington exchange and the Telstra facility at Oxford Falls. Aside from Australia, there are three potential single points of failure in Asia: Japan, Hong Kong and Singapore. All South East and North East Asia connect onto this submarine fibre corridor. Links to the outside world pass from Japan to the US, and from Singapore to India and onwards to Europe via Suez. The only other separate submarine fibre links to the US and Europe pass through Australia. Within the Asian submarine cable corridor, between the two key nodes of Japan and Singapore, Hong Kong is a critical node. If it were disabled,

Asia would be isolated on the north-south axis. Were Singapore and Japan taken out of service the only remaining international links pass via Australia. Consequently, Australia is a vital international node.

The satellite communication network comprises two systems, one international (INTELSAT) and one domestic (Optus satellites). Both Optus and Telstra operate separate INTELSAT gateways at Oxford Falls in Sydney, part of an international network of nearly 400 earth stations in over 150 countries. In addition, Optus operates an INTELSAT earth station at Lockridge in Perth, as does Telstra at Gnangarra in WA. The Telstra facility is also a major link in the international satellite control network.

The Australian domestic satellite fleet was sold to Optus communications in January 1992 as an integral part of the Optus licence bought from the federal government for $800 million. 'Although they are hidden from view, Optus' satellites are a surprisingly common part of the day to day lives of Australians and Australian businesses' (Optus, 1996, p. 10). In the same publication, Optus states that their satellites carry the following types of information:

- Parts of the Optus and Telstra telephone systems
- Extensive management data nets for banks
- Remote oil and gas pipeline monitoring
- Ground to air communications and air traffic control systems
- Secure defence signals
- Mobile satellite communications (Optus B systems only)
- The Internet, and
- Radio and TV services (Optus, 1996, p. 10).

The primary Optus satellite operations control facility is located at Belrose, a northern suburb of Sydney, with a backup facility in the Perth suburb of Lockridge. A broadcast operations centre and satellite network services centre are also co-located at the Belrose facility. From Belrose, the satellites can have their position in orbit or their direction altered (as is necessary to maintain geostationary position with antennas pointed in the right direction). It is also possible to access and manipulate the signals sent and received via the Optus satellites from Belrose, and to monitor the traffic that passes through all Optus spacecraft. There is no encryption on the control channel of the two A series. Anyone with the proper equipment could easily put the A's out of action. Clearly, Belrose is a highly critical node, with redundancy provided at only one other well-known location in Perth.

Finance

The central bank, the Reserve Bank of Australia (RBA), is responsible for the overall stability of the financial system. It is banker to the banks, and the main banker to the Commonwealth Government, and some state governments. As well as supervision of banks[6] the RBA is responsible for the accounts used for 'settlement of interbank obligations arising in the payments system' (Bank for International Settlements, 1994, p. 22). In other words, clearance of its customers' cheques and electronic funds transfers are the RBA's responsibility. The RBA operates the Reserve Bank Information Transfer System (RITS) which is a *real time* gross settlement system for all accounts held by the bank (Bank for International Settlements, 1994, p. 22). A range of associated organizations work with the RBA to ensure the smooth running of interbank, securities, equity, futures, and options, clearance and settlements. The RBA is either a shareholder or has representatives on these bodies. The clearance process involves consolidation of information on debts and credits and establishment of the net position between institutions. Settlement refers to 'payment or receipt of value of net obligations established in the clearing process' (Linklater, 1992: p. 196).

The clearance process is managed by the Australian Payments Clearing Association (Ltd), which is a limited liability company. 'Net obligations arising from the clearing of instruments in this system are settled across accounts at the Reserve Bank of Australia' (Bank for International Settlements, 1994, p. 13). APCA have outsourced their operation to the Society for World Wide Interbank Financial Telecommunication (SWIFT), based in Brussels (further discussion of SWIFT below). This means that every day Australian banks clear their netted position with one another via a computer in Brussels which then transmits the final result to the Reserve Bank computer in Sydney for settlement on the accounts held by APCA members (e.g. Australian banks). The RBA computer is located at Head Office (at Martin Place, Sydney), and is linked on-line with the Reserve Bank's state branches in each capital city (except Darwin).

The banks have just 45 minutes for the clearance and settlement process—from 0800 to 0845 on each day of trading. The remaining 15 minutes before 0900 allow the RBA to intervene, if necessary, as banker of last resort in cases where a bank cannot honour its commitments arising out of the clearance process. Forty-five minutes is not much time to act if something goes wrong. The domestic banking system could not survive more than a few days if this delicate system was disrupted.

In many cases with domestic personal banking electronic transactions, network members agree their net obligations bilaterally and notify their positions to the Reserve Bank. Consequently, all major banks have central data processing centres connected to one another and the main system at the Reserve Bank. Similarly, all ATMs and EFTPOS systems are linked by one of two national networks using common systems architecture (Bank for International Settlements, 1994, passim). Notably, for reasons of 'efficiency' the central data processing centres are few in number. Problems have already been recorded where such centralisation has caused major disruption. For example, in the early 1990s, the Melbourne ANZ bank data centre was disabled when the electricity line from a tram came into contact with the bank's tin roof as a consequence of a road accident[7].

Many other significant transactions pass through the RBA's computer. For example, the Government Direct Entry Service is owned and operated by the RBA. The system electronically disperses government payments to over 600 financial institutions, which in turn distribute government payments into the accounts of millions of Australians—which include, *inter alia*, public servants, those on social security benefits and members of the armed forces. In 1993, this system conducted up to 3 million transactions a day (Bank for International Settlements, 1994, p.10).
This is a key weakness in the system. If, for example, in the lead-up to major conflict, an adversary could disrupt government payments to the armed forces and their families, it would seriously affect the morale of the forces and society generally. This kind of disruption has been foreshadowed in the past with grave political consequences. The 1975 Federal Budget crisis which threatened Supply, quickly turned into a constitutional crisis, in part because of the fact that the incumbent Government was facing a hostile Senate that could have prevented the Government from paying the armed forces (and others). With all of the government's payments passing through just one computer, the financial security of millions of Australians as well as national political and economic stability is seriously vulnerable.

Risk Assessment

A **risk assessment** juxtaposes existing vulnerabilities against likely threats to determine what is most likely to happen. Like most OECD countries, Australian NII vulnerabilities are confronted by a range of dangers, both unintentional and intentional. Accidents include natural disaster, unanticipated problems (such as the Year 2000 Bug or Y2K problem), technical faults and user error. Threats include dis-information, hate/revenge (personal or work-related), crime, commercial or military espionage, state and non-state based terrorism and information warfare.

Threats, such as terrorism, are not necessarily more dangerous than accidents, if the likelihood of a terrorist act actually occurring (other things being equal) is very low. In some cases, the probability of an event occurring is remote but the consequences so grave that such a threat must be given a high priority.

Two points must be emphasised here. The consequences of a failure of the NII would be very severe indeed. Therefore, action is required regardless of any threat probability assessments. Once probability is added in - it will be clear which risks will require the most urgent action. Second, in some instances in the Australian context, there exists a combination of high levels of vulnerability, a high probability of an event occurring and associated severe consequences. A threat hierarchy exists where these three factors overlap.

This paper's risk assessment suggests a *hierarchy* of threats facing Australia's critical infrastructures. In descending order of probability and consequence of seriously damaging Australia's national security, wealth, and international standing, they are:

- Year 2000 incompatibility
- Information-terrorism at the Sydney 2000 Olympics
- Major crime activity
- Natural disaster
- State and non-state terrorism (excluding the Olympics)
- Information warfare—civilian systems, and
- Information Warfare—military systems

Year 2000 Bug

The greatest risk regarding Australia's NII appears to emanate from an unintentional but nevertheless ubiquitous 'threat'. The Year 2000 computer incompatibility problem affects all computers everywhere, as well as embedded chips. Not only would Y2K failures impact upon individual computers and networks, their effects would concentrate on the same critical choke-points in the NII identified above, as any malicious attack. Similarly, a cascading collapse could occur—spreading out from problem systems into the general network community—threatening systems that have been Y2K 'immunised'.

Not only would Y2K 'attack' all the vulnerabilities identified in the NII *simultaneously*, the *probability* of a Y2K event is *guaranteed*. Come 1 January 2000 it is a certainty that some kind of crisis will develop—the only question concerns the extent of the ensuing dilemma. The unintended or unimagined consequences of multiple interdependent systems collapse would cripple the nation more swiftly and comprehensively than any military attack ever could.

In essence, the problem is that most hard/software has been programmed in a shorthand that only uses a two-digit year reference e.g. DD/MM/YY. These two-digit dates exist on millions of data files, in millions of applications, and in a wide variety of operating codes and hardware systems. In 2000, computers will not be able to decipher whether it is 1800 or 2200, thereby sending all manner of code, programs, applications and calculations haywire. The problem affects most computers and software embedded in electronic equipment. Correction requires the inspection, evaluation, alteration and testing of literally millions of lines of computer code—it is complex, time consuming and costly.

A great part of the danger lies in the timing and magnitude of the problem. On 01/01/00 every computer system that has not been fixed will experience some difficulty. Indeed, when it comes to interdependent computers and networks, it will only take one non-Y2K compliant link to threaten the entire chain. There is a very high risk that critical infrastructures that rely on networked computers will face serious, if not catastrophic, failure. Because it will all happen at the same time right across the country (and indeed internationally within 24 hours), it is impossible to predict the scope of the impact. Its scale, however, will be unprecedented.

Not only are key civilian infrastructures dependent on computers and networks, so are nuclear warheads, missiles and reactors, for example. At a recent conference in Canberra[8], the author asked the Chief of the United States Air Force, General Michael Ryan, whether

US strategic nuclear forces were fully protected from Y2K. He gave reassurances that all required 'patches' have been put in place. 'The USAF will fly on the 1st of January 2000' he said. However, media reports cast doubt on the ability of Russian and former-Soviet strategic nuclear forces to keep up with Y2K threats. For example, *The Sunday Times* recently reported that western intelligence sources have warned political leaders that there could be 'a giant Chernobyl' if Y2K issues are not addressed within both military and civilian nuclear systems in the former Soviet Union (*The Australian,* 1998 (a), p. 1). The same paper reported President Clinton's new Y2K adviser, John Koskinen, who suggested even US systems were not as safe as General Ryan claimed. Mr Koskinen is quoted as saying that 'it needs to be worried about… if the data doesn't function… they [US warheads and missiles] actually [could] go off' (*The Australian,* 1998 (b), p. 7).
The military is not the only concerned group. The Australian Stock Exchange revealed it has spent '$12.5 million already to safeguard its systems from the millennium bug'. It is asking Australian companies to 'outline how much exposure the company has, what measures have or are being taken and the overall cost of addressing the problem' (*The Australian,* 1998 (c), p. 1).

The responses to the ASX letter inquiring into Y2K compliance makes interesting reading, especially with regard to critical infrastructure systems. The ASX Managing Director, Richard Humphry, said that 'I haven't yet received from any State government any assurance written or verbal, that [the] utilities will be okay by 2000' (*The Australian,* 1998 (d), pp. 56-7). Indeed, the Chairman of the ASX, Maurice Newman, who was appointed by the Australian Prime Minister to chair the Federal Government's Year 2000 steering committee, has predicted a global recession in 2000 (*Business Review Weekly*, 1998, pp. 40–8). He has also highlighted problems with staging the Olympics and the risk of major failures in critical infrastructures (*Sunday Telegraph*, 1998, p. 1). As the reports from top government advisers above suggest, Y2K is the greatest threat to critical civilian infrastructures.

Threats

Having established a very significant unintentional threat in the form of the Y2K problem, it is now necessary to consider the hierarchy of potential malicious threats. None of the vulnerabilities discussed above will be important if there is not a significant threat posed to Australia. It must also be remembered that there must be four core elements in identifying likely threats: motive, opportunity, capability and willpower.
In terms of a malicious attack, the NII can be attacked in a number of ways. There is a lot of animated talk of 'electronic Pearl Harbours' in the mainstream information warfare literature (Schwartau, 1994). Attacks on the NII are not as easy to organise as such comments suggest, but they are a lot easier than one might imagine. It all depends on the target and the scale of attack envisaged.
Mass attack on the NII where *all* core systems are *totally* incapacitated will not be possible without detailed planning, intelligence, and highly-skilled personnel, mostly available only to advanced states. The fact is that the incredible array of systems and their myriad interlinkages that constitute the NII provide a form of security in their very diversity. It would not be possible to completely disable these systems without detailed knowledge of their weaknesses and the location of critical nodes within and between them. Then only a well-timed and coordinated strike might have a total effect.

As discussed below, the consequences of attack may increase where system redundancy has been degraded due to commercial imperatives to cut operating costs, centralise critical nodes, minimise maintenance schedules, and use common 'off the shelf' hard/software solutions. Nevertheless, mass attack is unlikely. If significant intelligence and planning assets were deployed for the purposes of mass information attack it would certainly be by a state and only in conjunction with other more traditional forms of organised violence. Consequently, existing intelligence and other defence assets should detect and give warning of an impending attack. However, in the event of military action, attacking core NII sites and information nerve centres would greatly aid strategic surprise and the aims of conventional warfare.

This does not mean that Australia is invulnerable. On the contrary, an attack on critical nodes could set off a chain-reaction that could have devastating effects for society. The most likely attack would focus on disruption of one or two key systems. Even small scale disruption of key systems, without adequate recovery plans and established information hierarchies in the event of attack, could severely affect government, commerce or society. Aside from physical attack, the easiest form of attack would be a denial of service attack. This does not require penetration of information systems (which requires password, systems, or source code cracking), but rather overloads key nodes from the outside. It is a form of data overload that overwhelms the systems' capabilities to respond, thereby affecting its internal operations as well.

The Tools of Info-terrorism

- Denial of service attack
- Hardware/software chipping (where special inserts are made into microchips at the time of manufacture to allow unauthorised access)
- Systems intrusion (via password cracking or exploiting operating system weakness and source code)
- Computer virus attack (logic bombs, Trojan Horses, worms)
- Physical attack (including Electromagnetic Pulse—EMP—bombs)
- Jamming and other electronic warfare techniques
- Information interception (Van Eck radiation intercept).

The most sophisticated (and consequently most difficult) form of attack is a systems penetration attack. Gaining access to systems can be a difficult and time consuming process and most high-security systems, such as those used by the military and the banks, are either 'air-gapped'[9] from external systems or are protected by technological security solutions such as firewalls. Unless one is an insider, has chipped the soft or hardware being used, or can crack or get around the firewall (and all of these have been done), it is difficult, but not impossible, to access these systems from the outside. By de-linking systems however, one loses all the advantages of advanced networked computing, such as speedy multi-user connectivity. For some that cost is too high. Consequently, in a surprising number of cases, critically important infrastructure systems are interlinked with

other systems that can be penetrated from the outside. Indeed, some are specifically designed to be remotely accessed, such as the SCADA system (Supervisory Control and Data Acquisition) which is typically used in energy distribution networks, such as oil and gas pipelines.

Terrorism

These questions are further complicated in the case of info-terrorism, the second source of threat to Australia's NII after the Y2K problem. The interests of terrorists are well served by information technologies. Low entry costs, difficulties in identifying an attack and its origins (anonymity and ambiguity) and the potential for extreme chaos throughout governments, corporations and society in general, all offer rich opportunities to terrorists. Terrorists will also be attracted to the fact that conventional notions of deterrence will be increasingly irrelevant in the context of Information Operations (Info Ops) as counter-targeting becomes difficult when an attacker launches an assault via a number of different national or international jurisdictions, using an anonymous or spoofed ID, and from a mobile laptop—possibly from within the country the terrorist is targeting.

Sydney 2000 Olympics

A key opening for a terrorist act in the near future is the Sydney Olympics in 2000. A number of past Olympiads have experienced terrorism, including Munich and Atlanta. While law enforcement organizations are concentrating on physical security they do not appear to have canvassed cyber security issues. An attack could be mounted against Australia or more likely against another country participating in the globally televised sports extravaganza. A wide range of targets and opportunities present themselves in the Olympic context. With the world looking on and with the year 2000 computer 'bug' providing 'cover', one single large-scale act could ruin the games and profoundly damage Australia's reputation.

An anonymous Australian government official recently wrote an article in the *Australian Financial Review* warning that the Federal Government had seriously failed its obligation to develop and implement a strategic security plan for the Games. With the terrorist group Harkat ul Mujahideen threatening Australia with retaliation for the latter's support of US cruise missile strikes in Afghanistan and The Sudan, Mr 'X' has warned that Canberra is unprepared for Olympic terrorism and that significant acts of violence are quite likely to occur (Mr X, 1998, p.19).

An interesting example of a highly educated, motivated, dedicated and ruthless terrorist who could have used new information technologies to great effect is the 'Unabomber'[10]. With adequate resources to fund acquisition of a computer and modem and a profound grudge against society—a Unabomber-type terrorist could wreak all kinds of damage. Certainly they would have a motive, could seek an opportunity, easily obtain a capability, whilst already possessing the will to act. If they go undiscovered as the original Unabomber was able to do for so long, the potential implications for the society the terrorist loves to hate could be major.

Such a terrorist would be capable of researching critical nodes (freely available in open sources as this paper has demonstrated) and mis-representing themselves to gain access to codes and passwords, thereby gaining access to vital systems used to run the society

against which they hold a grudge. In the age of 'down-sizing', job insecurity, government cuts to welfare as well as a range of other services (including the Universities—remembering that the Unabomber was a Harvard mathematics whiz), the potential may well exist for Unabomber-type terrorism, especially in open societies like Australia and the US when more than ever before individuals have access to and knowledge of vital NII systems and the means to attack them. It would be all the worse if the proposed Unabomber-type terrorist also happens to be the systems manager of a critically important system.

Crime

The third significant area of information operations activity is in the realm of crime. Criminals and organised crime groups have been quick to seize the opportunity afforded by new communications technologies and their rapid spread throughout society. Indeed one expert claimed in *The Australian* recently that 'big crime cartels are at least two years ahead of the business world in their take-up of sophisticated technology' (McIntosh, 1997, p.33). Of the four areas of potential threat identified above, crime is currently the most common area in which to find the active utilisation of Info Ops techniques and strategies. In information operations the techniques for attacking an air traffic control system are essentially the same as those used to attack a bank. Consequently, statistics on cyber crime are valuable indicators, as hard evidence does not exist for terrorist or military information warfare.

In 1998 the Office of Strategic Crime Assessments (OSCA), within the Australian Attorney-General's Department, conducted a *Computer Crime and Security Survey* (OSCA, 1997). The study canvassed a number of Australia's top 500 companies, government departments and other large organizations, and investigated the type, frequency and kind of information attacks these organizations have experienced in the past and fear in the future. The results make for interesting reading and suggest what might be expected in the future from terrorists and the military's competitors.

The survey notes that Australian law enforcement agencies have reported significant increases in both the sophistication and number of external attacks on Australian companies in the past 18 months, a trend that is supported by AUSCERT statistics. 'Financial systems and confidential corporate data were the two most frequently attacked information types....a number of respondents...expressed concern as to the vulnerability of their financial systems to attack' (OSCA, 1997: para. 4.09). The survey shows the following motivations for the attacks: extortion and terrorism (10 per cent), espionage (26 per cent), financial gain (10 per cent), malicious damage (4 per cent), and curiosity (49 per cent). While the majority of attacks came from within (employees, contractors and consultants), 'the threat from outsiders is growing at an alarming rate'. This Australian finding is consistent with international studies. External attackers accessed information systems via the Internet (25 per cent), remote dial-in (16 per cent) and 'other' routes (19 per cent) (OSCA, 1997: para. 4.04). A compliance and fraud officer of a major bank estimated the cost of information attack to their organization alone to be 'in excess of $500 000' (OSCA, 1997: para. 4.14).

Military Information Operations

Currently Australia faces no threat from other states in the region (MoD, 1997). This premise has been the basis of strategic guidance and defence planning for quite some time and there is no immediate reason to challenge this strategic convention. However, the long-term trends in the Asia-Pacific region are of some concern. Already many Asian countries have been rocked by financial and economic problems unthought of a few years ago.

Information operations (Info Ops) offer advantages to developing states. Less dependent on information systems in their day-to-day existence, their vulnerability to an attack is reduced. With freely available information on the techniques of Info Ops and with low entry costs, Info Ops could no doubt be an attractive option. This is compounded when one considers the spiralling costs of conventional weapons and the requisite logistic, training and support expenses of keeping those forces in battle readiness. Because they offer anonymity, Info Ops are also compatible with the requirements of covert operations, the effects of which are deniable in an Info Ops context. With increasing regional tensions even the smallest, least developed countries could develop the motive, opportunity, capability and the willpower to launch an Info Ops attack. Info Ops could be seen to offer developing states a silver bullet to overcome the asymmetries of power between them and advanced states. Unlikely as it may now appear, who knows how things might look in 2010?

Info Ops would be a less attractive option for peer competitor states however. The consequences of attacking the financial system of a neighbour are just as likely to rebound on the attacker as they are likely to disable the defender when significant interdependencies exist between them. In addition, the systemic unintended consequences could be great and affect all manner of systems upon which the attacker depends, as well as causing friction within alliances.

Much of the writing on Info Ops suggests that it will be used in isolation from other forms of military action. This line of argument is suggestive of some interesting parallels between early air power theory and early information warfare texts (MacIsaac, 1986). Yet what would be the point of a large-scale coordinated attack on Australia's NII if it was not as a precursor to an invasion? If a major conflict was in prospect, then Info Ops would be an excellent tool for the aggressor. Used as the first shot in a major conflict, Info Ops would be a key element of surprise and could seriously disable core systems of the defender. This raises a number of interesting questions regarding proportionate response and escalation control in the event of an information attack. Would an assault on a country's financial system be an act of war, presuming the attack and the attacker could be identified? How might a country respond?

WHAT SHOULD BE DONE?

Until recently, it has been very hard to raise the profile of information security because it has been viewed as a technical issue, something computer managers should be aware of but not line managers, let alone those concerned about national security. But societal dependence on information systems demands that urgent attention be paid to information security. Because Australia possesses many advantages as an information economy, the

response must be multi-faceted, concentrating on how best to exploit the opportunities presented in the 'information age' as well as seeking the best possible protection from the vagaries of informational dependence. The stronger and more secure Australia becomes as an information base the more attractive it will be to investors seeking a safe and reliable space within which to conduct their business.

There are four main proposals that could be easily adopted with minimal expense that will be canvassed here. First, encryption. This is a very contentious issue for governments, essentially because they do not want that technology 'falling into the wrong hands'. It offers a level of information protection to all that use it and the fear is that as it becomes more difficult to crack bigger keys the government will lose its ability to read what people are saying. Without going into that debate, suffice it to say that encryption can offer systems protection.

Second, when one thinks of information security the immediate response is to think 'firewall'. However studies as well as expert opinion have shown that in many cases the most important safeguards start with simple security procedures in offices and homes, such as hiding passwords. What is really needed is a change in office culture that respects the gravity of information security demands. The best way to advance new thinking on corporate information security is through awareness programs and supplementation of training regimes that emphasise the implications of getting basic computer security wrong[11].

Third, in the immediate future corporate plans must be developed to cope with an information attack contingency. For example, if the telephone exchanges upon which the Department of Defence relies for terrestrial communications were attacked, does Defence have a plan to prioritise its communication needs with the remaining available systems? What if, in addition to communications, the energy supply from the Canberra grid were to collapse, putting further pressure on a wide range of defence systems? Is there a plan at ADHQ that is practised regularly that prioritises the operations of the organization so that it can still function when core energy and communications systems are degraded? The same question can be asked of the banks or any other vital part of the NII. Rather than having a solution to these problems imposed from above, information assurance plans are best designed at the organization level. However, that does not preclude cooperation or coordination with others, either locally or internationally, on best practice in the event of a failure of a part(s) of the NII.

Finally, a National Infrastructure Protection Agency should be established within the Department of Prime Minister and Cabinet(PM&C). It should comprise a Council, Warning Centre, and Secretariat. The Council's role should be to oversee the work of the agency and to make recommendations to Cabinet to ensure the security and proper functioning of the national infrastructure. Membership should be open to Government Ministers and senior representatives of the corporations that operate the infrastructures concerned. The Warning Centre, the core of the organization, should be a nation-wide government and non-government voluntary monitoring system that can detect and trace any irregularities in the operation of the infrastructure, once system-wide benchmarking has taken place. The Secretariat should have a very small staff, drawn from existing agencies with a contribution to make in infrastructure protection.

There is a trade-off between diversity and connectivity in information systems. Diversity in information systems equates with security. However, it also complicates monitoring

activity within a system and across the interconnections between systems. Because information attacks are potentially anonymous and ambiguous, a monitoring function is vitally necessary. This core organization would benchmark existing systems and monitor, on an anonymous basis, any suspicious activity. On discovering a flaw in a system or the evidence of a threat, the organization would notify users of the problem and develop solutions to overcome the attack. Anonymity in reporting events is vital if commercial and military confidence is to be maintained.

The need for such an organization is recognised by the officials responsible for assurance of the NII in the Attorney-General's Department who argue that, at a minimum, Australia needs:

> "some central repository of information on incidents that have taken place; otherwise… there would be no way of knowing whether security is adequate. Similarly, if the information remains distributed we need a mechanism for informing organizations of the latest threats and security techniques" (Ford, 1998).

Overseeing the work of the organization would be a committee comprising representatives of those participating businesses and government agencies whose role it would be to develop recommendations to Government on regulatory strategies to enhance the security of the NII. The Government conduit would preferably be a Cabinet-ranking Minister. It would not be preferable, or necessary, to create a new ministry for this purpose. Rather, the role should be delegated to an existing portfolio, such as PM&C, which would be a natural base due to its whole-of-government focus.

Superficially, one might suspect that various competitors would not be enthusiastic about participating in such a scheme. In exchanging information they could also be exposing their position. However, the initial trends suggest that most of the organizations at the heart of the NII realise that coordination will be vital to both their individual interests and those of the group. Indeed, never was security so mutually dependent as in the realm of information technology. As the OSCA survey demonstrates, when anonymity is assured, participants are eager to learn from each other's experiences. The OSCA research is particularly compelling as it draws on both corporate and government examples and demonstrates that the two groupings are willing to work together on this vital issue.

CONCLUSION

As an example of a typical OECD state, Australia is vulnerable to information attack. There are many exposed critical nodes in key elements of the National Information Infrastructure (NII) that could be exploited merely by the mischievous or, more seriously, by aggressors. Interdependence among systems, such as telecommunications, energy, and financial networks, as well as a general dependency in modern life on information systems, present new challenges to a wide range of government and corporate authorities. Criminals and organised crime syndicates already utilise weaknesses in the NII at a significant and growing cost to society. There are grounds to believe that potential threats to the NII exist which are likely to increase in time as terrorists and aggressive states seek to exploit new technologies that can cripple societies while permitting a degree of anonymity to the attacker. Nevertheless, there is a range of strategies that can be adopted to protect both specific units as well as the system that comprises NII. Some are quite simple solutions, others require more coordination but they do not have to be prohibitively expensive. A

comprehensive strategy for Australia which seeks to build on its strengths as an information economy, complemented by making its NII more robust, would be a good starting point to enable Australia to successfully engage in the economy and society of the new millennium.

There are important lessons in the Australian case for all advanced economies such as those in the European Union and North America. Dependence of critical infrastructures on networked computers presents a whole new world of challenges to strategic planners into the 21st century. Information warfare presents especially dispersed terrorists groups with excellent opportunities to attack and severely disrupt (and at the extreme disable) the foundations of modern society upon which daily life depend. It may well turn out that only a major crisis will force states to act to protect their citizens.

REFERENCE

Australian, The, 1998 (a), 'Doomwatch warns of millennium meltdown', *The Sunday Times*, re-printed in *The Australian*, 14 April 1998

Australian, The, 1998 (b), 'Millennium bug threatens to detonate or destroy nukes', *The Sunday Times*, re-printed in *The Australian*, 16 March 1998.

Australian, The, 1998 (c), 'Global leaders brace for casualties', *The Australian*, 7 April 1998.

Australian, The, 1998 (d), 'The world according to Richard Humphry', *The Australian*, 7 April 1998.

D. Ball, 1987, 'The Use of the Soviet Embassy in Canberra for Signals Intelligence (SIGINT) Collection', *SDSC Working Paper* No 134.

Bank for International Settlements 1994, *Payments Systems in Australia*, Bank for International Settlements, Basle.

K. Beazley, 1987, *The Defence of Australia 1987: A Policy Information Paper*, Australian Government Publishing Service, Canberra.

Business Review Weekly, 1998, 'Computer crash', cover story, (Australian) *Business Review Weekly*, 23 March 1998.

E.H. Carr, 1939, *The Twenty Years Crisis 1919-1939*, Macmillan, London.

E.H. Carr, 1942 *Conditions of Peace*. Macmillan, London.

E.H.Carr, 1945, *Nationalism and After*. London.

A.C. Cobb, 1996, *The Evolution of the Concept of Security Since WWII Among Western International Theorists*, Unpublished PhD thesis, Cambridge University. Held in Parliamentary Library, Folio No. 3768 c.1.

A.C. Cobb, 1997, ‘Australia’s Vulnerability to Information attack: Towards a National information Policy”, SDSC working paper #310.

F. Corr, and J. Hunter, 1992, 'Worldwide Communications and Information Systems', *IEEE Communications Magazine*, October; and 1994 'SWIFT Rolls Out Security Package', *Banking World*, March.
J. Fahey, 1998, Minister for Finance, Press Release, 24 April 1998.

P. Ford, 1998, 'Protecting the National Information Infrastructure', Australian Defence Headquarters Symposium, 12 May 1998, Information and Security Law Division, Attorney-General's Department.

M.B. Greenlee, 1996, 'Communications Security Standards', in J. W. Conard, ed, *Communications Systems Management*, Boston, Auerbach Publications.

W. Hope, 1992, 'Satellite Communications in Australia', in D. Ball, and H. Wilson, *Australia in Space*, Canberra papers No. 94.

A. Krepinevich, 1994, 'Cavalry to Computer: The Pattern of Military Revolutions', *The National Interest*, Fall.

Linklater, J., 1992, *Inside the Bank: The Role of the Reserve Bank of Australia in the Economic, Banking and Financial Systems,* Allen and Unwin, Sydney, p. 196.

D. MacIsaac, 1986, 'Voices from the Central Blue: The Air Power Theorists', in P. Paret, ed, *Makers of Modern Strategy: from Machiavelli to the Nuclear Age*, Princeton, PUP.

T. McIntosh, 'Forum to tackle hack attacks' *The Australian*, 30 September 1997.
(MoD) Minister of Defence, 1997, *Australia’s Strategic Policy*, Department of Defence.

OSCA (Office of Strategic Crime Assessments), 1997, *Computer Crime and Security Survey (1997)*, Canberra.

D. O'Neill, 1992, 'An Australian Defence Satellite Communications Capability', *Australia and Space*, Edited by D. Ball, and H. Wilson, Canberra Papers No. 94, SDSC, Canberra.

Optus, 1996, *Industry Development Report 1996*, an Optus Communication Publication.

Optus, 1996, *Satellite Information*, Optus publications, 1996.

W. Schwartau, 1994, *Information Warfare: Chaos on the Electronic Superhighway*. New York, Thundermouth Press.

SWIFT Annual Report, 1995, quoted in T. Manzi, 1996, *Financial Warfare: Assessing threats to the US Financial Infrastructure*, Unpublished thesis, Faculty of the US Joint Military Intelligence College.

Sunday Telegraph, The, 1998, 'Olympics threatened by Y2K', *The Sunday Telegraph*, 22 March 1998.

Telstra, 1996, *Broadband Bearer Network Australia Map*, 1996 produced by the National IDN Region Capacity Planning Centre in Melbourne.

TransGrid, 1996, *TransGrid Annual Report 1996*, Sydney.

A.Wrigley, 1990, The Defence Force and the Community: A Partnership in

Australia's Defence, Australian Government Publishing Service, Canberra.

X, Mr., 1998, "Canberra fails Olympic security test", *Australian Financial Review*, 2/9/98.

NOTES

1. The view expressed in this article are those of the author and may not be attributed to the Information and Research Services (IRS) or to the Department of the Parliamentary Library. Readers are reminded that this is not an official parliamentary or Australian government document.

2. RMA sceptics argue that the technologies associated with the RMA have existed for some time, for example, the first precision-guided munition was used in WWII.

3. One of the problems with this conceptualisation is that it is not well designed to overcome problems in asymmetric conflict—where an ill-equipped and poor adversary may not be susceptible to a computer attack because the most advanced forms of military technology they need are a machete and AK-47. The Vietnam and Afghanistan conflicts, as well as more recent events in Rwanda and Somalia, suggest the potential problems with over reliance on technology as a substitute for political solutions or sound security policymaking.

4. I am grateful to Dr Jerry Everard of the Australian Defence Intelligence Organization for this use of the term RMA. In fact, as some recent studies have shown, in past conflicts where roughly comparable technologies were available on each side, those that revolutionised their command structures and operational plans were those most likely to succeed. See (Krepinevich, 1994).

5. See for a US example the 15 July 1996 US Executive Order 'Establishment of President's Commission on Critical Infrastructure Protection Commission'.

6. Other bodies regulate the credit unions and securities, such as the Australian Financial Institutions Commission (credit unions), Australian Securities Commission (securities), and the Insurance and Superannuation Commission.

7. Example arose in discussion with ANZ officials, 16 August 1997.

8. Royal Australian Air Force 1998 Air Power Conference, 30–31 March 1998.

9. Air-gapped means simply that the systems are not connected to other systems (such as the Internet).

[10] The Unabomber (Theodore Kaczynski) was notorious in the United States for 17 years for sending parcel bombs that killed a number of people. He had a manifesto published that railed against society and presented his 'reasons' for seeking to destroy it. He was finally arrested in 1996 after a tip-off from his brother.

[11] At an information warfare conference at the Australian Defence Force Academy, a senior defence information security expert noted that if more people practised office procedure for hiding information then a significant amount of security violations would be reduced.

A SOFTWAR VIEW OF THE KOSOVO CONFLICT[1]

Chuck de Caro
Aerobureau Corporation, Mc Lean, Virginia, USA

ABSTRACT

The contemporaneous viewing of Global TV (GTV) during the recent conflict in Kosovo demonstrated that the Milosevic government used 'SoftWar' tactics to attempt to counter-balance US/NATO in the global mil-pol regime. The resultant effects upon the bodies politic of the NATO nations may well have helped to prolong the conflict. In this paper some Soft War aspects of the KOSOVO conflict are examined. The paper starts with an overview of ' who we are' and the philosophy and way of operations of Aerobureau Corporation. As the resident out-of-the-box-IW-guy I am very happy that to see that the pursuit of IW is having some effect on the way the US conducts itself on the international scene. But in all cases I think that the portrayals do not go far enough in that they are limited to activities that take place in an arena of nation-states (or in the case of Kosovo, proto-nation-states)

ORGANIZING FOR THE FUTURE OF IW

The reality is that the Information Age has already created war forms that go beyond conflict bounded by such Industrial Age geopolitical norms.

While my colleagues pay some attention to the Information Age in their references to IO/IW now and in the future, they miss the idea that the *nature of war itself has changed* due to the new dimension of the Infosphere. The examples of Somalia and Rwanda demonstrate *precisely* this point. Worse, instead of *adapting* to a world in full view of the glare of Global TV their recommend largely reflect a kind of Luddite view of trying to evade or hide rather than act fluidly on the "terrain" of the ether.

The Clauswitzian definition of war is the extension of politics that uses the controlled application of violence to constrain the enemy to accomplish our will. That definition, however, has been eroded by the advent of instantaneous global telecommunication, especially of global television, in that it is now possible to affect multiple bodies politic without the direct application of force. Why else did the US cut and run from Somalia, when the great US tactical victory was completely upended by the effects of video of a handful US casualties upon the American body politic?

As another example, consider that the United States has been engaged for the better part of a decade in a new kind of war whose main proponent is the stateless ex-Saudi terrorist Usama Ben Laden. That UBL has been successful can be very succinctly put: One individual, primarily self-supported, has managed to engage a superpower with various large scale acts of violence, and that after several years, that man and his cause are still alive...and thriving!

The long standing US countermeasures have thus been ineffective and arguably counterproductive, in that retaliatory cruise missile attacks, such as the one in Sudan, tend to outrage the local population and impel others to join UBL's cause.

This inability to stop UBL stems from US insistence on using Cold War legacy systems and even more archaic thinking in dealing with an asymmetric enemy who has totally adapted himself and his operations to the Infosphere; he is in effect a *virtual guerrilla* whose area of operations is global and four dimensional. His adaptation to the terrain of the Infosphere (of which cyberspace is a subset) gives him and his organization the advantage of amorphousness to appear and disappear at will.

Thus this stateless millionaire, whose operatives constitute a small *virtual nation*, has been able to conduct a new kind of guerrilla war on a global scale with attacks against American interests from the Middle East to Africa to the Philippines and even to the once sacrosanct shores of the United States itself.

Ben Laden has demonstrated distributed and dispersed intelligence and command functions. He has used global television to greatly magnify the size and scope of his attacks and create a kind of cult following based on the amplification of his alleged charisma. He has used cyberspace to conduct operational simultaneity in his attacks as demonstrated at the embassies in Africa, and has demonstrated a desire for global power by his seemingly one-man onslaught against the United States.

The US has worsened the situation by treating Usama's attacks the way an inept mechanic deals with an engine warning light: It makes the symptom go away by cutting the wires to the light! The same mentality applies to simply killing, or capturing and trying a terrorist. *The problem is in the engine*! And the *engine* here is the body politic and virtual body politic that support Ben Laden through contributions of personnel, intelligence and operational support.

To end the problem the US must affect those bodies politic and support mechanisms, which allow Ben Laden to carry on his operations. *Thus, the US must adapt to the Infosphere and attempt to out-guerrilla the guerrilla*.

And to do that the first thing that needs to be fixed is intelligence, especially adapting "steam gauge" data gathering to useful knowledge that is readily applicable. Again let me illustrate this by using UBL as an example:

EXAMPLES

The recent one-hour, highly produced television program developed by Usama Ben Laden and then transmitted via satellite from facilities in Qatar presents an opportunity to use non-verbal, televise cues to garner information that is simply not obtainable through industrial age intelligence gathering methods, because interpretation of video is simply not taught.

It is my experience with this specific matter that the only conventional method of ascertaining the intent of the TV program has been to have the script reconstituted by the Foreign Broadcast Information Service and then screen the words for meaning. While this worked fine for radio, it misses the whole point of television: TV is a cool medium where perception of images and sound is more important than the words that are carried along.

Moreover, like the "fist" of a Morse code operator, the stylistic nuances of a producer, director and writer are recognizable when compared against a body of work. Given that a satisfied end user will tend to go back to the same production company, and that the roster of quality TV producers in the middle east is a limited one, a television-oriented review of the existing video tape of the UBL program may bring forth information that may reveal the names and locations of the persons involved in its production and thus back to the paymasters and possibly even to UBL himself.

What may be even more intriguing is the possibility of "turning" the producers in place in a Information Age variation of the "Funkenspiel" of WWII. It may be possible to inject scenes, add subliminal effects or in other ways distort or make counterproductive any future programming against specific target audiences.

However, none of this is being done or even being contemplated at this juncture.

WHAT DOES THIS MEAN?

What all this means is that a band-aide fixes applied with superglue, do not make a novelistic war fighting capability fit for the Information Age future in a milieu of new entities beyond the nation-state. What will be needed is a new kind of warrior, who from the day he is recruited or possibly even drafted is optimized for this new kind of combat. This means smaller numbers of extremely well educated soldiers, fluent in media as well as languages and capable of four-dimensional combat against a worthy enemy.

Moreover, why would we organize such future soldiers in a rank structure copied from Industrial Age models? (Does UBL have 9 grades of enlisted, 10 grades of officer and 5 grades of warrants? does Bill Gates?) Or organize in a hierarchical structure (Does UBL have fixed Squads, Companies and Battalions? Does Bill Gates?)

Futurist Alvin Toffler in his book "War and Anti War" made a very important discovery: "Nations make war the way they make money." The way we make war is the way our grandfathers made war.

This new model military and intelligence system then must be organized in a kind of fluid matrix made possible by the communications potential of the Infobahn and which changes precisely, in real-time, to deal with the problem or problems at hand.

The first step on this quest must be to break down the formidable barriers to change inculcated by useless tradition in our national security organizations; for as Shakespeare once wrote: "*The fault, dear Brutus, is not in the stars, but in ourselves.*"

THE KOSOVO CONFLICT

Political Throw Weight I: Stealth Crash

In the background of the still burning F-117 were a couple of buses, some official cars and

lots of reporters, which indicates that the Serbs expected such a crash. (Was this an ambush using military operations to create a mil-pol event? Perhaps using radar signatures of one missile system then using a barrage of a second missile system with a different minimum range and optical/sound cueing? Or did the Stealth fighter operators get overconfident and fly down the same routes more than once?) Obviously, the logistics were preplanned and practiced, thus seducing GTV with great B-roll and thus opening an information channel to erode support in the US body politic.

This means that someone in the Yugoslav government was in charge of a mil-pol operation to maximize the "political throw weight" on GTV. Why was there no effort to backtrack that operation to delay or deny access? .

Political Throw Weight II: POWs

The capture of the US soldiers is a variation of the "Balkans Jacks" tactics used against Canadian Peacekeepers in 1994. Serb SW efforts were dominating the airwaves and continued to do so in a "Pit and Pendulum" manner leading to the Jesse Jackson "Let's Make a Deal" finale.
What was the impression upon the Serb audience of a hand-wringing, friend-of-the-president minister/would-be politician begging for the release of the US soldiers?

What was needed was a strong televised visual (not talking head) messages beamed directly to the Serb Body Politic so that the consequences of POW mistreatment would have been universally understood.

Body Politic Unification Measures:

Serb TV stayed on the air through most of the conflict and was used as an instrument for political solidarity. Thus the rock concerts and human shield tactics served both to demonstrate defiance and project a sense of safety in numbers, which again helped prolong the conflict.

It wasn't until late in the conflict that NATO realized this, and took action by wrong-headedly bombing the TV production facility and thus playing into the Serb propaganda organizations hands (see below.)

The Industrial Age myopia of simply destroying targets to preclude the Serb government's use of its TV transmitters missed the possibility to project a nationwide dis-unification TV campaign. The COMMANDO SOLO still does not have 24-hour counter-programming capability to beat a ground-based national TV system because TV shows remain the responsibility of the 4th POG which is grossly under equipped, under manned and especially under funded to deal with this situation.[2] What are needed are a UAV-based dissemination system and a Soft War 24-hour, Real Time/Near Real Time campaign.

State Department Efforts Using DBS Transmissions

While the idea of using European satellites to beam TV to the Serbs was at least a start, it was amateurish and randomly distributed. Apparently someone at the State Department figured out that there were in excess of 100,000 DBS receivers in Serbia. Fine, except that they did not take account of the idea of Ratings (number of TV sets turned on at any given time) or Share (the number of those sets tuned to a specific program at a specific time). Thus depending on power outages from the bombing perhaps half of less were turned on. Of those, the menu of Euro TV is in excess of 100 channels. Meaning that perhaps less than 500 sets were tuned to the State Departments broadcasts.

And what did the State Department's broadcasts consist of? Why the Secretary of State's talking head speaking in American accented Serbo-Croatian of course. The end result was printed on the front Page of the Washington Post. When asked about the SECSTATE's effect a Belgrader was quoted as saying: *"...all she was missing was her [witch's] broom."*

The idea of trying to affect that tiny fraction of the Serb body politic that receives DBS vice the huge demographic that gets local broadcast TV is simply an exercise in futility. Worse, without a demographic analysis system of some sort in place, the message cannot be tweaked for maximum results.

And while the Secretary of State speaking in Serbo-Croatian was perceived as an IW 'coup-de-main' over in Foggy Bottom, those macho Serb boys were not "mirror-imaging" and were not in the least bit daunted by what they perceived to be a sawed-off, over-aged, finger-wagging schoolmarm with a Rambo fantasy.

What was needed was visceral, B-roll-heavy campaign aimed at dividing the factions that exist in Serbia using the UAV system mentioned above.

Negative Telegenics Of SACEUR

In his public statements, SACEUR's body language, preference for the sitting position and inability to make eye contact with the camera (and thus the audiences he was trying to convince) worked against him. Moreover, his choice of uniform and lighting made him look ashen and perplexed. What was needed was very serious and meticulous coaching, better lighting, and a standing posture.

GTV Deception/Spoofing Operations:

The use of GTV by the Serbs to sow confusion amongst the bodies politic of NATO was commonplace. Note for example, the large number of English speaking Serb officials who stayed steadfastly "on-message" *("NATO bombing is driving Albanians out";* and *"Serb units are only attacking guerrillas")* on GTV. For every NATO speaker there was a near equality of Serbs, some of whom had pretty good telegenics.

Serbs also demonstrated "Orson Welles" attacks by using old video of negotiations with an Albanian faction leader and repackaged as current, so as to confuse and delay NATO political response.

Using SOF For Mil-Pol Effect

The lack of real-time or near-real-time video of Serb ethic cleansing operations while-in-progress eroded the credibility of NATO actions. What was needed is the immediate up-linking of on-going SOF special reconnaissance operations, because the video itself is far more valuable as a mil-pol weapon than the mere tactical identification and laser illumination of Serb units. Air recce stills, no matter how high their resolution, simply do not have the visceral impact of live video, especially the up close and personal stuff that SOF can deliver. This mission should have had unfettered number one priority, especially in the early parts of the conflict.

Kinetic Attacks On Serbian Television:

The attack on the Serb TV production studio in downtown Belgrade was grossly wrong-headed, unjustified and hugely counterproductive. The attack only temporarily put the institution off the air, an obvious conclusion because video footage showed wreckage of the microwave transmitter tower, not the broadcast antenna itself. Far worse, the ill-conceived attack provided the Milosevic regime with a massive propaganda lever, with gory B-Roll of dead civilian journalists alarming editorial institutions around the world. A subsequent attack against a generator building was needed to cut power to the remote transmitter, which should have been the sole target in the first place. Generators are easy to replace; it is the **klystron tube** in the transmitter that is the heart of the system. As long as the KT could be replaced, Serb TV continued to go back on the air. These tubes are serial numbered items and are in limited supply around the world. As a follow up, the US could have bought up all the tubes that fit the Serb transmitters and thus insure that after the Serb's finite of ready spares was exhausted, there were no alternative means for returning to the airways.

SoftWar Attacks On Serb TV

It was simply not enough to take out the transmitters and leave the receivers to lay fallow. By transmitting programming into the intact receivers using UAVs, the US could have affected the glue that holds the **Serb belief system** together. This should have been integral to the kinetic scheme of maneuver. Leaving out this methodology, cost the US a huge lever that could have greatly assisted in forcing the Milosevic regime into acceding to NATO's wishes much sooner.

Again developing TV programming for use through the trans-attack and then in the post attack/peacekeeping phase requires lead time and thus should have been in the works early on. The experience of trying to assemble the OHR (NATO) Open Broadcast Network (OBN) in Bosnia and make it into an effective system should have been a sobering thought and the lessons learned should have been applied right away.

Cyberattack (US POWs)

Given that the capture of US soldiers was an IW act to generate political throw weight, it might have been possible to have used another form of IW to get them back. A cyber attack against the personal back accounts of the Milosevic family especially Mrs. Milosevic, (probably in Cypriot banks) could have given the US the leverage to secure the POWs release. The money caches, generated from skimming the black markets in the last decade, would likely not be widely known to the body politic of the former Yugoslavia, and given the current state of the economy, Milosevic, et ali, would have been loathe to complain. Thus the money could have been returned quietly as each soldier was repatriated.

Political Throw Weight (US Train Attack)

Despite the degradation of facilities in Yugoslavia, their information campaign continued unabated and seemed to have improved despite the NATO attacks. For example, within 24 hours of the accidental attack upon a passenger train and the subsequent apology to the Serbs by SACEUR, the Serbs had computer generated animation demonstrating that the attack was not an accident but was intentional. Given the then continuing on-air capacity of Serbian television, it gave Milosevic still another unifying tool to keep his body politic in line. Moreover, the use of such unauthenticated but convincing and "news-balancing" video causes a slow erosion of the national wills within the NATO community and especially within the United States. This kind of counterpunch must be parried, visually, right away before it "sticks" in the minds of the bodies politics.

Near-Future Softwar Ops

With US forces now deployed in Kosovo it would be wise to have a modern IW plan in place to deal with both the AOR/AOI to keep possible problems in check.
Keeping the displaced Albanian Kosovars informed will keep other problems from cropping up, and there is the legitimate group of Serbian Kosovars who are going to remain in the country and whom NATO must now protect.

Takeover of existing TV transmitters or rebuilding them is important but as important is generating the PROGRAMMING is critical because of lead times needed. In addition, getting radio and print facilities operational is critical to support and promote TV programming.

Because the infrastructure will be down, it would be advisable to purchasing tens of thousands of battery powered TV receivers to hand out to the displaced people so they can receive the TV message.

The ultimate goal here is to attempt to change the inbred belief system, so that while US forces are in place and after they leave, the locals won't pull out their weapons and start again.

NOTES

[1] Copyright 1999 Chuck de Caro

[2] COMMANDO SOLO is useless as a TV platform for anything other than coastal targets.

INFORMATION OPERATIONS
Ideas for a strategic approach within a small country

Brigadier Dipl. Ing. Alois A. J. Forstner-Billau
Landsverteidigungsakademie - Wien

ABSTRACT

Just like other countries, Austria is confronted with the increasing dynamics of the development of Information and Communication Technology (ICT). Both the public sector, including defence, and the private sectors are depending on ICT. Discussing conflict scenario's, one has to discern international activities within the framework of a crisis response or peace support operation, and a military assault to a country. If Austria should be attacked it could theoretically be by an equally capable or by a far superior power. In this last case, it is like David and Goliath. This article introduces the idea to study 'associative communication' to arm David.

PREFACE

The general theme of the publication for the NL Royal Military Academy Symposium on 'Information Operations' is a real temptation for an author. He may try to find the best technically oriented approach to the general theme. In view of the enormous dynamics in scientific development of all related technologies, I will try to withstand this temptation. I will concentrate more on a, if I am permitted to use the expression, general (`s) approach. The following reflects my personal opinion and in no way should be regarded as an official Austrian political or military position. Nevertheless it is quite evident that more or less personal ideas of key personnel can and do influence the official view of organisations.

INTRODUCTION

Some of the key features of the Information Age are: the quantity of available information, the nearly unlimited access to this information and the resulting speed of activities of maintaining them.

All of these are and, over time, will increasingly be essential factors, that decide about the efficient combination of the traditional production factors: Labour, Money and Property, in a world of ICT-based processing. Computer aided decision-making has to guard and facilitate the different processes.

The information infrastructure, which is the vital backbone of our modern society, is unacceptably vulnerable to, intentional and pinpointed actions by terrorists, criminals and/or hostile organisations and governments. But not only by them. In the world of economy and business even competitors could try to use illegal means of intrusion into the data – and therefore knowledge bases - of another competitor. The vulnerability of today's ICT-systems in general is a serious problem and offers a tempting, rather inexpensive and very simple alternative for pinpointed intrusion or more likely assaults.

The ‘Superpowers’ in the world of today have recognised these threats and have therefore started to establish means and procedures to maintain ‘Information Superiority’ as a strategic objective to reach ‘Information Dominance’. Russian authors discussing this, have stated the following:

‘We are now seeing a tendency towards a shift in the centre of gravity away from traditional methods of force and means of combat, towards non-traditional methods, including information. Their impact is imperceptible and appears gradually. It is less burdensome economically and is not dangerous ecologically (....) Thus today information and information technologies are becoming a real weapon. A weapon not just in a metaphoric sense but in a direct sense as well.“[1]

In a report by the U.S. Centre for Strategic and International Studies, one finds the conclusion that the U.S. is aware that it is exposed to a host of new threats to society as a whole. This is because of the immense complex information infrastructure, being based on insecure foundations. The weapons of information warfare can outflank and circumvent military establishments and compromise the shared foundation of both the U.S. military and civilian infrastructure.[2]

As one can easily see, both views are more or less focused on the military part of Information Operations and are the source and background for mainly offensive concepts which might be indicated as ‘Strategic Information Warfare’.

The ‘Superpowers’ invest heavily in intellectual, scientific, and economic efforts and last but not least, invest vast amounts of money to be ahead in a global race for ‘Information Superiority’ with the objective to reach ‘Information Dominance’. For us, the authorities and citizens of the ‘Small Powers’, or shall I call them the ‘Powerless’ it is of high relevance as Campen makes us aware that:

“The information age world is one where geography, time, distance and space are irrelevant; where threats are diffused and obscure; **where Allies can also be non-traditional adversaries; and where Industrial Age laws and agreements among sovereign nation states have limited relevance“** [3]**.**

This means that in the ‘Information age’ one cannot fully rely on ‘friends & partners’ anymore. You either belong to a ‘club’ or your don’t. In the latter case everybody might threaten you, everywhere, and at anytime.

The national efforts in ‘Information Operations’ in general are based on three pillars: **‘Private Information Infrastructure’,** the **‘Federal Information Infrastructure’** and, within both information infrastructures as a subset, **’Defence related Information Infrastructure’**

THE PRIVATE INFORMATION INFRASTRUCTURE

In the early days of the implementation of Information Technology (IT), this technology was about the single user. Only highly qualified personnel and experts were able to run and

maintain these systems. IT was not of vital importance to the user respectively his organisation.

There was hardly any connection between one system and another. Data and information had to be printed out for use. For the manipulation and the possible abuse of data, one had to look for a direct, physical entry into the system. With physical barriers only, one could provide a high level of security. With the increasing upcoming of standardisation, the connection of networks and the recent dramatic growth of the worldwide interconnection via 'Internet', the 'solitude' in IT-privacy of the old days is over. It is now ICT, the combination of Information and communication that counts. 'Internet' is becoming increasingly essential for the economic survival of business organisations.

For a small country and its 'Private Information Infrastructure' this 'Globalisation' and ICT-supported 'Interworking' is, giving its opportunities, more of a challenge than a danger!

Within international partnerships of co-operating as well as competing business units, it is of mutual concern to fight the threats resulting from the application of modern information and communication technologies and their potential abuse by 'non- partners'. Small countries on the one hand, as well as small businesses on the other, cannot afford the full range of necessary investments of complex and expensive Research and Development (R&D) activities, to counter a wide variety of ICT-related threats and possible assaults.

Due to the vital interests of the 'Powerful', they will have to take care that the 'Powerless' (or 'Less powerful') have access to that kind of technology which maintains a required minimum standard and capability of protection against possible threats.

So what could the policy of the 'Less powerful' be? They have to bring required quality products and services to the market, in such a way that even the 'Superior' are interested and find so many benefits that they want the 'Less powerful ' as partners. Then, they will take all the measures to let the 'Less powerful' join the international 'Information Infrastructure'. That is what happens for example to and in the Middle and Eastern European (MEE)-countries at this particular time.

THE FEDERAL INFORMATION INFRASTRUCTURE

The particular political situation in Austria before we entered the European Community (EC), nowadays European Union (EU) was, and to some extent still is, that we do not have a real government. What we had and still have is a board of independent ministers who's political actions are limited only by a, what is called, coalition pact as a 'framework' of constitutional and legal rules. Therefore, from the very beginning of the ICT-age the implementation of an Information Infrastructure to support the public administration was of a rather unique design within each of the single ministries and other agencies.

By the time and, stemming from the demands for an increasing, mutual co-operation within the public administration, based on modern ICT-Infrastructure, a co-ordination board for ICT-matters was created under the lead of the Federal Chancellery. This co-ordination Board (KIT^4) tries to apply, on a more or less voluntary basis for the member organisations and agencies, common rules for ICT-hardware implementations, software applications and (i.e.

security -) procedures. Furthermore, this Board co-ordinates all the ICT-relevant matters with and to the EU-bodies as well.

Modern Internet-technologies nowadays provide the opportunity to overcome the former standardisation deficiencies between the different federal organisations and agencies and, step by step, the 'Federal Information Infrastructure' becomes more interoperable and homogeneous.

The fact that Austria is now a full member of the EU, requires that we stick to the common rules and directives for the ICT-based administration with and within the EU-bodies on the one hand, and for the relationship with the other member States on the other.

Besides this, the 'Federal Information Infrastructure' shares with its political and business partners the common 'year 2000-problem' (Y2K). The Y2K problem is a real nation- and worldwide testbed to address other issues, like handling large scale inter- agencies and inter-government processes and, last but not least, an opportunity for improved ICT-security. The first of January 2000 will prove if we have succeeded or failed. As far as these Y2K-issues are concerned, it is my strong belief that in general terms, the predicted catastrophic events will not occur. But we must be prepared to face rather minor but nevertheless unexpected problems, and there may be 'painful', and 'odd effects' of the Y2K-problem.

THE DEFENCE INFORMATION STRUCTURE

According to the existing Austrian 'National Defence Plan', based on the constitutional obligations for the national defence in general, homeland defence itself comprises the military and militia organisations as well as different federal agencies and civil emergency management organisations. The historical development after the Second World War of these different organisations, combined with their widely distributed responsibilities for management and operations, as well as their Information Infrastructure are unique and therefore different as well. As mentioned for the private and federal sector of information infrastructure, Internet technology facilitates the connection and interoperability of these different systems right now.

Combined endeavours and missions of this integrated Defence Organisation to handle peacetime tasks, like national disaster relief operations, are therefore not a real problem for the interoperability of the different information infrastructures.

Joint training, monitoring and control centres, and a common understanding, make sure that in case of national- or worldwide catastrophes, relief can be provided and maintained very efficiently.

TASK END MEANS

Missions require a partnership approach to Information Operations. Sometimes an 'environment' results in a high probability that Information Operations will occur. Sometimes one can be sure that this environment in general can be indicated as having a friendly and co-

operative nature. Extensive precautions to counter possible hostile attacks against the Information Infrastructure of relief units are therefore in most of the cases not necessary.

As far as crisis response (CR) and peace support operations (PSO) is concerned, given the pure military character and the actual political (neutral) situation in Austria, one has to differentiate between two scenarios:

1. International – trans-national crises and conflicts – PSO engagement within a UN-, OSCE - and/or Partnership for Peace (PfP) – framework.

   In such cases, Austrian military units take part as 'sub'-units of other military units and hardly in a „Lead Nation" role and responsibility. Therefore the information infrastructure, fielded with an Austrian military contingent, will serve primarily for contingent-internal and 'reach back' functions. For the interoperability with higher echelons of command in the crisis theatre, the 'Lead Nation' in charge has to take care. The more national information infrastructure is interoperable with the 'outside' world, the less the logistic burden for the 'Lead Nation'.

   So it is our national intention to follow, as far as possible, international standardisation processes. Already in peacetime we are highly interested to take part in ICT-related, comprehensive projects and programmes, following international military partners and participating in joint and combined ICT-training and -exercise events.

2. The least probable case – military assault directed against Austria.

   In such a case, Austria has to rely only on its own military capabilities and try its best to face the conflict. As far as the „Information Operations" within a, (at the moment in a conceptual stage), national command and control, communications, computer, intelligence, surveillance and reconnaissance (C4ISR) capability is concerned, one has to differentiate between an assault by an equally capable opponent or by a far superior hostile military power.

In the first case I assume that we would be able to run our own ICT-infrastructure and therefore 'Information Operations' in a rather secure and successful way.
In the second case, one has to analyse what has happened in earlier conflicts between rather small countries and, relatively lager power adversary countries or organisations.
In all these cases, the Armed Forces of the small countries were hardly able to operate their 'electronic' equipment in a systematic manner. To secure the 'Defence Information Infrastructure', the only thing they could do was to switch them off most of the time. However 'Dormant' systems are no systems'.

So, what to do to maintain a minimum C2-capability which is necessary to resist a military attack? What to do, yet to be able to command one's remaining (remotely deployed) military units?

To go for very expensive and risky programmes to develop, produce and implement highly sophisticated technical systems in order to secure a certain fraction of one's ICT-infrastructure, is, in my opinion, in most of the cases a 'dead end' approach. A small country can hardly outdo 'Superpowers' in highly sophisticated technical solutions. And, if I look at

the budgets we spend on R&D in general and on military research in particular, we might just as well even forget to try.

So what else to do? Let me remind you of the story where a prisoner shouts a certain number and all the other prisoners start laughing. On the question of a visitor, what was going on, a guard answered, that a particular joke has a certain number and just by calling that number, all other inmates remember the full joke and therefore start laughing.

ASSOCIATIVE THINKING

The lesson to be learned from this story is that the challenge of an 'Less powerful' military power is to use intelligent solutions, which do not require extensive economic and industrial resources and investments. But smart ideas, a high level of training and bright trainees. With a minimum of data transfer and therefore a minimum of information infrastructure, which minimises the effects of hostile countermeasures too, one can and one has to achieve a maximum of, what I would call '**associative'** information content.

Communication, based on **'associative'** thinking and not just on 'listening and/or viewing' – that is the challenge for the 'Less powerful'! If you can communicate, you can command! If one further pursues this idea, one should - for example - revive the efforts of scientific research on paranormal phenomena, like telepathy etc., to use the possible results for military purposes. '**High Tech**' can be mastered by '**High Intel**.

CONCLUSION

Goliath was not defeated by another Goliath, but by little smart David!.So the only way to survive in wartime as an IT-David, is to be smarter than the IT-Goliath is!

NOTES

[1] Yevgeniy Korotchenko and Nikolay Plotnikov, 'Information is also a Weapon: About what should not be Forgotten When Working wit Personnel', *Krasnaya Axezda,* 17 february 1994, p. 2.

[2] *SIGNAL*, June 1999, offical publication of AFCEA p. 65

[3] Col. Alan D. Campen, USAF (Ret.)

[4] **K**oordinationsgremium für **I**nformations **T**echnologie (KIT)

TO INFORM, EVEN IN DIFFICULT CIRCUMSTANCES...
How Switzerland plans to do this

Colonel (General Staff) (rt'd) Edwin Hofstetter
Editor in Chief 'Schweizer Soldat", Switzerland

ABSTRACT

In a democratic state, such as Switzerland, censorship of the media is unthinkable. The Swiss government decided to shape an 'Informations Regiment' to act if circumstances would disturb the normal activities of press, radio and television. This paper describes the history, task and organisation of this regiment.

INTRODUCTION

In the years before and during World War 2, difficult political circumstances influenced efforts to keep the population and the armed forces informed. German institutions were conducting a propaganda battle at an increasing scale, even towards Switzerland. The majority of the Swiss press actively countered this propaganda, reflecting the freedom and autonomy of the country. The government and the army tried, by direction and control, to prevent severe provocations against Germany. At the outbreak of War, this led to censorship of the media. An army directive in autumn 1939 created the Section 'Heer und Haus' (Army and Home).[1] This organisation was to inform the members of the armed forces. Very soon its task included informing the population on questions of national defence. It was all about strengthening national resistance and the will to preserve national identity.[2] A network of more than 100.000 trusted representatives and some 7000 correspondents in the whole country were active to inform Swiss nationals in the different languages. In this way it was also possible to measure the feelings of the population. This certainly had a positive effect on the concept of resistance. Another activity, 'Action National Resistance', a private enterprise, not connected to any party supplemented 'Heer und Haus'. The activities of these institutions were co-ordinated with the Intelligence Service and the Office 'Press and Radio' of the Government. Early after WW2 a new private organisation is founded: the Swiss 'Information Service' ('Schweizerische Auflärungsdienst') (SAD). 'Heer und Haus' falls apart. A new 'Truppeninformationsdienst der Armee' (TID) has to answer the need of the armed forces for information. Company Commanders have to inform their subordinates, on the so-called 'total defence' and the military defence of Switzerland.[3]

In the years before WW2 the Swiss General Staff prepared precautionary measures, such as control of the press. As war broke out in September 1939, the army determined that there should be preliminary censorship. Swiss government, the 'Bundesrat' prohibited this ruling and decided that there was to be censorship only after publication.[4] After discussions with media representative's regulations were given, in accordance with constitutional law for circumstances of war. In the beginning Army Command was responsible for this censorship and the enforcement of those regulations. Thus, the Department 'Press and Radio' (Abteilung für Presse und Rundfunk - APF) in the Army Staff was, in order to safeguard the inner and

outer security of the country and its neutrality, ordered to monitor the publication and transfer of messages and opinions, particularly by post telegraph, telephone, through press and other agencies, by radio, movie and pictures, and to take all necessary arrangements. The Commander-in-Chief of the Swiss Army, General Guisan, did not see press censorship as a military task, but more as a political affair. As a consequence in 1942, the APF was subordinated to the Director of the Swiss Department of Justice and Police. This did not affect the way in which censorship was practised. The military organisation of the ADF was preserved. It was no easy task for the journalists of those days to get through the trellis of rulings without pain. Especially reports and comments on foreign policy were scrutinised. Editors were warned and some editions of newspapers were seized by offices of the APF. The 'Bundesrat' could, if and when further offences would occur, prohibit the publication of a newspaper, either partly or completely. Almost sixty times such strong measures were applied during WW2.

INFORMATION REPLACES CONTROL

In a democratic state, such as Switzerland, censorship of the media was unthinkable after WW2. The lessons of this war and the new potential threats of the 'cold war' materialised however in what would be indicated as 'total defence'. The concept also included communications. They should be secured if war, terrorist actions or catastrophes would occur. The APF was given a new task. This Department should - as civil and private media could not, or only party could act as planned, function as an information medium of the 'Bundesrat' to inform the population. This new and complex task soon demanded 2500 men and women. Officers, NCO's and soldiers of APF normally were active within the media. As today those men and women were mobilised during exercises. In 1982 a first serious situation occurred. It concerned the occupation of the Polish Embassy in Bern. In this situation the 'Bundesrat' was focused on getting so-called 'open' information. The APF supported those efforts. Officers of the 'APF' also were active from October 1998 till May 1999 on behalf of the Ministry of Refugees. At the same time, the primary task of APF, the control of publicity and communications, was withheld during peacetime.

A REAL TEST

The preparedness of 4 Army Corps, elements of the Boarder Guards ('Grenzwachtkorps) and of the Air Force was tested in 1986. This was realised within the framework of a 'total defence exercise' 'Dreizack', in combination with large scale manoeuvres. Civil staffs, civil emergency organisations and elements of public transport took part in the exercise. Some 250.000 members of the armed forces and civilians actively participated for some two weeks at a stretch. The APF, with a thousand uniformed men and women, was ordered to realise its information function, using all available means. A theoretical crisis situation was used as scenario.[5] APF in fact officially counted 2800 people. All participants, as well as the population, in the villages, in cities, in factories and schools were confronted with an imaginary dangerous situation. To give an example: sirens would be activated. At the same time the radio would warn for radiation danger as the result of ' an enormous disaster in France, not far from Basel'. Trained to do so, people went to the shelters they were told to use. The voices on the different senders got weaker. In the end even foreign broadcasts fell silent,

telephones did not function. Finally, after some hours of distress, a voice is heard on transistor and other radios: ‘Attention, this is a broadcast of APF, the Department for Press and Radio. The APF is the information instrument of the ‘Bundesrat’. ‘Trust our voice ....’. The powerful broadcasts of APF-senders even penetrate the concrete of the shelters. Thus or in similar ways the APF hat to prove that it could inform the population in difficult circumstances. Operation ‘INFOSUISSE’ included the use of radio, television and press.[6] APF-television presented three times a day a thirty minutes programme in the three languages that are spoken in Switzerland. For almost five days APF-radio transmitted clock round on FM. The program included news, special announcements, as well as music for the population and soldiers. The speakers, both men and women, generally were well known from ‘normal’ radio and television. They were reservists and were activated to be trained as members of APF. The idea was to build confidence on the fact that they were known and people enjoyed listening to them. The final goal of this Media Units was, though within the limits of an exercise in time of peace, to meet the psychological demands that come with informing a population. In a real dangerous situation APF should strengthen solidarity and the will of the individual to survive, should reduce uncertainty and should keep up trust in its own government.

The public positively accepted APF-Radio and TV. The organisation of left-wing journalist and editors of so-called ‘left’ newspapers were quite critical in their comments. The public appearance of ‘State media’ which were planned to be used during an information crisis was not popular in those circles. During ‘Dreizack’ mobile radio stations were used. TV operated from fixed locations. Press detachments used civil printing facilities, most of the time during night hours. The employment of APF during this exercise was worthwhile. One had passed the test. Since this exercise APF personnel never again operated so publicly. Within a few years they would be militarily reorganised into Informations Regiment 1.

Figure 1: The INFOSUISSE Paper is also distributed via civil kiosks

INFORMATION IN EXTRAORDINARY CIRCUMSTANCES.

For special circumstances the Swiss 'Bundesrat' has at its disposal a separate staff the 'Stab Bundesrat, Abteilung Presse und Funkspruch' (Stab BR APF) to inform the population. Responsible for this Department Presse and Radio still is the Department of Justice and Police, the 'Eidgenössische Justiz und Polizei Departement' (EJPD). Activation only follows if and when the civil institutions are no longer able - partly or completely - to perform their information tasks. Truth is the guiding principle for all activities. Only with a credible information policy trust in political and military leadership can be maintained. On top of that, information should be accurate, relevant and understandable. Not in the least because of the principle of truth, this staff is no instrument for psychological warfare.

The 'Stab BR APF' has a managing board chaired by the Secretary General EJDP. A subordinated body is responsible for political-publicity guidance, the so-called 'Politisch-Publizistische Leitung' (PPL) and has to advice the government on information policy. The military organised Information's Regiment 1 leads the media activities and realises the broadcasts. Personnel of 'Stab BR APF' belong, with a few exceptions, to the conscript army.

INFORMATION REGIMENT 1

The Information Regiment 1 got its present structure on January 1, 1997.[7] It consists of a Staff and five 'Abteilunge', comparable with battalion level. One to support the staff and the Regiment, four - numbered 10, 20, 30 and 40 - are operational elements. The 'Input Abteilung 10' (three companies) is responsible for obtaining and processing information, with the help of foreign language specialist. Those specialists are recruited from Swiss living abroad or from naturalised Swiss citizens.

Radio and TV

The 'Radio-Abteilung 20' has five Radio-companies. They have to ensure that the Government and military command can quickly inform the population all over the country. Their high power FM radio stations, which are spread across the country, transmit national programmes in three languages. Those programs can even be heard in the third level of protective shelters. They may include an alarm in case of an emergency or catastrophe. Information may be broadcasted in other (foreign) languages in order to reach target groups in- and outside Switzerland.

The 'TV-Abteilung 30' (with three TV-companies) is able to produce emergency programmes in three languages. Thus they spread messages and directives of national or regional authorities.

The companies and detachments of both the Radio- and the TV-'Abteilung' can operate from prepared locations underground. They can also activate mobile elements.

Figure 2: The Radio Companies broadcast their programmes in German, French and Italian all over the Nation

Press

Finally, there is the 'Press-Abteilung 40'. This unit produces papers, leaflets and posters in the three national languages. Their products are distributed from special 'pick up places' to the population, the military, and civil emergency units. The companies and detachments use production facilities of press and publishers all over Switzerland. At this moment the Regiment counts for 1640 military.[8] Many of them are active in a civil job with the media. They all had basic military training, as an infantry soldier, an artilleryman, a medic, etc. Because of their civilian (media) background, they are employed within this regiment. Further electronic advances would make it possible to reduce the strength by a 1000 functionaries.

Figure 3: The editing room of the Press Company

ADDITIONAL REMARKS

For this regiment the regular recurrent courses as used within the army are not applicable. Almost every year officers, NCOs and soldiers serve for a week or a period of ten days. Usually a member of a media company changes into uniform and acts more or less according to his civilian occupation. A soldier at a maximum could serve three hundred days till the age of 40. Officers and NCOs could serve more days. In case of a crisis, the 'Bundesrat' decides when and how many personnel of the regiment are required. If there should be a catastrophe, detachments of platoon equivalent could be activated immediately for special tasks of orientation. For radio transmissions such detachments could be brought into action within a few hours.

Training for the most part consists of exercises to test readiness after mobilisation under difficult circumstances.[9] The staffs, command elements and the individual 'media-soldiers' are trained in different crisis scenarios. These exercises include effective media operations, in spite of special dangers and security measures. Staffs and elements of this regiment are, in part, called up every other year for a period of two weeks.
In 1997, to give an example, exercise [10]'Alpha' included elements of the Regimental Staff and of the 'Input-Abteilung 10' as exercise staff. Training is focussed on the staff of 'Radio-Abteilung 20' (with two of its companies) and the staff of 'Presse Abteilung 40' with elements of all of its four companies. The exercise takes 72 hours. The scenario is based on fictitious developments in the Balkans. In this situation the regiment has to support the remaining civil media. Operating new transmitters, using new technology and printing machines are part of regular training.

This regiment has a special responsibility. Exercises demonstrate the value of conscription, as specialist knowledge and experience are needed. The 'media soldiers' know their business, as it is their profession. It will be very difficult indeed to replace these professionals.

The Information Regiment 1, a special unit with a unique responsibility.

REFERENCE

Abteilung Presse und Funkspruch, Behelf für die Führung und den Einsatz der APF. Band 1 und 2.

Forster, Peter. *FAK4 Dreizack 86*. Frauenfeld 1986.

Gautschi, Willi. General Guisan. Zürich, 1989.

Hofstetter, Edwin. Das Informationsregiment 1 übt den Ernstfall. *Schweizer Soldat*, March 1998.

INFO SUISSE INTERN, Zeitung für die Angehörigen des Info Rgt 1, 1996, 1997, 1998.

Langenegger, Walter. *Schweitzer Soldat*, October 1987.

Wetter, Ernst. Schweizer Militär Lexikon 1985/86. Frauenfeld 1986.

NOTES

[1] Ernst, pp. 20 and 22.

[2] Gautschi, pp. 264, 329-336, 338, 351-353

.

[3] Ernst, pp. 86, 87 and 95.

[4] Gautschi, pp. 568-579.

[5] Langenegger, pp. 27-34.

[6] Forster, pp. 77-94.

[7] Behelf für die Führung und der Einsatz der APF.

[8] INFOSUISSE INTERN.

[9] Hofstetter, pp. 12-13.

[10] Hoffstetter, pp. 12

INFORMATION OPERATIONS IN SUB-SAHARAN AFRICA

Heinrich Matthee
Centre for Military Studies, University of Stellenbosch, South Africa

ABSTRACT

There are both opportunities and constraints regarding information operations in Africa. The specific context of each African country may differ. However, in general, the concentration of wealth and power in a ruler network in the capital creates opportunities for control-and-command warfare. Factions of socially fragmented militaries regularly use this opportunity to strike at their own ruler. However, the weak material base of many militaries constrains their ability to deploy large forces quickly over long distances elsewhere. The vast, rugged African terrain sometimes is a protection for distant adversaries.
Various social divisions and struggles for wealth and power create opportunities for psychological warfare in Africa. Linguistic diversity, different frameworks of meaning and the predominance of radio broadcasts and popular discussion often determine the parameters of such warfare.

The technological underdevelopment of most African countries means that computer warfare is largely irrelevant at this stage, except in countries like South Africa. Violence during widespread insurgencies in Africa may serve to accumulate wealth, ensure organisational survival and change patterns of personal and political power. While computer warfare may still become more relevant, physical violence and psychological warfare are likely to dominate present conflicts in Africa.

INTRODUCTION

Information operations have been an important part of human conflicts everywhere. Psychological warfare, command-and-control warfare and computer warfare form part of information operations. This essay looks at these forms of information operations in the low-technology environment of Africa.

The essay describes the socio-political order and military in many African countries to indicate the constraints and opportunities for command-and-control warfare, psychological warfare and computer warfare. Two countries are discussed to portray the concrete dynamics of information operations in Africa. Congo-Kinshasa is discussed because the biggest war in this century between different African armies, insurgents and militias has taken place there. South Africa is discussed because it is the African country most dependent on computerised information systems and therefore a good example of some dimensions of computer warfare in Africa.

Finally, insurgencies occur regularly throughout Africa. The essay investigates to what extent the roles and forms of violence in insurgencies may limit the use of computer warfare in Africa.

A DEFINITION OF INFORMATION OPERATIONS

Information operations are a contested concept. For the purpose of this analysis, information operations are defined as *"Actions aiming to establish information dominance."*

Information operations are conducted by exploiting, neutralising or destroying enemy information and information systems, while protecting and providing friendly information and information systems.

Information operations can include the overlapping areas of psychological warfare, command-and-control warfare and computer warfare. Psychological warfare consists of actions directed at the spirit of the adversary. Command-and-control warfare aims to hit the enemy's command structure or to decapitate the enemy's command structure from its body of command forces. Computer warfare is defined as the use of computerised information systems to defend and support own activities or to attack enemy computerised information systems.[1]

COMMAND AND CONTROL WARFARE

The Relevance Of Command And Control Warfare

Personal networks are a factor at the margins of all bureaucratic systems. In most African countries, however, the interaction between a personal leader and his extended following is the core feature of politics.[2] Colonialist bureaucracy influenced previous practices of personal rule, but informal networks of patrons and clients dominate the formal state structures. Because the ruling network does not necessarily have legitimacy, intense competition may occur.

African climate, politics and terms of trade tend to be structurally instable. Leaders often occupy bureaucratic offices to acquire personal wealth and standing while it is possible, not necessarily to perform public service. Jobs, contracts and licenses are provided in return for political support and deference.[3]

Elite political pacts and compromise settlements are difficult in these so-called neo-patrimonial orders. There are few institutional channels to negotiate rules and power sharing. In the weakly institutionalised environment, force plays an important role to resolve conflicts and maintain order. Power sharing is very precarious and winner-takes-all struggles tend therefore to predominate in politics and war.[4]

Resources or access to resources are concentrated in the ruler's network in state structures. This feature makes it attractive to groups excluded from the ruler's patronage to start a winner-takes-all struggle, in order to take over the State for their own benefit.[5] The state structures of most African states are concentrated in one city of the country. As a result, command-and-control warfare is normally suited for a struggle against the concentrated ruler network.

Constraints On Command And Control Warfare

Militaries in Africa range across a spectrum. Some armies, like the disciplined Malawi army and the experienced army of Rwanda, may have certain relative advantages for command-and-control warfare. However, other factors have placed constraints on the ability to wage command-and-control warfare.

Some rulers, fearing intervention from armed factions, regularly moved senior military officers around to prevent them from building a support base. Loyalty rather than competence affected some promotions. Underpaid soldiers also became involved in business and senior officers in countries ranging from Kenya to Zambia were allowed to acquire business interests to keep their political loyalty.[6]

Samuel Decalo has described the fragmented nature of a number of armies in Africa: "Many African armies bear little resemblance to the Western organisational prototype and are instead a coterie of distinct armed camps owing primarily clientelist allegiances to a handful of mutually competitive officers of different ranks. Seething with corporate, ethnic, and personal grievances that divide their loyalties, hardly national armies but armed factions reflecting wider societal cleavages, these mutual-advancement loyalty pyramids are only nominally beholden to military discipline and hierarchical command."[7]

Command-and-control warfare often occurs in the form of internal strikes against the ruler. Twenty-one members of the Organisation of African Unity have experienced successful coups since independence.[8] The economic weakness of many African states has affected their military capability. In the vast and rugged African terrain, military movement over long distances may be necessary to reach the adversary's command or separate the command from its main body of forces. Underdeveloped abilities regarding firepower, logistics and maintenance have limited the ability of most armies to move and deploy in a short time and over a large distance.[9]

SOCIAL FAULTLINES, MEDIA AND PSYCHOLOGICAL WARFARE

Many African states have a close symbiosis between relatively weak state structures, strong patron-client networks and diverse groups in society. During the competition over wealth and power the many social fault-lines, historical antagonisms and diverse interests provide a favourable theatre for psychological warfare.

Many conflicts in Africa tend to involve insurgencies, defined here as protracted low-level violence by groups to change patterns of power.[10] Psychological warfare is very prominent in most of these insurgencies but shaped by different drivers and constraints. For example, in Congo-Kinshasa, the theatre of the biggest post-colonial conflict between African states, there are more than 220 indigenous language groups. Similar diversities in community views and language occur in many African countries.

Interaction between indigenous traditional worldviews and religions like Islam and Christianity create frameworks of interpretation that may shape the understanding of communication. Traditional beliefs, reinforced by tensions in present societies, may play a role in perceptions about protection and enemy military actions. For example, in the

relatively well-equipped and professional Zimbabwean army, soldiers considered as spirit mediums may also play a role in intelligence and affect military patterns of authority.[11]

Words have the power to wound and to heal in all language communities. In the oral cultures of Africa, words are considered tantamount to actions in certain symbolic contexts. Oral combat by allusion, ridicule or curse and oral participation and peacemaking are therefore of great importance. Words may have layers of meaning and may in certain contexts evoke and invoke traditional frameworks of meaning.[12]

'Pavement radio' or the popular and unofficial discussion of current affairs in Africa, particularly in towns, is an important aspect of communication in Africa's towns. Such discussion transmits more than just idle gossip. The discussion is related to a populist restraint of politicians' power as well as the cementing of frameworks of interpretation in society.

Stephen Ellis therefore writes: "The fact that pavement radio in Africa operates within an essentially oral culture causes it to have special features of both structure and content. An African audience gives far more weight to the spoken word than a European one, which generally believes little, and certainly little concerning national politics, that is not written or broadcast on radio or television".[13]

Television is still limited by the underdevelopment of the electricity infrastructure in many African countries. Limited financial resources and censorship from rulers or social groups also place constraints on the printed media and radio in many African states. Nevertheless, because of the high rate of illiteracy in many countries, radio and pavement radio presently tend to be the most important communication media in Africa.

COMPUTERIZED INFORMATION INFRASTRUCTURES IN AFRICA

By contrast to western leaders, most African rulers have not voiced any concern about computer warfare. Much of Africa is not dependent on computerised information and communication systems. Over half of Africa's population is illiterate and there is an insufficient pool of experts able to organise computerised information systems. According to some calculations, more than 98% of Africa's population does not have access to telephones. The available telephones are also unevenly distributed between urban and rural areas, income groups and men and women.[14]

The basic infrastructure, necessary for developing telecommunications often is insufficient, with power outages, no, or unreliable telephone circuits and few digital systems. Rulers are also aware of the potential effect of outside information on their political hold. Over-regulation of the potential free flow of information and communication may therefore occur.[15]

Officials sometimes allow almost obsolete telecommunications frameworks to be installed in exchange for remuneration from the seller. Ruling networks, often unable to finance public expenditure out of their own resources, may also raise artificially high charges on imported telecommunications equipment.

Much of Africa today does not have and certainly is not dependent on computerised information infrastructures. Computer warfare therefore is not likely to be a widely used weapon or a great concern in those areas during the next few years.

The War In Congo Kinshasa 1996-1997

Two recent wars in Congo-Kinshasa portray some of the dynamics of information operations in Africa. Congo-Kinshasa, the third largest country in Africa, covers a total area of 2.35 million square kilometres. During the past three decades, the political system was based on military force, foreign support and costly patronage of certain power networks. As a result, infrastructure in the east was not maintained and very few communication links existed with the capital Kinshasa.[16]

In 1994 a massacre of hundreds of thousands of Tutsi and Hutu moderates by Hutu soldiers and youth militia occurred in neighbouring Rwanda. An exile Tutsi military under Paul Kagame stopped the genocide, but fear of revenge by the Tutsi caused over a million of Hutus to pour into the east of the neighbouring Congo-Kinshasa.[17]

Thousands of Rwandan Hutu ex-soldiers and militiamen settled among the unarmed Hutus in border camps and launched attacks against Tutsi settlements in the region. Mobutu Sese Seko, the ruler of Congo-Kinshasa, provoked the rulers of Rwanda by not doing anything to stop the attacks from his territory. In 1996-1997 an insurgency started in eastern Congo-Kinshasa, led by the harassed Congolese Tutsi and combined with military intervention by Uganda and the Tutsi military of Rwanda.

Psychological Warfare During The War

Only 10% of the country had electricity and most people and institutions were not dependent on computerised information infrastructure. Computer warfare therefore was not applicable. The insurgent campaign, under the able command of Paul Kagame, used information operations, but mostly in the form of psychological warfare combined with semi-conventional operations.

Quick military strikes were conducted to surprise and overcome initial opposition. The mai-mai militias, supposedly invincible fighters with mystical attributes, were initially allies and were employed to strike fear in Mobutu's soldiers in the east. When the campaign approached towns, the imminent fall of towns was announced to newspapers, electronic radio and 'pavement radio'.[18]

In this context, the illness of Mobutu and the fact that he stayed in France during the first few months of the conflict were exploited to increase demoralisation among the already fragmented Congolese military. The insurgent forces grew rapidly by recruiting members from the many teenagers marginalized in traditional communities and the exclusive system of state patronage.

The swell in numbers and one victory after another served to reinforce the image of insurgent invincibility. In addition, the insurgent forces often approached towns from three sides. This

method increased pressure by semi-encirclement and weakened resistance because there was a way out.

Many Congolese initially rallied around Mobutu against what they believed was a Tutsi invasion. However, popular support ebbed away with each insurgent victory. The apparent inevitability of insurgent victory, the known failure of state services under Mobutu, the weakness of patronage beyond Kinshasa and rekindled communal and factional ambitions provided no motivation to fight for Mobutu against all odds.[19]

Eventually, some of Mobutu's own generals, under pressure from the insurgent advance on Kinshasa, put it to him that he was an impediment to peace. Mobutu fled soon afterwards and Kabila became the new ruler in May 1997. The presidential networks of wealth and power were the main targets of the insurgency and the insurgency had some features of command-and-control warfare. Psychological warfare played a major role in the conflict but computer warfare never featured.

The Insurgency And Foreign Intervention In The Drc 1998-1999

Kabila initially depended on a small power base, impoverished state structures and the security net of his Rwandan and Ugandan patrons.[20] The presidential network of wealth and power was even less authoritative outside Kinshasa than that of Mobutu. Kabila proved unwilling or unable to stop the attacks by Congo-based insurgents against his patrons. He also allowed the Congolese Tutsi to be excluded from citizenship rights, which made them a target for attacks from land-hungry local militias. As a result, another insurgency supported by the rulers of Rwanda and Uganda started in 1998.

The insurgent approach was again based on psychological warfare and command-and control warfare. One group under Rwandan command hijacked Congolese aeroplanes and flew across Congo-Kinshasa to a major Congolese military base. Thousands of ex-Mobutist soldiers not yet integrated in the new Congolese military were turned against Kabila and Kabila's command was cut off from most of its forces elsewhere.[21] The insurgents cut off supply lines to Kinshasa and focused on the Kinshasa command. Kabila's position soon became very weak.

Kabila approached other African rulers in Angola, Zimbabwe, Sudan, Namibia and Chad for support. The intervention of their air forces and armies saved him. However, Kabila remained mostly on the defensive and the insurgents dominated the east and certain areas in the north.

Constraints On Command And Control Warfare

Before the war, Kabila had tried to fuse exiles from Angola, Katangese youths, Congolese Tutsi and ex-Mobutu soldiers into a new army. Financial favouritism towards Kabila's Katangan group and non-payment of salaries provoked rivalries and clashes. There was no military hierarchy with the reliable ability to control the situation.[22] When the war started, the Congolese military fragmented into factions, who looted and smuggled as they retreated.[23]

While the Congolese army was in a particularly bad state, other actors also focused on accumulation of wealth. Senior Angolan officers allegedly made deals with the UNITA insurgent group so that diamond production for both actors could continue. Uganda had strong trade networks in the east of Congo-Kinshasa and a number of Ugandan, Rwandan and Zimbabwean officers turned the war into a militarised business venture.[24]

Effective command-and-control warfare against the enemy implies good command-and-control in the executive forces and that was not always the case. Many underpaid or unpaid soldiers used the conflict, just as they had used peace, to accumulate some wealth by extortion, smuggling and looting.[25] In spite of the wide-ranging military intervention, fighting against the adversary was sporadic and accumulation of wealth was often a more important concern.[26] As a result, the forces available were not necessarily ready for command-and-control-warfare.

In addition, the tropical climate's unpredictability, heavy rains and bad to non-existent roads undermined planning and impeded the large-scale movement of mechanised troops. On occasion roads had to be cut through the rain forests and tropical infections and snakebites affected the condition of troops.[27]

Most participants had a limited ability to move combat support and logistical vehicles over the rough terrain. After the UNITA threat inside Angola grew too large, Angola withdrew most of its forces and logistics from Congo-Kinshasa. This state of affairs affected the deployment ability of Kabila's alliance. Command-and-control warfare remained out of the question and a military stalemate developed.

Psychological Warfare During The Second War

There were no signs of computer warfare during the conflict, but the Kabila government as well as two factions of the insurgents used Internet web sites to spread their message. Kabila tried to present the whole conflict as a foreign invasion, unrelated to bad government in Kinshasa. "We are victims of aggression", he stressed in many interviews.[28]

According to Pascal Mukeba, Kabila's intelligence chief during the previous insurgency, Kabila made a pact with the Rwandan Tutsi government in October 1996 in return for military support during the insurgency.[29] In terms of the pact Kabila would give the Congo's eastern region to the Tutsi minority on both sides of the border when he came to power.

Such a safe haven would have meant a realignment of the borders of Congo-Kinshasa to reflect the social patterns of diversity. Since many different groups lived within the colonial borders of most African states, a realignment of borders may have an explosive chain impact on the power base of most African rulers. While Rwanda accused Kabila of not keeping agreements, Kabila used the issue to obtain support from other African rulers.

To mobilise people against the insurgency, the erstwhile Marxist Kabila became an entrepreneur of ethnic emotions. He started to use a somewhat dualistic discourse, spread by the media and exploiting existing sentiments. The discourse divided all the forces in the conflict between a Bantu front and a Hima/Nilotic front. The rulers of Uganda and Rwanda were accused of wanting to establish a Hima/Nilotic empire in the region.[30]

The Hutus were defined as being part of the Bantu front. During and after the insurgency of 1996-1997 Rwandan Hutus suffered immense losses at the hands of Kabila's allies. The identity discourse allowed Kabila to appeal to Hutu fighters. Many of them were recruited in neighbouring countries, rearmed and deployed in the east of Congo-Kinshasa.[31]

The cascading conflict in the Congo involved insurgency, foreign military intervention and an almost hidden peasant war by local militias for land. Many local militias, who sometimes fought against insurgents and sometimes fought against Kabila's forces, became part of the anti-Tutsi campaign. The Hutu-Tutsi construct of antagonistic identities was extended to a regional Bantu-Nilotic construct of antagonistic identities and later used as justification by the leaders of Angola and Zimbabwe too.

Kabila's ethnic discourse brought more fighters to his banner. At the same time, the presence of Hutu fighters reinforced the security concerns of Rwanda's Tutsi rulers. The ethnic discourse, counter-productively, probably reinforced their determination to ensure their survival through much power and specifically military power in the east of Congo-Kinshasa.

THE VARYING RELEVANCE OF COMPUTER WARFARE

The two wars in Congo-Kinshasa portray the importance of psychological warfare and the constraints on command-and-control warfare in Africa. Many advanced societies increasingly depend on computerised information processes to control electric power, money flow, air traffic, fuel and health services. In January 1999 president Bill Clinton announced the Cyber Corps program to secure the US from a digital Pearl Harbor and in March 1999 the director of the American FBI again called such attacks a significant emerging counter-terrorism concern.[32]

No African leader has yet identified computer warfare as a security concern, since most African societies are not at this stage dependent on computerised information systems. In South Africa the situation is somewhat different. Parts of the country are dependent on computerised information infrastructures while others still lack basic infrastructure. On the whole, South Africa is the country in southern Africa that is most developed but also most dependent regarding information infrastructures.

Personal, social and state security concerns are all involved here. For example, the Internet and other computerised systems can provide tele-medicine, tele-education, tele-agriculture and electronic commerce to the advantage of many people in less-developed and remote areas of southern Africa.[33] The African Connection initiative of 44 African countries also strives to increase telecommunications infrastructure in Africa to promote such development.

South Africa's position in international relations is affected by the quality of its information infrastructure. Access to information outside South Africa influences the quality of decision-making by South Africans. The creation and dissemination of structured information on the country and the continent, influence African aid and investment policies elsewhere. The development of electronic commerce and global competitiveness in South Africa also depend on effective information infrastructures.[34]

In addition, South Africa has the strongest conventional military in Southern Africa. Any violent adversary in the region is therefore unlikely to restrict itself to direct conventional confrontation and more likely to consider asymmetrical warfare too. Such asymmetrical warfare, also by a domestic insurgent group, may include information infrastructure attacks.

Computer Warfare And Insurgencies In South Africa

South Africa did not experience much computer warfare during past South African insurgencies. The insurgency led by the African National Congress (ANC) against the white National Party government entered a period of peace talks in the period 1990-1994 before disruptive computer programs became more widely known. However, the ANC used computer systems for encoded communication and information during its insurgency campaign before 1994.[35]

In spite of the availability of computer skills and a focus on infrastructure sabotage, there also is no recorded incidence of the use of disruptive computer programs during the Afrikaner nationalist insurgency in the period 1990-1994. Some right-wingers sent a package bomb to a computer company with links to the African nationalist struggle.[36]

The Internet, a worldwide network of computer networks, only became prominent in SA after 1994. Insurgent groups can use the Internet for exchanging information, fundraising and putting across their message to a broad audience. Groups alleged by the state to be in the fore field of insurgency, like a mainly Muslim anti-crime group, use the Internet in this way.[37]

The first case of unauthorised hacking that came to the attention of the South African Department of Justice occurred in 1993, but was not related to insurgency.[38] Since 1994 several incidents of hacking, viruses and computer sabotage have occurred, but none has been linked to the rural insurgency in Kwa-Zulu Natal or the urban violence in the western Cape.[39] There is not even a focused targeting of vulnerable information infrastructures as such by these actors.

Specific Dimensions Of Computer Warfare In South Africa

The government policy seems to be the use of computerised information infrastructures in order to promote development.[40] While attacks on information infrastructure may seem like a concern for industrialised countries with prominent infrastructures only, such attacks may become even more of a concern to a partly industrialised country like SA.

The reason is that computerised information infrastructures will be established in spaces that will often have limited health, education and information infrastructures. Insurgent damage to the computerised information infrastructures would therefore tend to have a greater impact on people than in industrialised countries where other services could partly serve as substitutes.

The loss of limited and scarce resources in this way would also have a relatively greater impact on development than in the industrialised countries. Both the effect of warfare on information infrastructure and overspending on securing the information infrastructure could be detrimental.

The role of computer warfare in African conflicts is at this stage virtually non-existent. One reason for the minimal role of computer warfare is the lack of dependence and vulnerability regarding computerised information systems in most African societies. However, the forms and roles of violence in both African and non-African insurgencies may also minimise the utility of computer warfare.

In many societies, violent strategies by weak insurgents may mean that their strong adversaries take them seriously for the first time. Violence may therefore be chosen as part of a strategy of group empowerment. However, violence may also be chosen as a means of personal empowerment and status seeking.[41]

Participation in violence, as observed by Franz Fanon, may be a spiritually liberating event for those who feel abused and repressed by their adversaries, colonial or postcolonial. In many social contexts, there are traditions where social status and the affirmation of identity are linked to violent struggle against perceived enemies. Status-seeking and the desire to appear as soldiers, which is widespread in virtually all insurgent groups, may therefore lead to a preference for physical violence rather than computer warfare.[42]

Violence And Organizational Dynamics

Organisational dynamics and interaction with the environment and adversaries may also influence insurgent approaches to violence. An insurgent group may start operating with a clear strategy of selective violence, but violence may escalate or become more indiscriminate during the course of interaction with adversaries.

Competition for authority and publicity between two related insurgent groups or between different factions in a group may also motivate exceptional violence. The distribution of beliefs, also regarding violence, among members of an insurgent group is likely to be uneven. However, dissent is dangerous to clandestine insurgent groups. Violence may be employed to ensure discipline and to increase the costs of leaving the organisation for perpetrators.[43]

Violence And Money

Insurgent groups all over the world sometimes rely on economic crimes like theft, robbery and extortion for funding. In different African countries, the authority of state structures is so limited that there may also be areas where insurgents can sustain themselves from trade. Protection of illicit businesses or businesses in conflict-ridden areas, control of trade in different commodities and gaining access to land then become an important part of insurgent activities.

Examples of insurgent entrepreneurs abound. Dissident groups in Sierra Leone, Mozambique, Congo-Kinshasa and the Great Lakes area have been involved in the smuggling of arms, diamonds or gold.[44] According to UN estimates, the Angolan insurgent group UNITA has been able to produce diamonds worth US $ 3.7 billion during the past 7 years.[45]

Physical violence may in such cases serve important functions to protect and expand insurgent enterprises.

CONCLUSION

The neo-patrimonial political order of most African countries concentrates power and wealth in a ruler network situated in the capital. As a result, during conflict command-and-control warfare is quite suited against an adversary government. Many African militaries exhibit the social divisions and competing patron-client networks of the rest of society. Factions, who try to strike against the ruler, often employ command-and-control warfare in the capital city.

Fragmentation, patron-client networks and the focus on internal pacification affect the ability of some militaries to execute command-and-control warfare against opposing militaries. Limitations in firepower and logistical ability also make it difficult to perform the needed quick long-range movements in the vast and rugged African terrain.

The social fault lines and grievances in many African societies create opportunities for psychological warfare. However, linguistic diversity, different frameworks of interpretation, high illiteracy and financial and political limits on some communication media may serve as constraints. Radio broadcasts and unofficial discussions tend to be the media used most for psychological warfare.

Computer warfare is not relevant in most African conflicts at present. This situation is related to the technological underdevelopment of big parts of Africa. Violence during insurgencies may ensure a socio-political impact, organisational survival, personal power or the accumulation of wealth. Computer warfare may become more relevant in Africa, especially in more connected societies. However, in the medium term physical violence and psychological warfare are likely to dominate conflicts in Africa.

NOTES

[1] For the purpose of this contribution, Martin Libicki's conceptualization is used. See Libicki, M., *What is Information Warfare?* National Defense University, Washington DC 1995 and Khalilzad, Z. and White, J. (eds.), *The Changing Role of Information in Warfare* at http://www.rand.org/publications

[2] Decalo, S., 'The process, prospects and constraints of democratization in Africa', *African Affairs*, Vol. 91 No. 1 1992, pp. 7-35.

[3] Bratton, M. and Van de Walle, N., 'Neopatrimonial regimes and political transitions in Africa', *World Politics*, Vol. 46 No. 2 July 1994, pp. 453-489 on pp. 458-459. See also Guillaumont, P., Jeanneney, S. and Brun, J. -F., 'How Instability Lowers African Growth', *Journal of African Economies*, Vol. 8 No. 1 1999, pp. 87-107.

[4] Charles Tilly argues that the origin of most states, also outside Africa, lies in a faction that legalised itself and outlawed the opposition, by outmatching rivals in coercive capacity and displacing them by force. Tilly, C., 'War Making and State Making as Organized Crime' in

Evans, P.B., Rueschemeyer, D. and Skocpol, T. (eds.), *Bringing the State Back In*, Cambridge University Press, New York 1985, pp. 169-191.

[5] Compare Bayart, J. -F., *The State in Africa: The Politics of the Belly*, Longman, London 1993, chapters 8 and 9 and Chabal, P., *Power in Africa: An Essay in Political Interpretation*, Macmillan, London 1992, pp. 80-81, 96-97, 212-216.

[6] Baynham, S., 'Civil-Military Relations in Post-Independent Africa', *South African Defence Review*, No. 3 1992, p. 7.

[7] Decalo, S., *Coups and Army Rule in Africa: Motivations and Constraints*, Yale University Press, New Haven 1990, p.6

[8] Africa Institute of South Africa, *Africa at a Glance:Facts and Figures 1996/7*, Pretoria 1996, p. 91.

[9] For a comprehensive analysis of land, air and sea abilities, see Du Plessis, L. and Hough, M. (eds.), "*Protecting Sub-Saharan Africa: The Military Challenge"*, Human Sciences Research Council, Pretoria 1999.

[10] Schmid, A., *Political Insurgency: A Research Guide to Concepts, Theories, Data Bases and Literature*, Centre for the Study of Social Conflict, Leiden 1983, p. 111.

[11] Young, E., 'N'angas, Varoyi and Midzimu: The Institutionalization of Traditional Beliefs in the Zimbabwe National Army', *Armed Forces and Society*, Vol. 24 No. 2 Winter 1997, pp. 245-268. For similar cases in some other forces and countries see Omara-Otunnu, A., *Politics and the Military in Uganda, 1890-1985*, Macmillan, London 1987, p. 170 and Tordoff, W., *Government and Politics in Africa*, Macmillan, London 1993, pp. 111-112.

[12] Staewen, C., *Kulturelle und psychologische Bedingungen der Zusammenarbeit mit Afrikanern*, Weltforum Verlag, München 1991, pp. 41-44, 152-154. See also Bozeman, A., *Conflict in Africa – Concepts and Realities*, Princeton University Press, Princeton 1976, chapters 5, 10 and 17.

[13] Ellis, S., 'Tuning in to pavement radio', *African Affairs*, Vol. 96 No. 383 April 1997, pp. 321-331 on p. 322.

[14] 'On the cybermap', *Africa Confidential*, Vol. 38 No. 20 10 October 1997, pp. 3-4. Also see Best, K., 'Wireless telephony in Africa', *Corporate Africa*, No. 888 Winter 1998/1999, pp. 30-31.

[15] De Roy, O., 'The African challenge: Internet, networking and connectivity activities in a developing environment', *Third World Quarterly*, Vol. 18 No. 5 1997, pp. 883-898 on pp. 889-891.

[16] Central Intelligence Agency, *World Fact Book*, CIA, Washington DC 1997.

[17] Misser, F., 'Rwanda/Zaïre: Anatomy of crisis', *New African*, No. 347 December 1996, p. 12. See also Lemarchand, R., "The Fire in the Great Lakes", *Current History*, Vol. 98 No. 628 May 1999, pp. 195-201.

[18] Matthee, H., 'State Collapse or New Politics? The Conflict in Zaïre 1996-1997', *Strategic Review for Southern Africa*, Vol. XXI No. 1 June 1999, pp. 88-104 on p. 94.

[19] Ibid.

[20] Mamdani, M., 'Why foreign invaders can't help Congo', *Electronic Mail and Guardian*, 2 November 1998 at http://www.mg.co.za. Also see Mamdani, M., *Citizen and Subject: Contemporary Africa and the Legacy of Late Colonialism*, Princeton University Press, Princeton 1996 on political orders in Africa.

[21] *Africa Confidential*, 28 August 1998, pp. 4-6.

[22] *New African*, April 1998, p. 22. See also *Africa Confidential*, 26 September 1997, p. 5 and *Africa Research Bulletin*, 30 November 1997, p. 12901.

[23] The same avoidance of conflict and focus on accumulation was noted between presidential soldiers and opposing militia in neighbouring Congo-Brazzaville. See Bazenguissa-Ganga, R., "The spread of political violence in Congo-Brazzaville", *African Affairs*, Vol. 98 No. 390 January 1999, pp. 37-54.

[24] Young, E., 'Chefs and Worried Soldiers: Authority and Power in the Zimbabwe National Army', *Armed Forces and Society*, Vol. 24 No. 1 Fall 1997, pp. 133-149 on pp. 137-140. See also *Africa Confidential*, 9 October 1998, p. 3

[25] Compare Keen, D., 'The Economic Functions of Violence in Civil Wars', *Adelphi Paper 320*, International Institute for Strategic Studies, London 1998, pp. 15-17, 25-28.

[26] Steven Mailes, a television journalist stationed at the insurgent headquarters in Goma, in 'Congo', *AM Live*, Sound Archives, South African Broadcasting Corporation, 10 December 1998. See also Keen, *op. cit*., p. 28 and Michaels, M., 'The Bleeding Heart of Africa', *Time*, 22 March 1999, pp. 38-40.

[27] *Africa Confidential*, 11 September 1998, p. 3.

[28] Maureen Modea, 'Congo', *AM Live*, Sound Archives, South African Broadcasting Corporation, 10 December 1998.

[29] Knemeyer, T., 'Putsch gegen den Putschisten', *Die Welt*, 7. August 1998, p. 3.

[30] Vlasblom, D., 'Kabila bespeelt etnische haat', *NRC Handelsblad*, 12 August 1998, p. 4. See also Reyntjens, op. cit., p. 249.

[31] UN Security Council, '*Final Report of the International Commission of Inquiry (Rwanda)*', 18 November 1998, S/1998/1096, paragraphs 86-87.

[32] Freeh, L., 'Responding to Terrorism', *FBI Law Enforcement Bulletin*, March 1999, p. 3.

[33] De Roy, op. cit., pp. 891-893.

[34] See *Electronic Commerce Policy Process*, Press Release, Department of Communications, January 1999.

[35] Kasrils, R., *Armed and Dangerous: My Undercover Struggle Against Apartheid*, Heinemann, London 1993, pp. 301, 308, 332.

[36] See Kemp, A., *Dritter Burenkrieg: Der Kampf der südafrikanischen AWB und ihres Führers*, Nation Europa-Verlag, Coburg 1994, p. 172.

[37] See http://www.pagad.co

[38] Telephone interview on 15 June 1999 with advocate John Welch, deputy attorney general, Department of Justice.

[39] *Financial Mail*, 6 February 1998, p. 67.

[40] Speech of Jay Naidoo, Minister for Posts, Telecommunications and Broadcasting in the National Assembly, 8 March 1999, http://www.polity.org.za/parliament/papers/sp/1999/sp0308.htm

[41] Morris, D., *The Naked Ape Trilogy*, Jonathan Cape, London 1994, pp. 195-219.

[42] Peters, R., 'The New Warrior Class', *Parameters*, Summer 1994, pp. 16-26. See also Finch, R., 'A Face of Future Battle: Chechen Fighter Shamil Basayev', *Military Review*, May-June 1997, pp. 31-41.

[43] See Crenshaw, M., 'An Organizational Approach to the Analysis of Political Terrorism', *Orbis*, Vol. 29 No. 3 Fall 1985, pp. 465-489.

[44] Turner, J., *Continent Ablaze: The Insurgency Wars in Africa 1960 to the Present*, Jonathan Ball Publishers, Johannesburg 1998, pp. 221-223. See also *Africa Confidential*, 20 February 1998 p. 4.

[45] Echevarria, V., 'Unita beats the diamond ban', *New African*, March 1999, p. 33.

IS MORE NECESSARILY BETTER?
Advantages and disadvantages of the explosion of information technologies for political and military preparedness

Max V. Metselaar
Royal Netherlands Military Academy

ABSTRACT

It is widely accepted that the application of new information technologies has a significant impact on today's warfare and crisis management and that this impact will only become greater in the nearby future. This article examines several advantages and disadvantages of these technological developments with regard to one of the key elements of warfare and crisis management: i.e., the importance of being as prepared as possible against attempts of adversaries to achieve successful surprise attacks. To what extent and in what respect does the application of modern information technologies form a blessing for an actor's state of readiness during encounters with dangers like an enemy attack or terrorist acts? To what extent will it help to increase the so-called warning span and the readiness gap? Building forward on insights from empirical studies that have been conducted during the past four decades within various scientific disciplines, the conclusion will be drawn that the introduction of information technologies forms at least a *mixed* blessing. In many ways the introduction of new information technologies will appear to have a Janus head: On the one hand it will help the potential defender to acquire much more current, up-to-date, unbiased intelligence. Upwards, downward and horizontal dissemination of intelligence throughout all segments of C4I systems and decision-cycles can - at least technically - become more rapid than ever. On the other hand, one must at least be consciously aware of many dangerous disadvantages and cognitive traps as well. Besides significantly increasing a defender's capacities to acquire, analyze, re-check and disseminate all sorts of intelligence about threatening patterns, capabilities and intentions, it will also significantly increase the amount of noise. Furthermore, it may invite a dominant tendency towards micro-management among many central military and political leaders as well as a structural false sense of situational awareness and control. In most situations, it is likely to increase and accelerate many cognitive, psychological and organizational traps that tend to be quite common in past experiences with surprise attacks.

INTRODUCTION

A glance at many documentaries of the Gulf War in 1991 and the Kosovo war in 1999 as well as conferences, publications and promotion films about future warfare strongly suggest that the "information age" promises nothing but benefits. Such impressions can easily be reinforced by excited comments of military commanders and scientists. For instance, remarks like […]"Think of what it would mean to have real-time surveillance of a 200 mile wide battlefield, and to be able to send a ballistic missile anywhere on that battlefield in four minutes - a missile that goes reliably, and goes where you want it to go. That's marvel" (US Admiral Owens, quoted in Belknap, 1996: 2), or […] "It is this global C3I system that will be the master-weapon of the twenty-first century!" (Davis, 1996: 49) indicates that the

introduction of the continuing inventions of increasingly sophisticated information technologies into command, coordination, control, communication and intelligence systems (C4I) forms a fantastic blessing for the quality and effectiveness of future operations (cf. Toffler & Toffler, 1994). However, it can be seriously questioned whether such optimism is really justified. Isn't it often so that promising innovations are often too good to be true? Isn't it often so that every promising development contains at least some *dis*advantages? Isn't it often essential to ask more specific questions with regard to potential effects of innovations such as: in what respects will it have an impact and to what extent do the advantages outweigh the disadvantages?

In order to come to a deeper and more balanced insight, this article will focus on one specific area of warfare, namely the area of (early) warning responses and military and political preparedness against impending dangers. It will be concentrated in particularly on the question: Whether, and if so in what respect the application of modern information technologies and forms of information warfare will have positive and/or negative implications for the state of preparedness of military commanders and political leaders during encounters with actual or future dangers?

The outline of this article will be as follows. First, I will elaborate briefly on the essence of political-military preparedness and warnings. Then I will subsequently discuss the impact of new information technologies and information warfare on several factors that tend to be crucial in explaining serious shortcomings in the so-called intelligence cycle: i.e., the detection of potential dangers, the collection of signals and threatening patterns, and interpretation and dissemination activities (cf. Kam, 1988; Levite, 1987; Wirtz, 1991: 4-13; Handel, 1987; Metselaar, forthcoming). After that, I will briefly focus on the likely impact of "new" information technologies on the awareness, acceptance, coping responses and defensive preparations and preparedness of political and military leaders (see also Figure 1). The article will be closed with a few tentative conclusions and recommendations for further research.

Figure 1: Conceptual model of the presented analysis

POLITICAL-MILITARY (UN-) PREPAREDNESS AND WARNINGS

Preparedness can be characterized as a familiar, but at the same time complex and multi-interpretable and normative concept. In order to understand the implications that the ongoing introduction of modern information technologies may have in the nearby future, it is therefor necessary to start with a definition of preparedness. The following definition combines elements that according to descriptions in dictionaries, military doctrines, war studies and procedures can be regarded as essential for preparedness (cf. Metselaar, forthcoming):

> The degree and appropriateness wherein an actor (in this article specified as a small selection of individual political and military authorities in key positions) is mentally, conceptually, physically, organizationally and politically ready to respond as optimally as possible (given his potential capabilities) to (various aspects of) a danger during the first phases of an actual encounter.

Preparedness can be distinguished into three closely interrelated dimensions:

> 1. *The first dimension is formed by the state and appropriateness of the mental anticipation and alertness (of key decision-makers) with regard to the actual materialization of the (predicted) danger as well as its immediate effects and its probable immediate and long-term implications.*
>
> This dimension refers to the degree wherein key military and political authorities mentally and conceptually anticipated on the actual confrontation with the striking danger. More specifically, this dimension encompasses the degree wherein the direct responsible political authorities *mentally* anticipated and were in a moderate to high state of alert with regard to (a) the probability of an offensive; (b) the type of action(s) that the danger unfolds; (c) the location(s) on which the danger (the adversary's offensive) was directed; (d) the timing of the confrontation; (e) the strengths and weaknesses of the danger (i.e., the enemies troops against versus the strengths and the weaknesses of the defense (capabilities, organization, but also mentally); (f) (in case of a danger in the form of an attack) the objectives of the offensive and its place in the enemy's strategy; and (g) its (immediate) impact and consequences.
>
> *2. A second essential dimension is formed by the state and appropriateness of a decision-maker's awareness, and readiness to make use of conceptual, physical and mental components of the "basic measures" and "emergency measures" that can be applied almost immediately when a danger strikes in order to minimize the immediate and long-term risks and costs of the impact of the danger.*[1]
>
> 3. *A third dimension of preparedness that can be crucial for policy-makers (in particular during operations other than war) concerns the degree wherein national authorities have build up sufficient political acceptability and support that can be needed to ensure sufficient (political and public) acceptance and support as far as this is required to respond as optimally as possible to the danger and its effects.*
>
> This dimension refers to the decision-maker's state of anticipatory protective counter-measures and attempts of "public educating" to ensure the political acceptability and consensus that might be needed (a) to cope with (i.e., prevent or minimize) the impact

> and/or the implications of a encounter with the impending danger itself; and (b) to ensure the political and public acceptance and support that might be needed to ensure the feasibility and effectiveness of rapid counter-measures as well as support for the possible implications of these counter-measures. This may include the support or at least the acceptance from groups/actors who are not directly involved with the military operational aspects (e.g. the press, the public, other departments, potential allies) adequately anticipated the confrontation with the danger and its consequences and were ready to cope with it and (in case of a democracy) were ready to support possible crisis management options of their government (Cf. Handel, 1982, in: Gooch & Perlmutter, 1982: 149).

"Warnings" can be regarded as container term or a *label* for …

> A combination of indicators, patterns, as well as oral or written messages that may be observed, heard, read, or reconstructed by one or more receivers (i.e. the selected key authorities and/or parts of their organizations) whereby this data provides more or less ambiguous, uncertain, detailed and reliable predictions about (one or more dimensions of) a potential danger, and whereby this data may at least potentially create a sufficient time span to prepare protective counter measures (cf. Metselaar, forthcoming; Levite, 1987: 174; Kam, 1988: 24, 29).[2]

Just like preparedness, warnings consists of various dimensions. The following dimensions can be observed in most intelligence cycles and warning processes: (1) Content; (2) warning span; (3) accessibility; (4) reliability; (5) quality; and (6) quantity. Laboratory studies and studies on organizational and public communication have indicated that these dimensions, and more in particular the combination of specific values that are taken on each of these dimensions can significantly affect the leader's sense of awareness, and willingness to accept and respond to warning signals.

After defining preparedness and warnings, it is now time to elaborate on the likely impact that the application of the wealth of "new" information technologies that have been referred to in the opening of this article, may have on (1) the process of detection of potential dangers; (2) the collection, dissemination and interpretation of potential warning signals; (3) the awareness, interpretation, acceptance, coping responses of military and political leaders; and (4) their state of preparedness during encounters with actual and future dangers.

THE IMPACT OF NEW INFORMATION TECHNOLOGIES ON *THE DETECTION AND COLLECTION* OF THREAT INDICATORS

For intelligence agencies like the National Security Agency and the Central Intelligence Agency the impact of new information technologies on the collection of potential warning signals and threat indicators with regard to a wide range of potential dangers is still increasing. Early warning systems, possibilities for interceptions and eavesdropping, as well as technological possibilities to collect visual and transcribed facts and figures about actual developments on potential battle fields are becoming more widespread and sophisticated everyday. In turn, this will usually makes it much easier to exchange important intelligence from intelligence agencies of other countries. It will make intelligence agencies with less sophisticated capacities and expertise more dependable in times wherein they are confronted

with impending dangers. At the same time, experiences like the Gulf crisis and the Gulf war, Pakistan's unexpected tests of nuclear devices during a crisis with India in May 1998, the Kosovo air campaign and several unexpected moves from Milosevic and his army, have once more underlined that one must be careful not to over-estimate the power of technologies. Many static and more in particularly *mobile* objects are still difficult to trace with certainty, especially when they have to be identified from great heights, in short time, and under poor weather conditions. Dummies can still be used remarkably successfully in order to create serious misperceptions and threat estimations.

THE IMPACT OF NEW INFORMATION TECHNOLOGIES ON *THE DISSEMINATION* OF (POTENTIAL) WARNING SIGNALS AND THREAT ASSESSMENTS

The last decade, and in particular the last years as well as the nearby future suggests that (in comparison with the possibilities to collect warnings) the biggest innovation in the field of "preparedness and surprise attacks" appears to be made in the field of dissemination of intelligence, C4I-aspects and the decision cycles (Leonard, 1998). In principle, potential attackers as defenders may profit in many ways from this. At the same time it would be stupid to neglect several possible negative influences: For instance, the increasing need for real-time data may increase the commander's situational awareness. At the same time, however, it may increase the chance that the motivation of intelligence analysts and experts to double-check, analyze and interpret data as thoroughly as possible declines.[3] More than ever before analysts and staff members will have to cope with the dilemma whether they should disseminate data and advise their superiors and other allies more rapidly if they want to have some influence by policy makers and if they want to be a serious source besides a commander's other sources for information with the risk of being overhasty and losing credibility, prestige and self-esteem for wrong assessments or if they should not act in line with the increasing time pressures and creating thorough assessments that are hardly utilized. [4]

THE IMPACT OF TECHNOLOGICAL INVENTIONS ON *INTERPRETATIONS* OF COLLECTED SIGNALS AND OBSERVED PATTERNS

Past as well as recent experience reveal that the introduction of new information technologies tends to have a profound impact on most dimensions of the warning signals. It is quite likely that this impact will be even more impressive and in many senses still impossible to oversee in the recent future. Let us look more closely at the likely impact on several of the warning dimensions:

Dimension 1: "Content"

Warnings may encompass pieces of information with regard to one or more of the following content aspects of an impending danger: [5]

(1) An estimation of the probability that the danger (the attack) will materialize (*whether*);
(2) Identification of the precise identities of the attacker(s) (*whom*);
(3) A determination of the type of actions and technologies involved (*how*);

(4) An identification of the location(s) that will be in danger (e.g., that will be attacked) (*where*);
(5) A prediction of the timing when the danger may be materialize (e.g. the timing of the attack) (*when*), and.
(6) An assessment of the reasons and objectives (motivations, causes) behind the danger (*why*).

At first sight it seems obvious that the introduction of modern information technologies will make it less difficult than ever to improve the quality of warnings on each of these content aspects. Although, it will still be necessary to guess a lot and to rely on a combination of luck, *Fingerspitzengefuhl*, specific experience, defenders will be confronted much faster, with more detailed, more reliable and better controllable signals, patterns and threat assessments than ever before in the history of warfare.

At the same time, however, many biases, traps and disadvantages will be introduced as well. One relatively new structural trap that may be more relevant than ever can be called the *"What you see is what you get" (WYSIWYG) syndrome*. Leaders as well as analysts who become confronted with current, often visualized, real-time data which may potentially tell something about one or more of the seven dimensions above, will regularly have great difficulties to remain cautious for the possibility that they may deceive themselves and/or that they may be deceived by adversaries and often ambiguous circumstances. The usual strong and dominant impact of visual information on the human's mind can easily lead to profound misperceptions and failures. For instance, since it usually concerned coping with so called cynical dangers; there is always a chance that attacker changes his mind while the defender is still thinking and acting in accordance with the latest pictures that have caught his mind.

Furthermore, the actual situation of impending danger may have significantly changed because of situational dynamics and the timespan between the sending and the receiving of the signals. Although leaders may be well aware of this, simultaneously, they may frequently experience more inner pressures than ever to jump to quick decisions and actions. The fact that these leaders may be well aware that others in their direct environment see the same "real time" pictures and may began to wonder why there are still no decisions taken (they may suffer from the same syndrome too!) can become a major source of time pressure. Furthermore, doctrines and training that dictate that it can be crucial to walk quicker to decision cycles than your adversaries, as well as the impact of the press (i.e., all sorts of CNN and Internet effects) can become major sources of self-imposed deadlines as well.

Technological developments may also increase the chances that leaders and analysts fall into another cognitive and psychological trap as well. That is, people may become more or less obsessed by the visual, real-time data they become confronted with, spending most of their bounded time and span of attention to it. The price may be that they almost completely overlook crucial, but (at least for them) perhaps less accessible and controllable, and more complex *background* intelligence that could have told them more about one or more of the content aspects of the impending danger.

Dimension 2: The "warning span dimension"

Another crucial dimension of warnings is the so-called *time span ratio* between the moment of warning issuance and the moment whereupon it is predicted that the warning may probably

materialize (when nothing is done). This dimension is often described as the “warning span” or “warning interval” (Kam, 1988: 22-24, 29, 32-33, 57-59; Chan, 1979: 171). Ideally speaking (from the perspective of a defender) detailed and reliable warnings are issued at a moment upon which they still have sufficient time to prepare adequate counter-measures (at times including the option of a pre-emptive strike).
Historical evidence reveals that the introduction of various technologies during the past centuries has had an enormous impact of the warning span dimension. Probably the greatest revolutionary change in warfare and crisis management was the exponential increase in mobility. This development compressed time and space, quickened the movement of troops, offensive and defensive capabilities and supplies. As mobility increased, the warning span for counter-measures significantly decreased: From months or weeks in the early nineteenth century, to weeks and even days in the railway and combustion engine and tank period, to days and hours in the age of air power, and since the last decades to hours and even minutes in the nuclear age (see Figure 2).

*Figure 2**:** Conceptual model about the reduction of warning time due to the invention and introduction of technologies and its impact on chances to achieve surprise (derived from Michael Handel, 1989: 66).*

The trend that has been set during the past might be continued in an almost dramatic way. That is, the use of the latest information technologies by one or more adversaries may bring back the warning span to almost zero. Since information attacks and PSYOPS may be silent and hidden, it will become more complicated and sometimes even impossible to pinpoint the commencement of an offensive information attack at all, or to determine adequately who delivered it, when, where, why and how it started. It may even become unclear for some time how long threat assessments, decision-making and the implementation of counter-measures can wait before a defender’s entire C4I infrastructure is seriously damaged (at least for the time being) and an adequate response in no longer possible. In other words, the growing role

of information warfare is rapidly lowering the classic barrier between war and peace. In other words, the recent technological developments may blur a defender's assessments and awareness regarding the probability, the timing, the location, the initiator and the impact of an attack as well as the attacker's strategy and tactics. It is highly likely that there may become a trend towards constant low-intensity and diffuse information warfare (cf. Thomas in: Pfaltzgraff & Shultz, 1997). In fact, forms of largely unnoticed arms races and silent computer attacks, with far-reaching forms of anticipating on (new) possibilities of a wide variety (of often unknown) computer attackers and ones own vulnerabilities are going on for some years now. They will certainly continue to do so in the future.

Dimension 3: "Accessibility"

One of the biggest structural problems with warnings that has become evident many times during surprise attacks as well as confrontations with striking disasters is usually *not* the fact that there was no adequate intelligence available in time. Instead, the biggest problem is that key commanders and authorities were frequently inadequately informed by their subordinates or colleagues about the intelligence that has been collected or produced somewhere in their departments.
Lack of accessibility can be caused by many factors. For instance, compartmentalization or too much secrecy, bureau politics, too much specialization and fragmentation (Wilensky, 1967; Wohlstetter, 1962; Levite, 1987; Kam, 1988); as well as reactions on cry wolf syndromes, fear of losing credibility in case it appears to be a false alarm, intelligence-to-please syndromes, too long and complex lines and procedures; etceteras.
It remains to be seen whether the benefits of the introduction of new technologies will outweigh its disadvantages. Indeed, at least potentially, political and military leaders will have much more opportunities to become directly exposed to intelligence and to bypass a lot of hierarchic ladders in the C4I lines. At the same time, this may easily lead to too much noise, more appetite for the wrong kind of data, information overload, a shift towards micro-management and a false sense of control. Moreover, it may lead to wrong responses in case of all the confrontations with high numbers of rough information of which many subtle details and ambiguities are simply overlooked or misperceived. Last but not least, it may structurally distract the attention and information search of leaders (and partly as a consequence of that significant parts of their organizations) away from potential signals and indicators that tend to be much less accessible, but that can be at least just as crucial for making adequate decisions and preparations (e.g., data with regard to the adversaries motivations, hidden agendas and strategies).

Dimension 4: "Reliability"

Much of the research on warning responses and preparedness indicates that the attributed reliability of sources from which a person receives signals and warnings have a significant influence on the consideration whether or not warnings should be acted upon. The higher the credibility of a source and/or a message in the eyes of a receiver, the more likely the information that is offered will be noticed and accepted without a quite critical evaluation and the more likely that people will be willing to change their opinions and course of actions in accordance with its contents. Conversely, if a source is considered untrustworthy or uninformed, incoming information is more likely to be avoided or denied. This, in reality quite difficult distinction seems to become more blurred than ever due to the impact of Internet (and CNN) as one of the most dominant and accessible sources of the latest data. It is

a fascinating paradox that intelligence agencies who frequently try to affect others by manipulating information that is disseminated through Internet and news agencies like CNN can become a victim of the same media themselves. The conviction that they are quite capable to see the difference between reliable and unreliable data will frequently become a dangerous trap. A trap that can affect the quality of the whole further intelligence process as well as the degree of credibility that policy makers attribute to their agencies.

Dimension 5: "Quality"

One of the most crucial dimensions of warnings is its quality. In other words, the degree wherein a warning provides certain, accurate, timely and detailed predictions with minimal ambiguity and maximal certainty (cf. Kam, 1988: 28). Again, it is important to notice that most decision-makers will consciously or unconsciously have to make some evaluation of which warnings they appraise as accurate and reliable in a veil of ignorance about the future versus post hoc or hindsight evaluations of which warnings have been more or less accurate and can therefor be seen as high quality assessments (cf. Wohlstetter, 1962; Handel, 1976; Kam, 1988: 39-42, 50-51, 56).

Dimension 6: "Quantity"

The quantity of incoming warnings (in other words the amount of potential warning signals intelligence agencies or specific policy makers become aware of within certain time frames in comparison with there limited capacities to process them adequately) is one of the most mentioned dimensions of warnings (Wohlstetter, 1962; Breznitz, 1984; Levite, 1987; Kam, 1988: 49, 53-55). Like the other dimensions, the way quantity is experienced can be quite variable depending on what cues, signals, messages, or patterns are experienced or labeled as warnings.

For various reasons (depending on the strength and the imminence of the danger), more or less recent experiences like the Rwanda genocide in 1994, the Iraq attack on Kuwait in 1990, or the Kosovo crisis in 1998-1999; indicate that it is quite likely that the quantity of potential threat indicators that may be collected will drastically increase in number. Moreover, the same occasions illustrated that the impetus of relatively sophisticated technologies (satellites, interception capabilities) (accompanied by the widespread illusion that just the possession of better and more rapid data collection capabilities forms a guarantee for success) regularly tends to a significant increase in the organizational and decision-maker's appetite for more, real-time data. Simultaneously, however, the chance that intelligence analysts, military commanders and policy makers will regularly suffer from various forms of data overload will increase further as well. Better facilities will often create an increasing need by commanders and authorities for current, detailed, and rapid intelligence in order to increase their situational awareness. At the same time and at first sight perhaps paradoxically, it is quite likely that they will *experience* periods wherein they are significantly victimized by (timely) data *under*load. In many ways, one can observe a behavior pattern that can be seen in many other fields of economy as well. The more welfare, the higher the expectations and the more likely ambitions will be set higher and the more frustrations if needs cannot be fulfilled in time.

THE IMPACT OF NEW INFORMATION TECHNOLOGIES ON FACTORS THAT FRUSTRATE THE INTERPRETATIONS OF COLLECTED INTELLIGENCE (LIKE FALSE ALERTS AND NOISE)

Four decades of studies on surprise attacks reveal that most adequate warnings suffer from an overload of distorting signals, as well as uncertainty and ambiguity with regard to all dimensions of warnings and impending dangers (Wohlstetter, 1962; 1965: 691; Handel, 1977: 462-464; 1984: 236-237; Kam, 1988: 50-51, 56; Vertzberger, 1989; Whaley, 1973). However, one of the most influential factors beyond intelligence failures and surprise attacks forms the *called Cry Wolf syndrome* (Breznitz, 1984). The more warnings and alerts that for various reasons are attributed as false (for instance, because a potential attacker has changed his mind, or because intelligence agencies were insufficiently informed about the exact time, location of a dangerous encounter, the more likely the credibility of later warnings will decline and desensitization processes will become dominant. Usually, it will lead to wrong interpretations and responses to new relevant warnings. For example, there was an overwhelming number of warnings of an impending North Korean attack before North Korea actually attacked South Korea in June 1950 thereby completely stunning U.S. and UN authorities (Doyle, in Knorr & Morgan, 1984: 80-82). General MacArthur's intelligence staff in the Far East Command which was the major source of military intelligence on Korea warned Washington between June 1949 and June 1950 no less than *1,200 times* about the risks of a North Korean attack. In one sense all these warnings were accurate because North and South Korea were engaged in a protracted artillery battle accompanied by regular border crossings of military units. The warnings amounted therefor soon to continued cries of "Wolf! Wolf!" in the eyes of most of the key political authorities in Washington. It was therefor no coincidence that secretary of Defense Louis Johnson, first reaction on the news of the invasion was to dismiss it as just another border violation.

It can be expected that the introduction of new information technology will not only contribute to the quality of warning processing and responses. It is quite likely that they will lead to various forms of sometimes devastating productions of largely irrelevant information (noise) and cry wolf syndromes as well.

Deception as another source of noise production

Deception has always been a crucial element of warfare. It is usually meant to secure concealments of someone's real intentions, capabilities, the maneuver and concentration of troops for the purpose of achieving a surprise attack or a surprising defensive move. Deception may be conducted in various forms. For instance,

- By spreading up false rumors;
- By masking the operations of radios, by setting up dummy radio nets and by radio deception;
- By the introduction of false information into security systems, data networks of state institutions and Internet.
- By setting up dummy objects and by feats;
- By concealing real objects and movements from reconnaissance and observation;
- By changing the external appearance of objects and movements;

- By artificial noises;
- By the use of computer viruses (e.g. the “Trojan Horse virus”, the “Forced quarantine virus”, the “Overload virus”, the “Sensor virus”, the “Stealth virus”, and electronic warfare.
- By sound discipline and coordination.

As recent wars and battles have shown, information technologies are likely to play a more significant role in each of these forms of deception. Deceptive information operations can cause defenders (as well as potential attackers) to make incorrect judgments and decisions. Due to the introduction of new information technologies in deceptive actions, it may become less difficult than ever to reinforce pre-existing assumptions and values about the features that a dangerous encounter will have. That is, it will be easier for a well-sophisticated aggressor to feed a defender’s expectations in various well-coordinated ways with a number of subtle at first sight highly reliable hints. It may also become easier to enter the decision-making cycles of adversaries via information technologies. Moreover, due to strong innovations in the interception systems, it may become easier (that is at least in technological respect) to double-check whether and if so, to what extent, an attacker’s as well as a defender’s deception strategies and tactics are successful as well.

THE IMPACT OF NEW INFORMATION TECHNOLOGIES ON *THE CAPABILIES TO UNDERSTAND, INTERPRET AND RESPOND TO* COLLECTED WARNINGS

At least since the last three decades, studies in Communication Science, Cognitive Sciences and Managerial Sciences have regularly emphasized that the exponential growth of information production technologies have significantly enlarge existing gaps between information production and human capacities to utilize this data. In other words, more information production and collection is *anything but* the same as more information semantics and more information semantics is *certainly not* the same as information utilization (Idenburg, 1985; Simon, 1957). While our technologies to produce and disseminate more data in a more rapid way has increased almost exponentially over the last decades, human cognitive capacities to scan and process this data is at best growing steadily and slowly over generations. In other words, even *if* leaders will be able (and are willing) to create significantly more time on the processing of incoming warnings, it is still highly likely that many relevant signals will go blind. This discouraging truth is easily applicable for the subject of this article as well: The gap between what intelligence analysts, as well as military and political leaders know and what they *could* have know given the fact that (in hindsight) the data is or was within their reach is still becoming bigger and bigger (Idenburg, 1985: 5). Sometimes signals will go blind as a consequence of deliberate decisions to concentrate scarce resources on the transcription and interpretation of one type of sources and to ignore other collected data largely (like the decision of President Roosevelt and a small circle of key advisors in the months before the Japanese attack on Pearl Harbor in December 1941 to concentrate mainly on the transcription of “Magic”). The net result may be that policy-makers will frequently be confronted with bigger discrepancies than ever between all data they are exposed to, the information the asked for, the information they really needed (including relevant warning signals and threat assessments) and the data they actually process and utilize. In sum, Francis Aguilar’s conceptual picture about the discrepancies between various forms of intelligence may be more relevant than ever for actual and future situations in which

wrong responses to impending dangers can have far-reaching, unforeseeable consequences (see Figure 3).

*Figure 3**:** A conceptual relationship among different forms of information a decision- maker is dealing with (an adapted version from a idea of Aguilar, 1967).*

Denial and avoidance coping tendencies

Last but not least, the introduction of new information technologies will certainly have an impact on the cognitive appraisals, dilemmas, and coping strategies of political leader's. Given the fact that there are usually many political reasons and practical limitations (lack of resources) why intelligence (such as satellite pictures that of preparations for a large-scale

genocide) is not welcome, policy-makers will frequently reveal strong forms of denial and avoidance. “Intelligence to please” syndromes among the leader’s senior advisors, departments and agencies will certainly be one of the major (often frustrating) reactions. It remains to be seen to whether it will makes a real difference to deny and avoid repeating visual pictures in a time wherein journalists seem to be earlier aware than ever that intelligence has been ignored.

THE IMPACT OF NEW INFORMATION TECHNOLOGIES ON AN ACTOR’S PREPAREDNESS ITSELF

Given recent experiences and extrapolating to the nearby future, it is probable that the invention of information technologies and information operations may seriously affect the essence of preparedness itself as well. First, as we have already emphasized, due to their specific character and the range of variations most (if not all) policy makers are likely to have serious problems in attaining sufficient mental and conceptual readiness towards features of the danger itself as well as initiating an adequate response. They will usually experience serious problems in being ready for (a) the occurrence of the offensive; (b) in imagining the type of actions that are going on (because confrontations with such types of dangers are still relatively new in human history; (c) the locations on which the informational technological attack is directed; (d) the timing of the confrontation (because for some types of attack this can be better hidden than ever); (e) its strengths and weaknesses (in comparison with the strengths and the weaknesses of the defense (capabilities, organization, but also mentally); (f) and the specific objectives and consequences of the attack.[6] Second, it is quite likely that most policy-makers will have serious problems in becoming and keeping sufficiently informed about the set of conceptual, physical, and mental components of the “basic measures” and “emergency measures” they may have to mobilize in case of an attack. In fact, being consciously aware of the strengths and weaknesses of ones own potential measures for defense may become a bigger problem than ever before. To oversee the exponential increase in possible variety and numbers of basic and emergency measures, as well as the variety of potential dangers and vulnerabilities is often an impossible attack for experts. So, how will a political leader or a general, who usually tend to at best a small amount of their time and energy to these issues, be able to be ready to oversee them and suddenly base decisions on it in times of rising distress and time pressure? In the third place, it may become more difficult than ever to build up sufficient political acceptability in situations wherein the necessity to counter devastating computer attacks of terrorist units or states as soon as possible with military precision attacks. To response in situations wherein there are still many uncertainties about for instance the motives and identity of the attacker and wherein most of the public, policy forums, as well as the press are not mentally prepared for aggressive military counter measures may confront political leaders with really complicated dilemmas and escalation scenarios that are difficult to control.

CONCLUSIONS

Overall, the following tentative conclusions can be drawn:

- The introduction of new information technologies will lead to a further increase of the number of potential warning signals and threat indicators that will be collected.

- New information technologies will lead to a significant increase of a specific type of potential warnings (e.g. in principle current, observable activities or intercepted communications and documents). However, other types of data that may tell something about the specific features of impending dangers will still be difficult to assess.

- The timespan between the issuance of crucial warnings and the actual attack is likely to decline further. In case of various types of information warfare (e.g. computer attacks, for instance on C4I systems) the timespan may even become almost zero, leaving the defender for a long time after the attack in the dark about questions like whether, where, when, how, why, and with what damage.

- The application of new information technologies will have a profound and ongoing impact with regard to the dissemination of a particular type of threat indicators. Dissemination will go much more rapid. Top level military and political leaders get real-time battle field awareness so that they can judge themselves whether or not, and if so, when, where, how and why developments that can be observed makes it necessary to respond with which kind of preparations.

- The new information technologies may make it possible to work more rapidly than ever through decision cycles and surprise the adversaries with rapid counter measures. At the same time it will create many dangerous traps like unjustified "what you see is what you get" syndromes, "sense of false control" and "micro management". Furthermore, it will create a lot of specific distortions and both information overload and partly overlooked information underload.

- The appetite of commanders for the latest, more detailed information about what is and what will be going on in the immediate future will increase significantly.

- The thorough selection and interpretation of the right signals will suffer from various types of time pressures that are not directly created by the situation in the field.

- The gap between (a) information collection and production; (b) information semantics (interpretation); and (c) information pragmatics (adequate use of relevant signals) will increase further. A lot of collected and available relevant signals will go blind.

- In situations wherein for whatever reason military and/or political leaders are reluctant to act on visual pictures more sophisticated types of denial and avoidance by these leaders will be seen.

- It will be more complex and difficult than ever for most (if not all) political and military leaders to be totally prepared.

In sum, there is a lot to be studied and learned on the impact that the wealth of information technologies may have on various dimensions and types of warfare and crisis management. Besides (or perhaps partly due to) the explosion of new information technologies over the last decades Sun Tzu's 2,000 years old maxim, "Know the enemy and know yourself; in a hundred battles you will never be in peril," still seems to be a challenge for at least decades to

come. Technology may thereby be a major help. On the other hand it will continue to place the human decision-maker and intelligence analysts, given their bounded cognitive capacities and constrained freedom of manoevre, for many traps, gaps and puzzles.

REFERENCES

Aguilar, F. (1967), *Scanning the Business Environment*.

Breznitz, S. (1984), *Cry Wolf: The Psychology of False Alarms*, Lawrence Erlbaum, London.

Bosch, J.M.J., *Generaals, geleerden en goeroes: Kanttekeningen bij oorlog, informatie en informatie-oorlog*, Royal Military Academy, Breda, 1997.

Coroalles, A.M. (May 1996), On war in the information age: A conversation with Carl von

Clausewitz, *Army*: 24-34.

Davis, N.C. (Winter 1996), An information-based revolution in military affairs, *Strategic Review*: 43-53.

Handel, Michael (1987), "The politics of intelligence," *Intelligence and National Security* (October).

Hartog, W.W. & Susan Canedy (1997), "Operations in the information age," in: Pfaltzgraff & Schultz: 174-185.

Idenburg, Ph.A. (1985), *Informatie-overlast* (oratie), Tilburg.

Kam, Epraim (1989), *Surprise Attack: The Victim's Perspective* (Cambridge, Mass.).

Leonard, R.R. (1998), *The Principles of War for the Information Age*, Presidio Press, Novato.

Levite, A. (1987), *Intelligence and Strategic Surprises*, New York.

Metselaar, M.V. (1997), "Understanding failures in intelligence estimates: UNPROFOR, the Dutch, and the Bosnian-Serb attack on Srebrenica", *NL Arms: Netherlands Annual Review of Military Studies,* (edited by J.L. Soeters & J.H. Roovers): 23-50..

Metselaar, M.V. (forthcoming), *Coping with Impending Danger: A Study of Denial and Avoidance of Warnings in Political Decision Making* (PHD), Breda..

Molander, R.C., A.S. Riddile, P.A. Wilson (1996), Strategic Information Warfare: A New Face of War, *Rand*.

Owens, W.A. (May-June 1996), The emerging system of systems, *Military Review*: 15-19.

Owens, W.A. (Winter 1996), The American Revolution in Military Affairs, *Joint Forces Quarterly*.

Sun Tzu (Fourth Century B.C.), *The Art of War*.

Pfaltzgraff, R.L., Jr. & R.H. Schultz, Jr., R.H. (Eds.), *War in the Information Age: New Challenges for U.S. Security Policy*, Brassey's, Washington/London.

Vertzberger, Y. (1989), *The World in Their Minds*, Cambridge UP, Cambridge.

Wirtz, J.J. (1991), *The Tet Offensive: Intelligence Failure in War*, Cornell UP, Ithaca/London.

Wohlstetter, R. (1962), *Pearl Harbor: Warning and Decision* (Stanford, Calif.).

NOTES

[1] This dimensions includes a nation's potential, procedures and mental and physical state to recover quickly from the first hours wherein a danger materializes and unfolds (i.e. phase 1 of a surprise attack) and to mitigate and undermine the sustainment of an attacker's initial achievements (i.e. the second phase of a surprise attack) (cf. Handel, 1984: 230). Some historical events which nicely illustrate the crucial differences as well as the close relationship between both phases and dimensions are: Germany's attack on Western Europe (France, Belgium, and the Netherlands) in 1940, the first days of the Battle of Bulge in 1944, the allied landing on Sicily in 1944, the first days of the Six Days War in May 1967 and the Yom Kippur war in October 1973 in the Middle East. The same three dimensions of (un-)preparedness (including most of its components) can also be applied on most (if not all) cases of encounters with large-scale natural and man-made disasters.

[2] There are many studies in which warnings are defined as a type of information. It should be noted, however, that there are also many studies that define "warning" not as an information but as an activity or a stream of activities. For example, an act of alerting a recognized authority to the threat of a new (or renewed) conflict at a sufficiently early stage for that authority to attempt to take preventive action.

[3] The same tendencies may be seen with regarding of traditional sources of information abroad from ambassadors and military attachés in-the-field).

[4] For example, in the Summer of 1995 the fact that CNN came much earlier with the latest developments in advance of the Bosnian Serbian attack on the UN enclave Srebrenica than most intelligence agencies pressed and frustrated several airforce commanders and UNPROFOR staff members who wanted to react as quickly as possible before it was too late).

[5] This definition is derived from several theorists in the field of disaster studies and strategic surprise attacks. In particular: George, 1979: 12-24; Levite, 1987: 2-3; Kam, 1988: 8; Chan, 1979: 171.

[6] Example given in the first section of chapter 1. For instance, Stalin, complete mental breakdown/surprise.

The Legal Perspective

INTERNATIONAL LEGAL ASPECTS OF INFORMATION OPERATIONS

Karl F. Muusse
Staff of the Commander-in-Chief
Directorate of Materiel, Procurement Support Branch
Royal Netherlands Air Force

ABSTRACT

This article explores the international legal rights for states to conduct Information Operations during peacetime and discusses the appropriateness of applying the law of armed conflict to Information Operations during armed conflicts. International law does not explicitly prohibit Information Operations as such, therefore the general principles of international law have to be studied, although Information Operations challenges some fundamentals of international law like the territorial sovereignty of states.
International law contains two important exemptions to the ban. The first is the use of force with the explicit authorisation of the Security Council. To be able to authorise the use of force, the Security Council has to determine whether a threat to the peace etc. has occurred. The second exemption is the use of force in self-defence. When an information attack is launched upon a nation, there is no doubt that this nation has the right to react if the attack can be assessed as an armed attack. Actions taken in self-defence presume a degree of certainty of the identity of the attacker and of the intent of the attacker which in Information Operations often will be a problem.
Information Operations can, by way of disturbing information technology infrastructure which are protected by several international agreements, also constitute forbidden interventions 'below the threshold of the use of armed force'. When the actual hostilities commence, the law of armed conflict becomes valid. This law contains several basic principles codified in many conventions. The conventions apply whenever there is an 'armed conflict'.
The conduct of Information Operations on both sides can constitute an armed conflict, so the principles of the law of armed conflict like 'military necessity', 'humanity', 'distinction' and 'proportionality' do apply

INTRODUCTION

"At the end of 1998 a hacker group, 'Legion of the Underground', declared the 'cyberwar' to China and Iran, and just a few days later also Mexico was virtually offended by a guerrilla group acting under the name 'Intercontinental Cyberspace Liberation Army'. Cyberwar can hurt: according to American Defence specialists, the Russians would possess virus 666, which should be able to bring users of computers in trance and to cause severe spasms of the heart. The East Timor independence fighters acquired an international 'country code' and related to that an official domain name (like .nl for The Netherlands). In January 1999, the East Timor domain, as provided by an Internet service provider in Ireland, and the East Timor website content was attacked by hackers (in this case referred to as E-nazi's). The E-nazi's would have been acting under authority of Indonesia. The 'defence line' of the Irish provider Connect-Ireland broke down after eighteen simultaneous attacks by robots from different

countries", so far a recent statement from the 'Volkskrant'[1].

The rise of the information society confronts governments with important problems on several different subjects, problems that sometimes are strongly linked together. Beside problems as how to optimally facilitate the electronic social intercourse and how to guarantee elementary provisions necessary for the social functioning of citizens and companies in the electronic society, governments are also faced with the fundamental problem how to warrant core values of a democracy in the information society. These values can be at stake by gross violation of privacy rights, by criminal acts as distribution of child porn on the Net, or by threats to the internal and external security of a state. Security threats have changed and perhaps have significantly increased through the worldwide explosion of information technology. The development of the Internet has resulted in a global society dependent on IT[2]. The technological changes that have taken place, termed as 'the Revolution in Military Affairs' or 'the Third Wave' [3], faces governments with new threats and requires reviews of notions of how security threats should be dealt with. In short, these threats and the way they threats are countered can be characterised as 'information operations'. Other writers use terms as 'Netwar', 'Command and Control Counterwar', 'Third-Wave war', 'Knowledge war', and 'Cyberwar'[4].

In this article 'information operations' will be defined according to the NATO definition: *"Actions taken to influence decision makers in support of political and military objectives by affecting other's information, information based processes, C2 systems, and CIS while exploiting and protecting one's own information and/or Information Systems"*[5]. Although this NATO-definition creates some confusion using the phrase *"exploiting one's own Information System"*, physical attacks on information systems by traditional military means as well as psychological operations, military deception, and 'electronic warfare' operations, such as jamming radar and radio signals are supposed to be included in this definition.
It is clear that information operations in this definition contains a defensive and an offensive part, it may also be obvious that in practice there is no clear drawing line between defensive and offensive Information Operations. For instance, defensive Information Operations include the capability to assess the ability of an adversary to conduct offensive Information Operations. This assessment can in many times only be made with an intrusion in the information system of the adversary. How then is this assessment to be characterised? Defensive or offensive? Although the scope of Information Operations in this definition is rather broad, this article, when considering what means are used, will primarily deal with the concept of Information Operations as the use of Information Technology. In this article the term 'Information Attack' will be used to describe the offensive part of of Information Operations.

The focus of this article is to search for the international legal implications of Information Operations. The international legal questions concerning Information Operations sound traditional. Does Information Operations constitute aggression, is it a use of force against the territorial integrity, is it an armed attack against which states have the right of self-defence, is that right of self-defence limited to using the same information means, does it constitute a non-armed intervention, what legal rights does a state have if so? What are the implications of the law of armed conflicts on Information Operations?
To answer these questions, this article first explores the international legal rights for states to conduct Information Operations during peacetime. The article then discusses the

appropriateness of applying the law of armed conflict to Information Operations during armed conflicts. This article does not discuss national legal aspects of Information Operations, although there are several important aspects concerning topics like privacy rights of citizens and employees.

INTERNATIONAL LAW AND THE USE OF FORCE IN PEACETIME

International law.

International law consists of binding legal obligations among sovereign states and some of the international organisations. Sovereign states generally assume legal obligations only by affirmatively agreeing to do so. The most effective instruments in creating international law are international agreements. Beside these agreements there is also a body of customary international law, which consists of practices that have been so widely followed by the community of nations, with the understanding that compliance is mandatory, that they are considered to be legally obligatory.
Perhaps because of the newness of much of the technology involved, there is no international agreement that explicitly prohibits Information Operations. The absence of explicit prohibitions is significant because, as a crudely general rule, that which international law does not prohibit it permits. But the absence is not dis-positive, because even where international law does not purport to address particular weapons or technologies, its general principles may apply to their use. When applying these general and longstanding international legal principles however, some basic problems or challenges arise.

Legal challenges.

Two important challenges are to be mentioned[6]: Firstly, simply stated, international law defines war and peace. In making this distinction the 'level' of damage done is a criterion. The sort of damage that information attacks may cause may be analytically different from the physical damage caused by traditional warfare. The kind of destruction that bombs and bullets cause is easy to see and understand, and fits well within long-standing views of what war means. In contrast, the disruption of information systems, including the corruption or manipulation of stored or transmitted data, may cause intangible damage, such as disruption of civil society or government services that may be more closely equivalent to activities such as economic sanctions that may be undertaken in times of peace. This means that Information Operations further blur the already so often unclear line between war and peace.

Secondly, the subjects of international law are foremost states. States are entities, which have sovereign authority over a certain territory. The ability of signals to travel across international networks or through the atmosphere as radio waves challenges the concept of national, territorial sovereignty. Sovereignty holds that each nation has exclusive authority over events within its borders. Sovereignty may be at odds with an increasingly networked, or 'wired' world, as signals travel across networks or as electromagnetic waves, crossing international borders, quickly and with impunity, allowing individuals or groups to affect systems across the globe, while national legal authority generally stops at those same borders. Furthermore, the intangible violation of borders that signals may cause may not be the sort of violation

traditionally understood to be part of a military attack.

Bearing these challenges in mind, I will now discuss the general principles of international law concerning the use of force and apply them to Info Ops. In this discussion the difference between the concepts of 'armed force' and 'force' will be explored. In the subsequent part I will pay attention to the legal principles concerning acts that are 'short of force' or that do 'not amount to the use of force' and relate them to Information Operations.

BAN TO THE USE OF FORCE.

Since the end of the Second World War, the legal rights of states to resort to force in their international relations, traditionally referred to as '*ius ad bellum',* have been first of all laid down in the UN Charter. One of the primary goals of the UN, presently consisting of 188 nations, is to 'unite our strength to maintain international peace and security, and to ensure by the acceptance of principles and institution of methods, that armed force shall not be used, save in the common interest'[7]. It should be noted that the UN Charter does not know the concept of 'acts of war'. So, the often seen title of articles concerning legal aspects of Information Operations *"Is a cyber attack an act of war?"* are not legally relevant.

Armed force.

The question *"Is a cyber attack a 'use of armed force' "* is more relevant since article 2(4), often viewed as the cornerstone of the Charter, prohibits 'the threat or use of force against the territorial integrity or political independence of any state, or in any other manner inconsistent with the purpose of the UN'. The prohibition of article 2 (4) is part of '*ius cogens',* i.e., it is accepted and recognised by the international community of states as a whole as a norm from which no derogation is permitted and which can be modified only by a subsequent norm of general international law having the same peremptory character[8].

Is an information attack then ' the use of force'? What is 'force'? Force in the sense of article 2(4) is commonly understood as to at least include 'armed force'. The relevant question then is, is an information attack 'the use of arms'? This question can lead to an endless discussion. With Jacobson I would state that 'armed' simply means equipped with the weapons of war. Armed does not necessarily need to refer only to weapons that cause physical destruction [9]. The use of non-lethal weapons, such as sticky foam, certainly is understood as the use of arms. The conclusion in this opinion is that Information Operations can be the use of armed force and therefore, when it amounts to a level that the territorial integrity or political independence is at stake, be a violation of article 2(4). Criteria to assess whether this level is surpassed are the severity and impact of the damage caused by an information attack and the intent of the attacker. These additional criteria however are not decisive for the assessment whether article 2(4) is violated. Economic coercion measures like an oil boycott for instance, can wilfully cause severe damage, it is commonly not understood however as 'force' in the sense of article 2(4).

Interference short of armed force.

Next to the understanding as force being at least 'armed force' there are also further going

concepts of 'force'. Article 2(4) is elaborated in the General Assembly resolution of 1970 titled as the 'Declaration on Principles of International Law Concerning Friendly Relations and Co-operation among States in Accordance with the Charter of the United Nations', which is seen as an authoritative restatement of customary international law[10]. This resolution espoused the principle of non-intervention in the *"internal or external affairs of any other state, including armed intervention and all other forms of interference or attempted threats"*. According to some writers it is not possible to conclude anything else then that any interference in the affairs of another state constitutes a violation of article 2(4)[11]. In this perception of the scope of the prohibition of article 2(4) Information Operations can constitute a breach to it, no matter the outcome of the discussion whether Information Operations must be seen as the use of arms.

Exemptions To The Ban On The Use Of Force.

The Charter contains two important and well-known exemptions to the ban on the use of force. The first is the use of force with the explicit authorisation of the Security Council; the second is the use of force in self-defence.

SECURITY COUNCIL RESOLUTIONS

Chapter VII of the Charter constitutes the basis for the Security Council to mandate or, more recently, to authorise the legal use of force by states, acting individually, in ad hoc coalitions or through regional organisations. To be able to mandate or to authorise the use of force, the Security Council, according to the opening article 39, has to determine whether '*a threat to the peace, breach of the peace, or act of aggression'* has occurred.

Threat to the peace, breach of the peace, act of aggression.

The question here is whether an information attack can be a 'threat to the peace, breach of the peace or an act of aggression'? To start with 'acts of aggression' reference can be made to the *"Definition of Aggression"* Resolution of 1974, in which the General Assembly provided what acts by states are seen as 'acts of aggression'[12]. It is obvious that the drafters of this legally not binding resolution were only referring to the arms envisioned at that moment. However, information weapons can easily be seen as part of, for instance, the phrase *"use of any weapon against the territory of another State"*. [13]. With an information attack the 'sovereignty, territorial integrity or political independence' can be at stake, so it can constitute an 'act of aggression' leading to Security Council actions.

In actual UN practice it seems to be more common to conclude that 'threats to the peace' has occurred than to speak of 'acts of aggression'. See for instance Security Council resolution 1199 concerning the Former Republic of Yugoslavia and Kosovo and resolution 1264 concerning Indonesia and East-Timor. In both situations the Council had to balance between the concern of human rights violations and respect for the sovereignty and territorial integrity. Questions that create difficulties for some of the permanent members of the Council, therefore take a lot of time to unanimously address and solve. Is it wishful thinking to assume that information attacks will constitute threats equable important and valid for all of the permanent members? And will it be less politically sensitive? Will the situation be such that Security

Council resolutions, mandating the use of force to counter Info Ops threats, more easily reached than resolutions concerning human rights situations?

Any way, there is no explicit requirement that a 'threat to peace' takes the form of an armed attack, a use of force, or any other condition specified in the Charter. The Security Council has the plenary authority to conclude that virtually any kind of conduct or situation constitutes a 'threat to the peace' in response to which it can authorise remedial action of a coercive nature. Nothing would prevent the Security Council from finding that a Cyber attack is a 'threat to the peace' if it determines that the situation warrants such action. It seems unlikely that the Security Council will take action based on an isolated case of state-sponsored computer intrusion producing little or no damage, but a computer network attack that caused widespread damage, economic disruption, and loss of life could well precipitate action by the Security Council. The debate in such a case would more likely centre on the offender's intent and the consequences of the offending action than on the mechanism by which the damage was done[14].

All necessary means.

In the case of an information attack that is condemned as 'a threat to the peace' or 'act of aggression', the follow-on question then is how the authorisation to take remedial action of a coercive nature will be or should be formulated? When the Security Council, acting under chapter VII and condemning the information intrusion as an act of aggression or threat to the peace, does not explicitly state that 'all necessary means' can be used, is the use of Information Operations then in line with the mandate? In the UN-vocabulary the phrase 'all necessary means' is used as the most explicit mandate to apply 'armed force' to restore the peace in the specific country or region. When, due to a veto of one of the permanent members of the Council, it would not be possible to get a mandate to use 'all necessary means', it could be doubtful whether Information Operations would then be outlawed.

SELF-DEFENCE.

The second exemption to the ban on the use of force is the use of force in self-defence. Article 51 of the Charter recognises the inherent right of self defence 'if an armed attack occurs'. This article is a source of confusion in the international relations. Is an armed attack different from an 'act of aggression', mentioned in article 39? Does the reference 'if an armed attack occurs' imply that a would-be victim must actually wait for the other side to strike first before it can respond? Does the reference to self-defence as 'an inherent right' indicate that an armed attack may be only one of several circumstances under which action in self-defence could lawfully be undertaken, as it was in the pre-existing customary law before 1945[15]? In 1986 the United States bombed Libya as a response to Libya's continuing support for terrorism against U.S. military forces and other U.S. interests. In June 1993 U.S. forces attacked the Iraqi military intelligence headquarters because the government of Iraq had conspired to assassinate former President Bush. In August 1998 U.S. cruise missiles struck a terrorist training camp in Afghanistan and a chemical plant in Sudan in which chemical weapons should have been manufactured. The rationale articulated for each of these actions was self-defence[16]. The Dutch Government stated that the self-defence claim of the US in the 1998 missile attack was legally right[17]. The Israeli's have long argued and acted according to the doctrine of

'Nadelstichtaktik' (needle pricking tactics; ed). This concept holds that although each specific act may not constitute an armed attack, the totality of the incidents might entitle a nation to respond legitimately when the culmination of these acts rises to an intolerable level[18]. This doctrine can be opportune in the case of repeated information attacks, each with only little damage.

The following observations concerning the legality of Information Operations as acts of self-defence can be made:

- When an information attack is launched upon a nation, there is no doubt that this nation has the right to react if the attack can be assessed as an armed attack. The certainty of declarations that Information Operations constitute legitimate acts of self-defence will depend on how the nations and international institutions react to the particular circumstances of the case and of similar cases before. Relevant criteria for this assessment are the damage caused by the attack and the perceived intent of the attacker, more then the means used for the attack. When a power plant is attacked through carbon fire 'bombs' dropped from an aeroplane the consequences could be temporarily as severe as when a physical bomb bombed the plant. In a similar way, when the power plant is neutralised by an information attack the consequences could be equal.

- When a nation chooses to respond to an information attack by mounting a similar computer attack of its own, the issue of whether the initial provocation constituted an armed attack may become a tautology. If the provocation is considered to be an armed attack, the victim may be justified in launching its own armed attack in self-defence. If the provocation is not considered to be an armed attack, a similar response will also presumably not be considered to be an armed attack[19].

- When a nation has proven valid information of a coming attack, it has the right to take action in self-defence. The following conditions might serve as useful guidelines when considering to take action: a clear indication of intent of the adversary; adequate evidence that preparations for the attack have advanced to the point where a attack is imminent; the advantages of the pre-emptive attack must be proportionate to the risks of precipitating a war that might be avoided[20].

- Different reaction scenario's can be construed. A state can be attacked by an information operation or by an attack with traditional kinetic force. When attacked by electronic means is the state then free to choose the means of reaction or is the state, when it wants to defend itself in a legally correct way, only allowed to react with similar means? The classic requirements when acting in self-defence are of course necessity and proportionality. Proportionality does not necessarily require that an act of self-defence use the same means as the provocation. Conducting a responsive information attack as a measure of self-defence against foreign computer network attacks would have the major advantage that it would minimise the issue of proportionality, which would be more likely to arise if traditional military force were used, such as firing a cruise missile at the building from which a computer network attack is being conducted. Generally speaking, the intensity and scope of self-defence acts should be in line with the attack in order to limit possible escalations of the conflict. In the traditional sense the goal of self defence acts should be to stop the aggressive acts of the adversary and to force him to retreat to his own territory, not to punish or to take revenge. The problem with

information attacks is the fact that it is not possible to force the attacker to retreat, that the exact location of the attacker is unclear and that the intensity of an attack is not always immediately obvious and verifiable. Computer 'time worms' can disrupt information systems months after the intrusion and with in the beginning only little damage. Therefore, a self defence reaction should be allowed also when the only goal can be to dissuade the attacker from a further attack or to degrade him in his ability to undertake a future attack.

Identifying the attacker.

Actions taken in self defence presume a degree of certainty of the identity of the attacker and his intent. In Information Operations this will often be a problem. If the attacker is a State or if the attack is undoubtedly State-sponsored then acts of self defence against that State are legitimate. If the attack is not clearly state-sponsored the question then is in what cases attacks can be at least attributed to a state. Generally speaking, States are not responsible for acts of private persons done on their soil, unless there is a specific protection obligation as for diplomatic personnel. When a nation' s interest is damaged by the private conduct of an individual who acts within the territory of another nation, the normal reaction then will be to notify the government of that nation and to request its co-operation in putting a stop to such conduct. Only if the requested state is unwilling or unable to prevent recurrence does the doctrine of self-defence permit the injured state to act in self-defence inside the territory of another nation[21].

Transit states.

A special topic is the status of nations through whose territory or communications systems a destructive message may be routed. Transit States can be involved in an Information Operation either as a transit medium for the attacker or as a medium for the defender. If only the nation's public communications systems are involved, the transited nation will normally not be aware of the routing a message has taken. If it becomes aware of the transit of an attacker message or a defenders digital bomb, there would be no established principle of international law that it could point to as being violated. Even during an international armed conflict international law does not require a neutral nation to restrict the use of its public communications networks by belligerents. Nations generally consent to the free use of their communications networks on a commercial or reciprocal basis. Accordingly, use of a nation's communications networks as a conduit for an electronic (counter) attack would not be a violation of its sovereignty in the same way as a flight through its airspace by a military aircraft would be.

STATE ACTS 'SHORT OF FORCE'.

International law not only prohibits the use of 'armed force' and other forms of 'force' against other States, it also generally prohibits to interfere in the sovereign rights of that State in order to achieve submission to a foreign will even when the interference has not taken place with the use of force. Only in recent times the notion begins to appear that states loose their right of non-interference by other States in case of gross violations of human rights on their soil. Beside the case of human rights violations, nations whose rights under international law have been violated have the right to take countermeasures against the offending state in

circumstances where neither the provocation nor the response involves the use of (armed) force. Countermeasures can generally be divided in reprisals (measures that are normally violations of treaty obligations or of general principles of international law) and retortions (actions that are unfriendly but do not constitute violations of international law). Information Operations, dependent of several criteria as for instance the severity of the damage done, can constitute interference below the threshold of a 'use of armed force'.

Information systems of the other state can be the object of interference. This can done be against space-based systems, as space segments become more and more critical to many information systems. Several Space law treaties as the Outer Space Treaty of 1967, the Convention on International Liability for Damages caused by Space Objects of 1972 and the Convention on the Registration of Objects Launched in Outer Space of 1975 establish a specific obligation not to interfere with space activities of other nations. Other international agreements to mention here are the 1971 Agreement Relating to the International Telecommunications Satellite Organisation (INTELSAT), the 1976 Convention on the International Maritime Satellite Organisation (INMARSAT) and the European Telecommunications Satellite Organisation (EUTELSAT). These agreements also affect telecommunications and the use of space. The question whether these agreements bar information warfare activities that make use of satellite assets, is dependent on the answer to the question whether these Information Operations are qualified as 'peaceful' or not. Although the agreements in general outlaw use of the satellites for 'military purposes', there are many military applications are granted to the use of these satellites..

Reference can also be made to interference that involves networks and telecommunications. This interference can be a violation of obligations set out in international communications law, most significantly laid down in the International Telecommunications Convention of 1982. Provisions in this Convention seem to block the disruption or spoofing of adversaries' telecommunications. In times of armed conflict these provisions do not apply however.

INFORMATION OPERATIONS AND THE LAW OF ARMED CONFLICT

Whether acting in self-defence or with authorisation of the Security Council or acting as the aggressor, when the actual hostilities commence, the law of armed conflict becomes valid. The law of armed conflict contains several basic principles that are codified in many conventions. Before I will address these principles, two fundamental prerequisites have to be discussed when applying the rules during armed conflicts to information operations.
The first is the so-to-call moment of application of the law of armed conflict; the second is the place of application.

When does the Law of Armed Conflict apply?.

The law of (international) armed conflict applies whenever two or more nation-states are involved in an armed conflict. But what is an 'armed conflict'? The expression 'international (or non-international) armed conflict' is not defined in the Geneva Conventions. Does it require that armed forces engage other armed forces? Must the emphasis lie on physical confrontations and a physical entry of the territory of a foreign state or can virtual

engagements also lead to the application of these traditional rules during armed conflict?
If an information attack does not fit the definition of an 'armed conflict', then many if not all of the laws of armed conflict are not even applicable[22]. With reference to what is stated above concerning the application of the ban on the use of force to Information Operations, the conduct of Information Operations can constitute an armed conflict, dependent again on severity of the damage done, intent of the attacker and the type of countermeasures of the attacked state.

Where does the Law of Armed Conflict apply?..

The law of armed conflict deals with the issues of laws of war on land or at sea. Even the 1977 protocols to update the Geneva Conventions of 1949 continued this connection to the land or sea, while other law of war treaties dealt with the air and space. This corporeal division worked well for first- and second-wave societies dealing with agrarian and industrial matters, but falls short in proscribing conduct in the information age characterised as the third wave society. Information warfare takes place in what has come to be known as cyberspace, an ethereal place that does not neatly fit into the land, sea, air, and space dichotomy[23].

GENERAL PRINCIPLES.

The four fundamental principles of the law of armed conflict are military necessity, humanity, distinction and proportionality. I will briefly discuss these principles and apply them to Information Operations.

Military necessity.

Military Necessity permits that degree of regulated force, not otherwise prohibited by the law of armed conflict, required for the partial or complete submission of the enemy with the least expenditure of life, time and physical resources. Many information warfare weapons may not be considered 'regulated force'. This is especially true if they are not set to trigger upon the occurrence of a certain event, but are triggered randomly.
The stipulation that the submission of the enemy be accomplished with the least expenditure of life, time, and physical resources favours Information Operations. Information warfare is largely viewed as a bloodless type of warfare; it can take little time, as it can potentially travel at the speed of light.

Humanity.

The principle of Humanity prohibits the employment of any kind or degree of force not necessary for the purposes of war. The law of land warfare forbade the employment of '*arms, projectiles, or material calculated to cause unnecessary suffering'*. The 1981 Weapons Convention[24] identified, in until now four protocols, weapons that are deemed to be excessively injurious or that are deemed to have indiscriminate effects. Among the weapons banned in these laws are 'dum-dum bullets, projectiles filled with glass or other non-detectable fragments and laser weapons specifically designed to cause permanent blindness. The law of armed conflict requires any nation desiring to implement a new type of weapon to make a determination, prior to its use, regarding its compliance with the principle of

humanity[25]. Terming computer programs as 'weapons' may trigger the required review. At first view it seems safe to state that information 'weapons' more comply with the principle of humanity than most other weapon do.

Distinction.

A central principle is the principle of distinction. Attacks are to be directed at military targets and not at civilian objects, only at combatants and not at civilians. The law of armed conflicts currently defines combatants as 'any member of the armed forces of a party to the conflict'[26]. As only combatants are permitted to take a direct part in hostilities it follows that they may be attacked. Concerning Information Operations some difficult issues may arise: the nature of information systems makes them accessible to a wide group of people, not just enemy soldiers. The teenage hacker of an enemy country who decides to support his country by breaking into the computers of the other state, is he a combatant? The Kosovo-crisis showed that these questions are not hypothetical. Additional Protocol I makes it clear that this hacker can only be a combatant when he is a member of the armed forces or other organised groups that are a party to the conflict, when he serves under effective discipline and when he will be under command of officers responsible for their conduct. If he is not, and it seems to me that this is mostly the case, he is not entitled to the combatant-status. As a civilian he enjoys overall protection to the dangers of military operations [27]. This protection however seizes to exist when the hacker takes a direct part in the hostilities [28]. If combatants acts are conducted by unauthorised persons, like the teenage-hacker, their government may be in violation of the law of armed conflict, depending on the circumstances, and the individuals concerned are at least theoretically subject to criminal prosecution either by the enemy or by an international war crimes tribunal. The long-distance and anonymous nature of computer network attacks may make detection and prosecution however unlikely[29].

The law of armed conflicts also requires making a distinction between military targets and civilian objects. Military targets are defined as '*those objects which by their nature, location, purpose, or use make an effective contribution to military action and whose total or partial destruction, capture or neutralisation, in the circumstances ruling at the time, offers a definitive military advantage*'[30]. In practice for the target-selectors this definition does not make it always clear which target is permissible. During the Kosovo-crisis for instance NATO attacked on 23 April 1999 the Yugoslavian Serb broadcast station in Belgrade. Discussions still continue whether this was a permissible military target.
The dual-use nature of many telecommunications networks and much equipment contribute to the blurring of the distinction between military and civilian systems and, consequently, between military targets, which are legitimate and civilian ones, which are not. Some information weapons may not permit their users to distinguish between military and civilian targets. In the United States, for example, it has been estimated that 95% of the telecommunications of the Department of Defense travel through the Public Switched Network, and during the Persian Gulf War, commercial communications satellites reportedly carried almost a quarter of the U.S. Central Command's transcontinental telecommunications. The interdependence and interconnectivity of civilian and military systems may further exacerbate the difficulty in distinguishing among civilian and military targets. Attacks directed at predominantly military targets may cause civilian systems that are connected to those military systems to fail; alternatively, a virus that is directed toward an adversaries military systems may spread, inadvertently or otherwise, into civilian (and even friendly)

systems [31].

Proportionality.

The principle of distinction is closely related to the principle of proportionality. This principle requires armed forces to use force no greater than necessary to accomplish legitimate military objectives. It also seeks to prevent forces from attacking in situations where civilian casualties would clearly outweigh military gains. The rule is more easily stated than applied in practice, especially in the case where in adopting a method of attack that would reduce incidental damage the risk to the attacking troops is increased[32], as may have been the case in the Kosovo-crisis.
The weapons of information warfare must severely impact an entire network of information systems and all the users of those systems, military and civilian. Denying all information-transfer media and disrupting or destroying every transmission goes beyond a military objective by incapacitating the entire civilian populace as well. Taking out all information-transfer media could bring down a country's stock market, banking system, air traffic control, emergency dispatches and more, leading to civilian casualties and a disproportionate effect as compared to the military objective.

CONCLUSION

The information society creates important problems. Governments are faced with the fundamental problem how to warrant core values of a democracy in the information society. These values can be at stake by threats to the internal and external security of a state. Information Operations can be applied both during peacetime and during armed conflicts. Article 2(4) of the Charter of the UN bans the use of force between states.At this pointthe conclusion has to be that there are different opinions in International Law what actions are to be included in the term 'force', only 'armed force' or also other forms of force. This complicated matter is far from being solved.

---

1 Volkskrant (Dutch daily newspaper), 4-9-1999.

2 Elliot Cohen, A Revolution in Warfare', Foreign Affairs 75/2, April 1996

3 A. And H. Toffler, The Third Wave, Bantam Books 1984, New York

4 R.W. Aldrich, The international legal implications of information warfare, INSS Occasional Paper, April 1996

5 NATO MC 422

6 Greenberg/Goodman/Hoo, Information Warfare and International Law, National Defense University Press

7 Preamble of The UN Charter

8 B. Simma, 'NATO, the UN and the Use of Force: Legal Aspects, European Journal of International Law, Volume 10, nr.1, 1999

9 M.R. Jacobson, War in the Information Age: International Law, Self-Defence, and the Problem of "Non-Armed-Attacks", in: Journal of Strategic Studies, Vol.21, No.3 (September 1998), p.15.

10 UN GA res. 2625

11 For instance, O. Schachter, International Law in Theory and Practice 1991, p. 111.

12 UN GA res. 3314. Article 1. Aggression is the use of armed force by a State against the sovereignty, territorial integrity or political independence of another State, or in any other manner inconsistent with the Charter of the United Nations, as set out in this Definition.
Article 2. The first use of armed force by a State in contravention of the Charter shall constitute prima facie evidence of an act of aggression although the Security Council may, in conformity with the Charter, conclude that a determination that an act of aggression has been committed would not be justified in the light of other relevant circumstances, including the fact that the acts concerned or their consequences are not of sufficient gravity.
Article 3. Any of the following acts, regardless of a declaration of war, shall, subject to and in accordance with the provisions of Article 2, qualify as an act of aggression:
(a) The invasion or attack by the armed forces of a State of the territory of another State, or any military occupation, however temporary, resulting from such invasion or attack, or any annexation by the use of force of the territory of another State or part thereof;
(b) Bombardment by the armed forces of a State against the territory of another State or the use of any weapons by a State against the territory of another State;
(c) The blockade of the ports or coasts of a State by the armed forces of another State;
(d) An attack by the armed forces of a State on the land, sea or air forces, or marine and air fleets of another State;
(e) The use of armed forces of one State which are within the territory of another State with the agreement of the receiving State, in contravention of the conditions provided for in the agreement or any extension of their presence in such territory beyond the termination of the agreement;
(f) The action of a State in allowing its territory, which it has placed at the disposal of another State, to be used by that other State for perpetrating an act of aggression against a third State;
(g) The sending by or on behalf of a State of armed bands, groups, irregulars or mercenaries, which carry out acts of armed force against another State of such gravity as to amount to the acts listed above, or its substantial involvement therein.

13 Ibid, article 3(b).

14 Department of Defense, Office of General Counsel, An assessment of International Legal Issues in Information Operations, May 1999

15 A. Arend & R. Beck, International Law and the use of Force, Routledge 1993, p.36

16 Department of Defense, Office of General Counsel (note 14), p.12.

17 Letter of the Secretary of State to the Parliament, 10 February 1999

18 H. McCoubrey/N. White, International Law and Armed Conflict, England 1992, p. 36.

19 Department of Defense, Office of General Counsel (note 14), p.18.

20 M.R. Jacobson (note 9), p.15.

21 Department of Defense, Office of General Counsel (note 14), p.23.

22 See Aldrich (note 4), p. 4.

23 Ibid note 22

24 Formal title: United Nations Convention on Prohibitions or Restrictions on the use of certain conventional weapons which may be deemed to be excessively injurious or to have indiscriminate effects.

25 Additional Protocol I (1977) to the Geneva Conventions of 1949, article 36.

26 Additional Protocol I (1977) to the Geneva Conventions of 1949, article 43.

27 Additional Protocol I (1977) to the Geneva Conventions of 1949, article 51, para 1.

28 Additional Protocol I (1977) to the Geneva Conventions of 1949, article 51, para 3.

29 Ibid, note 6

30 Additional Protocol I (1977) to the Geneva Conventions of 1949, article 52, para 2.

31 Ibid, note 6

32 A.P.V. Rogers, Law on the battlefield, Manchester/New York 1996, p.17

APPENDIX

BIOGRAPHIES

Brigadier-general Hans Bosch was born on April 13, 1947 in Heemstede, the Netherlands. In 1970 he was commissioned into the cavalry. He served in various command and staff functions in 103 Reconnaissance Battalion. Between 1987 and 1989 he commanded 43 Tank Battalion. His various other positions were at the Army Staff, in Army War College, and in the Military Intelligence Service. In 1994 he became private secretary of the Commander RNLA. He is a graduate of the Royal Military Academy (1966-1970), the Army War College (1980) the Higher Defence Course (1993) and Course 84 of the NATO Defence College. In 1995 he was appointed brigadier-general and professor at the Royal Military Academy. He lectures on Military Operational Management. Since 1996 he is chief editor of the 'Military Spectator' (founded 1832).

Mr. Chuck De Caro is President & Founder, AEROBUREAU Corporation. He is the creator of STARS (Strategic Television Airmobile Reports-via-Satellite) TV news system, TESA (Television Enhanced Situational Awareness) military C3 STARS variant. He is the developer of the SOFTWAR strategic methodology. He has broad experience in broadcast management, technology integration, airborne remote sensing, and market development. He demonstrated numerous platforms like the all-up AB-1 aircraft with 4 TV edit/director systems, with SLAR, SLOS, FLIR, & video inputs, integral RPV systems and real-time global video links. He designed World's 1st Satellite News Gathering Remotely Piloted Vehicle (rocket-launched, dual-camera, downlinked & mixed with ground video inputs & graphics; uplinked to Ku-band satellite; turnaround to C-Band satellite, illuminating North, South America, Europe in real-time. He is a consultant to numerous government agencies and private companies. He serves as a lecturer to the National Defense University, Senior Information Warfare Course, and Basic Information Warfare Course, all in the USA. He is also is an adjunct lecturer in Information Warfare at the School Of Information Warfare and Strategy of the National Defense University. He is contributing author of the books, "Cyberwar" and "Cyberwar 2.0." He served with 20th SFGA.

Major General Jose Gardeta was born in Barbastro (Spain), on 23 November 1940. He joined the Spanish Military Academy (Army) in 1960 and was promoted to Lieutenant in 1964. He spent most of his carrier in the ranks of Lieutenant, Captain and Major in command positions of light Infantry Platoons, Companies and Battalion in different mountain and airborne units. From 1984 to 1987 was assigned to the Spanish Embassy in Washington DC (USA) as Assistant Military Attaché. In 1987 he was promoted to Lt. Col. and assigned to the MoD in the Directorate for Defence Policy. From 1990 to 1992 was appointed as an augmentee to the International Staff, NATO HQ as a member of the Rapid Reinforcement Planning Cell, contributing to the production of the document "The new concept of reinforcement", still in place in today's NATO doctrine.
In February 1992, he was promoted to Colonel and from this date he served as the first Assistant Military Delegate to the Spanish Representation to the WEU. In December 1994, he was nominated as Chief of Staff for the Military Command of the Balearic Islands. In December 1996, he was assigned to the CHOD's Joint Staff as Chief of the Political Military Branch in Plans and Policy Division. Since March 20,1997 until November 1997, he

contributed to SFOR as CJ1 Chief in SFOR HQ, Sarajevo (BiH). On 3rd April 1997 he was promoted to Major General.At its meeting on 10 Jul 1997, the NATO Military Committee elected MG Gardeta to the post of Deputy Assistant Director, IMS, Operations Division, taking over his new position in November 1997. General Gardeta has participated in numerous qualification courses nationally, in NATO and in allied countries. He holds several national, NATO and allied nation's commendations.

Dr Adam Cobb has served in the military and in several government posts in Australia and the United States, and has advised numerous public and private sector organisations. A former officer in the Royal Navy (UK), Dr Cobb has worked in the Congressional Liaison Office of the Australian Embassy in Washington DC, and on the staff of a member of the United States Congress. He has held a number of prestigious academic Fellowships at the following international institutes: the Institute of Advanced Studies, Australian National University; the RAND Corporation in Washington DC; and the University of Amsterdam. In 1998 he was appointed to the Australian Parliamentary Fellowship by the Speaker of the House of Representatives and the President of the Senate to write a book on the future of Australian defence spending and its relationship to the deteriorating strategic outlook. He is currently a senior defence adviser to Senators and Members of the Australian Parliament. He has also authored several major parliamentary research papers on various aspects of Australia's national security, including the only open-source risk assessment of the National Information Infrastructure. Dr Cobb's PhD, from Cambridge University, is a history of changes in the concept of security.

Bgdr General Dipl. Ing. Alois Forstner-Billau joined the AAF in 1958 and left the Military Academy in 1962as a Lieutenant. From 1964-1972 he studied at the Technical University, Vienna, for his Masters in EEE. From 1972-1987 he went through several command and staff positions. In 1987 he was promoted to Bridadier General. From 1992-1997 he was Head of the Informatics Division and MoD Representative to the Federal Board of IT experts within the Public Administration. Since 1998 he serves as the Official in Charge for interoperability in IT for the Chiefs of Defence, Austria

Lieutenant Colonel Félix Faucon served, at the time of writing of this article, at the *Çentre d'Etudes et de Prospective de l'Etat-Major de l'Armée de Terre* (Centre for Strategic Studies of Staff of the French Army). Without presenting an official position, his statement reflects the current opinions within the French Army in relation to the information war. The paper is based on studies in which the author personally took part. The (now) Colonel Faucon serves as the *Chef de Corps du 2ème RA*, in Landau, Germany.

Henrik Friman is a He holds degrees in Engineering (Computer Sciences), Economic Science and Business Administration. He has been appointed as Principle administration Officer in the Armed Forces Headquarters, Plans and Policy Department as a civilian to develop and improve a new command and control structure in the Swedish Armed Forces. He was assigned as a Department Director at the Wargaming Centre, responsible for modelling and simulation for civilian elements in crisis- and wargames. Presently he is a full-time

Researcher of The Swedish National Defence College, Department of Operational Studies, in the area of C2 at the Military Joint Operational level. His special interest is in the area of strategic management.

Mr Friman is a member of the Committee for the Swedish Defence Scientific Society, and a member of the board of AFCEA, Stockholm Chapter.

Colonel (Oberst i Gst) Edwin Hofstetter was born on April 19, 1927. After obtaining his degree as Diplom-Ingenieur he began a career as artillery Officer. He followed a two-year education. At the Department of Military Sciences of the Eidgenösische Technische Hochschule at Zürich. As a Captain he commanded from 1955 a howitzer Battery and commenced his General Staff Officers training. He in following years served in several command and staff Officer's positions. In 1971-'72 he studied at the US Army General Staff College, Fort Leavenworth. He commanded several Officers's and enlisted artillery schools and spent the final five years of his career as commander of the Artillery training unit at Frauenfeld. He retired at the end of 1985 and accepted for the following ten years position of Chie-editor of the military magazine 'Schweizer Soldat'. During five years he was president of the Vereinigung der Redaktoren Schweizerische Militärzeitschriften (VRSMZ). He was also vice-president of the European Military Press Association (EMPA).

Eric Luiijf, M.Sc.Eng. is a principal consultant and programme co-ordinator on Information Operations and Information Assurance at the TNO Physics and Electronics Laboratory (TNO-FEL) in the Netherlands. He graduated at the Mathematical Department of the Technical University of Delft in 1975. He has written numerous articles and papers on the topics information security, information assurance distributed interactive simulation, and telematics. He is the Netherlands representative in the NATO RTO/IST/Task Group 3 on Information Assurance and contributes as technical expert to the development of the NATO directive on the secure interconnection of NATO networks to other networks.
Eric is the co-author of a Dutch book on Internet security and has contributed to two Internet RFC's on best security practices for system/network administrators as well as users of the Internet. He is one of the authors/reviewers of the German-Netherlands study on Information Operations and was responsible for TNO's contributions to that study.

Heinrich Matthee was born on 14 January1964 at Cape Town, South Africa. He holds degrees as BA (Law) and LL. B., BA Honours in Strategic Studies and a Masters in International Security (UK). He served as a Prosecutor and District Court Judge 1989-1997, senior researcher at Centre for Military Studies, University of Stellenbosch 1997-1999.
His research interests are Information Warfare and African conflicts.

Drs. M.V. (Max) Metselaar is a lecturer at the Royal Netherlands Military Academy. He studied Political Science at the Vrije Universiteit of Amsterdam and at the Royal University of Amsterdam. He has published a book on Political Decision Making (as co-editor) as well as various articles on surprise attacks, crisis decision making and leadership. His Ph.D. research is focused on the problem as to what extent dilemmas, and denial and avoidance of political leaders explains lack of preparedness despite early warnings.

Lieutenant Colonel (RNLAF) Albert R. Mollema joined the Air Force in 1964 as an enlisted. After graduating from the Hogere Technische School, Haarlem, as an Electronics Engineer, he started an officer's career. In 1977 he was trained in the USA as an Electronic Warfare Officer (EWO). From 1978 till 1981 he was a member of the Multinational Operational Test & Evaluation Team for the F-16, where he served as test engineer for EW systems. He then served in various EW positions in The Netherlands, including Chief EW Section of the Airstaff. In 1992 he joined the staff of the staff of the Supreme Allied Commander Europe in Mons, Belgium, where he was a Staff Officer responsible for EW and C2W matters. In early 1996 he was deployed to Bosnia and Croatia where he served as a member of the Allied Implementation Force (IFOR). Since 1997 is a lecturer at the Royal Netherlands Military Academy, lecturing Air Power Doctrine and Information Warfare.

Lieutenant Colonel (RNLAF) mr.drs. K.F. (Karl) Muusse lectured Military Law at the Royal Netherlands Military Academy (RNLMA) from Spring 1998 till Autumn 1999. He graduated from the RNLMA in 1985. After being commissioned he served for five years as a personnel Officer at several RNLAF Airbases. From 1988 to 1993 he read Law as well as International public Administration at the University of Leyden. After finishing his studies he worked for five years as a legal advisor in the Staff of the Commander-in-Chief of the RNLAF. Since October 1999 he serves as senior contract manager in the Staff of the commander-in-Chief of the RNLAF.

Richard Parker

Dr George J. Stein (BA, Assumption College, MA, Pennsylvania State University, and PhD, Indiana University) is director, International Security Studies Core and professor of European Studies at the Air War College, Maxwell AFB, Alabama. Before joining Air University in 1991, Professor Stein had taught in the School of Interdisciplinary Studies, Miami University, since 1977. He was active in SPACECAST 2020 and continues his research in information warfare.

Dr W. (Willi) Stein is a Senior Scientist and Consultant in the field of Information Systems and Human Factors at the Research Establishment for Applied Sciences (FGAN) in Wachtberg (near Bonn), Germany. He graduated in Information Technology from the Technical University of Aachen and wrote a doctoral dissertation on modeling human operator behavior in vehicle and process control. He conducted various theoretical and experimental studies in the field of human-machine systems as well as remotely piloted vehicles (RPV), wrote more than 50 conference presentations and articles, and lectured

Human Factors at the University of Bochum. His current studies include issues of Information Assurance and Information Warfare. He is a German Delegate of the NATO/RTO Task Group on Information Assurance (TGIA), started in 1998.

Richard Szafranski (BA, Florida State University, MA, Central Michigan University) is a partner in Toffler Associates. His assignments while on active duty included staff positions in the headquarters of Strategic Air Command, North American Aerospace Defense Command, and Air Force Space Command. He commanded B-52 units at the squadron and wing levels and was also the base commander of Peterson AFB, Colorado. Before his retirement from active duty as a colonel in 1996, he was the first holder of the Chair for National Military Strategy at the Air War College, Maxwell AFB, Alabama. Szafranski is the author of many writings on military strategy and operational art that have appeared in *Airpower Journal, Parameters,* US Naval Institute Proceedings, *Joint Force Quarterly, Military Review, Naval War College Review,* and *Strategic Review*. He is a graduate of Air Command and Staff College and Air War College.

Mr Tiit Romet just recently retired as a Defence Scientist from Canada's Department of National Defence. In his last role as Group Head, Scientific Intelligence and Emerging Technology, he was actively involved in the development and introduction of Information Operations into the Canadian Forces. He was a member of the Expert Advisory Group on IO for the Privy Council, a member of numerous inter- and intradepartmental committees on IO and represented Canada at numerous international meetings. He currently works as a consultant and Senior Associate and Director, S&T Intelligence for Ibis Research Inc., a competitive intelligence firm.

Commodore (Royal Navy, UK) Patrick Tyrrell joined the Royal Navy as an Instructor Officer in 1976. He qualified as a submariner and a sonar specialist. He served in the Defence Intelligence Staff from 1982 to 1985. Promoted to Commander in 1987 he attended the Joint Service Defence College in 1988 before taking up an appointment on the staff of the Supreme Allied Commander Europe in Mons, Belgium. His tasks included development of the mechanism of successful implementation of CFE within NATO and the NATO equipment transfer programme. He was awarded the Order of the British Empire for this work.
In 1991, he was appointed back to into the MoD to work on UK Defence Policy matters. Promoted Captain in 1992 he was appointed Assistant Director (CIS) Policy. Among other things he was involved in the development of the Joint Command Systems Initiative and a number of studies, including the development of the UK's policy towards Information Warfare.
He attended The Royal College of Defence Studies in 1996 before taking up an appointment as Commander, Defence Intelligence and Security School in 1997. He assumed the post of Deputy Chief Executive and Director of Operations at the Defence Communications Services Agency in March 1999.
Commodore Tyrrell holds degrees in chemistry (Oxford) and law (London).

Maarten Veltman is an information security consultant and research engineer at the TNO Physics and Electronics Laboratory (TNO-FEL) in The Hague, the

Netherlands. His field of expertise includes network security topics such as, boundary protection devices and intrusion detection. He is responsible for the TNO-FEL Red Team activities.

LIST OF ABBREVIATIONS

ADP	Automated Data Processing
ANSIR	Awareness of National Security Issues and Response
ANAO	(AUS) Australian National Audit Office
ASDSC	(AUS) Australian Strategic and Defence Studies Centre
ASIM	Automated Security Incident Measurement
CA	Civil Affairs
CEC	Co-operative Engagement Capability
CAAP	(US DoD) Critical Asset Assurance Program
CERT	Computer Emergency Response Team
CESA	(US) Computer Electronic Security Act
CCD	Camouflage, Concealment, and Deception
CCM	Communication Counter Measures
CCU	Computer Crime Unit
CIAO	(US) Critical Infrastructure Assurance Officer
CICG	(US) Critical Infrastructure Coordination Group
CIMIC	(NATO) Civil-Military Interface and Co-operation
CIP	Critical Infrastructure Protection
CIPU	Critical Infrastructure Protection Unit
CIS	Communications and Information System
CITAC	(US FBI) Computer Investigation and Infrastructure Threat Assessment Center
CNA	(NATO) Computer Network Attack
CND	(NATO) Computer Network Defence
COMINT	Communications Intelligence
COMPUSEC	Computer security
COMSAT	Communications satellite
COMSEC	Communications Security
COP	Common Operational Picture
COTS	Commercial-off-the-shelf
CYW	Cyber(netic) Warfare
C2	Command and Control
C2CS	(NATO) Command and Control Communication System
C2IS	(NATO) Command and Control Information System
C2W	Command and Control Warfare

C3 (1)	Command, Control and Communications
C3 (2)	(NATO) Consultation, Command and Control
C3CM	Command, Control and Communications countermeasures
C3I	Command, Control, Communications and Intelligence
C3ISR	Integrated Control, Communications, Intelligence Surveillance and Reconnaissance
C4D	Chaos, Catastrophe, Confusion, Computers and Deception
C4I	Command and Control, Communications, Computers, Intelligence
C4ISR	Command and Control, Communications, Computer Intelligence, Surveillance and Reconnaissance
DARPA	(US DoD) Defense Advanced Research Projects Agency
DASD	Deputy Assistant Secretary Department
DBS	Digital Broadcasting System
DCFL	Defense Computer Forensic Laboratory
DEII	Defense Essential Information Infrastructure
DEW	Directed Energy Weapons
DIAP	(US DoD) Defense-wide Information Assurance Program
DII	Defense Information Infrastructure
DISA	(US DoD) Defense Information Systems Agency
DoD	Department of Defense
DoDD	(US) Department of Defense Directive
DOS	Denial-of-Service
DSB	(US) Defense Science Board
EA	EW - Electronic Attack
EC	Electronic Combat
ECCM	Electronic Counter-Counter Measures
ECM	Electronic Counter Measures
EFT	Electronic Funds Transfer
EEI	Essential Elements of Information
EIW	Economical Information Warfare
ELINT	Electronic Intelligence
EM	Emergency Management
EMCON	EMissions CONtrol
EMP	Electromagnetic Pulse
EO	Executive Order
EO/IRCM	Electro-optical/Infrared Counter Measures
EP	EW - Electronic Protection
EPM	EW - Electronic Protection Measures

ES	EW - Electronic Support
ES	Electronic warfare Support
ESM	Electronic (warfare) Support Measures
EW	Electronic Warfare
FISINT	Foreign Instrumentation Signals INTelligence
GAO	(US) Government Accounting Office
GCCS	(US DoD) Global Command and Control System
GII	Global Information Infrastructure
GPS	Global Positioning System
GSM	Global System for Mobile Communications
HackInt	Hackers Intelligence
HERF	High Energy Radio Frequency
HPM	High Power Microwaves
HUMINT	Human Intelligence
I3	Information, incursion, impediment
IA	Information Assurance
IATF	Information Assurance Task Force
IAP	(US DoD) Infrastructure Assurance Program
IBDA	Information Battle Damage Assessment
IBW	Intelligence-based Warfare
IC2	Inverse Command & Control (unravel and destabilise adversary C2)
ICT	Information and Communication Technology
ID	Information Dominance
IETF	Internet Engineering Task Force
IITF	(US) Information Infrastructure Task Force
ILS	Instrument Landing System
IMINT	Imagery Intelligence
Info Ops	Information Operations
IO	(US) Info Ops (same abbreviation as International Organisation)
INFOSEC	Information systems security
IPB	Intelligence Preparation of the Battlespace
IPTF	(US) Infrastructure Protection Task Force
IRT	Incident Response Team
ISAC	(US) Information Sharing and Analysis Center
ISDN	Integrated Services Digital Network
ISSB	(US) Information Systems Security Board
IW	Information Warfare (xinxi zhangzheng)
IWAAS	Information Warfare Attack Assessment System

IW-C2W	Information Warfare topic area Command and Control Warfare
IW-D	Defensive Information Warfare
IW-EM	Information Warfare topic area Emergency Management
IW-EW	Information Warfare topic area Electronic Warfare
IW-Infra	Information Warfare topic area Infrastructure Warfare
IW-O	Information Warfare–Offense
IST	Information Systems Terrorism
IT	Information Technology
J-2	Intelligence Directorate of a joint staff
J-3	Operations Directorate of a joint staff
J-6	C4 Systems Directorate of a joint staff
JCS	(US) Joint Chiefs of Staff
JIC	Joint Intelligence Center
JOIT	Joint Operational Tactical System
JP	(US) Joint Publication
JTF	Joint Task Force
JTIDS	Joint Tactical Information Distribution System
JV 2010	Joint Vision 2010 (US DoD Publication)
LOAC	Law of Armed Conflict
LSS	Survivability of large scale systems (DARPA/ITO program)
MAD	Mutual Assured Destruction
MASINT	Measurement and Signatures Intelligence
MEDII	Minimum Essential Defence Information Infrastructure
MEII	Minimum Essential Information Infrastructure
MEF	Marine Expeditionary Force
MIE	Military Information Element
MISSI	(US) Multilevel Information Systems Security Initiative
MoD	Ministry of Defence
MOOTW	Military Operations Other Than War
MT	Management Team
NASA	National Aeronautics and Space Administration
NATO	North Atlantic Treaty Organisation
NCW	Network Centric or NetCentric Warfare
NDU	(US) National Defense University
NIAP	(US) National Infrastructure Assurance Partnership
NII	National Information Infrastructure (e.g. US and Australia)
NIPC	(US) National Infrastructure Protection Center
NMO	Non-Military Organisation

NRIC	(US) Network Reliability and Interoperability Council
NRO	(US) National Reconnaissance Office
NSA	(US) National Security Agency
NSTAC	(US) National Security Telecommunications Advisory Committee
OASD	(US) Organization of the Assistant Secretary of Defense
OODA	Observation-Orientation-Decision-Action
OPSEC	Operations Security
OSCINT	Open Source Intelligence
PCCIP	(US) President's Commission on Critical Infrastructure Protection
PIRA	Provisional Irish Republican Army
POTS	Plain Old Telephone System
PSO	Peace Support Operations (NATO)
PSPA	Peace Support Psychological Activities (NATO)
PSTN	Public Switched Telephone Network
PSYOPS	Psychological (Warfare) Operations
PSYW	Psychological Warfare
RADINT	Radar Intelligence
RBPR	Reversed Business Process Reengineering
REC	Radio Electronic Combat
RII	Relevant Information and Intelligence (Info Ops component)
RIP	Recognised Information Picture
RMA	Revolution in Military Affairs (junschi geming)
RMB	Revolution in Military Business
RMP	Risk Management Program
ROE	Rules of Engagement
SCADA	Supervisory Control and Data Acquisition (energy distribution)
SIGINT	Signals Intelligence (ELINT and COMINT)
SID	Strategic Information Dominance
SIW	Strategic Information Warfare
SKI	(GE) Schutz kritischer Infrastrukturen
TELINT	Telecommunications Intelligence
TEMPEST	Transient Electro-Magnetic Pulse Emanation Standard
TIW	Transnational Infrastructure Warfare
TW/AA	Technical warning/Attack assessment
WMD	Weapons of Mass Destruction
Y2K	Year 2000 (millennium)

URLography

Info Ops - general

http://www.afcea.org/ and http://www.us.net/signal/
AFCEA regularly publishes articles about Information Operations, Intelligence and C2 in their monthly Signal.

http://www.aracnet.com/~gtr/archive/info_war.html
K.Anderson's bibliography of Information Warfare and Infrastructure Vulnerability Documents

http://huachuca-usaic.army.mil/
US Army Intelligence Center: publications and doctrine

http://www.aipio.asn.au/links.htm
Australian URLography with links to many Intelligence resources in the world

http://www.dodccrp.org/bostoc.htm
Lessons From Bosnia: The IFOR Experience (electronically available book)

http://www.dodccrp.org
US DoD C4ISR Cooperative Research Program with Network Centric Warfare resources

http://www.ndu.edu/inss/books/diw/index.html
Defensive Information Warfare publication by the US National Defense University (NDU)

http://www.jya.com
Daily updated website with international articles and news on cryptography, information warfare, Echelon and intelligence

http://www.rand.org/publications/MR/MR880/contents.html
In Athena's Camp: Preparing for Conflict in the Information Age. John Arquilla and David Ronfeldt

http://www.ndu.edu/inss/siws/cont.html
Sun Tzu Art of War in Information Warfare, electronic book with a collection of articles

http://www.infowar.com
Winn Schwartau's Information Warfare and security site with many links and article

http://www.informatik.umu.se/~rwhit/IW.html
Randy Whitaker's IW webpages at the Swedish Umeå Universitet

Info Ops resources

http://www.tno.nl/instit/fel./infoops
TNO-FEL's URLography on IW, Info Ops, Information Assurance and InfoSec

http://www.psycom.net/iwar.1.html
Institute for the advanced study of information warfare (IASIW)

http://www.twurled-world.com/Infowar/Update2/cover.htm
World wide overview of Information Warfare resources based upon a webscan analysis

http://cryptome.org/fm100/fm100-6.htm
US Field Manual 100-6: Information Operations

http://www.dtic.mil/doctrine/jel/c_pubs2.htm
US Joint Publication 3-13: Joint Doctrine for Information Operations, 9 October 1998
US Joint Publication 3-54: Joint Doctrine for Operations Security, 24 January 1997

http://www.dtic.mil/doctrine/jv2010/jvpub.htm
US Joint Vision 2020

Info Ops Legal Aspects

http://www.usdoj.gov/criminal/cybercrime
US Dept. of Justice Computer Crime and Intellectual Property Rights - articles and resources

http://www.dodccrp.org/iwilindex.htm
Information Warfare and International Law by L.T. Greenberg, S.E. Goodman, K.J. Soo Hoo. NDU

http://www.cs.georgetown.edu/~denning/infosec/DOD-IO-legal.doc
Long publication on International legal aspects of Information Warfare (Denning and Baugh, 1999)

http://www.leglnet.com/libr-inwa.htm
Information Warfare Law Library

Information Assurance

http://www.cesg.gov.uk
CESG: UK Communications-Electronics Security Group

http://www.itd.nrl.navy.mil/ITD/5540/main.html
US Navy Center for High Assurance Computer Systems - R&D

http://cve.mitre.org
Common Vulnerabilities and Exposures database by MITRE

http://www.robertgraham.com/pubs/network-intrusion-detection.html
Network intrusion detection systems frequent asked questions

http://www-rnks.informatik.tu-cottbus.de/~sobirey/ids.html
Overview of and links to over 80 intrusion detection systems

http://www.clark.net/pub/roesch/public_html/secinfo.html
Intrusion detection papers and tools by Martin Roesch

http://jedefense.com
Journal of Electronic Defense, EW oriented articles

http://www.jya.com/soft-tempest.htm
Interesting article describing soft-tempest

http://niap.nist.gov/index.html
US National Information Assurance Partnership (NIST and NSA)

Infrastructure

http://www.aph.gov.au/library/pubs/rp/1997-98/98rp18.htm
http://coombs.anu.edu.au/~acobb/X0016_Australias_Vulnerabi.html
http://www.infowar.com/CIVIL_DE/civil_100497a.html-ssi
Thinking about the Unthinkable: Australian vulnerabilities to information attack by Dr./ Adam Cobb

http://www.aracnet.com/~gtr/archive/index.html
Kent Anderson's bibliography of Information Warfare and Infrastructure Vulnerability documents

http://www.iwar.org
CIWARS: Journal of Infrastructural Warfare

http://www.nipc.gov
NIPC: US National Infrastructure Protection Center

http://www.pccip.gov
PCCIP: US Presidential Committee for Critical Infrastructure Protection - PDD 63 and the PCCIP report

Information Security

http://www.cs.purdue.edu/coast/hotlist/

The COAST archive at Purdue University is probably the most complete archive of security-related links on the Internet.

http://www.tno.nl/instit/fel/infosec
Information security URLography maintained by TNO-FEL, a starting point for many information security related resources.

Hacking

http://www.attrition.org/mirror/attrition
Mirror site that contains an up-to-date archive of defaced websites, their defaced webpage and their original

http://www.ccc.de
CCC: German hackersgroup "Chaos Computer Club"

http://www.l0pht.com
L0PHT overview of hacks, tools and articles

http://www.tno.nl/instit/fel/infosec
Hacking and scaring resources URLography maintained by TNO-FEL

Computer Emergency and Incident Response

http://www.cert.org
CERT® Coordination Center: guidance on handling an incident, incident reports and advisories

http://ciac.llnl.gov/
CIAC: US DoE Computer Incident Advisory Capability, up-to-date security bulletins, security tools, information about hoaxes and other information resources

http://www.assist.mil/
DOD-CERT: US DoD computer emergency response team announcements and information resources

http://www.first.org
FIRST: Forum of Incident Response and Security Teams

http://www.telstra.com.au/info/security.html
TELSTRA: Australian Computer and Network Security Reference Index