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.

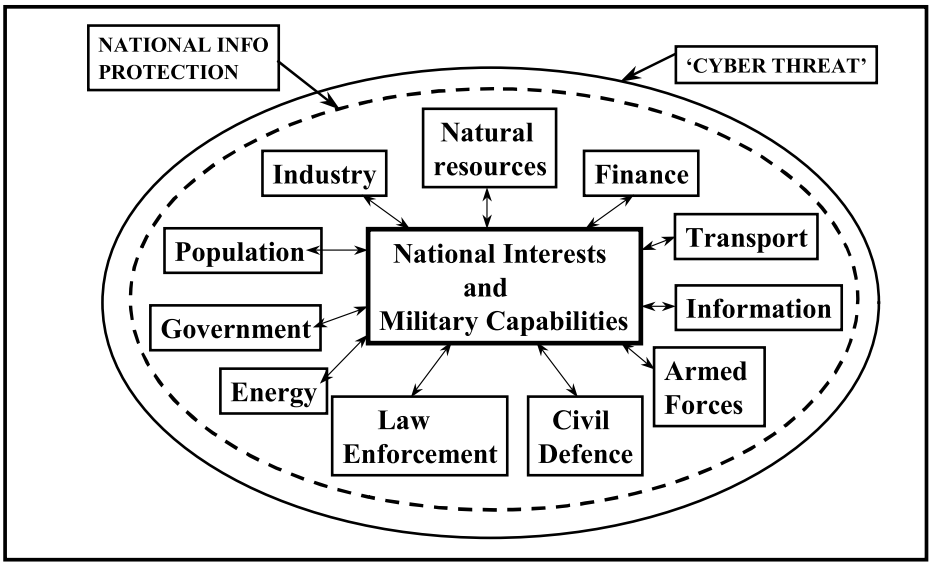

Figure 1: Risks in a Civil / Military environment

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.

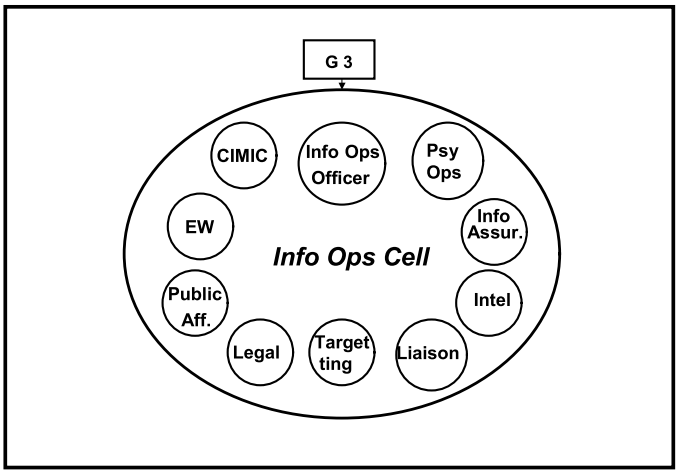

Figure 2: Composition of an Info Ops Cell (IOC)

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