Chapter 1 – INTRODUCTION

1.1 AIM OF SAS-057

The overall goal of RTO Task Group (RTG) SAS-057[1] was to contribute to an improved understanding and development of a coherent concept for analysis of information operations (Info Ops).

The group focussed its work on the following objectives:

- Develop a structured approach to the assessment of Info Ops;
- Identify analytical requirements to support Info Ops; and
- Review methods and tools for supporting Info Ops analysis.

1.2 BACKGROUND

During the recent work on the "Handbook on the Analysis of Smaller-Scale Contingency Operations in Long Term Defence Planning" [1], SAS-027 noted that Info Ops are likely to be one of the major instruments employed by a commander to achieve his campaign objectives in many types of smaller-scale contingencies[2]. However, SAS-027 did not cover information operations in its work, noting that there were no agreed definitions and that analytical methods in this area were immature. SAS-027 recommended establishing an exploratory team "to identify approaches to analysis of information operations".

SAS-057 took up the challenge to provide contributions to close the gap – both for definitions and for analytical methods. In contrast to SAS-027, SAS-057 chose not to focus on support of Long Term Defence Planning but to gain an overview on Info Ops analysis requirements in general and to provide recommendations for improved analysis.

For analysis support to operations, SAS-027 refers to the work of SAS-044 "Decision Support to Combined Joint Task Force and Component Commanders" [2]. The results from SAS-044 were available early enough within the working period of SAS-057 to provide a valuable foundation for the group's work.

With regard to Long Term Defence Planning, the group wishes to point to ongoing work on developing future concepts for the effects-based approach to operations including Info Ops, e.g. the MNE experiment series led by US JFCOM[3] and the related limited objective experiment series led by Germany: the Multi-national Information Operations Experiment (MNIOE) series[4].

---

[1] See Annex A for information on participants.

[2] Smaller-scale contingencies basically include any alliance operation that involves less than about 100.000 personnel.

[3] MNE = Multi-national Experiment, here: US-led experiment series for future concept development; see http://www.jfcom.mil/about/experiments/multinational.htm, visited 28 August 2005.

[4] For a short description of MNIOE, see e.g. the minutes of the 2005 annual meeting of the Multi-national Interoperability Council (MIC), http://www.jcs.mil/j3/mic/mic_docs/docs_aug05/MIC_2005_FinalReport_9Aug05.pdf (visited 16 August 2005), p. 29 f.

1.3 REDEFINITION OF THE STUDY OBJECTIVES

The original intent was to primarily focus on smaller-scale contingencies (SSC) including counter-terrorism. The findings of the group are, however, generic to an extent that they are applicable to all types of contingencies. Aspects of specific relevance for SSC are addressed where appropriate.

In the terms of reference for SAS-057, it is stated that "work is needed to close the gap between requirements and current capability for analytical support to Info Ops within NATO small-scale campaigns". Based on this rationale, the group saw the need to bring together, from within nations, individual views and information on requirements for analytical support to Info Ops as a basis to arrive at a coherent international perspective.

The focus of the study was therefore to identify requirements for Info Ops analysis in general and on a generic level, take a look at current national, multi-national and NATO practices, and develop recommendations to improve analysis support to Info Ops.

1.4 RATIONALE FOR INFO OPS ANALYSIS

Info Ops still have to be considered an evolving concept notwithstanding the fact that NATO and nations have started to work on Info Ops policies and doctrines from the mid 1990s[5], and that many operations of the last decade had billets assigned to Info Ops tasks. NATO released its first Info Ops policy in 1998, revised it in 2002 [4] with the next revision expected by the end of 2005, and is continuing to develop its Info Ops doctrine, AJP 3.10.

The lack of endorsed NATO doctrinal guidance has resulted in some ambiguity about what Info Ops should achieve and how Info Ops are integrated into planning, executing, and assessing military operations, and where responsibilities rest. A result of this ambiguity is that at present there seems to be limited demand for Info Ops analysis from the operational staff and, therefore, theoretical work relevant for the analysis of Info Ops receives little attention. Practical analysis for Info Ops is also rather limited.

For the purpose of this study, the group had decided not to use the current NATO definition for Info Ops from NATO's Info Ops policy MC422/1 [4] but rather base its investigation on a description for Info Ops that is oriented towards evolving developments in the course of NATO's transformation process (see also glossary at Annex B):

> *Info Ops are co-ordinated military activities within the information domain to affect information and information systems to achieve desired effects on will and capabilities of adversaries and others in support of mission objectives while sustaining own information and information systems.*

Assessment especially of effects on will involves many more dimensions than the assessments in the context of traditional military operations aimed at the attrition of an adversary force. Most of the effects on will are accomplished in the cognitive and social domains. Therefore, the assessments are characterised not only by a higher degree of complexity, but also by soft factors that are in most cases neither easily measured nor well founded in theory.

The results of this study shall contribute to improving awareness for the analytical requirements of Info Ops, supporting the development of analytical capabilities and promoting coherence in the analytical approach to Info Ops across the national, multi-national and NATO operational analysis community. This would move forward analytical support in providing assistance to force planning authorities, operational commanders and their staffs in the field.

[5] See Chapter 2 for more detail.

1.5 STRUCTURE OF THIS DOCUMENT

Chapter 2 summarises the results of an overview of current concepts, policies and doctrines for Info Ops that was undertaken to identify common aspects and differences in the various approaches from NATO and nations. A common understanding for Info Ops as a basis for the work in this study was achieved by developing a conceptual model for Info Ops (Chapter 3). This model served as a basis to derive requirements for analysis in support of Info Ops (Chapter 4). Chapter 5 summarises findings on current practice in Info Ops lessons learned processes and provides recommendations to improve both the processes and the essential empirical data basis. An overview of existing and evolving methods and tools to support Info Ops analysis is provided in Chapter 6. In Chapter 7, conclusions and recommendations as derived from the results of the study are summarised, while Chapter 8 contains some suggestions for follow-on research activities.

Chapter 2 – OVERVIEW OF CURRENT INFO OPS DOCUMENTS

A review of current concepts, policies, and doctrines for Info Ops and other relevant literature was made to:

- Obtain an overview of the conceptual understanding of Info Ops in NATO and nations;
- Identify common aspects and differences in the various approaches; and
- Provide a common understanding in pursuing this study.

Thus, the purpose of the review was to learn about the maturity of Info Ops doctrine and whether there are fundamental differences in the conceptual understanding of Info Ops throughout NATO and nations. Doctrine belongs to the fundamental baseline elements for education, training, and operations and should reflect the central issues which analysis should focus on.

The study group considered comparing doctrines as indispensable for learning about common and differing aspects of the various approaches to Info Ops that need to be taken into account when developing a conceptual model or when identifying requirements for Info Ops analysis, including data collection and supporting methods and tools.

2.1 BASIS OF THE REVIEW

The first Info Ops doctrine document that became openly available was the US Army Field Manual 100-6 in 1996. Since then, a considerable number of Info Ops-relevant documents have been released, and some have already been replaced by new releases. About 20 documents from 11 different countries and international organisations or projects were reviewed in this study (see table 1).[6] For documents that were not releasable to all group members (marked with an asterisk in the last column of table 1), a structured summary was available to the group[7].

The release dates of the reviewed documents range from 1998 until 2005. Taking into account that considerable changes in the political and military environment have occurred since 1998, three phases were identified:

- Before 2000: Info Ops documents released before 2000 reflect the national approaches to a new area of military activities of that time.
- Between 2000 and 2002: With several documents and the first NATO policy for Info Ops at hand, national considerations also take into account what has already been released. The second phase was extended to 2002 as most documents released in 2002 were drafted before 11 September 2001 and did not take into account the "War on Terrorism" and related changes.
- 2003 to date[8]: All Info Ops documents released in 2003 and later take into consideration the changed political and military environment after 11 September 2001.

[6] The study refers mainly to doctrine and policy documents currently in use. It also looked at some drafts currently under development to include an estimate of current developments, being aware that changes on the way to the final versions can be substantial. See also the result of WP 1: "Overview of Info Ops Documents" [5].

[7] For the Belgian, the German, and the EU documents, the summaries were prepared by a group member, for the Netherlands and Norway, contacts of these countries provided the information.

[8] Documents identified after March 2005 were not considered in the review.

Table 1: Info Ops Documents Reviewed for the "Overview of Documents"

Country / IO / project	Type(s) of document	Status / release date	Access restrictions[9]
Belgium	Doctrine [6]	Draft	Access only to BE*
Canada	Policy, doctrine [7, 8]	2004 ,1998	Policy avail. to RTG
Germany	Subconcept [9]	2005 (1st rel. 2002)	Access only to GE*
The Netherlands	Policy [10]	2001	Access only to NL*
Norway	Concept [11] Policy whitepaper [12]	2002 2003	Available to RTG Access only to NO*
Sweden	Doctrine [13]	2004	Available to RTG
United Kingdom	Doctrine [14]	2002	Available to RTG
United States of America	Joint / Army / Air Force doctrine [15, 16, 17] Draft joint doctrine [18]	1998 / 2003 / 2002 Draft	
NATO	Policy [4] Draft doctrine [19]	2002 Draft	Available to RTG
EU	Concept [20]	2003	Available to EU*
MNIOE[10]	Whitepaper (policy), CONOPS [21, 22]	Both 2004	Available to RTG

Since the purpose of this review was to compare current doctrine, documents that have been replaced by updated versions were not considered. Two of the reviewed documents were released in the first phase (US JP 3-13 [15] and CF Info Ops doctrine [8]), three in the second (NATO Policy MC 422/1 [4], US AFDD 2-5 [17], and UK JWP 3-80 [14]), and five in the third phase (US Army FM 3-13 [16], CF Info Ops policy [7], Perspective IO from Sweden [13], the German subconcept on Info Ops [9], and the EU concept [20]). In addition to this, the current drafts for one update (for US JP 3-13 [18]) and one new document (NATO AJP 3.10 [19]) were considered plus the policy and doctrine level documents from the Multi-national Info Ops Experiment (MNIOE) series [21, 22]. Additional information on the status of doctrine and policy development was available from Belgium, France, the Netherlands, Norway, Portugal and Switzerland.[11]

[9] If no restrictions are given, the documents were available from the internet. Documents marked with an asterisk were not releasable to all members of the group.

[10] The Multi-national Information Operations Experiment (MNIOE) experiment series is led by Germany and has participants from Australia, Canada, France, UK, and the US, plus participation from several other nations including Belgium, Portugal and Sweden. The documents reviewed for WP 1 have been superseded by the White Paper "Info Ops in Future Coalition Operations", version 1.7 and the CONOPS "Info Ops in Support of Effects-Based Operations", version 1.6, both released on 30 September 2005. In particular the common understanding of Info Ops as a coordinating and integrating function has evolved, and the respective MNIOE definition has fundamentally changed to reflect current developments in effects-based operations.

[11] Additional information from France (release of an Info Ops concept in March 2005 [23]) and Switzerland (framework for an Info Ops doctrine, final version expected by end 2005) were received after end of March and not included in the overview.

2.2 INFO OPS DEFINITIONS

The comparison of the definitions of the early phase (before 2000) shows that the approaches follow a common line of understanding with some differences: The US Joint definition suggests that Info Ops are a military tool, while the Canadian and the NATO[12] definitions emphasise the support of political and military objectives through Info Ops. Regarding the definitions of the second phase (2000 – 2002), the US Air Force follows the US Joint definition, referring primarily to the operational, rather technical aspects of Info Ops. In the NATO (MC 422/1) and the UK definition, the potential strategic role of Info Ops is reflected.

In the documents of the latest phase (since 2003), the definitions of the US Army (and the draft Joint definition), Germany, the non-NATO nation Sweden, and the MNIOE group do not refer to the NATO definition valid at the time of writing this report. The US definitions differ from the others by an explicit inclusion of core capabilities to be applied in Info Ops. A new development reflected in the Canadian, the Swedish, and the MNIOE definition is that it is not just own and adversary aspects but also "others" that have to be taken into account. It should be noted that following this work, NATO issued a new draft definition which also widens the applicability of Info Ops.

In summary, all documents follow the line of addressing Info Ops as a coordinating or integrating function. The definitions for Info Ops following the NATO line, as well as the Swedish, and the MNIOE definition, emphasise the coordinated employment of activities, while some of the US documents use the term integrated employment of capabilities. Most of the documents released in 2004 and 2005 describe Info Ops as (part of) effects-based operations (EBO), which is also reflected in the new definitions.

2.3 THE ROLE OF INFO OPS IN MILITARY OPERATIONS

Info Ops are not seen as a new activity or set of activities but rather a synergetic way to employ selected traditional and new military capabilities or activities. Older documents focus on the use of various activities or capabilities for offensive or defensive purposes. Several of the newer documents classify Info Ops into core, supporting, and related activities, while others distinguish influence activities, counter-command activities, and OPSEC.

All documents include EW, PsyOps, CNO, and OPSEC as military activities that can support Info Ops. The documents also refer to CIMIC, PI, and deception, but there are some differences of how they are to be included: in most cases, CIMIC and PI are explicitly excluded from Info Ops, but all of those documents postulate close coordination with CIMIC and PI activities. Sweden and the US refer to CIMIC / CMO and PI / PA as related activities.[13]

Differences were also observed for the role of Info Ops in military operations:

- A supportive role for Info Ops as an operational force multiplier is reflected, e.g. in the US Army doctrine [16] and in the Swedish document [13].
- A central role for Info Ops where Info Ops are embedded in a network of bidirectional relationships between military and non-military activities is given, e.g. in the Canadian and in the UK doctrines [8, 14].
- An integral role for Info Ops as a force effectiveness facilitator is presented, e.g. in the approaches of MNIOE [21, 22] or the draft of the US Joint doctrine [18].

[12] The definition of MC 422 (superseded by MC 422/1) was taken into account for completeness as at least one of the reviewed documents uses a definition based on the MC422 definition.

[13] Annex C gives an example of the wide spectrum of military capabilities / functions available to support Info Ops, using the classification of the UK JWP 3.80 [14].

The documents also differ in focus. Most address issues at the operational / tactical level and the technical / organisational level, with less than half offering coverage of the overall political approach and only a few of the recent documents addressing military strategic aspects in some detail (see Table 2).

Table 2: Levels Addressed in Info Ops Documents

	NATO [4]	US AF [17]	UK [14]	EU [20]	Canada [8]	US Army [16]	US JP dr.[18]	Sweden [13]	MNIOE [21]	NATO dr.[19]	Germany [9]
Policy level	X		X	X	X						X
Strategic level	X							X	X		X
Operational / tactical level	X			X	X	X	X	X	X	X	X
Technical / organisational level		X	X	X	X	X	X		X	X	

2.4 CONCLUSIONS

A comparison of conceptual approaches for Info Ops solely relying on a review of conceptual documents is not complete. The conceptual understanding of Info Ops reflected through the definitions and descriptions presented in the reviewed documents is just one step on the way to identify and understand common or different conceptual approaches. It should be noted that a full understanding of commonalities and differences requires a deeper analysis of additional information on the application and practical implementation of Info Ops which are generally not addressed in the reviewed documents and therefore beyond the scope of this review.

The scope of this study did not allow extensive research on the current status of practical implementation. However, a small survey addressing current practice of Info Ops analysis (see also Chapter 5 and [24, 25]) provided some insight on how Info Ops are currently applied in the field. The conclusions in this section are based mainly on the review of the documents but also take into account general trends derived from the survey.

The review revealed that differences in the early documents have greatly reduced over time indicating the emergence of a common understanding of Info Ops and their implications among nations. However, the convergence of the conceptual approaches only indicates the ongoing development towards a common understanding – there are still differences. One of the reasons is that there are culturally different approaches to military operations that are reflected in the national views on the role of Info Ops.

The various documents use “generic” terms such as *co-ordination*, *integration*, or *harmonisation* to define and describe the specific conceptual approaches. However, an intuitive understanding of those terms may vary from their defined meaning within the context of the respective documents. It should be noted that the terms mentioned above can have a (qualitatively) different meaning for individual nations, even in the same context, especially for aspects such as command & control relationships or directive authorities.

One of the common aspects in documents released since 2003 is that they increasingly refer to Info Ops as "effects-based operations in the information domain" designed to shape, through co-ordinated actions and effects, the information environment and thereby producing an operational advantage. For small-scale contingencies with a focus on operations other than war (OOTW), Info Ops can be expected to play a key role. Several documents emphasise that Info Ops provide non-lethal contributions to a military campaign.

The international strategic environment highlights that resolving or preventing future conflicts will increasingly involve a close coordination of all activities affecting the social, political and economic arenas as well as the traditional military battle space. In this context, the Info Ops contributions to influence the will and behaviour of adversaries or conflicting parties, and to affect the means they could use to implement their will, are strategically important.

The full integration of Info Ops in the overall context of military operations is a challenge that is addressed in most current Info Ops documents. Recent documents clearly show that a common understanding of Info Ops and its role in current and future conflicts is emerging. They also indicate that Info Ops fit with an effects-based approach to operations that has become a key element of the transformation process in NATO and many nations.

Chapter 3 – DEVELOPING A COMMON UNDERSTANDING OF INFO OPS

Developing a common understanding of Info Ops requires both theoretical and practical considerations. The study of policies and doctrines, in particular of their underlying conceptual approaches and with a view to research on the practical implementation of Info Ops, present a clear identification for the need of a shared understanding. The lack of an endorsed NATO Info Ops doctrine made it mandatory for the group to develop a shared understanding that the readers of this study should be able to follow. From the practical perspective of Info Ops, the current ambiguity led to the implementation of different Info Ops structures within the staffs of ACO, JFC HQs, CC HQs and even NATO HQs deployed in theatre.[14] Latest developments in NATO Info Ops doctrine suggest that it will attempt to resolve this issue.

Chapter 2 describes the theoretical consideration. The variety of Info Ops concepts indicates a development towards a common understanding while national approaches still show important differences. Developing a conceptual model (CM) for Info Ops proved to be a helpful process for elaborating a shared understanding as well as supporting the other tasks of this study – namely deriving analysis requirements (see Chapter 4), requirements for lessons learned (Chapter 5) and requirements for methods and tools (Chapter 6) in support of Info Ops analysis.

As a starting point for development of the CM and the identification of analytical requirements, the group agreed on the following views to be taken into account:

- **Info Ops process view** addressing the internal processes and tasks carried out within an Info Ops organisation (in the widest sense) and how these processes are linked within the operation.[15]
- **Info Ops effects view** addressing Info Ops and the environment to be affected by them, with particular emphasis on the effects on targets and target audiences, intended or unintended side-effects, and Info Ops activities undertaken by adversaries and others.
- **Resource view** addressing resources in terms of knowledge, expertise, and analytical tools required to support Info Ops tasks and processes.

The description of Info Ops given in Section 1.4 reflects the common understanding of the group members that Info Ops development is part of NATO's transformation process. Thus, Info Ops should be considered to be an integral part of an effects-based approach to operations. Therefore, the group decided to reflect this in this study in order to provide coherence with emerging effects-based concept development.

Being aware that there are several descriptions of effects-based operations (EBO), for the purposes of this study, the group has adopted the philosophy of the evolving multi-national concept of EBO as developed by the MNE community[16]. This approach considers EBO as operations focussed on influencing or changing system behaviour or capabilities using the integrated application of selected instruments of power in order to achieve policy aims.

[14] For example, JALLC reports indicate the TIC structure at ISAF HQ as very effective and advantageous and it should be considered for inclusion in the NATO Info Ops doctrine.

[15] It should be pointed out, however, that the study group did not undertake to analyse the organisational aspects such as headquarters organisation, operational responsibilities, and lines of command involved in Info Ops.

[16] See also footnote 3.

3.1 STARTING POINT FOR A MODEL FRAMEWORK

At the beginning of the work of SAS-057, it became apparent that there were various potential starting points and perspectives from which to construct a conceptual model (CM) of Info Ops. The "area of responsibility" for Info Ops is the information domain being an integral part of the operational environment which can be seen as a complex adaptive system. Elements in the information domain of primary interest for Info Ops are information systems which can be described as socio-technical systems consisting of sub-systems, particularly those for the efficient provision of information and communication. Socio-technical systems are characterised by the interrelations and interactions of humans and technical / organisational systems as well as their behaviour. Therefore, Info Ops address a broad spectrum of scientific domains and analytical problems.

Such a broad analysis spectrum cannot be covered by a single model or exclusively by one specific type of models. Rather, a set of partially overlapping and mutually supporting complementary models of different types is required. These models should allow for comprehensive Info Ops analysis from different perspectives and be based on expertise from various scientific domains. The following list outlines some of the areas where CMs may yield insight:

- Operations across the OOTW spectrum;
- Concepts of operations;
- Efficient planning, execution, and assessment processes;
- Organisational and communication requirements for supporting processes and operations;
- Operational analysis (OA), especially to establish measures of performance and effectiveness;
- Coalition requirements for specialisation and synchronisation;
- Intelligence requirements, both theatre and strategic;
- Lines of development and balance of investments;
- Simulation and war gaming; and
- Interdependencies and de-confliction of all aspects given above.

For the purpose of this study, the CM of Info Ops is primarily used to provide a common basis of understanding to support the work of the study, especially the identification of analysis requirements of Info Ops. The model described in the following sections is tailored to this purpose.[17]

3.2 MULTI-LAYER MODEL

The group agreed to develop a "multi-layer" model that features a top-down structure describing the group's understanding of Info Ops and the underlying processes on each layer. The layers of the model represent different levels of abstraction and detail (see Figure 1).

The first layer provides a high-level overview of Info Ops processes comprising planning, execution, and assessment. The second layer describes the planning process in more detail addressing the various steps involved. For the purpose of identifying Info Ops specific analysis requirements, it is sufficient to limit the consideration to planning (as depicted in Figure 1) as all Info Ops relevant aspects of the execution and assessment processes that require analytical support are inherently covered by corresponding sub-

[17] For a detailed description of the conceptual model approach, see WP 2/4: "Conceptual Model for Info Ops / Analysis Requirements" [26].

processes addressed in planning.[18] The third layer addresses certain process steps and highlights related Info Ops specific analysis requirements.

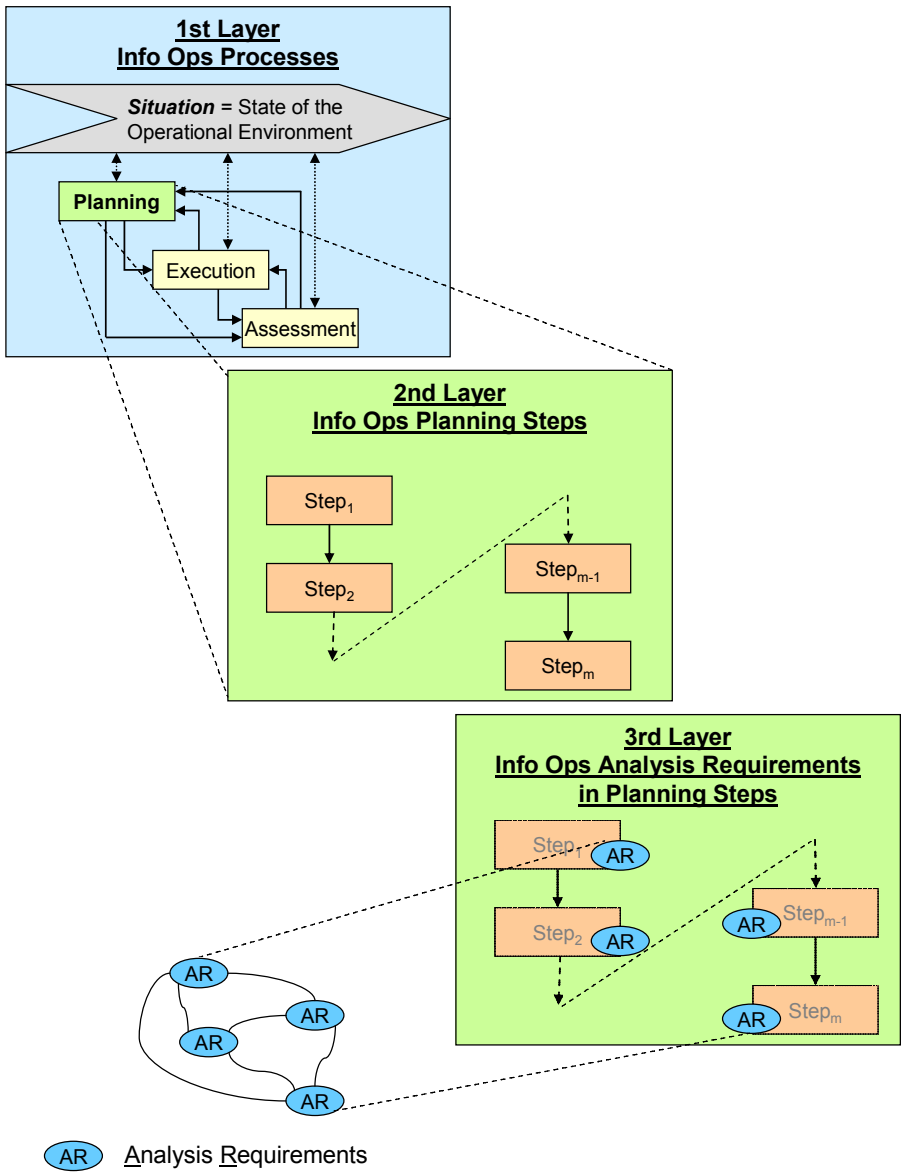

Figure 1: Multi-Layer Approach for a Conceptual Model for Info Ops Analysis.

3.2.1 The First Layer

Figure 2 shows the top-level specification of the 1st layer of the CM which explicitly reflects the effects-based description of Info Ops process given above. Figure 2 considers a situation in which the decision has been made to employ the military in support of a political aim. The situation at a given point (n) in time is represented by "State* (n)" including the states of all parties concerned (own, coalition, adversaries, others) and the relevant operational environment. The given (current) situation is a quasi baseline for assessing effects caused by subsequent actions.

[18] While the actual execution of Info Ops is not expected to be supported analytically, both planned and executed Info Ops actions need to be documented, preferably in quantitative terms, to support assessment and provide the basis for deriving "lessons learned" and empirically based cause-effects relationships.

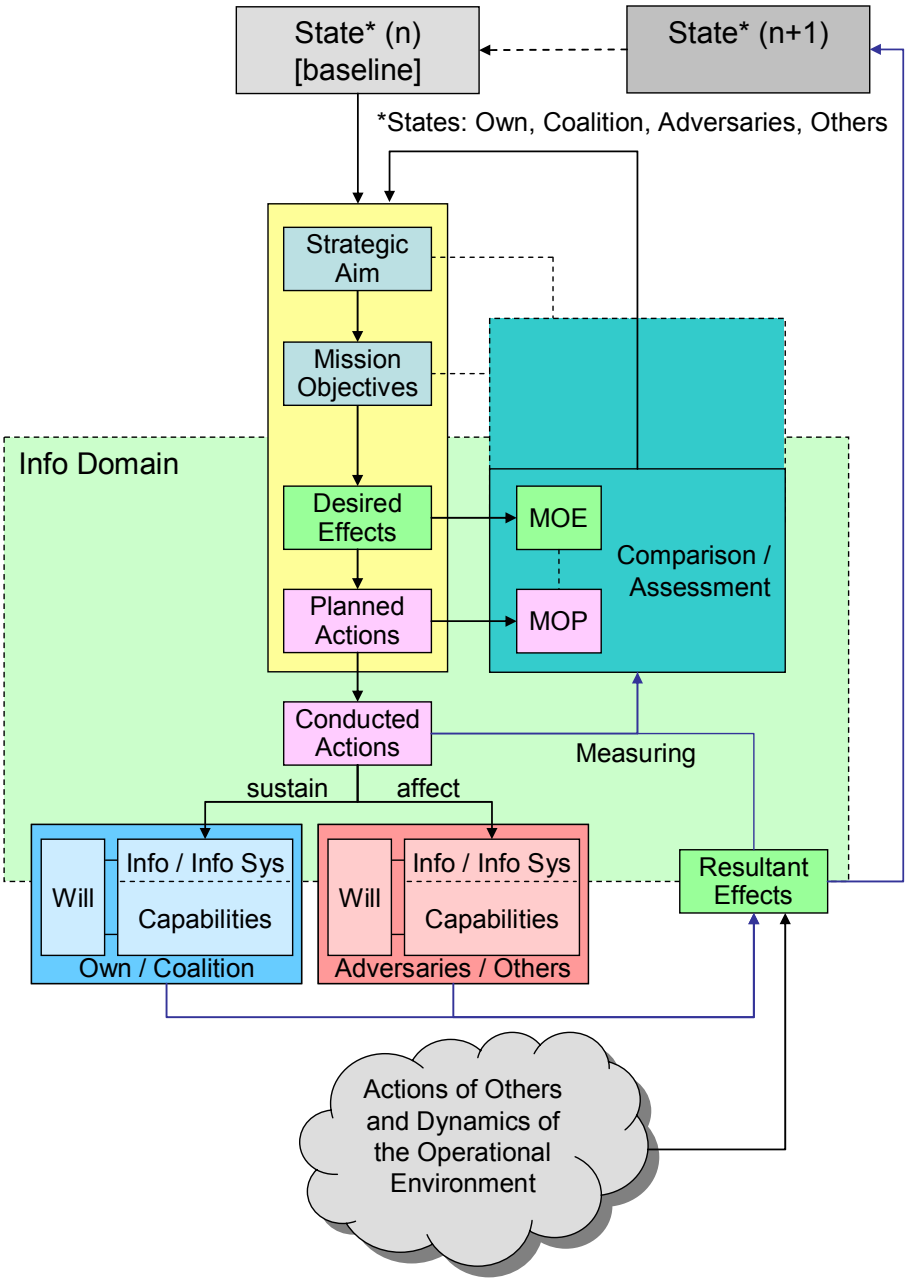

Figure 2: A Conceptual Model for Info Ops Analysis – First Layer.

The military strategic aim is derived from the political strategic aim and reflects the desired end state. Mission objectives expected to support the achievement of the desired end state are derived from the military strategic aim.

Info Ops planning, execution, and assessment focus on desired effects and military activities within the information domain. Therefore, a key part of Info Ops planning is to identify desired effects in the information domain which are expected to contribute to achieve the mission objectives and the planning of actions to produce these desired effects. However, it is also an important part of Info Ops planning to consider undesired and secondary effects. Actions have to be co-ordinated, de-conflicted, and synchronised with other military (and relevant non-military) actions to achieve desired effects and avoid undesired effects.

The definition of criteria for measuring the degree to which the desired effects are accomplished (measures of effectiveness – MoE) is required. Planning of actions also involves the determination of criteria for the assessment of actions conducted (measures of performance – MoP).[19]

The sum of the (resulting) effects caused by the actions (including planned inaction) and the developments of the operational environment (including all parties / actors involved) determine the "outcome". Figure 2 is a discrete depiction of a continuous process symbolising the dynamics in terms of the "next state" (outcome: (State* (n+1)).

3.2.2 The Lower Layers

In the second layer, the conceptual model identifies in detail planning steps and the involved tasks as a basis to investigate where and what kind of analysis support should and can be provided. To this end, the group decided to use as a second layer the steps which define the flow of the effects-based planning (EBP) process in the EBO concept of operations (CONOPS) as described in [27] as a proxy as there was no extant multi-national Info Ops planning process at the time of conducting this study[20]. However, in its development of the NATO Info Ops doctrine, AJP-3.10, it is expected that NATO will provide a detailed Info Ops planning process that is in line with the NATO GOP. This process could be used instead of the EBP process mentioned above.

As indicated in Figure 1, the third layer addresses detailed process steps. Any model describing the planning process in detail can therefore be adopted on this level to identify where Info Ops planning (and assessment) can be supported by analysis[21]. In the following Chapter 4 the requirements for analysis support are discussed.

[19] While MoEs are the basis to assess whether and to what extent an effect has been achieved, MoPs are criteria to assess whether and to what extent an action was conducted as planned. Possible reasons that an effect was not achieved as planned may be, e.g. that the action conducted was not appropriate to achieve the effect, or that the action has not been / could not be conducted as planned. For the assessment of cause-effect relations between Info Ops activities and observed effects, it is important to differentiate between MoEs and MoPs. MoPs must be functionally related to MoEs.

[20] In the German-led Multi-national Info Ops Experiment series, such an effects-based planning process for Info Ops is being developed and tested. The concepts developed in MNIOE are also used and tested in the MNE series (see footnotes 3, 4).

[21] For a detailed discussion of analysis requirements related to the EBP steps as given in the EBO CONOPS [27], see Section 3.4 of WP 2/4: "Conceptual Model for info Ops / Analysis Requirements" [26].

Chapter 4 – REQUIREMENTS FOR INFO OPS ANALYSIS

The core question investigated by the SAS-057 study was about the analysis requirements to support planning, execution, and assessment of Info Ops applying the effects-based approach reflected by the description introduced in Section 1.4: Info Ops are co-ordinated activities within the information domain to affect information and Information Systems using military capabilities to achieve desired effects on will and capabilities of adversaries and others in support of mission objectives while sustaining own information and information systems.

Following this understanding, Info Ops are focused on influencing, by means of appropriate capabilities, the will of parties / actors in a given scenario and / or affecting those capabilities that support decision-making or directly enable the application of will and protecting oneself and friendly parties from Info Ops by adversaries.

Analysis support for Info Ops planning involves three fundamental questions:

- What information activities are available for generating desired effects on will and capabilities and how can effects be measured?
- How can science support building a knowledge base on Info Ops, in particular with regard to influencing will?
- How can analysis support the coordination of information activities and other military and non-military activities?

4.1 ACTIVITIES AND EFFECTS

An effect is a changed state or behaviour of a target brought about by one or more actions or activities directed against it or other interlinked targets. The type of effects that an activity may generate directly or indirectly may be physical, perceptual or psychological. The indirect (higher order) effects associated with direct (1st order) physical effects of an activity may be perceptual and / or psychological. Similarly, psychological affects may be caused indirectly via activities directly aimed at creating perceptions. In other words, there are a number of pathways for generating the desired effects as depicted in the flow diagram in Figure 3.

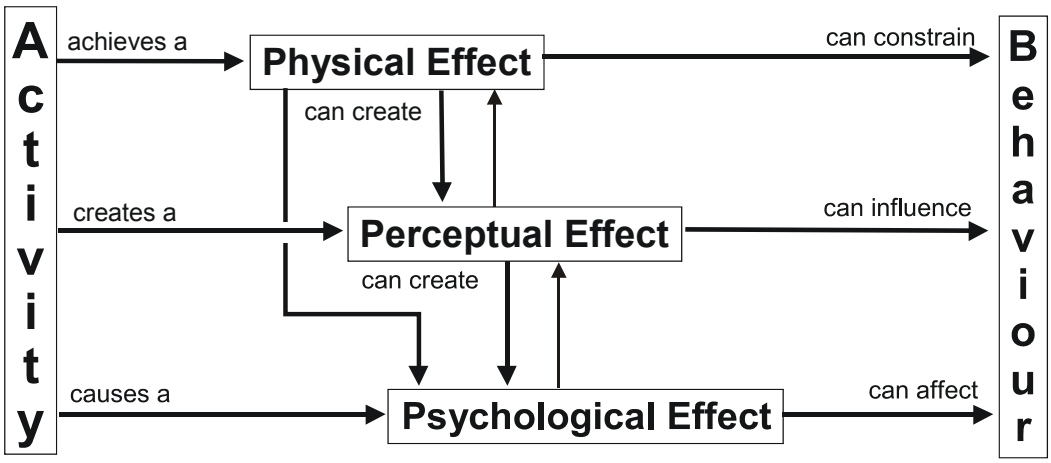

Figure 3: Effects Pathways.

Thus, a physical effect (e.g. target is bombed) can create a psychological effect (e.g. target is intimidated), and a perceptual effect (e.g. target perceives "I'm being victimised") can create a psychological effect (e.g. target feels anger or determination). Communications or presentational activities can enhance these effects. Any such effect can contribute to a change in behaviour. For example, perceptions created by reports on activities may create physical effects such as the deaths resulting during the demonstrations organised in many Islamic countries in response to an (unsubstantiated) *Newsweek* report (May 9, 2005 issue) on alleged misuse of the Quran by interrogators at Guantanamo prison. An illustrative list of the three types of effects and desired behavioural outcomes is provided in table 2 of [26].

While empirically tested analytical models for estimating the degree to which physical effects can be achieved are widely available and used in traditional military operational analysis, this is not the case for perceptual and psychological effects aimed at influencing will, behaviour, and attitudes of individuals and groups. Moreover, measuring the performance of these effects is problematic and varies for the different effect pathways. For example, the physical effect of "flooding" a decision-maker with information through appropriate computer network operations activities may lead to perceptual effects of "not being in control" and "uncertainty" which in turn may lead to the psychological effect of "hypervigilance" (i.e. the frantic sifting of the information) which may, eventually cause a "delay" or "error" in the decision-makers behaviour. However, the contribution of such a CNO activity to the effect is very challenging to measure due to the difficulty of attributing causality and the need to directly access the target. Measures of effectiveness will, last not least, address short, mid, and long term effects – where the latter address not just changes in behaviour, but lasting changes in attitude.

4.2 DEVELOPING A KNOWLEDGE BASE

Developing a knowledge base is a continuous activity that comprises two main areas where analytical support and scientific expertise are required:

- Collecting and developing Info Ops relevant knowledge regarding effects, actions, causality, and resources through empirical research, supported by experiments, and evaluation of field operations on the basis of systematic data collection, structured mission reports and debriefing of personnel returning from operations by domain experts.
- Organising and storing data, information and knowledge in a manner that it can be easily accessed, expanded, valued (relevance) and explained to support planners and operators in gaining and maintaining situational awareness and understanding by providing them with relevant background information throughout the process of planning, execution, and assessment of Info Ops contributions to a campaign.

While the means and processes to affect capabilities of individuals and organisations through kinetic or electronic actions have been studied for some time, relatively little is known about how and to what extent the will of individuals and groups can be influenced through non-kinetic effects, and how and under what circumstances kinetic / electronic effects directed at capabilities and non-kinetic effects directed at individuals and groups interact in affecting the will of individuals and organisations. Building up, through empirical research and evaluation of Info Ops in the field, a knowledge base in this area is critical, especially for small-scale contingencies where the primary objectives are related to shaping the environment and behaviours of people and adversaries rather than defeating military forces on the battlefield.

Thus, the development of a knowledge base for Info Ops is a multi-disciplinary effort requiring, in addition to military systems analysis and computer science expertise, contributions from many human science disciplines. For example, as part of the development of a conceptual model for command and control, SAS-050 has identified nearly 100 individual and team characteristics variables that influence the

decision-making and behaviour of individuals and groups or teams respectively. Their study is subject to research in disciplines such as genetics, physiology, cognitive, personality and social psychology, organisational science, sociology and cultural anthropology.

4.3 COORDINATION OF ACTIVITIES

All Info Ops efforts should be considered within the overall information strategy and the strategic context. In other words, military operations are but one contribution in the DIME[22] spectrum in which Info Ops constitute the military contribution to the "I" in DIME. Actions undertaken in one area may cause effects in the others. Similarly, in each DIME area, actions taken at the political, strategic, operational, and tactical level may cause effects at any of the other levels. And actions taken in one area or at one level may be incompatible in the sense that they neutralise or adversely affect effects to be generated by them. Therefore, actions and related effects and effects chains (1st, 2nd, 3rd, etc. order effects) need to be de-conflicted, coordinated, and synchronised both laterally and vertically at all levels of the planning and execution process. Thus, the interactions and interdependencies of actions and effects resemble a highly complex process operating within dynamic constraints that is not accessible to rigorous mathematical optimisation. Analysis assisting the development of an execution plan (synchronisation matrix and effects-based orders) is, to a certain extent, likely to imply a trial and error approach involving expert discussion supported by (war)gaming experiments and analytical trade-off analyses.

4.4 AREAS OF RESEARCH AND ANALYSIS SUPPORT FOR INFO OPS

As Info Ops as an explicit discipline are a largely novel contribution to military operations, empirical knowledge about the causes and effects associated with them is limited, and analysis methodology and decision-support tools are relatively immature compared to traditional military operations, notwithstanding the fact that organisational procedures and the steps of effects-based planning seem to be conceptually well defined. The discussion on analysis support in the previous sections supports this diagnosis. Accordingly, the issues to be addressed in the context of providing analytical support for Info Ops are considered to fall into four categories:

- Research to support the development of a knowledge base:
  - Systems science: Contextual relevance of information / knowledge on all actors in prototypical / generic scenarios (catchword: system-of-systems analysis); dynamic behaviour of complex socio-technical systems in response to external and internal stimuli (theories and hypotheses relating bodies of knowledge to one another and explaining causal relationships);
  - Human and organisational science: Effects and actions through which will and behaviour of individuals, groups and organisations can be influenced and manipulated; hypotheses and empirical evidence on cause / action-effects relationships; synergistic and conflicting effects; metrics for measuring the impact of effects;
  - Knowledge engineering: Organising and storing data, information and knowledge in a manner that it can be easily accessed, expanded, valued (relevance) and explained to support planners and operators in gaining and maintaining situational awareness and understanding by providing them with relevant background information[23] throughout the process of planning, execution and assessment of Info Ops in military campaigns;

[22] Diplomatic, information, military, economic, also called the instruments / levers of power.

[23] EBO require information in the following areas: technical, geographic, infrastructure, organisational, socio-political, psychological, context (to determine the relevance of information), and dynamics (causal relationships between action and effects over time) (see Desmond Saunders-Newton and Aaron B Frank: Effects-Based Operations: Building the Analytic Tools. *Defense Horizons* Number 19, October 2002).

  - Concepts, methodologies and tools: Common analytical framework that facilitates Info Ops across the DIME spectrum; concepts and tools for computational experimentation and computer-assisted reasoning that allow large numbers of scenario and behavioural hypotheses to be tested and possible assumptions and outcomes to be visualised (e.g. through agent-based modelling approaches), qualitative models; and
  - Appropriate model mix for cross-functional analysis, force planning, exercise and field support.

- Exploratory analysis:
  - Requirements analysis under uncertainty: Investigation of resource requirements and strategy options for Info Ops, implications for force structure and equipment, C2 organisation, personnel requirements, selection and training;
  - Contingency analysis: Info Ops packages for generic scenarios, risk assessment including risks associated with constraints and restraints, efficient rules of engagement (RoE); and
  - Experimentation: Testing Info Ops hypotheses to support e.g. concept development (CD&E).

- Exercise and field support:
  - Development and testing of analytical support and assessment tools that can handle all types of effects, in particular cognitive (perceptual and psychological) effects;
  - Incorporating human science expertise in human-in-the-loop experiments (wargames) to support the development of courses of action;
  - Assessment of optional courses of actions including the deconfliction and sequencing of effects and actions (synchronisation); and
  - Analysis to update the knowledge base, including system-of-systems analysis, target analysis, etc.

- Development of lessons learned:[24]
  - Identification of data collection requirements (such as success indicators (MoMs) and metadata); and
  - Data analysis to support the development of cause-effects relationships and their relevance.

In addition to the areas of research and analysis support for Info Ops outlined above, an overview of the principal categories of methods and tools is given in Chapter 6. Moreover, some background information on relevant scientific research being conducted to support both the development of underpinning knowledge and methods and tools is provided.

[24] For more details, see Chapter 5 and the result of WP 3: "Empirical Data Basis for Lessons Learned" [24].

Chapter 5 – REQUIREMENTS FOR INFO OPS LESSONS LEARNED

As for all other types of military activities, a thorough analysis of operations is essential in order to assess the success of Info Ops activities, to identify shortfalls in the application of Info Ops, and to improve understanding and effective use of Info Ops in future operations. Empirical data is fundamental for analysis and for identifying lessons to be learned.

Lessons learned are essential for the transformation process for organisations such as NATO. Undertaking the lessons learned processes should not be considered a burden or overhead, rather they provide the ground truth on which effective transformation should be based. Therefore, investments for lessons learned should always be assessed in the light of their significant benefit to efficiency and effectiveness of the forces.

Furthermore, the integration of new concepts of operations into day-to-day practice may cause unforeseen situations. Familiarity with an adequate conceptual framework and proper training should prepare forces to handle such situations. Finding out how well this is achieved requires analysis of events for evaluation of any chosen course of action. Identifying lessons and deriving lessons learned is not just aimed at providing guidance for similar situations in the future but also to improve situational understanding and to minimise the negative effects of unprecedented situations.

As Info Ops still have to be considered a relatively new concept, the lessons learned from past and ongoing operations are essential to assist the full integration of Info Ops into military operations in order to fully exploit the potential of Info Ops in planning, execution, and assessment. In addition, lessons learned and the underlying analyses are important contributions to areas such as concept development, training and exercises, and force development.

5.1 CURRENT PRACTICE FOR INFO OPS LESSONS LEARNED

In order to understand current practice for deriving Info Ops lessons learned from operations and to support identifying trends and areas where additional investigation is required, the group undertook a small survey[25] addressing a number of questions, e.g.:

- How are Info Ops documented today? What are the criteria and methods for documentation?
- What are the criteria and methods for data collection and processing, and what methods are used for what kind of analysis?
- How are analysis results transformed into lessons learned? Which products are created? Who are the addressees / customers of those products?
- How are insights from lessons learned fed back in respective areas such as:
  - missions / operations;
  - education / training / exercises;
  - concept development;
  - force development;
  - coalition co-operation; and
  - rules of engagement / rules of conduct.

[25] About twenty completed questionnaires covering experience from the mid 90's until recent and ongoing operations and exercises were evaluated (see [25]).

Answers to the questionnaire indicate that, although there seem to be established lessons learned processes in NATO and in most nations covered by the survey, it would appear that they are not working effectively with respect to Info Ops. From the evaluation of the answers, potential reasons for this are:

- The absence of an endorsed Info Ops doctrine can be seen as a major problem.
- No clear guidance to develop Info Ops lessons learned seems to exist.
- NATO commands are still learning about how to coordinate and integrate Info Ops in real-world operations.
- Apparently, there is no established process for implementing Info Ops – for example, within ISAF and KFOR, there were two different approaches.
- The current Info Ops structure across NATO commands appears to be inconsistent and may not meet requirements for the effective implementation of Info Ops.
- There are different understandings both between and within nations on the role, meaning, and implementation requirements of Info Ops.
- There seems to be a lack of resources available to apply the lessons learned process.

Most of these potential reasons can be directly attributed to the first one: the absence of an endorsed doctrine. From the answers to the questionnaire, it can be concluded that although for most deployments or exercises some doctrinal basis was used (based on existing national doctrines and available national and multi-national drafts), a variety of implementations of Info Ops emerged, which in turn leads to the assumption that approaches to identify lessons from Info Ops, if established at all, varied widely.

Answers referring to recent deployments and exercises indicate that there have been improvements driven by experience and identified lessons. However, even these indicate that well established processes on the basis of a structured and commonly accepted guidance are widely missing and would be welcome.

5.2 REQUIREMENTS FOR EMPIRICAL DATA ON INFO OPS

Empirical data are prerequisite for the analysis and indispensable for the assessment of Info Ops. Basically, the analysis of operations comprises the analysis of *effectiveness* (including cause-effects relationships, assessment of planned effects, conducted actions, and applied resources) and of *performance* (related to process, organisation, technology, and other aspects such as capabilities, resources, and training status) of the deployed forces.

As analysis is supposed to support all phases of an operation, there should be a continuous dialogue between the operational planners / practitioners and analysts. Based on a set of generic data requirements[26], addressing aspects such as type, quality, and format of data, concrete data requirements accounting for the respective operational context need to be articulated and refined prior to and during an operation.

The clearer data requirements are, the greater is the chance that the required information is collected (and transferred to the analysts) at the right time and in the required quality. As data collection is a resource-consuming process, including procedures such as for data gathering, structuring, pre-evaluation, and storing of data to be analysed, the respective procedures have to be planned and their implementation has to be prepared as early as possible for an operation. Consequentially, the data collection plan should be based on and integrated with the overall operational plan and reflect the various phases of an operation.

[26] See a detailed discussion of data requirements in WP 3: “Empirical Data Basis for Lessons Learned” [24].

Complementary data analysis needs to take place immediately (in the field) and ex post (after action analysis at home). For both alternatives different data requirements can be assumed. Analysis efforts during an operation have to be documented to support ex post analysis. A generic description of the steps of the analysis process as guidance to a structured documentation is provided in [24][27].

A data base for empirical data could be a tool to support the following:

- Enable analysis as a source of data and reference material.
- Improve availability and accessibility to stakeholders to help improve situational awareness, planning of effects and actions, and the assessment of courses of actions.

Field reports are one source to collect empirical data. From an initial survey of accessible Info Ops field reports the study team members concluded that, while they primarily addressed performance aspects, effectiveness aspects are generally missing.

The study team concluded that field reports offer an effective opportunity to report on both performance and effectiveness issues – including success and lack of success of activities and the related causes – to complement empirical data from other sources.

5.3 ENHANCING THE INFO OPS LESSONS LEARNED PROCESS

A broader and deeper understanding of current practice regarding the development and exploitation of Info Ops lessons learned, including data collection and analysis procedures, should be addressed in further investigations to allow a better identification of effective practice as well as especially practical deficiencies and shortfalls in the lessons learned process.

Based on the findings of the report at hand and the recommended continued research, a more effective Info Ops lessons learned process should be established. This should include establishing standardised guidelines for the development of empirical data bases. As field reports are considered a valuable tool for the collection of empirical data from operations, they should be standardised to some extent in terms of content, structure, and format.

This report should be considered a first step for identifying the requirements towards such standardisation efforts. Further investigation in this direction is recommended as an essential contribution to improve the lessons learned process.

[27] See Section 4.3 of WP 3: “Empirical Data Basis for Lessons Learned” [24].

Chapter 6 – SUPPORT FOR INFO OPS ANALYSIS

In Chapter 4 it was highlighted that there was a need for decision-support methods and tools as part of the analytical requirements for supporting Info Ops. Included in these requirements is the need, in particular, to develop and implement methods and tools in the areas of:

- Network dynamics: Understanding how a system is organised and identifying key vulnerabilities and dependencies within networks that could be exploited.
- Dynamic behaviour of complex socio-technical systems in response to external and internal stimuli.
- Cause / effect relationships to support the improved understanding of the resultant effects of actions taken to alter the will and behaviour of individuals, groups and organisations.
- Measures of merit[28].

The group could not identify a readily available tool set dedicated to Info Ops analytical support. However, there are a number of national research initiatives and other activities that have been, and are being, undertaken in the areas addressed above aimed at developing such a tool set. Whilst these approaches are often complimentary the group could not identify any coherent international programme. This lack of a coherent programme is in part a reflection of the, at present, differing national approaches to Info Ops.

The research initiatives can be set within the wider context of the development of analytical approaches and underpinning scientific knowledge to support the development of an effects-based approach. This wider context is illustrated at Figure 4 (taken from [28]).

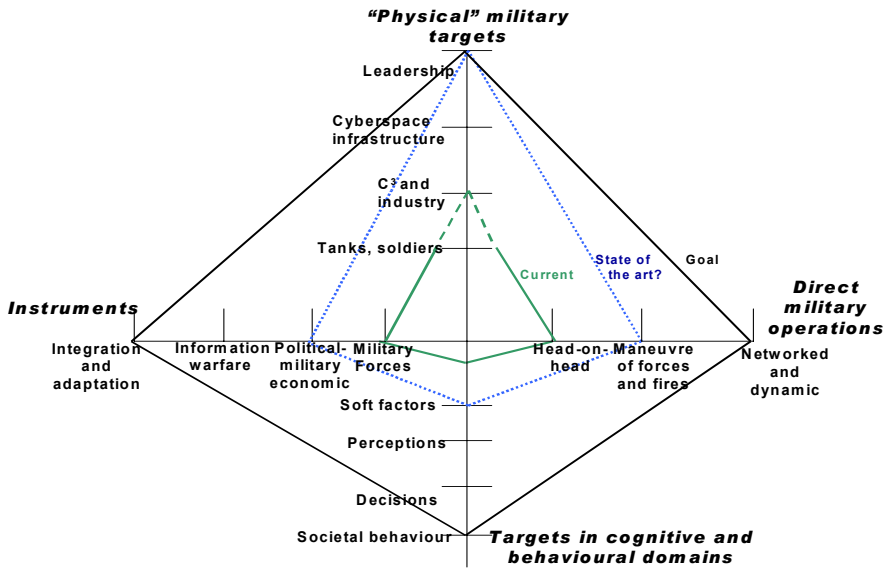

Figure 4: OA Coverage to Support an Effects-Based Approach: The RAND 'Diamond'.

The centre diamond shape (labelled "current" when written in 2001) represents the perceived 2001 baseline of analysis and modelling capability, with the dashed lines indicating limited analysis and modelling capability with respect to indirect effects. The middle dotted diamond indicates the state-of-the-

[28] Include: measures of performance (MoP); measures of effectiveness (MoE); measures of success (MoS).

art of current modelling and analysis capabilities assessed in 2001[29]. The outer diamond indicates the ultimate goal for analysis and associated modelling to fully support an effects-based approach.

From this wider perspective it can be seen that there are large gaps at present in the OA in the areas of knowledge that will underpin Info Ops. The information in this chapter provides a high-level view on efforts of nations related to methods and tools that SAS-057 considers being relevant to Info Ops analysis, more detailed information is contained within the results of WP 5 [29]. It should be noted that information in [29] is not exhaustive and only covers unclassified work being undertaken.

6.1 OVERVIEW OF APPROACHES

The following information grouped under national headings provides an overview of research activities and models & tools of relevance for Info Ops analysis.

6.1.1 Sweden

The Swedish Armed Forces (SwAF) has been given the task by the Swedish government of both developing an operative capability to counter Info Ops, and to provide an operative resource base for society in general, in accordance with its overall responsibilities. SwAF are in the process of outlining the doctrinal framework for information operations and is also contracting military research and development within this area. There are several agencies and other commercial and academic institutions in Sweden conducting research of relevance for Info Ops, for example the Swedish Defence Research Agency, the Swedish National Defence College (SNDC) and the Defence Materiel Administration.

The following outlines selected methodologies used and projects being conducted in Sweden that are of relevance to Info Ops.

- **Non-quantified modelling with morphological analysis**: General morphological[30] analysis (MA) is a non-quantified modelling method for structuring and analysing complex socio-technical problem fields, e.g. for scenario development or the assessment of relationships between means and ends in strategic planning. MA can also be used in combination with other methods such as Bayesian networks, and is an excellent starting point for developing gaming frameworks.[31]

- **Sensemaking**: The project studies the process to solve joint military problems and assesses the results of this process, e.g. the quality of decisions created by the process.

- **Planning method**: This study focuses on fundamental issues as how to create an efficient planning method for a small staff where the commander has a more central role than before and where the amounts of accessible information are very large. This new planning method concentrates completely on national tactical level and will be synchronised with the NATO adjusted operative planning method.

[29] This assessment was made in 2001 by Dstl staff. Research work in the international analytical community is developing an underpinning science base to start to move small areas of the start-of-the-art into current practice - mainly along the 'Physical' military target axis.

[30] Morphology means "the study of form". Morphology is found in specific disciplines such as geology, zoology and linguistics. Fritz Zwicky developed general morphology. See Ritchey, T. *Fritz Zwicky, Morphologie and Policy Analysis*. 16th Euro Conference on Operational Analysis, Brussels 1998. (www.swemorph.com/downloads.html)

[31] For further information, see MA page at the website of the Swedish Defence Research Agency: www.foi.se/ma and the Swedish Morphological Society's website at: www.swemorph.com.

- **Information selection**: An empirical study is undertaken to support the decision which kind of information selection (role-based operational picture based on "pushing" or purpose operational picture based on "pulling" information) is to prefer in different situations.

- **Gaming in the C2 process**: Recent developments in computer gaming may have the potential to contribute to the development of military war gaming and more specifically gaming the C2 process. Ongoing study work will look into current practice of war gaming by SwAF, including the need for digital support at higher decision levels and the applicability of (customised) commercial games.

- **Strategic management system**: This project has built a number of models that can be simulated on an operative level and used in strategic group modelling.[32] Ongoing work aims at including e.g. linking the commander's intent together with new balancing functions. Examples regarding the NATO concept of commander's planning guidance (CPG) and its meaning have been studied in several exercises. Suitable ways to model and mediate CPG will be examined, especially in terms of effectiveness.

- **Staff working support – Cupol**: The SNDC has developed a tool to support operative planning according to the NATO guidelines for operational planning (GOP), called Cupol. Cupol has been connected to a document management system (DMS) and offers an environment in which to follow up ongoing work, including traceability on individual orders and documents, and also a tool for follow-up on the planning process as a whole.

- **C2 in crisis management operations**: The project focuses on required changes in the operative C2 process with transformation to an effects-based approach of operations, including the coordination of the various means of security policy: military as well as diplomatic, economic, and psychological.

6.1.2 Germany

Operational research and analysis support for Info Ops planning and execution is coordinated at the Centre for Transformation of the Bundeswehr (Zentrum für Transformation der Bundeswehr), technological research and analysis support by the Federal Armed Forces Office for Information Management and Technology (Bundesamt für Informationsmanagement und Informationstechnik der Bundeswehr). Research and supporting studies are being conducted by several industrial / commercial and academic institutions under contract with these agencies. The following provides an overview of selected projects related, directly or indirectly, to Info Ops that are currently underway.

- **Human behaviour modelling**: This research program is aimed at investigating the essential factors and the cognitive and social processes underlying human behaviour to support modelling behaviour of individuals, teams / groups, organizations, and amorphous groupings and masses. The results as well as the emerging behavioural models have the potential to support Info Ops planning, execution, and assessment.

- **Command and control concepts**: The work focuses on the investigation of variables capturing individual and team characteristics and behaviour, and the relationships between them, that together with the technical, organisational, and doctrinal parameters of the C2 system affect individual and collective situational awareness and understanding and decision-making behaviour. This work is part of a wider research initiative aimed at providing a reference basis for instantiating C2 system models for exploring new C2 concepts such as for network centric operations and agile mission groups.

[32] The models are run at the operational level and the results aggregated to support a strategic level modelling.

- **Knowledge base concept representation and pre-selection of effects in EBO**: The objective of this research project is to develop an integrated, knowledge based approach for the representation of concepts related EBO that provide a basis for the development of an IT-supported process and concept for the pre-selection of effects in the EBO planning process.

- **Agent based modelling (ABM)**: Germany is participating in Project Albert of the U.S. Marine Corps dedicated to exploring the potential of ABM for the simulation of complex military systems and new operational concepts. ABM is an approach to simulating the behaviour of a complex system in which agents interact with each other and with their environment using simple local rules which describe the response of individual actors in specific situations such as in peacekeeping scenarios. Such simulation experiments may well be suited to generating and investigating hypotheses on cause-and-effects relationships in individual and collective human behaviour given, among others, the effects of Info Ops actions.

- **Development of simulation systems**: Efforts are undertaken to widen the scope of existing systems for the simulation of joint and combined operations beyond the traditional military aspects in support of concept development & experimentation (CD&E), computer-assisted exercises (CAX), and analysis, especially systems-of-systems analysis (SoSA) and capability analysis.

  One goal of broadening the scope is to enable the simulations of asymmetric warfare scenarios including the representation of military and civil elements and events such as human behaviour, patrols, checkpoints, refugee movements, riots, non-governmental organisations (NGOs), provincial reconstruction teams (PRTs), and civilian security issues.

  The current focus of the further development of simulation systems is on components to simulate political scenarios allowing the consideration of aspects from all PMESII (political, military, economic, social, information, and infrastructure) areas of an operational environment.

- **Verification & validation:** A major research area is verification and validation (V&V) emphasising risk assessment, tool support, and fundamental questions of methodology in the context of modelling and simulation of technical processes and directly observable socio-technical systems. A major issue for such research is the validation of models and simulation of complex systems which are difficult to observe or, like most future military systems and operations, not directly observable at all in reality.[33]

- **Information technology support for Info Ops** research is under way to investigate how information can be provided for the coordination and synchronisation function of Info Ops and to develop a planning support tool for that purpose. In the context of providing information, the study analyses what kind of information related to Info Ops is required from which sources and how this information can be made available and tailored to the needs of authorised users.

- **Analysis of critical infrastructures:** The methodology for the "Analysis of Critical Infrastructures (ACIS)[34] is aimed at identifying the criticality of business processes and the services and components required to maintain these processes. There are several potential applications of this methodology (or variations thereof) for Info Ops. For example, the methodology can be used to analyse relevant business processes of an adversary – looking for IT-dependencies of high criticality, looking for interdependencies of services and infrastructures, etc.

[33] The result of WP 5: "Methods and Tools to Support Info Ops Analysis" [29] contains a short summary paper discussing alternative approaches to validation.

[34] A general description of the method is available at http://www.bsi.bund.de/fachthem/kritis/acis_paper_en.pdf.

6.1.3 Australia

A major focus of DSTO Research and Development (R&D) in this area is the development of a single integrated toolset that supports a shaping and influencing and information operations planning capability for the Australian Defence Force (ADF). A number of individual tools and processes will be integrated technically, but more importantly they will be united in an underlying effects-based conceptual model of the planning domain. A further thrust in Info Ops R&D is social systems analysis and modelling to facilitate an improved understanding of individual and group dynamic behaviour.

6.1.4 UK

The UK's Defence Science and Technology Laboratory (Dstl) has been conducting research into decision-support tools to aid Info Ops planning. Current decision-support tools are generally concentrated on representing physical or technical elements of a system. Explicit static representation of social interactions is possible by the use for example of social network diagrams and belief / causal maps[35]. A number of analysis methods and tools are available to support such approaches[36], an example method is social network analysis (SNA) which identifies network characteristics (such as the most central component) and vulnerabilities (such as suggesting how best to fragment the network). However, there are few, if any tools in service that are capable of dynamic S-T modelling and the analysis necessary to fully support the Info Ops planning process. This is in part due to the fact that S-T modelling requires multi-disciplinary research that harnesses both computational and social science expertise. Only a very small proportion of the social and technical network analysis research being undertaken attempts to cross this disciplinary divide and recent work by the UK identified that the main research efforts that do so are taking place in the US. Therefore, both the discipline and modelling tools available are currently immature and are co-evolving.

Socio-technical modelling and analysis models and tools are anticipated to help planners understand the properties of (complex) S-T systems and how they respond to perturbations. The predictive capability of such models and tools is expected to be limited to better understanding of the range and likelihood of future events, rather than attempts to provide specific predictions[37]. When considering S-T models it must be remembered that they are decision-support not decision-making models and are not designed to replace the decision-making process. In Chapter 3 the conceptual model of Info Ops developed in WP 2 was reviewed and whilst the exact point at which models and tools could be used is still not clear it is felt that they would be of most use at the strategic level of planning and would probably be of limited value at the operational or tactical levels due to the development time involved.

6.1.5 Switzerland

In the Swiss Armed Forces, the Info Ops process at operational level comprises three pillars: operations (wage Info Ops), education (preparation of the personnel) and development (permanent update of the Info Ops capabilities and methods). Education in the widest sense itself comprises education as such, training / exercises and awareness. Because of the necessity to bring Info Ops to all MoD personnel, it is a complex task, consuming time and resources and requiring specific tools. This problem is exacerbated by the extension of Info Ops education to audiences outside the MoD, and additionally the development of interoperability goals and JOINT / COMBINED visions.

---

[35] Social network diagrams tend to look at the connectivity and relationships between people and groups, whereas belief / causal maps display how underlying beliefs interact.

[36] Example tools : I2 Analysts Notebook; Netvis; Belief and causal maps; Centre of Gravity Networks Effect (COGNET).

[37] It is perceived that the value of prediction is in its quality and utility to planners; exploratory models may be helpful, through broadening understanding of a situation, without attempting to accurately predict the real world as such predictions are not a necessary characteristic for a model to provide some utility.

A project named IOLANDA (which stands for the "world of Info Ops" or the "Info Ops environment") was therefore started to create the instruments to support a dynamic management of Info Ops materials (in the form of real or at least realistic multi-media), programs, methodologies, exercises, etc. The project, which is expected to be fully operational by the end of 2008, comprises four entities: training / exercises (developed with the practical experience gained during VIKING 05), education (articulated in 15 programs under development), awareness (to increase attention of Info Ops threats and solutions) and an "Info Ops room" (containing the technical instruments and a knowledge management system for the practical realisation of the three first elements).

6.2 CONCLUSIONS

In order to fully realise the benefits of Info Ops, it is important to develop methods and tools for the analytical support of the Info Ops process providing, amongst others, for more effective network analysis, understanding of causality in and the dynamic behaviour of complex systems. In addition, methods and tools are required for the development and assessment of performance and effectiveness. As illustrated at Figure 4, there are at present considerable gaps in the knowledge required for effective analytical support. Even though there are several national programmes that promise to close knowledge gaps and develop some models and tools to support Info Ops, this work is a long way from maturity and too fragmented for realising the full analytical support required in the near future. Thus, coherence of research across nations should provide for more effective research. As highlighted in Chapter 5 (see also [24]), today's limited procedures of Info Ops data collection and analysis yield insufficient empirical evidence to support any specific research on and modelling of the effectiveness of Info Ops.

Chapter 7 – CONCLUSIONS AND RECOMMENDATIONS

The emergence of global information networks and the ensuing changes in society have created both new threats to national and international security beyond the traditional military threats and possibilities to counter them. Modern information technology provides the potential for using information as an asset for reinforcing the effectiveness of the traditional instruments of national power at all levels. Thus, using information and related systems and technology to maintain information superiority has become an indispensable prerequisite to retain freedom of action in crises and war. Information operations provide an essential contribution in reaching that end. The aim of information operations is to support the achievement of strategic objectives with, ideally, limited use of physical force. In order to maximise the potential benefits from information activities, they must be orchestrated with all other military activities. In that sense, understanding the role and use of information as an operational factor has become essential for planning military operations in the information age, for which analytical support is a key enabler.

This study was focussed on the requirements for analytical support to Info Ops. The following conclusions and recommendations are drawn from the findings gained both from the specific analysis undertaken and also wider knowledge acquired through interaction with Info Ops specialists.

7.1 CONCEPTUAL UNDERSTANDING OF INFO OPS

A review of Info Ops documents was conducted in order to compare conceptual approaches for Info Ops as a starting point to identify commonalities and differences. From this review, it can be concluded that the approaches are beginning to converge towards a common conceptual understanding of Info Ops. However, different views on the role and implementation of Info Ops still exist, especially with regard to aspects such as C2 relationships and directive authority. This conclusion is supported by the evaluation of the answers to the Info Ops lessons learned survey undertaken in this study.

Further analysis on the application and practical implementation of Info Ops is required in order to evaluate the coherence of the various approaches. In particular, the following issues merit attention:

- Incorporation of Info Ops expertise into the NATO command structure (NATO HQ, ACT, ACO, JFC, CCs, JALLC);
- Role and responsibilities of Info Ops staff within national defence departments; and
- Composition of Info Ops staff within operational HQs.

The present lack of an endorsed NATO Info Ops doctrine has led to different organisational structures being established for the implementation of Info Ops within NATO deployments. Latest developments in NATO Info Ops doctrine suggest that it will attempt to resolve this issue.

In order to support the refinement of the NATO conceptual approach to Info Ops, the CD&E methodology should be applied to test and validate the process and organisation as outlined in the updated draft of AJP-3.10.

7.2 PROCESS MODEL FOR THE IDENTIFICATION OF ANALYSIS

The conceptual model for Info Ops developed by the group proved to be useful for arriving at a common understanding. In order to identify analysis requirements for the support of Info Ops, the conceptual model focused on a process view utilising the description of an effects-based approach to operational planning. This analytical framework should be applied to the detailed planning process that is expected to be

provided by the NATO Info Ops doctrine, AJP-3.10, in order to refine the analytical requirements identified in this study.

7.3 IMPROVING THE INFO OPS LESSONS LEARNED PROCESS

Lessons learned are essential for the transformation process for organisations such as NATO. However, it seems that existing lessons learned processes in NATO and nations are not working effectively with respect to Info Ops. Also, it would appear that current lessons learned processes are focused on performance rather than effectiveness aspects related to Info Ops.

There are a number of reasons for this, including the lack of priority given to, and understanding of a need for, the lessons learned process. As the group only undertook a limited review, it recommends that a detailed review of Info Ops lessons learned processes is undertaken in order to identify shortfalls and good practice(s). This can be used to support the development of relevant processes across NATO and nations to provide a coherent approach for lessons learned in support of concept development, implementation and the conduct of operations.

7.4 METHODS AND TOOLS FOR DATA COLLECTION AND ANALYSIS

Empirical knowledge about cause and effect relationships associated with information activities is limited. In addition, the analytical methodology and related decision-support tools for Info Ops are relatively immature compared to those used in the analysis of traditional military operations, and the study group could not identify a readily available tool set dedicated to Info Ops analytical support. However, there are a number of national research initiatives and other activities that have, and are, being undertaken aimed at developing a tool set.

The group identified that for both the lessons learned process and for the building of knowledge there is a need for a well-structured and standardised approach for the documentation of empirical data drawn from operations. Allied to this is a need to store the data in a manner easily accessible to a wide variety of stakeholders, e.g. analysts, Info Ops planners, and staff responsible for the lessons learned process. It has to be recognised that there has to be a balance between data collection and operational needs, and also that there may be data desired that are uncollectible.

To obtain the essential data for the analysis of Info Ops planning, execution and assessment, the study group recommends that further work is conducted in developing methods and tools for data collection. The use of embedded analysts in military operations would enhance and support the collection of data.

In parallel to obtaining data, there is a need to develop a tool set for Info Ops analysis. This development will require empirical data from real-world operations, experiments and empirical research as well as the consolidation of existing knowledge.

The group recommends that there are agreed guidelines for the collection of data – including the standardisation of field reports – based on common processes throughout NATO for the organisation, storage, and distribution of data and information.

The involvement of embedded analysts in operations is a key element for improving data collection and thus enhancing the data basis for lessons learned, operational analysis to support decision-making, and further analysis tasks. The group recommends that analysts and analytical support are always integrated from the outset into national, multi-national and NATO operations. This is aided by their support of permanent and deployed command structures.

7.5 COORDINATION OF INFORMATION ACTIVITIES

The group recognised the key requirements for the de-confliction, synchronisation, and coordination of information activities within the overall operation. It is recommended that the specific analytical requirements to support such processes are investigated.

7.6 INFO OPS EDUCATION, TRAINING AND EXERCISES

The results and findings of the SAS-057 study reinforce the need that military personnel, as well as civilians, have relevant ongoing education and training in Info Ops.

We therefore recommend that education, training and exercises in Info Ops are implemented at national, multi-national, and NATO levels in accordance with the following principles:

- All personnel have a basic, coherent understanding of the implications of military operations in the information age.
- There is individual Info Ops training tailored to the specific requirements of staff functions.
- There is a robust system to incorporate Info Ops lessons learned in education, training and exercises.

Chapter 8 – RECOMMENDATIONS FOR FUTURE ACTIVITIES

In addition to the recommendations given in Chapter 7, the group identified the following activities which RTO may wish to support in order to advance the theoretical and empirical foundations and practices of Info Ops.

8.1 SYMPOSIUM ON INFO OPS LESSONS LEARNED

As a starting point for more in-depth analysis of current practices in Info Ops lessons learned processes, the group recommends that a symposium is organised bringing together:

- Military personnel that have served as Info Ops officers;
- Analysts and experts from lessons learned communities that have an interest or experience in Info Ops;
- Individuals involved in developing Info Ops concepts, doctrine, handbooks, etc.; and
- Individuals responsible for Info Ops education and training.

The aim of the symposium would be to develop an agreed view on areas for improvement and initial views on ways and means, including prioritisation, to implement these improvements.

8.2 ROADMAP FOR THE PROVISION OF INFO OPS KNOWLEDGE

As the group has identified that broad access to Info Ops knowledge – based on theoretical foundations and empirical data / practical experience – is a key requirement in providing both effective analytical support and the undertaking of Info Ops, the group suggests that a clear roadmap is developed to facilitate collaborative or coordinated research and promote coherence among nations. The roadmap should address, among others:

- Establishing an analytical framework for generation and testing of cause-and-effects hypotheses;
- the identification of the relevant scientific fields and the experts to be consulted to support the development of the requisite knowledge; and
- the development of generic MoM, especially MoE, and procedures to build, maintain and continuously update relevant knowledge including the incorporation of Info Ops lessons learned.

8.3 VERIFICATION AND VALIDATION

The group recommends developing guidelines for the verification and validation of “soft science” methods and tools used to support Info Ops and the wider effects-based approach that will contribute to building the confidence of both decision-makers and analysts in such methods and tools.

Chapter 9 – REFERENCES

[1] "Handbook on the Analysis of Smaller-Scale contingency operations in Long Term Defence Planning", RTO Technical Report TR-SAS-027, February 2005.

[2] "Decision Support to Combined Joint Task Force and Component Commanders", RTO Technical Report TR-SAS-044, December 2004.

[3] "NATO Code of Best Practice for C2 Assessment", RTO Technical Report TR-081 / SAS-026, January 2004.

[4] MC 422/1 "NATO Military Policy on Information Operations", April 2002, NATO RESTRICTED.

[5] "Overview of Info Ops Documents", SAS-057 – WP 1 (see also Annex D).

[6] Belgische intercomponenten doctrine voor informatie operaties, drafteditie mei 2004 (Belgian joint doctrine for Information Operations, draft edition May 2004), currently under revision as based on the AJP-3.10.

[7] Information Operations Policy for CF International Operations, December 2004.

[8] CF Information Operations, 15 April 1998, National Defence, Chief of the Defence staff, Doc code B-GJ-005-313/FP-000, available at http://www.forces.gc.ca/dcds/jointDoc/docs/af010_e.pdf.

[9] "Teilkonzeption Informationsoperationen der Bundeswehr (TK InfoOpBw)" *(Subconcept Information Operations of the Bundeswehr)*, February 2005, Germany, Ministry of Defence, VS-NfD (RESTRICTED).

[10] "Beleidskader Information Operations (Info Ops)" (Information operations policy), June 2001.

[11] Forslag til "Konsept for militære informasjonsoperasjoner (Mil Info Ops)" (Concept for military information operations (Mil Info Ops), 20 December 2002.

[12] "Kapasiteter for offensive og defensive militære informasjonsoperasjoner" (Capabilities for offensive and defensive military information operations), 14 March 2003, policy whitepaper, RESTRICTED.

[13] Perspective IO – Swedish Armed Forces view on information operation, English version, September 2004.

[14] Information Operations: Joint Warfare Publication 3-80, Joint Doctrine and Concepts Centre (JDCC), June 2002.

[15] "Joint Doctrine for Information Operations", Joint Pub 3-13, Joint Chiefs of Staff, USA, 09.10.98, available at http://www.dtic.mil/doctrine/jel/new_pubs/jp3_13.pdf.

[16] Field Manual No. 3-13 (FM 3-13): "Information Operations: Doctrine, Tactics, Techniques, and Procedures", November 2003, US Army, available at http://www.adtdl.army.mil/cgi-bin/atdl.dll/fm/3-13/fm3_13.pdf.

[17] Air Force Doctrine Document 2-5: "Information Operations", 04 January 2002, available at http://www.e-publishing.af.mil/pubfiles/afdc/dd/afdd2-5/afdd2-5.pdf.

[18] Revised JP 3-13 Joint Doctrine for Information Operations – second draft, 14 December 2004, available at http://www.dtic.mil/doctrine/jel/ddrraafftt_pubs/3_13sd.pdf, visited 24 January 2005.

[19] AJP-3.10 "NATO Information Operations Doctrine", Study Draft 3, 12 January 2005, NATO Unclassified.

[20] "Concept for EU Military Information Operations", Council of the European Union, Military Committee, 27 February 2003, RESTREINT UE.

[21] Whitepaper "Information Operations (Info Ops) in Future Coalition Operations", Version 1.0, 4 October 2004, Unclassified – releasable to the internet.

[22] CONOPS Information Operations (Info Ops) Planning for Effects-Based Operations", Version 1.0, 4 October 2004, Unclassified – releasable to the internet.

[23] PIA 03.152 "Concept interarmées des opérations d'information", N° 294 /DEF/EMA/EMP.1/NP du 11 mars 2005, English version: "Joint Concept of Information Operations", PIA N° 03-152, N° 294 /DEF/EMA/EMP.1/NP – 11 March 2005.

[24] "Empirical Data Basis for Lessons Learned", SAS-057 – WP 3 (see also Annex D).

[25] "Evaluation of Answers to the Questionnaire", SAS-057 – WP 3 (see also Annex D).

[26] "Conceptual Model for Info Ops / Analysis Requirements", SAS-057 – WP 2/4 (see also Annex D).

[27] Joint Forces Command-Joint Experimentation Directorate-EBO Prototyping Team: "The Multinational Effects-Based Operations Process – Concept of Operations (CONOPS)", Draft Version 0.65, 07 January 2005.

[28] Paul K. Davis: "Effects-Based Operations (EBO): A Grand Challenge for the Analytical Community", RAND, MR-1477-USJFCOM/AF, ISBN: 0-8330-3108-2, 2001.

[29] "Methods and Tools to Support Info Ops Analysis", SAS-057 – WP 5 (see also Annex D).

Annex A – PARTICIPANTS AND LIAISONS

The RTG SAS-057 "Information Operations in Smaller-Scale Contingencies – Analysis Support and Capability Requirements" consisted of a core team of members from Belgium, Germany (lead nation), Portugal, Sweden, Switzerland and the United Kingdom. The core team was augmented by occasional participation and contributions from France and NC3A.

Members of Task Group SAS-057[38]:

- Maj. W. Kreemers, Belgium
- Dr. S. Jantsch (Technical Team leader), Germany
- Mr. B. Schmidt, Germany
- Prof. Dr. R. Huber, Germany
- Commander U. Röhrs, Germany
- Maj. P. Nunes, Portugal
- Ms. M. Löw, Sweden
- Ms. A. Marklund, Sweden
- LtCol. G. Vernez, Switzerland
- Mr. J. Uren, United Kingdom
- Mr. T. Parsons, United Kingdom

In addition, points of contact in Australia, Canada, the Netherlands, Norway, the USA, NATO ACT, NATO JALLC, and NATO School Oberammergau received drafts and products of the group's work throughout the duration of the study and were invited to comment and contribute.

An information exchange existed with SAS-050 "Exploring New Command and Control Concepts and Capabilities" as two members of SAS-057 are also participants of SAS-050. This liaison provided valuable input to the group, especially for the consideration of human behaviour aspects.

Members of the group also played key roles in MNIOE which ensured the cross-pollination of ideas between this study group and the MNIOE community.

[38] Detailed contact information is available through the SAS secretariat.

Annex B – GLOSSARY

This annex provides descriptions of key terms that are used in the study SAS-057 "Information Operations in Smaller-Scale Contingencies – Analysis Support and Capability Requirements". The descriptions are based on existing definitions.

Information Operations

Info Ops are co-ordinated military activities within the information domain to affect information and information systems to achieve desired effects on will and capabilities of adversaries and others in support of mission objectives while sustaining own information and information systems.

Based on the definition given in the MNIOE Whitepaper Version 1.0, 4 October 2004.

Information Domain

The information domain is the (virtual and physical) space in which information is received, processed and conveyed. It consists of the information itself and information systems.

Based on: E. Smith: Effects-Based Operations – Applying Network Centric Warfare in Peace Crisis and War, CCRP, 2002.

Information System

Information systems are socio-technical systems consisting of sub-systems for the optimal provision of information and (technical) communication. They comprise personnel, technical components, organisational structures and information-based processes that collect, perceive, analyse, assess, create, manipulate, store, retrieve, display, share, transmit and disseminate information.

Based on: US Joint Pub 1-02 – Department of Defense Dictionary of Military and Associated Terms, and: H. Krcmar: Informationsmanagement. Berlin 2000.

Effect

The physical or cognitive consequence(s) at any level within the strategic environment of one or more military or non-military actions.

Based on: UK military view of effects, definitions, and relationships, 3 June 2004.

The physical and / or behavioural state of a PMESII system that results from a military or non-military action or set of actions (DIME).

Based on: EBO CONOPS Joint Forces Command Joint Experimentation Directorate EBO Prototyping Team, Version 0.6, 15. October 2004.

Effects-Based Operations

The coordinated national and international activities conducted to realise the objectives necessary to obtain strategic aims. The military contribution to EBO is the synchronised application of military capabilities to achieve effects.

Based on: UK Draft EBO concept, October 2004.

Operations that are planned, executed, assessed, and adapted based on a holistic understanding of the operational environment in order to influence or change system behaviour or capabilities using the integrated application of selected instruments of power to achieve directed policy aims.

From: EBO CONOPS Joint Forces Command Joint Experimentation Directorate EBO Prototyping Team, Version 0.6, 15. October 2004.

Measures of Merit

Measures of Merit (MoM) is a generic term to encompass different classes of measures. The measures are defined in hierarchical levels related to each other, each in terms of its own boundary. From the conceptual viewpoint, it is important to keep in mind the level of analysis and the context in which the measurements are made.

Adapted from RTO Technical Report TR-081: NATO Code of Best Practice for C2 Assessment, p. 5-2.

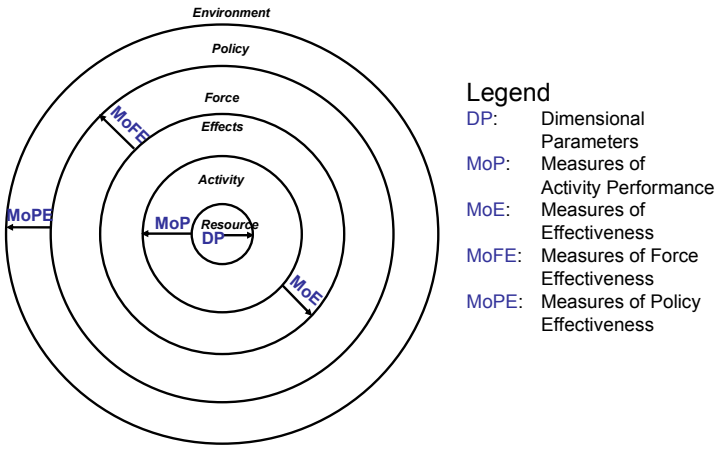

Figure 5: Relationships of Measures of Merit.

The MoM shown in Figure 5 are the following:

- Measures of policy effectiveness (MoPE) which focus on policy and societal outcomes (strategic end state).
- Measures of force effectiveness (MoFE) which focus on how a force performs its mission or the degree to which it meets its objectives. Examples include territory secured / gained or lost, rate of advance, combat loss ratios, and casualty rates.
- Measures of effectiveness (MoE) which focus on the impact of (synchronised) activities within the operational context.
- Measures of performance (MoP) which focus on criteria used to evaluate accomplishment of actions.
- Dimensional parameters (DP) which are the properties or characteristic inherent in the physical resources.

The boundaries between the MoM depicted in Figure 5 are necessarily oversimplified. The linkages among the MoM are often much more complex. It can be difficult to discern the linkages between the levels of MoM unless analysis design is crafted to capture them.

Measures of Effectiveness

The criteria used to evaluate how actions have affected system behaviour or capabilities; MoE are tied to effects and effects assessment.

MoE are criteria used to evaluate how actions have affected system behaviour or capabilities; they are tied to effects and effects assessment.

From: USJFCOM – Pre-CDC Final / Approved Definitions, 02-04 June 2004.

Measures of Performance

MoP are criteria used to evaluate accomplishment of friendly actions; MoP are tied to tasks and task assessment.

Based on: USJFCOM – Pre-CDC Final / Approved Definitions, 02-04 June 2004.

Annex C – SPECTRUM OF INFORMATION ACTIVITIES

With a view to the ultimate functions of Info Ops – of influencing will and affecting capabilities for influencing will (of adversaries and neutrals), and protecting against the capabilities of adversaries for influencing one's own will – three categories of Info Ops activities, complemented by related activities that may enhance the direct and indirect effects of Info Ops activities, may be distinguished:[39]

- **Influence Activities** aimed at decision-making leaders and members of adversary parties / groups as well as populations in the theatre of operations to change their behaviours:
  - Psychological Operations (PSYOP);
  - Presence, Posture, Profile (PPP);
  - Operations Security (OPSEC);
  - Deception;
  - Electronic Warfare (EW / ECM, EPM);
  - Physical destruction (specifically targeted); and
  - Computer network operations (CNO: attack, defence, exploitation).
- **Counter-Command Activities** directed at the C4I infrastructure of potential adversarial parties:
  - Physical destruction;
  - Electronic Warfare (EW / ECM); and
  - Computer Network Operations (CNO).
- **Information Activities** to provide information required for planning and execution Info Ops and for protecting one's own decision-makers and capabilities:
  - Electronic Warfare support measures (ESM);
  - Provision of information (Intelligence, Surveillance, Reconnaissance ISR);
  - Information assurance (IA); and
  - Computer network defence (CND).
- **Related Activities:**
  - Civil-Military Co-operation (CIMIC); and
  - Media Operations, Public Information.

[39] This categorisation of Info Ops activities follows the UK Info Ops doctrine (JWP-3.80) because it is the most comprehensive among the doctrinal documents reviewed by SAS-057 in WP 1 with a view to the activities included. For example, only JWP 3.80 explicitly considers PPP an Info Ops activity. MNIOE regards PPP as another type of military operation hardly ever undertaken only to influence people. It is stated, however, that PPP may cause effects in the information domain or may even be intentionally employed to convey messages. Similarly, the individual performance and behaviour of soldiers in the field may cause effects in the information domain which may assume strategic quality because of media presence.

Annex D – LIST OF WORK PACKAGE RESULTS

The work of SAS-057 was organised in the following work packages:

- WP 1: Overview of documents;
- WP 2: Conceptual Model for Info Ops;
- WP 3: Empirical Basis for Lessons Learned;
- WP 4: Analysis Requirements for Info Ops; and
- WP 5: Methods and Tools.

The following documents detail the results of the work of the group and have been the basis for writing this report:

- "Overview of Info Ops Documents", SAS-057 – WP 1 [5];
- "Summarised Information on Info Ops Documents", SAS-057 – WP 1, This Annex is NATO UNCLASSIFIED, releasable to Sweden and Switzerland and requires the RTO Members Password;
- "Conceptual Model for Info Ops / Analysis Requirements", SAS-057 – WP 2/4 [26];
- "Empirical Data Basis for Lessons Learned", SAS-057 – WP 3 [24];
- "Evaluation of Answers to the Questionnaire", SAS-057 – WP 3 [25]; and
- "Methods and Tools to Support Info Ops Analysis", SAS-057 – WP 5 [29].