



FORSVARSAKADEMIET

RESEARCH PAPER

TACTICAL INFORMATION OPERATIONS IN CONTEMPORARY COIN CAMPAIGNS

By Thomas Elkjer Nissen, Dept. of Joint Operations,
Royal Danish Defence College



FORSVARSAKADEMIET

RESEARCH PAPER

TACTICAL INFORMATION OPERATIONS IN CONTEMPORARY COIN CAMPAIGNS

By Thomas Elkjer Nissen, Dept. of Joint Operations,
Royal Danish Defence College

Thomas Elkjer Nissen, MA has from 2001 worked at the Royal Danish Defence College (RDDC) as a Subject Matter Expert responsible for Strategic Communication (StratCom), Information Operations (Info Ops) and Psychological Operations (PsyOps). He conducts research, advises and teaches in the fields of Info Ops, PsyOps, Media Operations (Public Affairs) and the military's role in Strategic Communications and Public/Defence Diplomacy.



Royal Danish Defence College

The Royal Danish Defence College is the Danish armed forces' powerhouse for education, training and research-generated consultancy. Our research is conducted within a broad range of military-related topics. Our research priorities, such as topics and resource allocation are determined by the Commandant of the Royal Danish Defence College, who is aided by a research council.

Research at the Royal Danish Defence College should enlighten and challenge the reader, whether they are in the armed forces or in the surrounding environment. This is only achievable if the employees have the freedom to administer their own research projects and draw their own conclusions. This is a principle, which is honoured at the Royal Danish Defence College.

We hope you enjoy reading the Royal Danish Defence College's publications!

© Royal Danish Defence College

All rights reserved. Mechanical, photographic or other reproduction or photocopying from this book or parts thereof is only allowed according to agreements between The Danish Defence and CopyDan. Any other use without written consent from the Royal Danish Defence College is illegal according to Danish law on intellectual property right. Excepted are short extracts for reviews in newspapers or the like.

Copenhagen August 2011
Royal Danish Defence College
Ryvangs Allé 1
DK-2100 Copenhagen
Denmark
Phone: +45 3915 1515
Fax: +45 3929 6172
Editor: Flemming Splidsboel
Layout by Bent-Ole Kure
ISBN: 978-87-987720-3-3
Number printed: 300

Royal Danish Defence College Publishing House

Acknowledgments

The author would like to thank the staff of Royal Danish Defence College, several anonymous external reviewers and contributors and especially Professor Steve Corman, Arizona State University, Professor Dennis Murphy, US Army War College, Commander Steve Tatham, UK Defence Academy, Captain Henrik L. Schiott, Captain Thorboern Hein and not least Dr. William Mitchell, Royal Danish Defence College for their help with this paper.

In memory of Professor Philip M. Taylor, University of Leeds.

Abstract

This paper examines how the modern information environment affects the operational environment in contemporary COIN operations and how Information Operations (INFO OPS) fits into and supports these operations at the tactical level. Furthermore the paper looks at the techniques and capabilities that can be utilised for influence purposes in COIN, and not least all the things that lies behind the INFO OPS - specifically training and education, leadership, intelligence and planning principles unique to the successful conduct of Tactical INFO OPS in COIN.

Table of Contents

Acknowledgments	3
Abstract.....	4
Table of Contents	5
Table of Figures	6
Table of Acronyms	6
Introduction	9
PART I - COIN Operations Theory	11
The Contemporary Information Environment.....	14
The Role of Information in a COIN Environment	15
Insurgent’s Use of Information Warfare and Propaganda	17
People as the Centre of Gravity (CoG)	18
The Target Audiences	18
The Desired Effects	21
Target Audience Analysis – the link between the audiences and the effects	22
PART II - Tactical Information Operations	23
The Techniques	26
The Capabilities.....	29
Other Capabilities.....	32
The Missing Link – Public Affairs (PA)	35
PART III: Enabling factors	37
Education and Training.....	37
Leadership.....	41
Full spectrum Intelligence (knowledge development)	42
Planning.....	44
Planning principles.....	45
PART IV: From Theory to Practice	49
Way Ahead	51
Conclusion	53
Closing Perspectives	54
References:	55

Table of Figures

Figure 1.1 Characteristics of the modern information environment	15
Figure 1.2. Generic Target Audiences.....	21
Figure 1.3. Generic desired effects.	22
Figure 3.1. Education and training.	40
Figure 3.2. Planning principles for INFO OPS.....	49

Table of Acronyms

2iC	Second in Command
ACOS	Assistant Chief of Staff
AIDO	Afghan Information Dissemination Operations
AJP	Allied Joint Publication
ANA	Afghan National Army
BDA	Bomb Damage Assessment
BG	Battle Group
C2	Command and Control
C2W	Command and Control Warfare
CA	Civilian Affairs (See also CIMIC and CMO)
CA	Comprehensive Approach
CCIR	Commanders Critical Information Requirements
CCT	Combat Camera Team
C-IED	Counter-Improvised Explosive Device
CIMIC	Civilian – Military Cooperation
CMO	Civilian Military Operations (See also CIMIC and CA)
CNO	Computer Network Operations
CoA	Course of Action
CoG	Centre of Gravity
COIN	Counterinsurgency
COM	Commander
CONOPS	Concept of Operation
COS	Chief of Staff
CP	Counter-Propaganda
CST	CIMIC Support Team
CULAD	Cultural Advisor
CWA	Consent Winning Activities
DA	Direct Action
DCOM	Deputy Commander
DDR	Disarmament, Demobilisation and Reintegration
EBAO	Effect Based Approach to Operations

EBT	Effects Based Thinking
EW	Electronic Warfare
F2F	Face to Face Communication
FETS	Female Engagement Team
FOB	Forward Operations Base
FP	Force Protection
HN	Host Nation
HNSF	Host Nation Security Forces
HTA	Human Terrain Team
HTS	Human Terrain System
HUMINT	Human Intelligence
ICP	Intelligence Collection Plan
IE	Information Environment
IED	Improvised Explosive Device
INFO OPS	Information Operations
IO	Information Operations (US abbreviation)
IO	International Organisation
IPB	Intelligence Preparation of the Battle space
IPIE	Intelligence Preparation of the Information Environment
IW	Information Warfare
KLE	Key Leader Engagement
LI	Lessons Identified
LL	Lessons Learned
LOO	Lines of Operation
LTT	Lines To Take
MA	Military Assistance
MC	Major Combat
MCA	Military Cultural Advisor
MDMP	Military Decision-Making Process
MEDCAP	Medical Civilian Affairs Patrol
MILDEC	Military Deception
MISO	Military Information Support to Operations
MoE	Measurements of Effectiveness
NATO	North Atlantic Treaty Organisation
NCO	Non-Commissioned Officer
NGO	Non-Governmental Organisation
OPSEC	Operational Security
OSINT	Open Source Intelligence
PA	Public Affairs
PIR	Priority Intelligence Requirements
PMESII	Political, Military, Economic, Social, Infrastructure and Information
PPP	Presence, Posture and Profile
PSYACT	Psychological Action
PSYOPS	Psychological Operations
R&D	Rebuilding and Development

RFI	Request for Information
RIAB	Radio In A Box
RoE	Rules of Engagement
S	Staff
SC	Strategic Communication (See also StratCom)
SCAME	Source, Content, Audience, Media, Effect
SOF	Special Operations Forces
SR	Special Reconnaissance
StratCom	Strategic Communication (See also SC)
TA	Target Audience
TAA	Target Audience Analysis
TIC	Troops In Contact
TP	Talking Points
TPT	Tactical PSYOPS Team
TTP	Tactics, Techniques and Procedures
UAV	Unmanned Aerial Vehicle
USIA	US Information Agency
WAHM	Winning Hearts and Minds
WUR	Wind Up Radio

Introduction

Counterinsurgency (COIN) can be described as walking a fine line between on the one side winning the local population over to the side of the government, while fighting an armed insurgent that may also be a part of the local population.

Coalition forces currently conducting COIN campaigns are aware of the challenges that they face at the conceptual level, but still have some way to go in order to deal with the challenges. Especially, when it comes to dealing with the cognitive dimension of the fight to the degree necessary in a modern battle space and Information Environment. This has created new challenges for operational planners that partially have to be addressed by the focused application of Information Operations (INFO OPS.)

The aim of this research paper is to compile and organise as much information as possible about lessons identified concerning INFO OPS in support of a COIN campaign at the tactical level - primarily at the brigade, battle group, and company level.

The paper is intended to serve as inspiration for operators and not, on its own, a proposal for new doctrine. It intend to provide a taxonomy of general characteristics based on lessons identified on how INFO OPS can be used in a COIN environment, that can contribute to the future planning of education and training in, and operational planning of INFO OPS in a COIN environment.

Most can agree that INFO OPS plays an important role in counterinsurgency operations. Within NATO there are though differences in opinion on policy and doctrine in regards to INFO OPS application in COIN, but still most can also agree to the basic intention with the concept of influence in COIN. So the forces engaged in COIN generally appreciate the concept, and acknowledge the importance of INFO OPS. However little of the training offered help create the preconditions for effective INFO OPS in COIN.

Some forces engaged in COIN today have to some extent have been given some training in INFO OPS and capability the form of INFO OPS staff positions and Psychological Operations (PSYOPS) capability and so on, but what about the things – or preconditions – that lie behind? This is for example the organisation of staff elements for INFO OPS, the necessary training in Cultural Awareness, Human Factor Intelligence and leadership training at all levels to really understand the type of warfare that the units are about to embark on. The latter is especially a question of whether or not COIN theory has been operationalised to a level where it is directly applicable on planning and execution of tactical operations, or 'is it truly integrated into the military culture? Do the tactical leaders and commanders have the necessary focus on the strategic implications at the lowest levels of tactical operations? If they do not, the units and their commanders will most likely “fall back” to the “comfort zone” – kinetic operations – when “Winning Hearts and Minds” is found too fluffy to fit into the Military Decision-Making Process (MDMP).

The term “Winning Hearts and Minds” has become an integral part of the public, political and military discourse in recent times, but should we be talking about “Winning Hearts and Minds” at all? Moreover, how could we seamlessly integrate the term in modern COIN operations at the tactical level?

In order to do so, it can be argued that we need to get away from the not very easily implemented rhetorical concept of “Winning Hearts and Minds” and talk about more concrete relevant concepts such as the target audiences’ “*consent and trust*”. The target audiences *consent* to the forces’ presence and to its operations, and *trust* in what the forces say and do (words and deeds). Or in other words gain and maintain legitimacy and credibility. Not only for own forces, but to a larger extent the national security forces and the local government that the COIN forces are supporting. In consistency with that, it can also be argued that one of the key preconditions for obtaining this legitimacy and credibility is the structured and integral use of INFO OPS in COIN at the tactical level, since legitimacy and credibility first and foremost is a question of perception – and *Perception becomes reality!*

It can furthermore be argued that this practical implementation of COIN theory at the tactical level must be seen in conjunction with, or be held up against, the immediate strategic framework and information environment, as the two levels continuously influence one another and cannot be dealt with separately. This is one of other the major challenges in modern COIN at the tactical level. The development in the modern information environment and “new media” continuously lift the tactical actions and effects into the immediate strategic framework. So on one side, INFO OPS needs to be pulled down the funnel and be seamlessly integrated at the tactical level, and on the other hand it needs to be considered for within the strategic context.

The term “winning hearts and minds” might be misunderstood in the general discourse, as the benchmark description that indicates the degree to which one should be good to people and get them to love us; these normative and culture laden concepts are hard to measure in practice outside of a military discourse let alone in the kinetic realities of a battlespace; it does however offer a clear juxtaposition opportunity for explaining why the terms “consent and trust” are better suited as fundamental elements of INFO OPS integration in COIN, and easier to relate to practice.

In 1952, the Director of Operations and High Commissioner for Malaya, General Sir Gerald Templer, said that “*The answer lies not in pouring more troops into the jungle, but in the hearts and minds of the Malayan People*”. What he really meant was that the success in COIN lies in the population’s *perception* of the situation, and this perception comprises an emotional (hearts) and a cognitive (minds) component¹. These are the components of the population’s perception that INFO OPS have to address.

At first glance this might seem to be in stark contrast to today’s surge strategies in Iraq and Afghanistan, where there respectively have been poured over 30.000 more troops in order to halt the insurgency and turn around the situation; but the quote and the surge strategy is not necessarily an oxymoron. Taking that the surge it is not a question of pouring more troops in to fight the insurgency, but to protect the population and thereby creating a perception of the security that the population wants, then the surge contributes to perhaps not winning the populations *hearts and minds*, but to creating the desired *consent and trust*.

The paper is structured in four overall parts. Part one addresses COIN operations theory and its dilemmas, the modern information environment that contemporary COIN operations are conducted in and who, why and what Tactical INFO OPS should address in these operations. Part

(1) Dilegge, 2007.

two addresses Tactical INFO OPS, its capabilities and techniques. The purpose of this part is not to develop doctrine or to describe how to plan Tactical INFO OPS, but to discuss the employment of these capabilities and techniques specifically for COIN operations. Part three addresses all the factors behind the successful use of Tactical INFO OPS in COIN based on lessons identified. These lessons include findings on education and training, leadership, intelligence support and planning. Finally, part four discusses how the lessons identified can be operationalised, and present conclusions, reflections and perspectives on the topic.

The empirical data compiled and referenced in this qualitative study is drawn primarily through document analysis consisting of 'End-of-Tour' reports, interviews with commanders, Information Operations practitioners, and their subsequent briefings to Danish PSYOPS and Info Ops courses. This empirical trove of data is further supported by actual fact finding tours to mission areas, as well as relevant references to studies of contemporary literature and articles on COIN and influence. The majority of field data referred to throughout this study is drawn from Danish experiences in Iraq (Basra province) and Afghanistan (Helmand province), covering a period of seven years, from mid 2003 to early 2010.

PART I - COIN Operations Theory

Before we pull INFO Ops in a COIN environment down through the funnel to apply it at the tactical level, let us have a look at some of the basic theory behind COIN operations and the information environment that they are conducted in. First and foremost to distil the key elements of COIN theory directly shaping the execution of tactical INFO OPS. Much has been written about insurgency and counter insurgency in both academia and in military doctrinal sciences in recent times. Not only on the backdrop of Iraq and Afghanistan, but also to a large extent on historical conflicts. In classical COIN theory the main goal is the support of the population and the creation of a situation where the local population is mobilised and active, without the support of foreign forces, supporting the fight against the insurgents in the disputed area². This makes the local population the centre of gravity in COIN for both parties in the conflict. The emphasis on marginalising the insurgent in both the military and political dimensions is a defining feature in the classical COIN paradigm³. A fundamental understanding within this current stream of research is there is a need for an increased focus on attacking the political ties between the population and the insurgents by ways of persuasion. Establishing a perception of legitimacy amongst the local population is crucial⁴. This also means that a COIN fight will involve a wide range of instruments of power, including military, political, economic, and other civilian means – not only military capacities in a comprehensive approach. It also means that even though most COIN activities are conducted at the tactical level, the fight will entail all levels from strategic to tactical, blurring traditional lines of distinction.

Another defining common factor is that the support of the population should be focused on the Host Nation Government and not so much on the foreign forces conducting the COIN operations. The creation of government legitimacy, or a perception thereof, is hence crucial. The lack

(2) Thruelsen, 2009, p. 28.

(3) Ringsmose & Thruelsen, 2010, p. 59.

(4) Ringsmose & Thruelsen, 2010, p. 61.

of legitimacy of the government in the eyes of the local population is one of the most important factors igniting and prolonging an insurgency. The supported government must therefore be able to provide basic services to the population, because if it does not, it gives the insurgents an obvious issue to exploit for propaganda purposes. A large part of the government's legitimacy is the legitimacy and credibility of its security forces. The local population needs to be able to see a legitimate and credible alternative to foreign forces to satisfy their security needs, because in the long term the foreign forces will depart and the only thing left will be the host nation government - if the population cannot see an alternative they will support the insurgents for various reasons⁵, as it also goes for the provision of basic needs. As Sir Robert Thompson has said "*what the peasant wants to know is – does the government mean to win this war? Because if not, he will have to support the insurgent*".

Looking at the insurgency, the insurgent's goals may be diverse. It is about seizure of power through armed uprising, perhaps an attempt to establish an autonomous breakaway state, or a more limited aim of political concessions that is unattainable without the use of violence. Regardless, the aim the insurgent will attempt to force political change by a mix of *subversion, propaganda* and the application of *violence* aiming at *persuading or intimidating* the broad mass of the local population to support or at least accept such a change.

All insurgencies are unique, but there are some similarities. They all include inherent ethnic, cultural, religious or ideological cleavages in the society that result in a lack of national cohesion and a weak, inefficient, unstable or unpopular government. These cleavages form the basis of the root causes that the insurgents will try to exploit, by adopting methods and tactics that are suitable to the circumstances, and to their own particular needs. In order for the insurgents to have success they must have a unified leadership and organization. They must also have a vision for the future that is attractive to a sizeable part of the population, either because it is desirable or because it simply offers a perceived better situation compared to what the government can offer - for example basic security. The insurgents also need to control some territory from where they can operate like they also need external support to supply political / ideological / religious legitimacy, resources, training and sanctuary. That makes most insurgencies transnational⁶.

For the counterinsurgent this means that COIN is transnational, and to defeat an insurgency in a state, one must strive to break the insurgent's internal and external support. This is done through military, paramilitary (police), political, economic, psychological (informational) and civic activities with a high degree of host nation involvement at strategic, operational and tactical level. In other words, the employment of all elements of power at all levels. The main desired military effects are to provide security to the population, reducing the popular support for the insurgency, and to cut the insurgent's external support⁷, or to separate the insurgent from his support.

This effort also involves some degree of neutralization of the insurgents. In other words, kinetic operations are a part of COIN, ideally conducted by host nation security forces. The kinetic operations, however, should not be focused on reducing the number of enemies, but on the protection of the population. Kinetic operations that are likely to alienate the local population should therefore be considered in terms of risk, and mitigated in the planning process and execution (e.g.

(5) Thruelsen, 2009, p. 29 – 30.

(6) All though it is not the case in insurgencies as the one we see in Indonesia and the Philippines'. They do not need sanctuary, but can often find that in their own nations e.g. Aceh.

(7) For more on the desired effects see paragraph 1.2.3.

the consideration of non-kinetic effects of kinetic operations). Also, due to the fact that rumours' often drive public opinion or perception, all kinetic operations should be sought explained to the affected population.

The latter means employing effective INFO OPS as an integral part of COIN kinetic operations focusing on insurgents amongst the local population. Messages must be target audience analysis based, and tailored to the specific part of the population you want to influence. At the same time, multiple target audiences must be considered, since they in the modern information environment cannot be separated. INFO OPS must be proactive and maintain a steady drumbeat dominating the overall strategic framework while managing the implications of unfolding tactical events. It is also vital that local media is engaged and educated by COIN force. Concurrently Public Affairs must interact with the international and troop-contributing nations' media.

To be able to do this full spectrum, intelligence plays a vital role in COIN since the people are the "decisive terrain". Understanding the culture is a force multiplier and will reduce the insurgent's advantage, but the counterinsurgent must make sure that that message gets to every individual soldier⁸. The soldiers on the ground are key communicators in COIN interacting constantly with target audiences.

For the application of military force this means that the focus should be on protection of the population and capacity building of the local security forces and their ability to fight the insurgents rather than conducting anti-insurgent warfare, e.g. continuously offensive operations against the insurgents.

Every military action therefore needs to be viewed through the prism of its likely political consequences, and the local population's perception of these. Consistently, every political action carries with it implications for military operations⁹.

The counterinsurgent must therefore think carefully about everything that he does and understand the impact of his actions on the local population¹⁰. The counterinsurgent must simultaneously fight a war and build a nation, while having to work with the local population. A precondition for this that the counterinsurgent understands the culture and the complicated balance of power and the relationship between formal and informal leadership in the mission area in order to influence decision-making at the tactical level¹¹.

"In essence, effective COIN is a matter of good governance, backed by solid population security and economic development measures, resting on a firm foundation of energetic Information Operations, which unifies and drives all other activity"¹². COIN is in reality a two-front war. On the one front is the security operations and on the other is INFO OPS, and winning one and not the other will nearly always mean losing. They must be considered and planned together in order to achieve the desired effect. The latter – INFO OPS - is again on two levels – a strategic and a tactical. On both levels the development of the modern information environment has a large impact on the conduct of COIN operations, specifically on the counterinsurgent's ability to influence the situa-

(8) Based upon AJP 3.4.4.

(9) Amend, 2010, p. 219.

(10) COMISAF, 2009, p.1-2.

(11) Ferguson, 2010, 439.

(12) Kilcullen, 2009, p. 60.

tion. In other words, COIN conflict is conducted in an information environment, where perception and misperception very often outstrips and overtakes ground truth.¹³

The Contemporary Information Environment

The last two decades of technological development within information and communication, permits anyone to film, edit, and upload information and imagery in virtually real time, whether the normal news media are there to witness situations or not. Furthermore, modern communications technologies compress the operational levels of war. For example the ability to communicate instantly means that tactical events or actions can take on unexpected strategic meaning¹⁴. This is also known as “time – space compression”. Web blogs and YouTube are examples of new media platforms that empower individuals to achieve strategic political and military effects: easy upload of their videos, without editorial oversight, allows access to a nearly unlimited audience¹⁵.

This availability of off-the-shelf relatively affordable and portable media technology therefore makes it possible for anyone, insurgents, own soldiers, local nationals and many others to act as “citizen journalists”. Normal people have become empowered to film or otherwise capture situations in even the most hostile environments, to edit those images, and then upload them for the entire world to see; this includes news media that use the images in their news coverage of the situation.¹⁶ This very feature of the modern information environment is also what Sir Rupert Smith references in his book *“The Utility of Force”* when he discusses “war amongst the people” and states that the theatre of operations should be considered as a “theatre” with audience participation¹⁷, and that war has become a spectator sport. The audience consists of the general news media, and the local and international populations as direct or indirect spectators to the various media. The camera and the internet connected computer have therefore become weapons of war¹⁸, especially in low intensity conflicts as COIN.

The result of this empowerment created by the modern information environment is a matrix of real-time information flows that challenge the inadequacy of the structures of power (e.g. the military chain of command) to respond both with effective impact and in a timely manner.¹⁹

That information has value as an enabler for military operations is nothing new, but the rapid developments in the information environment have caused information to rise in importance.²⁰ In the last 15 years we have seen the development of a war fighting environment defined in two distinct domains for strategic reference: one physical and the other cognitive. There are many historical examples of the physical domain influencing strategic decisions, but we have comparatively little to offer when it comes to the cognitive one. Recent conflicts have shown that it is not easy to engage the cognitive domain once physical domain dominance has been achieved. Much strategy has in recent years been based on achieving physical dominance, where our opponent’s

(13) Mackey and Tatham, 2009, p. 6.

(14) Amend, 2010, p. 221.

(15) Murphy, 2008, p. 6.

(16) Dauber, 2009, p. 5.

(17) Smith, 2005, p. 289

(18) Murphy, 2008, p. 8.

(19) Gowing, 2009, p. 1.

(20) Murphy, 2009, p. 18.

main term of strategic reference has been the cognitive domain. The challenge is, amongst others, to understand the strategic informational impact of kinetically or otherwise tactically insignificant events, such as the Abu Ghraib scandal or other results of the “strategic corporal” incidents.²¹ This phenomenon also stresses the importance of the cognitive domain, where the media’s use of single tactical events to explain, or frame, the campaign’s success, or lack thereof, affects political decision-making. The medias access to single events has increased in tact with the extent news media outlets capitalise on viewers desire to produce their own content.²² The modern information environment, amplifies the ‘en masse’ cognitive impact of acts of violence²³ and thereby make them readily available to audiences’ world-wide to react on, including local nationals in conflict areas, publics and decision-makers in troop contributing nations, and to insurgents.

But having discussed the characteristics of the modern information environment, it is also important to bear in mind that even though “New Media” is playing an ever increasing role, traditional media (e.g. storytelling, Shuras in Afghanistan ect.) are still as important. So one must rather than only talk about “new” media talk about the “right” media.

Figure 1.1 Characteristics of the modern information environment



The Role of Information in a COIN Environment

The developments within information and communication technology and the unlimited access to information and distribution thereof have created new global challenges – also for COIN operations. No actor can operate in the modern operations environment without encompassing the importance of influencing the information environment of one’s opponents, possible opponents, and others, in order to achieve effects in support of the mission – that being a COIN or other forms of operations. Likewise, one’s operational planning must include taking into account the effects of opponents’ or possible opponents’ information activities directed towards own forces, population and other target audiences’ of importance to one self; not least decision-makers and populations in the mission area. In this context are also the coordinated and synchronised employments of activities that affect the information environment in order to create the desired effects on it of vital importance.

(21) Mitchell, 2009, p. 43 – 47.

(22) Dauber, 2009, p. 8.

(23) Cassidy, 2009, p. 118.

Insurgents as an asymmetric opponent will try to achieve effects on public opinion both at home, in the mission area, and globally through small, but spectacular, attacks followed up by propaganda, misinformation and intimidation²⁴. Likewise it must be expected that the insurgents will try to fill gaps between the counterinsurgents words and deeds with propaganda²⁵. Lessons from Iraq and Afghanistan show that the way operations are conducted and how they are told and framed are often more important in the long run than their actual tactical outcome²⁶. It is therefore the relevant target audience's perception of the outcome of the operation that is the most determining factor in regards to the final effect of the operation. In COIN it is therefore a decisive clash between two opposing entities, a process of persuasion, played out over time, where the population decides the outcome²⁷. Essentially, the counterinsurgent and the insurgent are presenting an argument for the future to the people of the country at hand. The population will decide which argument is the most attractive, most convincing, and has the greatest chance of success. The people are sceptical and unwilling to commit active support to either side until convinced of a winning proposition²⁸.

In this environment, the cognitive domain represented here by information and perception, moved from historic second place in terms of conventional conflicts and often become one the primary domain for determining the success of COIN. COIN can therefore be seen as a battle between competing narratives.

A narrative is a system of stories that share common themes, forms, events, and participants, and create expectations for how those elements can be assembled to satisfy a desire that is rooted on conflict²⁹. As such a narrative forms "a thematic and sequences account that conveys meaning from authors to participants about specific events"³⁰. Narratives are the organising framework for conveying a specific strategy or policy when events or decisions are to be argued and described. The purpose is to bind together all the actions of a government or alliance. Narratives should provide the structure for all messaging at all levels, from strategic to tactical. Narratives must therefore be designed with an inherent flexibility so that their essence is not destroyed as messages are crafted at different levels of command. It is though important to bear in mind that stories that are not "authored" by you (thus that you don't design) can become part of the system and affect the narrative in ways you can't control. In the end the narrative should be the framework for the planning of Tactical INFO OPS. In COIN, especially when fought by alliances or coalitions, the narrative must therefore be able to convey the policies of both the alliances, the troop contributing nations, and the supported government policies, as well as being able to mitigate known opponents' narrative or messages. As will be discussed later in the paper, it is one of the big challenges for Tactical INFO OPS to break down the political-strategic narrative to something useful and tangible for the local population at the tactical level in the mission area. Especially at this level the opponent (insurgent) will deploy his "counter-narrative". Insurgents often find it easier to appear successful in the information environment, by simply blowing up things, killing

(24) Ruca, 2008, p. 54 and AJP 3.4.4., 2010, point 0525.

(25) AJP 3.4.4., 2010, point 0230.

(26) Ruca, 2008, p. 55.

(27) Amend, 2010, p. 218.

(28) COMISAF, 2009, p. 1.

(29) Halverson, Goodall, & Corman, 2011

(30) Tatham, 2008, p. 9.

people and intimidating, and blaming the counterinsurgent or the supported government and its security forces. The counterinsurgents on the other hand face a far more difficult task of building governments and institutions. Destruction and violence have an immediate informational impact, whereas construction projects are slow to achieve effect³¹, and therefore not easily exploitable in the information domain.

Insurgent's Use of Information Warfare and Propaganda

What has often been ignored, however, are the challenges arising from the other side of the equation³². One of the most profound differences between past and present-day insurgencies lies in the exploitation by insurgents of modern information technology for information warfare³³. Modern insurgents have been very good at capitalising on this environment in their strategic engagements. The insurgents fight a battle to shape the perceptions and attitudes of the public, a battle over the public's very will to continue fighting. Be it the local population; or the domestic population in the troop contribution nations which the insurgents seek to influence in order to force the COIN force to withdraw from the mission prematurely³⁴. Insurgents therefore use the possibilities afforded by the modern information environment to create both strategic and tactical effects that go beyond traditional battlespace topographical demarcations.

Strategically insurgent groups try to influence globally. To an ever increasing degree insurgent groups will use "new media" like online video sharing sites such as YouTube, Liveleak, and social network applications as Twitter and Facebook in their strategic activities³⁵. This makes them less depended on normal news media to communicate with the outside world, although it is still a part of their propaganda effort to use normal news media as an intermediate channel. In fact, to an unprecedented degree, normal news media have become dependent upon the insurgents for information and imagery along with what "citizen journalists" provide. Today, insurgents can both act as the owner or direct sender of information via new media and act as citizen journalists, both overt and covertly. Insurgent groups also try to influence the global information environment and specifically the troop contributing nations' public debates.

Tactically insurgent groups try to influence local population's perceptions, attitude and behaviour through a combination of propaganda and violence. Insurgent attacks may be designed to trigger disproportionate government (counterinsurgent) response that alienates the local population³⁶ or exploit gaps between the government's words and deeds.

Insurgents embed communications at the very heart of their operations, and conduct physical operations and other significant actions that are designed to create psychological impact far beyond the immediate victims. They do not try to win battles, but to portray omnipresence and a determination to stay the course. Also, as an integral part of their modus operandi, insurgents will try to generate spectacular media events at the tactical level in order to attract media attention and get into the strategic mainstream news – this can e.g. be hostage situations, claims of

(31) Cassidy, 2009, p. 117.

(32) Ringsmose & Thruelsen, 2010, p. 57 and Nissen, 2007, p. 6.

(33) Amend, 2010, p. 221.

(34) Dauber, 2009, p. 2.

(35) Dauber, 2009, p. 4.

(36) Amend, 2010, p. 220-221.

collateral damage inflicted by the counterinsurgent, IEDs, and so on. The insurgents will adapt to local conditions. They influence the population through intimidation and attraction. In their propaganda they claim to protect the local culture and religion. They incite social strife and undermine traditional structures. In places, they control the roads, collect revenues, and mete out swift justice. They co-opt disenfranchised groups and pay young men to fight. They exploit the counterinsurgents mistakes and inappropriate actions to reinforce their argument³⁷.

The counterinsurgent – and the supported government - on the other hand must undermine the insurgent’s argument while offering a more compelling alternative, backed up with actions (deeds), to the contested people. Both strategically and tactically, people and their perceptions are considered the Centre of Gravity.

People as the Centre of Gravity (CoG)

COIN is a contest to influence the real and very practical calculations on the part of the people about which side to support. Every action, reaction or lack thereof becomes a part of the people’s debate. The people in the audience watch, listen, and make rational choices based on who can better protect them, provide for their needs, respect their dignity and their community, and offer opportunities for the future³⁸. This is why the people are the Centre of Gravity (CoG).

But even though there is a general consensus about the people being the CoG of COIN this notion has been challenged by some that state that it is the root causes and not the people that are the CoG³⁹. The argument is that the insurgency needs a cause to attract people to in order to win them over to their side. But the problem in this argument is that there might be several causes or fundamental problems. Furthermore the reason for continued struggle can be caused by many other factors other than the ones initially sparking the insurgency, especially the longer the insurgency goes on. Both the insurgent and the counterinsurgent must therefore address both the root causes and the causes for the continued struggle when trying to win the population’s support. For the counterinsurgents part, this is done through the comprehensive approach to tackling the problem with military as well as political, economic, and other civilian means addressing security, governance and development, the insurgent then tries to counter the progress in these areas. Addressing and perhaps solving the root causes does not necessarily mean that the insurgents will stop their campaign, and if not they will still need the support of the people. Likewise, the people whom the insurgent do win over might not support the insurgent’s cause, but support the insurgent for other reasons, based on practical calculations. In the end it is therefore still about the people and their perceptions, making them the Centre of Gravity.

So if the Centre of Gravity is the people, then they are also the Target Audiences (TAs) for the INFO OPS.

The Target Audiences

People as the Centre of Gravity can be broken down to a series of generic Target Audiences in COIN, although these need to be further segmented dependent on the situation. Besides the “strategic” target audience, the home audience, the coalition / alliance audiences, the wider

(37) COMISAF, 2009, p. 2.

(38) COMISAF, 2009, p. 3.

(39) Krieger, 2007, p.96.

international audiences, and the regional audiences, there are the theatre based or local target audiences. It goes for all the above mentioned audiences that they, as with the design of the effects, in general terms need to be segmented in the “supporters”, the “natural” and the “hostile”, and furthermore need to undergo “target audience analysis” (TAA).

The “strategic” audiences are addressed by Strategic Communications, Public Diplomacy and Public Affairs, whereas the theatre or local audiences are addressed by INFO OPS and Public Affairs.

When talking about target audiences it is important to think not just about finding the audiences but also to think about the mechanism, person or group that will influence the target audience for us.

The generic theatre based or local target audiences include:

- **Local population in general.** They can then be divided or segmented into sub-target audiences such as men/women, young/old, urban/rural and otherwise geographically, but also ethnicity, religion, languages, political views, profession and so on can be used to segment the target audience⁴⁰.

An often underestimated target audience is women. Especially in connection with getting messages into family structures or networks, women in Iraq and Afghanistan, and elsewhere, have shown themselves to be an important target audience. Can you mobilise family networks via the women you are one step closer to reaching parts of your target audiences that you otherwise would be excluded from reaching⁴¹. It is, though, a precondition that you have female soldiers and interpreters in your unit at the tactical level that can be a part of Tactical Psychological Operations (PSYOPS) Teams (or TPT), Civilian – Military Cooperation (CIMIC) Teams and the like as needed⁴². Alongside this approach, Face-to-Face communication in the streets done by normal patrols, and Key Leader Engagement can be employed.

The geographical segmentation of local target audiences at the tactical level can be very important as there can be large differences on the local perceptions and attitudes even within a few kilometres of each other. Even if the target audience is of the same ethnicity, religion, language, just living on different sides of a distinct terrain feature can alter their conditions to such a degree that different Lines of Persuasion must be used to achieve the same effect⁴³.

(40) A Target Audience especially valuable, or be of special concern, is “local workers” inside own bases. They can act as intermediate target audiences (communicators by proxy) and give information on the effect of engagements with other target audiences, including giving atmospherics or reports on what is going on “outside the wire” on a daily basis. On the other side they will also see how own forces behave “inside the wire”, and will report this where they come from making them a very important target audience in terms of our “deeds” and the signal they send. (McKenna and Hempsey, 2010, p. 12.)

(41) Kilcullan, 2006, p. 33.

(42) The use of Female Engagement Teams (FETS) in Afghanistan coupled with CULADS is increasing but opinion on the effect is divided. Are women the power behind the throne or completely devoid of influence on the men? There is no conclusive evidence either way in current LL/LI or literature.

(43) One also has to be aware that even locally many audiences outside the intended one will hear the messages. Crafting messages with this risk in mind is important.

-
- **Leadership and opinion makers.** Dependent on the social and political structures these can be very different, but are often divided into sub-target audiences as formal and informal powerbrokers, influential public figures, religious leaders, and cultural or media personalities. In general, people that due to their position or status have an impact on other target audiences perception/understanding, attitude/will and / or behaviour, or who themselves have the power to affect an outcome or a desired effect.
Government agencies and institutions, local administrative structures and political parties also belong to this target audience.
 - **Local security forces.** Be that military, police or some other part of the local security forces. They to need to be segmented into sub-target audiences, such as their branch, and within these branches into low-level, mid-level and high-level (leadership).
 - **Insurgents and their supporters.** Again divided into low-level, mid-level and high-level (leadership). It can also be necessary to divide them into local and foreign members, just as well as there can be more than one insurgent group in the conflict. Their supporters can also be internal and external, and need to be divided accordantly.
 - **Other armed fractions.** This can be local militias not necessarily opposing own forces, criminal organisations, and so on.
 - **Local media.** Local media outputs and journalists can be a very valuable target audience to getting one's messages out, have local security forces framed in a positive way and insurgents in a negative; or making it harder for the insurgents to get their messages into the local media. The problem is, though, that Military Public Affairs deployed in theatre often almost exclusively focus their resources and time on international and national media. National media understood as the troop contributing nations own media to service national interests and audiences. This is naturally important taking the strategic framework, the modern information environment and the strategic Centre of Gravity into the consideration; but it leaves out a tool to reach, and influence, many of the other target audiences (local population, leadership and security forces). How many Public Affairs Officers for example normally speak the local language and can therefore interact with local journalists and media outlets?
Local media and journalists also need to be divided into sub-target audiences dependent on their political affiliations, editorial line or their reach / food print or own audiences.
 - **Third parties in theatre.** This can be different interest organisations, non-governmental organisations (NGOs), and to some extent media. Also some alliance, coalition government or host nation contractors can be third parties in theatre.

Figure 1.2. Generic Target Audiences.

Generic Target Audiences
<ul style="list-style-type: none"> • Local population • Leadership and opinion makers • Local Security Forces • Insurgents and their supporters • Other armed fractions • Local media • Third parties in theatre

Although not a target audience, own forces must also be informed about the messages being sent out in order for them to act accordingly, and not contradict the messages by their own behaviour⁴⁴. Having identified the Centre of Gravity and the Target Audiences we need to look at which effect we need to achieve on them.

The Desired Effects

As with target audiences there are a series of generic desired effects (influence objectives) in COIN operations. Common for these effects are that they are local population centric in order to support the focus on the Centre of Gravity in COIN. This does not mean that the effects should not be focused on the opposing forces, other armed fractions or supporting own forces as well, but that the main effort is on “supportive” and “natural” target audiences in order to adhere to one of the principles in COIN: maintain and reinforce the support of the friendly, win over the undecided and weaken the will of and undermine the support for the hostile⁴⁵. The generic desired effects include:

- Gain and maintain *consent and trust* with the local population, local powerbrokers, and local security forces. This is in order to build credibility and legitimacy for own forces, and to support Force Protection (FP) and Force Multiplication initiatives.
- Foster and create local acceptance of and trust in host nation (NH) administration, government and security forces in order to support them and create the conditions for their control. This entails promotion and empowerment of local government. Image Enhancement of local security forces (their legitimacy and capability) in order to make them credible in the eyes of the local population and the opposing forces, as well as boost their moral and self-confidence. Special attention ought to be given to those that serve the people.
- Foster local ownership for the political project and the end-state.
- Reduce the local support for the insurgents, undermine the insurgents credibility and lower

(44) McKenna and Hempsey, 2010, p. 12.

(45) AJP 3.10.1(A), 2007, point 0106. And Galula, 1964, p. 53. Galula describes the three main target audiences as: The minority that supports the counterinsurgent, the majority that is natural and the minority that supports the insurgent.

the insurgents morale, to include undermining the insurgent's will to fight and his perception of his ability to win. This can entail support for Disarmament, Demobilisation and Reintegration (DDR) programs⁴⁶.

- Drive a wedge between the insurgents internally and between their internal and external ideological, political and financial supporters. This can include driving a wedge between low level fighters and their leaders. If an approach like this is chosen, one has to be very careful not to alienate target audiences that one wants to win over, such as members of the local communities that might have been recruited by the insurgents.
- Counter and mitigate the effects of insurgent's propaganda and intimidation of the local population⁴⁷.

Figure 1.3. Generic desired effects.

Generic desired effects:

- Gain and maintain the local population's consent and trust
- Foster local Government and Security Forces
- Foster local ownership for the political project
- Reduce support for the insurgents and undermine their will
- Drive a wedge between the insurgents and their supporters
- Counter and mitigate the effects of insurgent propaganda

Besides the "tactical" desired effects centric to target audiences in theatre there is of course also a series of effects linked to the strategic level, to include gaining and maintaining international and home audience public support and the support of international organisations and media, at the same time discouraging unwanted third party involvement. Common for both the tactical and the strategic desired effects is that they are centred on legitimacy and security.⁴⁸ Also common for the desired effects at both levels, which are all cognitive, is that they are tied to subsequent desired behaviour!

Target Audience Analysis – the link between the audiences and the effects

Target Audience Analysis (TAA) is the key to successfully being able to influence 'just' the "the minds of the people that matter".⁴⁹ TAA is a methodological approach to analysing and understanding the audience and is the beginning and end of military INFO OPS as it links the audiences to the effects and the assessment of success.

TAA aims at constructing a profile of the audience and how it can be influenced, with which means, and how to measure the success of the influence activities⁵⁰. TAA is an integral part of the overall

(46) Terence, 2006, p. 57.

(47) AJP 3.4.4. 2009, point 0526. And Terence, 2006, p. 54.

(48) Labarre, 2009, p. 75.

(49) Adams, 2009, p. 5.

(50) Rowland and Tatham, 2010, p. 2 – 4.

INFO OPS planning and focuses on identifying whom to influence to achieve the desired effect, and the conditions (physical and psychological), vulnerabilities (or motivations), susceptibility and accessibility of the target audience⁵¹.

For the TAA to have success it must therefore achieve at least four overall objectives⁵².

- The precise identification of the optimal target audience to achieve the desired effect.
- Measure the “influenceability” of the target audience.
- The best process to influence the audiences (means).
- Produce and deploy the “triggers” that will effectively and measurably change the audiences behaviour.

The latter also links to the necessity for the assessment of success to be observable with “impact indicators” which are therefore constructed in connection with the TAA process as a part of the overall influence planning.⁵³ In connection with the TAA process and the development of Measures of Effectiveness is also the establishing of a baseline against which success can be measured an important task.

Having discussed the fundamentals of COIN operations, the information environment wherein they are conducted, the Centre of Gravity for it, the Target Audiences the analysis of them, we now need to look at the means with which to cause effect – Tactical INFO OPS.

PART II - Tactical Information Operations.

Defining what we are talking about might just be one of the hardest things when talking about INFO OPS, especially in multinational contexts. Within the last decade research into information as a military tool, and the coordination thereof, has become a growth area. Starting back in the early 1990s and up through the 2000s we have been talking about Command and Control Warfare (C2W), Information Warfare (IW), Information Operations (Info Ops or IO) to name just a few, and now INFO OPS. Recently also Strategic Communications (StratCom or SC) has become a part of the development and the vocabulary⁵⁴.

It has been heavily discussed at which level the activity should reside, which capabilities (Electronic Warfare - EW, Psychological Operations - PSYOPS, Physical Destruction and so on) it encompasses, how these capabilities are related to it (core, related, or supporting), and whether or not it is a function or a capability in itself such as the current relationship to Public Affairs (PA), an ongoing discussion.

The result is a developmental process that has muddied the waters, even for those working with “influence”. It is even worse for commanders in the field, who increasingly have to be able to think beyond current doctrine; doctrine, which tends to focus on the employment of Influence (or Information Operations) in Major Combat (MC) operations and not in COIN, and moreover tends to treat Info Ops and its capabilities somewhat isolated⁵⁵.

(51) FM 3-05.302, chapter 6.

(52) Rowland and Tatham, 2010, p. 2 – 4.

(53) For more on assessment see point on assessment in planning principles (3.4.1.)

(54) Strategic Communication (StratCom) can be defined as: A systematic series of sustained and coherent activities, conducted across strategic, operational and tactical levels, that enables understanding of target audiences, identifies effective conduits, and develops and promotes ideas and opinions through those conduits to promote and sustain particular types of behavior. (Tatham, 2008,)

(55) Larson [et al.], 2009, p. xxi.

A number of countries most notably the US, but also the UK and others, have for a long time had Information Operations doctrines and manuals. NATO as an organisation have for a long time been struggling with the concept of Info Ops, and with getting policy and doctrine in place. On the backdrop of the Kosovo Air Campaign in 1999⁵⁶ NATO realised that it needed an Info Ops doctrine and started the development work in early 2000. But it was not until 2009 that NATO finally agreed on a policy and a doctrine for Info Ops. The new challenge is to come up with concepts for the application of Information Operations in COIN Operations. In this process Info Ops is increasingly being referred to as INFO OPS, which is muddling the waters.

Since there is no commonly agreed definition of "Tactical INFO OPS", let's take a look at the US, UK, and NATO definitions on Information Operations in order to find some commonalities upon which to build an mutual understanding of what Tactical INFO OPS in COIN is, or can be.

- US defines Info Ops (or IO) as "The integrated employment, during military operations, of information-related capabilities in concert with other lines of operation to influence, disrupt, corrupt, or usurp the decision-making of adversaries and potential adversaries while protecting our own".⁵⁷
- UK defines Info Ops as: "A military function to provide advice and coordination of military information activities in order to create desired effects on the will, understanding and capability of audiences, consistent with a UK Information Strategy".⁵⁸
- NATO defines Info Ops as: "Info Ops is a military function to provide advice and co-ordination of military information activities in order to create effects on the will, understanding and capability of adversaries, potential adversaries and other NAC approved parties in support of Alliance mission objectives".⁵⁹

The US definition talks about the integrated employment of information-related capabilities and other lines of operation to affect decision-making, where the UK definition talks about the co-ordination of information activities to affect will, understanding and capabilities of audiences. The NATO definition sounds a lot like the UK definition, but talks about "approved audiences". All three definitions talk about Info Ops as supporting the achievement of objectives, being that information strategy (UK) or mission objectives (NATO).

However, at the end of the day -regardless of policy, doctrine, definitions, inclusion or exclusion of capabilities - the basic planning assumption for Info Ops is that it should coordinate the effects of military information activities and capabilities on the information environment. Furthermore that Info Ops therefore basically, based on the commanders mission and intent, looks at identifying desired effects on the information environment, targets, or target audiences to be affected, to achieve the effect, means (techniques and capabilities) to apply and measurements of effectiveness (MoE).

(56) Operation Allied Force (OAF)

(57) OSD, 2011, p. 2.

(58) Briefing by Commander TIO/UK MoD at IQPC Info Ops Conference Europe, London June 2009. (authors notes).

(59) AJP 3.10, 2009, p. 1-3.

A new discussion between academics and practitioners started after the wars in Iraq and Afghanistan on how to apply Information Operations on counter insurgency operations. A discussion that has also been heavily influenced by other developments in military affairs such as the Effects Based Approach to Operations (EBAO), or Effects Based Thinking (EBT) as it is referred to in NATO today, and the reinvention of COIN doctrine.

But can you at all talk about “*tactical*” INFO OPS in COIN? Some would argue no! - And they might just be right. Everything done on the tactical level in COIN can quickly have strategic impact, and should first and foremost be driven by a strategic intent (narrative as far as the communication goes) and end state. But it is however at the tactical level that military forces conduct information activities in support of COIN, and therefore on the tactical level you will find the techniques and capabilities employed – with due consideration to the strategic framework!

As stated in the introduction it is not the purpose of this paper to come up with yet another definition on INFO OPS that can confuse even more, but to put forward a *view* on what Tactical INFO OPS in COIN should be able to do:

First of all Tactical INFO OPS should be consistent with, or in alignment with, the strategic framework, e.g. the strategic narrative, the information strategy or the like, but naturally transformed to the appropriate level to make sense. Secondly, advice on desired effects, and second and third order effects of own planned actions as well as coordinate (planning) the effects of the techniques and capabilities employed.

Figure 2.1. Techniques and capabilities in INFO OPS

Techniques	Capabilities
<ul style="list-style-type: none"> • Key Leadership Engagement (KLE) • Presence, Posture and Profile (PPP) • Psychological Actions (PSYACTs) • Military Deception (MILDEC) • Counter-Propaganda (CP) • Operations Security (OPSEC) 	<ul style="list-style-type: none"> • Staff organisation • Psychological Operations (PSYOPS) • Civilian Military Cooperation (CIMIC) • Combat Camera Team (CCT) • “Other Capabilities”
Full spectrum Knowledge Development (KD)	
Planning (to include target audience analysis)	

It is imperative, though, to bear in mind that Tactical INFO OPS, and the techniques and capabilities employed, like fires and manoeuvres, logistics and engineers just to mention a few, are not planned, executed and assessed in isolation, but as an integral part of the operations.

The purpose of the discussion on the techniques and capabilities below is not as much how to plan for them, but more what their role and function in COIN are.

The Techniques

The techniques are all considerations and actions that INFO OPS as a staff function can advise on and plan for. The techniques, however, requires other capabilities, commanders and troops as an integral part of the operations plan, to be executed.

- **Key Leadership Engagement (KLE):** KLE and other Face-to-Face communication (F2F) activities are some of the most important forms of influence activities in COIN operations, as they to a very high degree involve the target audiences. In many traditional societies, personal relationships hold the key to getting business done. Making the effort to build relationships – sitting for hours, drinking green tea, and simply listening – will make a profound difference⁶⁰, and can serve to identify one another’s motives. KLE however can be frustrating and unproductive, because people in many cases are untrained in the art of gathering information in a discussion format. Training of commanders to engage in KLE is therefore imperative⁶¹.
KLE is an often misused term. It is many places used to describe all interactions with the local population, whether these are powerbrokers or not. KLE is the planned interaction between own forces’ high ranking leaders, on several levels, and their peers in the local community, within the civil society, the government or administration, and the security forces. All other interactions, no less important, is F2F communication - most often conducted by patrols and others operating amongst or otherwise interacting with the local population.
A part of KLE is the building of networks within the local society between the force and local powerbrokers and other influential figures such as political, religious, economic or media leaders. These networks can then be used for messaging, mobilising the population or simply gaining information, particularly if the networks are established before they are needed. Actions that can help facilitate the establishment of such networks and relationships must therefore not be overlooked.⁶² When networks are established and KLE is undertaken it can help the force in identifying key issues and concerns of the local population, provide the ability to see how local security forces are accepted by the local community, and how the local security forces, especially their leaders, are interacting with local key leaders⁶³.
All KLE and F2F activity ought to be based on Talking Points (TP) to ensure “Unity of Message”.⁶⁴ But as discussed later on in this paper the use of talking points requires training to avoid the messages coming out as memorised “one-liner’s”. The TP’s must be used according to context – a skill that not all leaders and soldiers that engage in KLE and F2F today possess.
- **Presence, Posture and Profile (PPP):** Also known as “own forces behaviour” is essential in COIN. The way that the counterinsurgent acts has to be in line with the message or the signal that he wants to send to local population or the target audiences. This can often mean a soft approach to the local population even though it means a lower level of force protection. On

(60) Amend, 2010, p. 228 and Ferguson, 2010, p 439.

(61) McKenna and Hampsey, 2010, p. 10.

(62) Kilcullen, 2006, p. 32.

(63) McKenna and Hampsey, 2010, p. 10.

(64) Talking Points (TP) are also sometimes referred to as Lines to Take (LTT). TP are short lists over relevant themes and messages and or the unit’s response to current topics of concern in the local information environment. TP are derived from the current information strategy or influence plan to ensure unity of message with all other ongoing information activities.

the other hand, a good relationship to the local population can also mean an increased force protection on the longer term. In the other end of the spectrum, a hard approach can also be used to send a signal to the opponents.

Boiling PPP down, it is often a question of the individual soldier's behaviour, and the consequences thereof. There is sometime a need to ask the troops to pause for a while and think how they would expect a foreign army to operate in their own neighbourhoods, amongst their children, and ask them to act accordingly⁶⁵. The doctrinal approach to PPP is:

Presence is about being at the right place at the right time. The mere presence of forces can have a perceptual effect on the target audiences by for an example reinforcing messages about commitment.

Posture is all about appearance, how the soldiers on the ground are dressed, the classic question of helmet or beret, and whether the force patrols mounted or dismounted, in armoured or un-armoured vehicles.

Profile is mostly about the public appearances of commanders, interviews with mostly local media and participation in meetings and so on⁶⁶.

To achieve unity of message in deeds (PPP) and words, centralised instructions on PPP have to be issued, normally in the form of PPP instructions in the operations order under "coordinating instructions". But even though such centralised instructions have been issued, the local commander and leaders must also have the freedom to adjust them to the situation he or she stands in to meet local conditions⁶⁷. Conditions around a remote Forward Operation Base (FOB) might for example be different from the general operational environment. Hence local PPP might be suitable for shorter periods of time. This can also apply to strike or combat operations where a specific enemy target is engaged. There, a hard approach can be the most suitable both serving force protection and influence purposes, especially in connection with targeting the enemy's will and morale. Still since "war can no longer speak for itself"⁶⁸, a hard approach has to be chosen on the basis of an analysis of the perceptual impact on the local population. At least a plan for explaining the local population and the media why perhaps overwhelming force has been used must be in place. PPP ties into PSYACTs as well.

- **Psychological Actions (PSYACTs):** a PSYACT can be defined as "an action conducted by non-PSYOPS personnel that is planned primarily to affect the behaviour of a target audience"⁶⁹, or in other words actions or activities planned primarily for its psychological impact. PSYACTs can in the one end of the spectrum be raids, strikes, show of force or exercises and in the other end for an example Consent Wining Activities (CWA) done by CIMIC. All military operations and activities have some form of psychological impact, but it only becomes PSYACTs when it is planned to have a specific effect. The assets used for PSYACTs will normally be

(65) COMISAF, 2009, p. 5.

(66) AJP 3.10, 2009, p. 1-8.

(67) Kilcillen, 2006, p. 32.

(68) Quote: Professor Philip M. Taylor (conversation with the author 30. April 2010)

(69) FM 3-05.302, 2005, Glossary-14.

either manoeuvre units or Special Operations Forces (SOF), but all PSYACTs will be supported by PSYOPS.⁷⁰

PSYACTs therefore closely tie into other INFO OPS techniques such as PPP, MILDEC and capabilities like PSYOPS and CIMIC.

- **Military Deception (MILDEC):** Tactical deception can be used to divert enemy attention from areas where you want to operate and thereby uphold operational security and freedom of manoeuvre.⁷¹ This can be done by utilising for example PSYOPS assets and techniques in a supporting role, without lying⁷², or through manoeuvre. The purpose can be to make the enemy think that you are preparing to attack a certain area or objective that you are not and thereby manipulating him into disposition his forces wrongly; or to make the enemy disclose his positions by manning combat positions, taking weapons out of hiding places or activating his command and control systems, making it possible for you to target him. It can also be in support of combat operations through the classical use of smoke, vehicle noise, loudspeakers and the like in order to conceal your own movements and dispositions.⁷³ On the other hand you also have to be aware of the risks involved with using deception in relation to the local population in regards to long term credibility, and the effect on other communicative activities conducted in the area.⁷⁴
- **Counter-propaganda (CP):** At the tactical level more often than not insurgent propaganda is directed at the local population in order to influence its will and ultimately its behaviour. All units engaged in COIN therefore continually have to monitor the tactical or local information environment in order to identify insurgent and third party propaganda: directed towards the unit itself or the target audiences of importance to it. This is of course to be able to analyse it and counter it. When countering or mitigating the effects of insurgent propaganda it is not always through the use of words, it can also and often be through actions that prove that the insurgent propaganda claims are wrong. Insurgents are acutely aware of this and try to exploit it as well. Insurgents might for example try to mirror own forces PSYOPS techniques, products and messages in a slightly altered version (imitative deception).⁷⁵ In Iraq, for example, there have been several examples of propaganda posters that have been booby-trapped with Improvised Explosive Devices (IEDs), detonating when coalition soldiers have torn them down. It can also upset parts of the local population, and thereby alienate some of the uncommitted, if coalition forces go after the propaganda products themselves instead of focusing on countering the intended effect of the propaganda, sometimes best done through actions (deeds) rather than words. The challenge is, though, that insurgent propaganda is often based upon the actions of own forces, or mis-actions such as collateral damage; or that insurgents “frame” own forces’ operations

(70) FM 3-05.301, 2003, p. 6-24 to 6-26.

(71) CALL, 2006, p. 35.

(72) When planning deception operations using PSYOPS capabilities in some form or another it is important to be careful not to compromise PSYOPS credibility.

(73) CALL, 2006, p. 36.

(74) Todd, Paul and Glenn, 2007, p. xix.

(75) Also described as “black propaganda” in NATO PSYOPS doctrine, where a false source is advertised and the product or activity is produced by a different individual, organization or government then claimed. AJP 3.10.1, 2007, Glossary, p.3.

to fit their claims, and own forces thereby have delivered some of the “ammunition” for the insurgent propaganda.

An important part of counter-propaganda is therefore education. Education and training in how to report identified propaganda; how PPP can help to prevent insurgents from getting material substantiate their claims; in use of New Media⁷⁶, and in what the insurgents want to achieve and their techniques in order to pre-emptively minimise the effect of insurgent propaganda if it is directed at own forces.

- **Operations Security (OPSEC):** In both NATO and different national doctrines Operations Security is a part of Information Operations. OPSEC is a process which gives a military operation the appropriate level of security, using passive or active means, to deny the enemy knowledge of own dispositions, capabilities and intentions.⁷⁷ OPSEC is thus *fundamental to all military operations*, not only INFO OPS. It can therefore be discussed whether or not OPSEC should be a part of the INFO OPS techniques, but OPSEC on the other hand ties into quite a few of the core activities in INFO OPS. First of all the planning and execution of deception operations, but also in PSYOPS to protect planned themes, messages and products until they are disseminated to avoid enemy countering our PSYOPS. It also ties heavily into Public Affairs, primarily in what information a PA can release to the press and the public. OPSEC also ties into own forces’ use of “new media”.

The Capabilities

The capabilities are all actual capabilities that can be tasked to perform specific actions as a part of the Operations Plan (OPLAN):

- **Staff organisation:** The staffs on Battle Group and larger formations (brigade and division) levels in COIN ought to be organised in a way that enables special focus to be put on INFO OPS. It is an on-going discussion whether Influence should be organised as an integral part of the operations section; spread over the entire staff structure; or whether it should be organised in a separate section or cell directly under the Chief of Staff (COS) or Deputy Commander (DCOM) with an Assistant Chief of Staff (ACOS) as chief. It can be argued that it should be placed in the operations cell in order to fully integrate it into the operational planning and execution. The premise for this argument is, though, that ACOS operations and the rest of the operations staff understand and integrate influence into the planning, and do not “overlook” it, when planning manoeuvres and fires. INFO OPS is a process of advice and coordination and that is why all members of staff most understand INFO OPS and their role in its planning. This is not always the case. On the other hand it can also be argued that INFO OPS in COIN is so important that it needs to have a more prominent role within the staff and be represented by an ACOS in order to have that necessary visibility in the staff. Furthermore, it can be argued that having the subject matter experts in INFO OPS in a single staff section and thereby having the core competencies and experience to plan the integration of Influence, the section as a

(76) See also the discussion on New Media in “education and training” under “what lies behind” later in this paper.

(77) AJP 3.10, 2009, p. 1-9.

whole can better contribute to the “Concept of Operations” (CONOPS) development⁷⁸. Either way influence ought to be a part of the commander’s intent driving to staffs planning in the first place – including an “information-end state” as a part of the intent.

Danish experiences at Battle Group level from six teams in Afghanistan have shown the value of a non-doctrinal concept called “S9 INFO OPS Cell”. The Cell consists of six people in all, an ACOS who is the principal Influence advisor to the Commander and the staff, an Influence planner, a PSYOPS planner, a CIMIC planner and two Public Affairs Officers.

Besides the INFO OPS section staff sections in all staffs starting at battle Group level ought to have Influence (primarily PSYOPS) trained personnel embedded, especially intelligence and operations sections, in order to ensure the integration of Influence into intelligence collection and operations planning⁷⁹. The role of the intelligence section is discussed at length later in the paper.

Having an organisation tailored for tackling INFO OPS is a planning and advisory capability in itself and it ensures that the influence techniques and other influence capabilities are taken into the planning.

Military Cultural Advisor (MCA) is a new concept at tactical level. The MCA situated in the Intelligence section is contributing to intelligence, command and INFO OPS with operationalised tactical advice on culture based upon cultural analysis. On the basis of the Danish Defences traditional *Military Linguistic Officer* education, which originally focused on language and intelligence / interrogation, this new concept’s core competence is still language – but with an increased focus on the history, politics, religion and social conditions of the language area, combined with cultural analysis methodology and operations / tactics.⁸⁰

- **Psychological Operations (PSYOPS):** PSYOPS is one of the most important core INFO OPS assets amongst the capabilities. It is, besides the techniques KLE, F2F and PPP, the only direct provider of information and messages to the target audiences in the operational area. The availability of PSYOPS capability is therefore a precondition for effective INFO OPS in COIN at the tactical level. PSYOPS should perform three overall tasks. Firstly drive the understanding of the local target audiences through collection of information (along with other Influence capabilities that are in contact with the target audiences), second disseminate information and messages, and thirdly assess whether or not proposed or previously disseminated products have any effect (MoE).⁸¹

The PSYOPS capability should be able to analyse (*especially target audience analysis, TAA*), plan, produce and disseminate PSYOPS messages through printed products, tactical FM radio and other tactical means. Tactical means which include the capability to conduct Face-to-Face communication, loudspeaker and mobile cinema operations. This normally entails having Tactical PSYOPS Teams (TPT). Depending on the information environment it can also be necessary to have the capability to use “new media” at the tactical level⁸² for PSYOPS purposes. This can include for example the ability to disseminate messages and audiovisual products

(78) Rosin, 2009, p. 6.

(79) Moir, 2008, p. 7.

(80) Bryder and Andersen, 2009, p. 423.

(81) Hampsey, 2010, p. 2.

(82) CALL, 2006, p. 34.

through Bluetooth technology via mobile phones. Face-to-Face communication on the ground has shown itself to be one of the most important PSYOPS means, along with tactical FM radio, in COIN operations. Tactical FM radio makes it possible to reach a relatively large part of the target audiences without the insurgents being able to interfere. A precondition for the use of tactical FM radio is though that the target audience is aware of the frequency, finds the programmes sent credible, and none least has access to a radio. These preconditions can be met through “branding” campaigns for the radio, tailoring the content to the target audience including audience participation, and through the distribution of “Wind Up Radios” (WUR). Experiences from especially Afghanistan, but also places like Africa, have shown that the use of Radio-In-A-Box (RIAB) systems can have a huge effect in remote areas or in connection with Forward Operations Bases (FOBs) when it comes to influencing very locally specific and sometimes isolated target audiences.⁸³ Likewise, Mobile Cinema Capacity can be used to great effect in the same context.

PSYOPS radio capacity set up in the initial phases of a COIN operation can also be the first step in creating locally run radio capacity in order to meet requirements of local inclusion; “local face”; and communication per proxy in COIN operations communication. One stepping stone in this is to quickly begin using local radio hosts.

However, the key to PSYOPS success in COIN lies in two things. Firstly in being proactive and influence the information environment and the target audiences that matter, and second in responsiveness. PSYOPS doctrine prescribes fairly complex approval processes and PSYOPS products that are not pre-approved can be a long time underway in this process. This makes the products less effective in the time critical competition with the insurgents in the information environment. Preapproved products are great when it comes to standing messages such as tip lines, reward programmes and educational data such as FM radio frequencies, but when it comes to countering an enemy that bases its entire campaign on influence and intimidation PSYOPS needs to be very responsive in order to compete.⁸⁴ This means more flexible approval processes and approval authority delegated to low levels of command in order for PSYOPS to be effective. Of course PSYOPS at all levels should be in line with the overall narrative, themes and messages given in the information strategy and in subordinated plans for information.

- **Civilian Military Cooperation (CIMIC):** CIMIC plays a large role in INFO OPS in COIN. Firstly by putting actions and tangible prove (deeds) behind the words and thereby contributing to ensure coherence in word and deeds, or unity of message. Secondly CIMIC plays a role in message and product distribution through CIMICs natural interaction with local population and opinion / decision makers and through the distribution of for example Wind-Up-Radios (WUR) and so-called Novelty Items.⁸⁵ This can also entail distribution of PSYOPS products that either directly support CIMIC actions and activities or support other ongoing PSYOPS programmes. CIMIC is also a direct contributor to INFO OPS when it conducts so-called “Consent Wining Activities” (CWA) and to a certain extent when setting up for example Medical Civil Affairs

(83) Lamb, 2006 and CALL, 2006, p. 34.

(84) Hampsey, 2010, p. 1.

(85) The interaction (messaging) need to be based on Talking Points to ensure unity of message. Novelty Items are gifts such as pencils, toys, clothing or other items that make sense for the target audience and gives some sort of affordance to them and can carry a message.

Patrol (MEDCAP) to the benefit of the civilian population.

The passive contribution to INFO OPS that CIMIC provides is just as important. Especially, through the gathering information on the civil and information environment (human factors) which is crucial for the analysis and planning of INFO OPS, and which contributes to the overall intelligence picture (PMESII).⁸⁶ Secondly, through the delivery of tangible and relevant results that can prove the “words”, and through pictures and stories to be exploited in PSYOPS, PA and other Information Activities.

Although CIMIC assets and activities to great effect can be utilised for INFO OPS purposes, you also have to be a bit careful and it can be a balancing act between the need for influencing the environment and upholding good working relationships with local and civilian actors in the area. Especially when it comes to working with civilian actors as International Organisations (IOs) and Non-Governmental Organisations (NGOs) on one hand and on the other hand supporting the commander’s mission and intent with INFO OPS related activities, and thereby utilising those influence opportunities that a lot of CIMIC’s work naturally represent.

- **Combat Camera Team (CCT):** The ability to document operations and enemy actions (exploitation)⁸⁷ in order to support Psychological Operations and Public Affairs initiatives in relation to local, regional and international media is very important. This is to be able to counter enemy claims of misconduct, collateral damage, or other misinformation, to distribute information out about operations, development projects and other stories where the conventional media are not interested or do not have access.⁸⁸ The CCT capability does not necessarily have to be an independent capability, it can be embedded in other capabilities: either in TPTs, manoeuvre units, Special Operation Force units, or in so-called “Effects Teams” (to be discussed later).

Other Capabilities

Nearly all capabilities in a unit or formation can in some form or another be utilised in INFO OPS, either in a direct or an indirect (supporting) role. Normally Electronic Warfare (EW) and Computer Network Operations (CNO) appear in Info Ops doctrine as being “core” capabilities, but in reality CNO capabilities rarely appear at the tactical level, even though CNO support can be requested; and EW normally “lives” its own life, but supports INFO OPS. Other capabilities that can support INFO OPS entail Air Assets, Medical Capability, Special Forces and direct physical destruction / kinetics.

- **Staff personnel:** Besides the “Military Cultural Advisor”, intelligence staff personnel, and personnel directly involved in INFO OPS, other personnel from the staff can also contribute to the planning and execution of INFO OPS in COIN. One example is the religious personnel in the staff (Army Chaplain or the like) who can interact with peers in the local community as a form of Key Leadership Engagement. Another example could be medical personnel whom interacts with local nationals or local medical personnel.

(86) McKenna and Hampsey, 2010, p. 8.

(87) See also “planning principles” on exploitation.

(88) Murphy, 2008, p. 5.

- **Electronic Warfare (EW):** EW can support INFO OPS both directly and indirectly. Directly through intelligence collection in the electromagnetic spectrum collecting information on key influencers, and through directly disseminating messages to insurgents on the INS' own command and control nets, as well as jamming of enemy propaganda capabilities (e.g. FM radio or television). The latter two, though, need to be based on an intelligence gain-loss analysis, and on an analysis of the perceptual impact on the local population. Indirectly EW can support deceptions plans and contribute to measurement of effectiveness (MoE) assessments.
- **Computer Network Operations (CNO):** CNO rarely plays a direct role on the tactical level in COIN, but as the use of “new media” and other Internet Protocol (IP) based means of influence become more and more integrated in INFO OPS, CNO can also be a direct contributor.
- **Targeted Physical Destruction:** Physical destruction or other use of kinetic means can be used as an incitement to reinforce for example PSYOPS or other forms of messaging and thereby getting the target audience to assume the desired behaviour. It can also be used to more directly degrade or destroy enemy propaganda capability, take out enemy key communicators, or simply to create fear. The use of physical destruction, though, always has to be assessed in regards to second and third order effect in the information environment, as a part of the planning process.

When it comes to EW, CNO and Physical Destruction, it is worth noticing that in today's operational environment, and into the foreseeable future, we will be fighting amongst the people, not in full-scale wars. This means that we will be fighting against opponents that use the same information infrastructure for command, control and operations which the local population use for “normal” purposes. The notion of “command and control warfare” or “counter command activities” against the opponents with the aim of degrading, destroying and exploiting the opponents command and control systems are full of complications. In a contemporary operational environment, where we are trying to influence the population, we cannot just destroy or degrade mobile phone networks, internet connectivity, and satellite and terrestrial radio and television: these are used both by us for influence purposes and by the local population in their daily life. It would incite anger in the population and it would deprive us of means to reach our target audiences.⁸⁹

- **Use of Air Assets:** Air Assets are naturally used in support of INFO OPS for PSYOPS leaflet dropping and loudspeaker operations, but can also be used for generating psychological effects (PSYACTs) themselves. For an example for Show of Force or to stress enemy forces. In Iraq, Fast Jets have been used to fly along roads and routes that have been IED problem areas to reduce the number of IEDs on these roads. Likewise, UAV have been used for stressing insurgents in certain areas, making them feel watched and thereby reducing their freedom of movement. In the same way photos and video collected by Air Assets have been used in PSYOPS products.

One just has to be very aware of the psychological impact on the local population in COIN when planning the use of air assets; not only in connection with INFO OPS, but in general.

(89) Rosin, 2009, p. 8.

- **Medical Capabilities:** The use of medical capability for influence purposes have been practised for some time in both Iraq and Afghanistan, especially in connection with CIMIC initiatives⁹⁰, such as Medical Civil Affairs Patrols or MEDCAPs. It has also been practised in connection with passive intelligence gathering in support of INFO OPS.
- **Special Operations Forces (SOF):** Special Operations Forces fulfil a range of indirect and direct roles in INFO OPS in COIN. SOF units can support INFO OPS through the performance of Special Reconnaissance (SR) missions, collecting information and visual material to be used in PSYOPS products - including documentation of Direct Action (DA). DA could mean the calculated and prudent targeting of insurgent leadership to physically and psychologically erode key leaders and their sources of support⁹¹. SOF can also be used for disseminating messages and products in hostile environments and to perform KLE in enemy controlled areas. SOF can also be used in connection with Military Assistance (MA) missions to include capacity building of Host Nation Security Forces (HNSF).
- **Human Intelligence (HUMINT):** HUMINT, although not a direct part of INFO OPS, can still support these through identifying and collecting information about key figures' roles, values, attitudes, vulnerabilities, accessibility and so on, to be used for influence purposes later on. Protection of sources is, though, a vital consideration for the INFO OPS planner when using information collected by HUMINT. Interrogation and questioning of detainees can also be a HUMINT task with the purpose of influencing detainees. Also, supporting MoE and assessment of INFO OPS effectiveness⁹². HUMINT can also support INFO OPS through dissemination of for example rumours and indicators to sources and others in order to get these to act as proxy-communicators and finally HUMINT can support the overall measurement of effectiveness process.
- **Manoeuvre units:** Besides disseminating PSYOPS products, a huge part of the role of manoeuvre units in INFO OPS is linked to their own performance of PPP and information collection in connection with patrols and other engagements with local nationals and HNSF.
- **"Effects Teams":** It can be an advantage to create so-called "Effects Teams" – in lack of a better terminology - which are made up of two or more of the capabilities discussed above to deliver effects using one or more of the techniques in INFO OPS, and deploy these together with manoeuvre units on the ground. Effects Teams can consist of elements and personnel from PSYOPS, CIMIC, Engineers, CCT, PA, and staff officers or non-commissioned officers (NCOs) from intelligence staffs, amongst others. The composition of the team depends on the desired effects and the task and purpose that derive from the Influence plan. If the task is to engage with women in a very patriarchal society it might be an idea to create an ad hoc all-female TPT or CST (CIMIC Support Team). (Somewhere referred to as a "Female Engagement Team"). One just has to remember that the interpreter has to be female as well!

(90) CALL, 2006, p. 35.

(91) Cassidy, 2009, p. 122.

(92) Coffey, 2009, p. 7.

Effects Teams will be able to perform a series of the tasks related to INFO OPS as an integrated entity in the manoeuvre units, and performing operations on the ground in a coordinated way. Amongst other things, this allows for influence related intelligence gathering and for giving the manoeuvre unit an integrated Influence capability it can employ as needed. The teams can also, as an integrated capability, be deployed to Forward Operations Bases (FOB) for a longer or shorter period of time, either supporting framework or deliberate operations, or training the unit it is attached to in INFO OPS. The creation of Effects Teams can also minimise the need for Force Protection as only one patrol needs protection, but performs a variety of influence related tasks, instead of a TPT going out one day, a CIMIC team going out the second day, and PA going out the third, all requiring Force Protection and thereby tying up many resources that could have been used for other operations.

The Missing Link – Public Affairs (PA)

In NATO doctrine and in many national doctrines Public Affairs (PA) is to varying degrees separated from other communicative disciplines: namely from Information Operations, and especially Psychological Operations and military deception. This is primarily in order to uphold good working relationships and not least credibility with national, regional and international media, and not to be seen as trying to influence them. This trouble is, though, that the characteristics of the modern information environment make it virtually impossible to separate target audiences and information due to the free flow of information on the internet and between groups of people. What is said to a newspaper in Copenhagen about Danish forces operations in a certain mission area can very well find its way to the mission area through Diaspora, internet based media, or otherwise. Likewise, PSYOPS leaflets dropped over the same mission area can easily be scanned and sent back home to Denmark via the internet only minutes after they have landed on the ground. The same characteristics also allow national media to report on on-going operations in the mission area either through embedded journalists, citizen journalists or by picking up stories from the local media. This reporting can also reach local media in the mission area and be re-mediated there.

Public Affairs' role in COIN operations is therefore twofold:

Strategically, the relation to international and national (home audiences) media is a vital part of Public Affairs role in COIN in order to address the strategic Centre of Gravity (CoG): to gain and maintain popular support for the mission and to explain the operations which the media maybe already report on.

Operationally and tactically the PA role is to engage local (host nation) media. Unfortunately the latter role is often downplayed by PA due to lack of resources. How often do PA officers, for example, speak the local language? Resources are instead used to maintain and service mostly national media.

The local media in mission areas can, for the reasons discussed above, be just as an important actor to address as the national and international media. PA therefore ought to monitor local media outlets and interact with them in order to ensure that own messages get out, and to identify and if necessary counter opponent messages, misinformation and propaganda in local media.

Not only on theatre level, but also locally in Brigade and Battle Group areas of responsibility. Especially within the latter very few resources are used to engage the local media. PA can also play an important role in local media capacity building, either themselves or via CIMIC or NGO dealing with local media.⁹³ Building local media capacity and educating local journalists can very well be a part of Rebuilding and Development (R&D) programmes in the framework of the Comprehensive Approach.

The discussion in regards to Public Affairs is therefore how PA can be closer integrated with the INFO OPS directed towards the local target audiences without losing credibility with the national and international media, and without getting involved with deception operations. The latter is a specific challenge in the modern information environment where the press very well can get information and report about a visible military operation which in reality is a deception operation through manoeuvre aimed at the opponent; but if and when the press is enquiring about the operation, PA cannot very well say that it is a deception operation. It is on the one hand not possible to avoid deception operations or elements thereof being reported on in the media with the media knowing that it is a deception operation, and without PA having any other option than to let the media believe that it is a “normal” operation; but for a variety of reasons they should on the other hand not be used deliberately as a part of deception operations. As several incidents in recent history have shown, deception operations aimed at the opponent through regional or international media have backfired. For example when a US Marine Corps Public Affairs Officer in Falluja in 2004 gave an interview to CNN, giving the impression that an invasion of Falluja had started when it in fact had not, possibly in order to mislead or deceive target audiences inside Falluja as to when a large scale attack on the town was going to take place.⁹⁴ The intended audience for this was therefore not the CNN, US or international audiences, but the insurgents in Falluja.⁹⁵

This example just shows how difficult it is to control information while maintaining an “honest” or “truthful” message in the modern information environment.

At the end of the day, which techniques and capabilities that are brought into play in the planning and execution of Tactical INFO OPS depend on: the desired effects that you want to achieve on which target or target audience in what time and space.

(93) Todd, Paul and Glenn, 2007, p. xix.

(94) USMC PAO: “The troops crossed the line of departure. We had artillery fire, prep fire, going out. Aircraft had been moving through the area all day, helicopters providing transport. It’s been a pretty uncomfortable time”. BARBARA STARR, CNN CORRESPONDENT (voice-over): “Marine Corps Lieutenant Lyle Gilbert from the First Marine Expeditionary Unit outside Falluja appeared on CNN October 14 offering words that sounded like the invasion of Falluja had begun, but further reporting indicated that the long-expected large-scale ground offensive against Falluja had not started. It would be another three weeks before that would happen. So was Lieutenant Gilbert just wrong? Or was the U.S. military using CNN to convince viewers in the battle zone that the attack was already underway?” The chief spokesman for Defense Secretary Donald Rumsfeld insists deception of the news media is never allowed. “Never, it’s just not”. (http://archives.cnn.com/TRANSCRIPTS/0412/04/i_c.01.html) (20.09.10)

(95) Adams, 2009, p. 19.

PART III: Enabling factors

In order for INFO OPS to be effective there are a number of preconditions that need to be met. These preconditions all relate to the techniques and capabilities in one way or another. They include education and training to include knowledge and appreciation of the principles of COIN; the role of INFO OPS therein at all levels; leadership; full spectrum intelligence or “knowledge development”; and planning.

Education and Training

Pre-mission training for COIN operations often sets a course for frustration while deployed in theatre.⁹⁶ In most instances the training has prepared units for “kinetic” operations, followed up with some “cultural awareness”. The training, however, often lacks the substance to accurately address issues that prepare the unit for the fight in the cognitive domain.

In the framework of counter insurgency, cultural awareness and understanding and insight into local customs can be as important competences⁹⁷ as weapon skills⁹⁸. Successful INFO OPS in counter insurgency therefore depends on the soldiers’, non-commissioned officers’ and officers’ initiative to learn and understand relevant aspects of local language, culture and Media’s tactical and strategic impact on operations, kinetic as well as non-kinetic.⁹⁹

Commanders, leaders, and soldiers will in connection with operations on the ground be faced with situations where decisions must be made rapidly. This is no different from normal conventional operations, but in counter insurgency the operations are to a higher degree conducted “amongst the people”, to quote General Sir Rupert Smith, and amongst the people there are also media and journalists and others who can report what happens. The decisions can therefore impact the strategic level even though they are made in a tactical environment due to the media’s presence and the insurgents’ ability to exploit tactical mistakes in the media¹⁰⁰, for an example collateral damage. In order to avoid this, or at least mitigate the consequences of it, everyone should have an understanding of why they are there (in theatre), what the purpose is, and what long term consequences of their tactical actions can have on mission success, and the end-state, however distant that may seem. To include the understanding of how everything they say and do can become public knowledge almost instantly due to the characteristics of the modern information environment.¹⁰¹

This understanding can be brought about through briefing to the troops about the political backdrop for the military engagement before deployment, and subsequently during the deployment by updating this through discussions at company and platoon level. Although this might come across

(96) McKenna and Hampsey, 2010, p. 3 - 4.

(97) Cultural awareness, understanding and competencies can be pulled together under one heading “Cultural Capacity”. *Cultural Awareness* which is the basic level of comprehension required to mitigate threats and exploit opportunities at the tactical level. *Cultural Understanding* which requires a broader and deeper knowledge in order to deal directly with cultural groups, for an example key leaders and host nation security forces. *Cultural Competence* which is the top, advanced level and is applicable to cultural advisors (CULAD) to senior commanders. (DCDC, 2010, p. 3-19)

(98) Ringsmose, 2007.

(99) Moir, 2008, p. 8, CALL, 2006, p. 38 and Ferguson, 2010, p.441.

(100) AJP 3.4.4. point 0231.

(101) Kilcullen, 2006, p. 30 and 32.

as an encouragement to introduce old Soviet style “political officers” in military units, it is far from that. It is simply a question of making the conflict make sense to the soldiers, especially to the ones that really do not care why they are there: the ones that are there because the military told them to go there, and they are going to do what they are trained to do – fight. These are the soldiers that are most likely to act in a way that makes them a “strategic corporal”: burning a Quran or in other ways being insensitive to local culture, or whatever else has happened in missions lately. Including this understanding of the mission in pre-deployment training through realistic scenarios that show the consequences for INFO OPS, both good and bad, is important.

Another method is the use of “Soldier’s Cards” which besides Rules of Engagement (RoE) and the use of force, also describe the mission, its narrative in simple lines to take (LTT), and how the soldiers should interact with both the local population and the media (local, national and international) that may be in the area where they operate. The use of these Soldier’s Cards has to be a part of the pre-mission training and be integrated in exercises. On the other hand you must also be aware that the soldiers often are the unit’s best ambassadors especially in regards to the media, and they generally do know how to act and what to say. Too rigid a use of LTT can compromise the credibility of this ambassador like role.

There is also a very real risk of some of the soldiers becoming “virtual strategic corporals” through their actions on the internet and not just on the battlefields or in the bases. Pictures and videos placed on social network sites as YouTube, LiveLeak, Facebook and the like, as well as postings in blogs, chat rooms and mails, can have a strategic impact on the mission. First of all when pictures of illegal actions done by own troops, like the ones from the Abu Graib prison in Iraq, come to the media’s and public’s knowledge and creates strategic effects. Effects not only on the home audience, but also on the population in the mission area and on world opinion, thereby hampering mission success and creating doubts about the overall credibility of own forces.

Incidents like these can furthermore become viral or spiral campaigns with a life of their own. They are not only referred to in the mainstream media that picks up on the story from social network sites, they will also be used by others, amongst them the enemy for propaganda purposes.

One example of this is Al-Qaeda use of video material posted by Danish troops on YouTube in early 2007. The video showed Danish reconnaissance forces patrolling and doing operations in the desert of Helmand province in Afghanistan. In June 2008, the Danish embassy in Islamabad Pakistan was bombed by a suicide bomber and several people were killed. Al-Qaeda soon after took responsibility for the attack, and shortly after that a propaganda video appeared on the internet on a jihadist website. The video had clips of the Al-Qaeda second in command (2iC) in Pakistan claiming that the attack was retaliation for the Muhammad cartoons printed by a Danish newspaper in November 2005, the Danish government involvement in attacks on Muslims in Iraq and Afghanistan. Most of the imagery not showing Al-Qaeda leaders was taken from the internet showing the then Danish Prime Minister Anders Fogh Rasmussen, one of the cartoonists, and Danish forces in Afghanistan. Footage was taken from the reconnaissance unit’s “private” video on YouTube.

Another implication of soldiers having personal digital media recorders in theatres of operations is the risk of losing them with images and recordings stored that potentially can be used by the enemy for propaganda purposes¹⁰². The units must have clear guidelines for the use of personal digital media and the use of the recordings.

(102) Dauber, 2009, p. 25.

Other aspects of new media can be just as challenging. For example when media and news organisations offer soldiers money for their pictures or stories about current operations or other “breaking news”, and thereby making the soldiers into “citizen journalists” – willingly or unwittingly. Most media today have in both their main news broadcasts and on their websites advertise contact information for the would be citizen journalist: SMS numbers and e-mail address references along with encouragements to the viewers to send in tips, pictures, video or other things relating or leading to journalistically interesting stories. It is a fact that such is the trend in the modern media environment. It cannot be stopped. The question is how it can be mitigated.

There is no question that the actions creating or being used in strategic discussions come primarily from the tactical level, but often the largest impact is on the strategic level. Several countries and organisations have seen the potential negative impact of own troops’ use of social network sites and other new media, such as mobile phone technology, but the answer to the challenge is very different. Some simply try to ban the use, others try to mitigate the potential negative consequences through education and information. It shall be this paper’s claim that banning will not work.

As touched upon earlier, education in cultural awareness and understanding, to some extent local language, use of interpreter and contact skills are important in counter insurgency operations in general. These qualifications are also important as preconditions for effective INFO OPS.

As a result emphasis must be put on both education and training in cultural awareness and on contact skills, to include the importance of how the behaviour of own forces impact on local populations perceptions, as crucial skill sets for the units and formations ability to influence the Centre of Gravity – the local population.

It therefore doesn’t help much if the culture awareness training is a two hour lecture in a hot, overcrowded lecture hall at ten o’clock in the evening after a four day field exercise, as unfortunately it has been seen.

Contact skills have to be practised as an integral part of the pre-mission training and exercises, and they have to be trained in a way so the two somewhat contrasting competences - combat skills and contact skills - become natural (seem mutually supportive) for the soldiers¹⁰³.

Especially when the soldiers do not have the power of language and cannot communicate directly with the local population they have a tendency to freeze up and act differently than they normally would. Their posture (body language) changes and their decision-making ability diminishes; they make decisions than they normally would if they had to act in a situation they are trained well for – combat. Therefore the training in communicating with the local population in COIN becomes so much more important¹⁰⁴. The ability to read the situation and communicate without the use of a common language has to be trained in advance.

Combat skills are still the core and have to be prioritised, but when training for counter insurgency operations the influence piece must not be a mere “add on” or an afterthought. It has to be an integral part of the education and training, the subsequent operations and the planning thereof.

It is important that the unit’s education and training to support INFO OPS is not only theoretical but also materialised in practical exercises and scenarios. All lectures and theory lessons must be supported by practical examples. Otherwise, the lesson learned is that the soldiers have a

(103) Nørgaard og Holsting, 2006, p. 112.

(104) Liburius, 2010, p. 516.

hard time recalling the lessons when standing in the mission area¹⁰⁵. So when planning this training (KLE, F2F, PPP, execution of PSYOPS, use of cultural knowledge and language, and use of interpreters) three principles must be observed:

- Realism in all the scenarios: having role players that act like locals culturally and not react to the soldiers' use of their own language. Have well worked through scenarios with background information.
- Interaction: give the soldiers the possibility to act in multiple ways or to have several courses of action (CoA).
- Complexity: the scenario and the role players must be able to handle the CoA the soldiers chose, and act upon it.

In order to obtain this realism and get the scenarios to work also for INFO OPS it requires single-focused and educated observer-controllers on the influence play throughout the pre-deployment training.

The discussed elements of education and training for COIN operations will help create the needed preconditions for effective tactical INFO OPS. It will support the use of Presence, Posture and Profile (PPP) in operations, framework as well as deliberate; improve the general interaction with the local population and thereby reduce the risk for a "words and deeds" gap; and contribute to the units understanding and appreciation for the support that they have to give to for an example PSYOPS and CIMIC.¹⁰⁶ Especially an understanding of why the units have to handout PSYOPS handbills, play football with kids, and collect information on atmospherics. Furthermore, a focused knowledge about the situation and the background of the conflict through troop information and other command activities will contribute to the effectiveness of INFO OPS. Through creating an understanding of the consequences for both the soldiers and their families' safety and operational security (OPSEC) and the potential strategic impact associated with the use of new media, the education and training can also help mitigate "strategic corporal" and "citizen journalist" effects.

Figure 3.1. Education and training.

Education and training:

- Briefing on the political backdrop (Troop Information)
- Cultural awareness and understanding
- Language training
- Use of interpreters
- Contact skills
- Use of (extended) Soldiers Card
- Use of New Media
- Realistic training with influence consequences

(105) Liborius, 2010, p. 518.

(106) Terence, 2006, p. 55.

Leadership

There are a series of leadership challenges connected with training for and conducting COIN operations. These challenges cover the integration of influence into education and training, command group involvement in intelligence and operational planning, and command and leadership in execution of tactical level operations.

The success of INFO OPS depends on commanders' view of the battle space, their understanding of how to employ INFO OPS to achieve desired effects, and their interest and involvement in integrating INFO OPS with other combined arms operations.¹⁰⁷ This makes command group involvement essential. Creating effective INFO OPS is an inherent and essential responsibility of command.¹⁰⁸ Commanders therefore need to reemphasise the importance of INFO OPS on a regular basis, and continuously take it into their direction and guidance.¹⁰⁹

Leadership involvement in INFO OPS is therefore important in at least three areas: Education & Training of troops, units and formations; Direction & Guidance in planning; and Command on the ground in execution of operations.

First of all it is a challenge integrating "influence skill sets", as discussed above, into an already packed pre-mission training programme, where units and commanders that are going to fight "the alligator" naturally are more focused on combat skills than on influence skills. Partly because it is within their "comfort zone", which INFO OPS usually are not and partly because of lack of direction and guidance from top level command on INFO OPS.

Secondly guidance from commanders is also very important when it comes to intelligence and operational planning. Without this guidance there is a risk that the Intelligence section does not collect and analyse the Human Factors and other influence relevant information and knowledge.¹¹⁰ In direction and guidance commanders must also be aware of the continuity of their influence efforts and not try to monitor too many variables, shift resources back and forth in response to the daily competition with the insurgents in the information environment, change themes and messages randomly, and thereby lose track of the steady long-term "drumbeat" stated in the information strategy.¹¹¹ In other words, priority intelligence requirements (PIR) and commanders critical information requirements (CCIR) must include influence related issues in COIN.

Thirdly, command on the ground is challenging: one minute tactical units are engaged in high intensity combat operations and the next they are interacting with the local population. It can be hard for commanders and leaders at tactical level to cope with this paradox, especially when there has been a TIC (Troops in Contact) at a certain point, and the same troops have to be nice to local villagers three hundred metres down the road; not knowing whether or not the villagers sympathise with the enemy the soldiers have just fought, or if the locals have even perhaps been involved in the fighting.

(107) Larson [et al.], 2009, p. xv.

(108) On the basis of Flynn, Pottinger and Batchelor, 2010, p. 10.

(109) Larson [et al.], 2009, p. xv.

(110) Flynn, Pottinger and Batchelor, 2010, p. 7.

(111) Larson [et al.], 2009, p. xv.

Besides the education and training and leadership aspects in what lie behind INFO OPS there are also two other preconditions, as alluded to in the second point above, for its effectiveness, namely full spectrum intelligence, or knowledge development, and integration into operational planning.

Full spectrum Intelligence (knowledge development)

Intelligence plays an essential role in COIN operations and in the support for INFO OPS. Perhaps some of the most critically needed information in COIN have to do with the understanding and knowledge of the culture in general, attitudes, beliefs, and the mood of the local population and how these are likely to shift especially after single traumatic incidents caused by own operations. Or in other words the analysis of the “Human Terrain”.¹¹² Likewise how the insurgents are perhaps more capable of exploiting the local information environment and the counterinsurgent therefore needs intelligence to support the “competition” for the local population’s perceptions.¹¹³ In this also assessment or Measurement of Effectiveness (MoE) plays a vital role. One of the biggest challenges for both INFO OPS and Intelligence sections is how to assess the impact of the unit’s influence efforts on the local population and on the insurgents.

The Intelligence section must therefore be organised and manned to cope with all aspects of the operational environment, i.e. Political, Military, Economic, Social (cultural), Infrastructure and none least Information (PMESII).¹¹⁴ This is in order to be able to deliver Human Factor and Social Network intelligence to support INFO OPS planning, execution and assessment. And not as it is often seen only focus on “red” intelligence, although these intelligence products still are very necessary and appropriate. Traditionally having focused the overwhelming majority of its collection effort and analytical brainpower on insurgent groups, the vast intelligence apparatus is unable to answer fundamental questions about the environment and the people that the counterinsurgent seeks to persuade.¹¹⁵ Often intelligence officers diagram insurgent networks and recommend individuals who should be killed or captured and use the available collection assets on this effort.

Intelligence personnel therefore ought to have a basic understanding of INFO OPS and its basic intelligence requirements. At least one person in the Intelligence section should be tied into, or permanently be in, the INFO OPS Cell and act as liaison and ensure coordination between the two.

The intelligence community can also gain from this insight and might therefore be able to utilise INFO OPS better as an enabler for intelligence collection. For an example in connection with IEDs use INFO OPS targeted at relevant Target Audiences to elicit information “left of the boom”

(112) Human Terrain Analysis (HTA) or mapping should not be confused with geospatial products showing the distribution of ethnic, sectarian or tribal groups in a geographic area. Human Terrain is defined as the social, ethnographic, cultural economic and political elements of the people among whom a force is operating. HTA should follow that intelligence cycle and inform all stages of planning process. (DCDC, 2010, p. 3-16 to 3-17)

(113) Larson [et al.], 2009, p. xiv – xv, and Mitchell, 2009, p. 56 – 57.

(114) NATO’s PMESII represents a system of system approach, or a way to analyse interacting social networks. It deals with a complex battlespace by dividing it up in different dimensions for strategic reference and decision-making or planning. (Mitchell, 2010, p. 448)

(115) Flynn, Pottinger and Batchelor, 2010, p. 7.

- meaning left of the timeline of the IED attack, “the boom” - and perhaps save scarce collection resources that otherwise would have been used to reactively “defeat the device”. Another example could be using INFO OPS to provoke the insurgents into using for example their command and control (C2) systems in order to observe these systems.

The information needed to conduct INFO OPS, even at the tactical level, in COIN covers the entire system or PMESII. Besides the formal political structures, the still needed information about the insurgents, the fundamentals of the local economic system and the basic infrastructure such as location and conditions of roads, bridges, mosques, markets and wells, and other key terrain – besides all this, the main intelligence requirements for INFO OPS are Human Factor centric. What do the social networks look like, who are the powerbrokers and local personalities, and what are the local grievances that, if skilfully exploited, could drive a wedge between insurgents and the greater population – and what are the local perceptions and atmospherics. This could also be correlated and synchronised between various development projects and the level of cooperation amongst the local population, or the lack thereof.

There is therefore a need for a cultural competency and Open Source Intelligence (OSINT) capacity in the Intelligence section in order to develop cultural knowledge in support the operational influence planning and the Course of Action (CoA) development in COIN.¹¹⁶

INFO OPS Request for Information (RFI) must be integrated into the units overall Intelligence Collection Plan (ICP) and reports, intelligence about the information environment, atmospherics and civil society collected by Tactical PSYOPS Teams (TPT), CIMIC Support Teams (CST) and the like must be fed to the Intelligence section as these are some of the primary suppliers of information to form the above mentioned full spectrum intelligence picture. Target Audience Analysis (TAA) and counter-propaganda analysis (SCAME)¹¹⁷ done by INFO OPS contribute to this picture with vital information as well.

Influence Estimate should be an integral part of the overall Intelligence Preparation of the Battlefield (IPB). It can be argued whether or not a separate Intelligence Preparation of Information Environment (IPIE) should be made as well, but in order to minimise the amount of intelligence products and reports, it is probably best that they are an integral part of existing intelligence products.

The precondition for this is through a sufficient number of analysts, also on battle group level, and guidance from commanders.¹¹⁸ Creating effective intelligence – on the entire system (PMESII) – is an inherent and essential responsibility of command¹¹⁹ and a precondition for effective INFO OPS planning. It also may require a “reach-back” capability out of theatre that can rapidly respond to RFIs.

(116) Mitchell, 2010, p. 442.

(117) SCAME = Source, Content, Audience, Media and Effects.

(118) Flynn, Pottinger and Batchelor, 2010, p. 7.

(119) Flynn, Pottinger and Batchelor, 2010, p. 10 and Mitchell, 2010, p. 443.

Planning

Besides recognising the population as the CoG and the cognitive domain in general being a central planning parameter, a vital precondition for INFO OPS' ability to support COIN operations is early involvement in and influence on the operational planning. After "The Bay of Pigs" fiasco in Cuba in 1961, the U.S. Information Agency (USIA) was asked to mitigate the damages through information campaigns. The USIA had not been involved in the planning of the operation and the agency director of the time said: "If they want me in on the crash landings, I'd better damn well be in on the take-offs"¹²⁰. The quote describes very well what is unfortunately still heard in theatres around the world today when Information Operations or Psychological Operations are asked to "sprinkle some magic dust on it, and make it go away" when kinetic operations have gone sour, or when an otherwise successful operation is framed negatively by the enemy due to lack of Influence planning for the aftermath of the operation. Unfortunately Influence concepts are widely misunderstood by war fighters and often applied as afterthoughts by senior commanders. Consequently, they become inherently reactive and often ineffective¹²¹. For an example when misinformation and rumours about collateral damage is circulated by the enemy after an operation, where there were none, as it has been seen several times in Afghanistan¹²². Based upon the known intelligence picture or known modus operandi of the enemy or insurgents this can for an example be a predictable second order effect of an operation that INFO OPS can plan for mitigation activities.¹²³ INFO OPS therefore must be in on the planning and the course of action (COA) development from the very beginning of the planning process.

All INFO OPS planning in COIN, as with all other operations, are driven by and derived from the commanders mission, intent and stated main effort. But INFO OPS is not a separate Line of Operation (LOO) within the plan, it must be integrated into and support all LOOs, and the output of Influence core and supporting capabilities and techniques need to be integrated within these, rather than constructed in a separate LOO.¹²⁴ Consequently, senior commanders should consider and emphasise the "information effects" they wish to achieve in an operation and articulate them in the clear statement in their "intent" that will drive planners and subordinate units planning – the commander's intent. The commander's intent as part of the formal military planning process is the key to proactively include the information environment in the planning to include an "information end state". This should consider both the cognitive and physical dimensions of the end state and thereby the identified target audiences' perceptions, attitudes and behaviours, as well as opponent media capabilities.¹²⁵ With a commander's intent including INFO OPS, planners can include this in Courses of Actions (CoA), and finally in plans.

Besides the planning role Assisting Chief of Staff (ACOS) S9/G9 also has an advisory role in the staff. ACOS S9/G9 should advice the commander and the rest of the staff, especially S3/G3 and

(120) Kelly, 2009, p. 72.

(121) Murphy, 2008, p. 12.

(122) Nissen, 2007, p. 7.

(123) Mitchell, 2009, p. 59.

(124) Rosin, 2009, p. 4 – 5, and McKenna and Hempsey, 2010, p. 13. Conversely it can be argued that INFO OPS ought to be a separate LOO that may act as a forcing function in a unit that has not inculcated a culture of influence into their planning, as LOOs must be briefed and considered. If INFO OPS is not a separate LOO in units like these it can easily be forgotten or not given the necessary emphasis.

(125) Murphy, 2008, p. 12, and McKenna and Hempsey, 2010, p. 13.

5 operations, throughout the planning process and the staff work on INFO OPS. This should insure that the information environment is incorporated into the estimation process and the Intelligence Preparation of the Battlefield; secondly on INFO OPS´ integration into the Course of Action (COA) development, the War Gaming and on final COA selection. Main emphasis in this advising should be on the perceptual and psychological effects of planned kinetic actions, tactically and strategically, including second and third order effects. This includes identifying, shaping, and exploiting opportunities presented by the opposing forces´ exploitation of Friendly Forces actions.¹²⁶ INFO OPS / ACOS S9 also have an advice function in, and are an integral part of, the targeting process. ACOS S9 or others in the S9 staff contribute to the nomination of targets and participate in the targeting board in order to advice on effects of kill/capture options and the subsequent influence exploitation of these, as well as the preparation of mitigation packages.

While recognising that the basic planning processes remain valid, a review of the techniques and capabilities used in INFO OPS, the role of new media, and the characteristics of the modern information environment reveals a requirement for a significant cultural shift in current planning processes: the aim of this is to give Influence a more dominating role in the operational planning in COIN.¹²⁷ It points to the importance of competing in the information battle space and to a series of planning principles to ensure just that ability.

Planning principles

Behind the planning and execution of Tactical INFO OPS there is a set of principles that both the planner and the tactical commander or leader must adhere to and integrate in their activities and actions:

- Place the population at the forefront of the operational design and in the planning¹²⁸.
- Early involvement in planning of operations in order to thoroughly integrate INFO OPS into the plan.
- Consider the strategic backdrop when planning operations at the tactical level. As shown throughout the paper so far even tactical planning needs to take into account the strategic information environment, the strategic narrative and the effects that tactical activities and operations can have on them. The tricky part is how to ensure that the message is tuned to local events and local perceptions, while retaining awareness of the operational and strategic context.¹²⁹
- Commander´s mission and intent drive the planning. Although the strategic backdrop has to be taken into account it is still the supported commander and his mission and intent that drive the INFO OPS planning, coordination and advice at the tactical level. As former Commander ISAF, General McChrystal has stated: “The conflict will be won by persuading the

(126) Todd, Paul and Glenn, 2007, p. xix.

(127) Murphy, 2008, p. 5.

(128) Mackey and Tatham, 2009, p. 13.

(129) Mackey and Tatham, 2009, p. 15.

population, not by destroying the enemy:" That is not just a slogan, which is an expression of his intent.¹³⁰

- Understand the battlefield as an "area of influence" rather than an "area of operations" and attack the insurgent's information strategy and not the insurgent himself.¹³¹ This will often mean concentration on the local population – both in words and deeds.
- Unity of Message. Communication and actions (words and deeds) must build on a common narrative, a narrative which again makes out the framework for all themes and messages. This narrative should apply to the entire mission. But as this narrative is created at political-strategic level, and it is the tactical units on ground that know the local target audiences, the tactical units will have to adapt the narrative, and thereby the themes and messages, to the local circumstances in order to make them relevant and hence effective.¹³² The units will also have to be prepared to respond to anomalies that are counter to the narrative such as collateral damage.
- Do not promise or threaten to do something that you do not have the intention, will and/or resources to fulfil.
- Compete in the Information Environment through being pro-active in order to *shape* target audiences' perception of the situation. It is probably not possible to be completely superior the modern information environment, not even on tactical level, as has been proven in previous conflicts.¹³³ Doctrinal definitions on "Information Superiority"¹³⁴ are clearly unachievable - just look at "wildcards" as the Abu Ghraib photos¹³⁵. Units engaged in COIN must be as pro-active as possible in order to exercise as much influence on the environment as possible. The goal is to ensure that it is the narrative of own forces – or rather the narrative of the supported host nation – that is the most visible, credible and attractive the information environment. If pro-active use of information can force the insurgents to be re-active one is well on one's way to if not having information superiority, then influential in the information environment.¹³⁶
- Inclusion of local population, local power brokers (all levels of government) and security forces in parts of both the message formulation and dissemination in order to create local ownership for the message. To include the use of proxy-communicators in the dissemination of messages.
- Communication per proxy, the use of so called proxy-communicators: primarily the use of local key opinion-makers to disseminate their own messages or the messages of own forces in

(130) Flynn, Pottinger and Batchelor, 2010, p. 24.

(131) Kilcullen, 2006, p. 29.

(132) Kilcullen, 2006, p. 33.

(133) Roca, 2008, p. 52.

(134) Information Superiority:"The state of a relative superior ability of an actor to collect, process and disseminate information compared to competitors in the same arena and to draw an operational advantage from it". (NATO Info Ops Handbook, 2009, p. 87)

(135) Murphy, 2008, p.9.

(136) Kilcullen, 2006, p. 35.

isolation, as a part of, or concurrent with own forces INFO OPS. This substantially enhances the credibility and effectiveness of messages.¹³⁷ It entails the use of networks created in connection with Key Leader Engagement, and other local opinion-makers in the area. It can also be female networks, as discussed earlier in this paper. Proxy-communicators can be used for both pro-active messaging and for crisis communication or mitigation. American forces in Afghanistan have for example used what has been called “mobile mullahs” as proxy-communicators.¹³⁸ Mobile Mullahs have been used in two ways. Either they have travelled on their own and held sermons in mosques, or they have been a part of a Civilian Military Operations (CMO) team. The CMO teams have also contained medical capability or units (MEDCAP), Female Engagement Teams, PSYOPS operators, development advisors and representatives from local government and security forces. The CMO teams have been deployed right after combat action in a given area.¹³⁹ Also local security forces can play an important role as proxy-communicators in for example the dissemination of PSYOPS messages. Normally local security forces are not trained in PSYOPS planning as a part of capacity building programs or security sector reforms, but they can with great effect be trained in dissemination operations. In Afghanistan a concept called “Afghan Information Dissemination Operations”, AIDO, has been developed and entails the training of Afghan National Army (ANA) in the execution of tactical PSYOPS on ground.¹⁴⁰ A similar programme has been run in Iraq.

A professional discussion goes on as to whether or not PSYOPS products should have a source on them or not - even have a local government or security forces source on when the product is through produced by own forces.

Communication per proxy gives the message more credibility, and it gives the messages a “local face” which is important in COIN. Finally “local face” can also mean convincing captured and perhaps turned insurgents to give statements to the media and in PSYOPS products, encouraging their former comrades to surrender or give up their fight.¹⁴¹

- “Local face” also entails giving operations local names and naming bases and posts with local names. One has to be aware, though, that it can have a strategic impact on the home audience as well, as the Danish Army had to learn recently. The naming of a Forward Operations Base (FOB) in Afghanistan was linked to an officer killed in action in the area. As a part of “partnering” and giving the operations an “afghan face” the FOB was renamed with an afghan name. This worked as planned and had the desired effect in the local area, but it turned out to have a somewhat different effect in Denmark, especially on soldiers formerly deployed in the area and their families. Among this unintended target audience the renaming was initially seen as a desecration of the late soldier’s memory.¹⁴² One of the responses was the creation of a Facebook support group which subsequently came to the attention of the

(137) Todd, Paul and Glenn, 2007, p. xix.

(138) CALL, 2006, p. 35. In the planning and use of concepts like the “mobile mulla” one must be aware of the danger involved for the individual. There is also an political – ethical dimension to this concept that one must consider.

(139) CALL, 2006, p. 36.

(140) CALL, 2006, p. 36-37.

(141) Sullivan, 2007, p. 121.

(142) <http://forsvaret.dk/HOK/Nyt%20og%20Presse/ISAF/Pages/Baserf%C3%A5rafghanskenavne.aspx> (8. FEB 10).

mainstream media which again turned it into a media story that the Army had to handle. The story yet again shows how tactical actions so easily can have strategic implications.

- Culturally attuned, not sensitive. INFO OPS must be planned in a way that takes local culture into account. This oftentimes means that local culture is respected and you do not plan on doing something that is offensive in the local culture. It does not mean, though, that you coming from another culture try to be as one from the local culture; you are not, and by trying to hard it can backfire and you can lose credibility. That it is “attuned” and not “sensitive” stems from the fact that it is sometimes necessary to deliberately do some things that are offensive according to local culture. Perhaps in order to provoke the insurgents to take on certain behaviour that facilitates your operations. But if doing so you still need to assess the potential second and third order effects on other target audiences.¹⁴³
- Exploitation of events. Exploitation can be both pro-active (planned) and re-active. The planned exploitation of events or operations is about gathering material and stories during operations for later use. Naturally primarily if the operations are successful. This can be having Combat Camera Teams following the soldiers – be it conventional forces or Special Forces - in an operation and later using the gathered material for PSYOPS products or media events. It can also be used to document an operation where it is assessed that there is a high risk that the enemy will try to exploit it in the form of propaganda about for example Collateral Damage. To use the photo or video material collected by CCT you must through have a regime or a process that can ensure a rapid declassification of footage or a pre-operational decision not to classify.
Exploitation can also be about using footage from surveillance and recognisance assets that puts the enemy in an unfavourable light. This could be the enemy breaking international law, local cultural habits, or in other ways doing something that can be used to undermine his credibility and image; or where his actions contradict his messages, i.e. breaking his unity of message. The reactive exploitation is about acting quickly in crisis situations and getting one’s message out first. The reactive exploitation could be about an event caused by the enemy, and be the first to frame the situation for the local population. This could be in the case of a suicide bomber killing local civilians or where the enemy in other ways targets the Centre of Gravity.
- Assessment. All influence activities must be assessed in order to measure the effect, but in order to be able to do this, Measurement of Effectiveness (MoE) and Performance (MoP) must be considered already in the early stages of the planning process and the target audience analysis. While military planners are familiar with conducting Battle Damage Assessment (BDA) in the physical domain, planners struggle to evaluate success of INFO OPS in the cognitive domain. Likewise can the management of commanders’ expectations in regards to immediacy of results and “return of investment” of INFO OPS be somewhat of a challenge. Assessment of INFO OPS must be based on a “baseline” derived from the desired effects in order to have a “start state” to which the “end state” can be measured. The success of INFO OPS in COIN is therefore determined by observable modifications of target audience’s behaviour. But

(143) Ferguson, 2010, p. 440.

since there are so many actors in the information environment, and many of the events that influence target audience behaviour are unanticipated or outside one's own control, realistic and pragmatic evaluation models do not attempt to establish a direct link between Influence activities and target audience behaviour change. Rather, they try to characterise behaviour trends over time¹⁴⁴, linked to the desired effects. In order to do this, a "baseline" must be established, a series of "impact Indicators" linked to the desired effects must be incorporated in the units Intelligence Collection Plan (ICP), and significant events and friendly, neutrals and hostile actions – as they relate to the desired effects – must be monitored and analysed to get a picture of the confounding variables that impact target audience behaviour.

Figure 3.2. Planning principles for INFO OPS.

Planning principles:

- Early involvement in the planning process
- Consider the strategic backdrop
- Commander's mission and intent drive the planning
- Understand the Battlefield as an "Area of Influence"
- Unity of Message
- Fulfil promises and threats
- Compete in the Information Environment
- Inclusion of local population
- Communicate per proxy
- Local face on words and deeds
- Culturally attuned, not sensitive
- Exploit events
- Assessment

PART IV: From Theory to Practice

In order to put into practice the theories presented so far, the planning and execution of INFO OPS in COIN operations will in this chapter be viewed in the framework of the "clear – hold – build" approach. "Shaping" activities or operations will be discussed as well, since they also play an important role in COIN operations.

The purpose of INFO OPS in COIN is to affect the information environment for the deployed forces positive way, This is done by influencing selected target audiences' will, perceptions, and behaviours through planned influence activities in concert with other military and civilian activities. These influence activities consist of both the use of techniques and of the employment of capabilities that can contribute to the desired effects; behind the activities lie also a series of preconditions in the form of the forces' education and training and the staff's planning that need to be met and incorporated in the shaping activities and the execution of the "clear – hold – build" phases in the approach.

(144) Seese and Smith, 2008, p. 31.

The “clear – hold – build” approach consists of civilian and military actions combining the counterinsurgents and host nation actors in order to counter an insurgency in a specific area. The approach encompasses offensive, defensive and stabilising activities, and shaping activities. The military contribution to the “clear – hold – build” approach consists of two phases: an offensive phase (clear) that aims at braking the insurgent’s “military” dominance in an area and secure the area; and a defensive phase (hold) that aims at protecting the population and alienate the insurgents in order to facilitate development programs in the area, often quick impact and consent winning activities. These programmes are then continued in the last phase (build), but with the emphasis on addressing the root causes of the insurgency¹⁴⁵. Once one area is secured the counterinsurgent and the host nation security forces can continue to expand the controlled areas into contested areas. Often INFO OPS and special operations are also conducted outside the controlled areas to locate, harass and destroy insurgent elements in order to keep them out of balance.

Shaping. Almost all actions, messages and decisions made will contribute to the shaping of the operation and information environment and in turn the local population and other target audiences’ perception, attitude and behaviour.¹⁴⁶ If the counterinsurgent does not try to shape the battle space, the insurgents most surely will. INFO OPS are therefore at the very core of “shaping”.¹⁴⁷ This “phase” can contain elements of deception operations directed towards the insurgents, psychological operations aimed at the insurgents will to fight, attempts to drive a wedge between the local population and the insurgents, information about the counterinsurgent’s intentions, and behavioural instructions to the local population in case of future offensive operations (clear). Shaping can, besides being a “pre-clear” activity, also be an integral part of the entire “clear – hold – build” approach in a broader sense: “framing” activities conducted in order to continuously shape the perceptions and attitudes in the controlled areas, and thereby deprive the insurgents the possibility of telling their side of the story convincingly.

Clear. The phase primarily consists of offensive activities in order to clear an area of insurgents and deny them their safe-havens. In this phase INFO OPS is firstly directed towards the insurgents in order to shatter their cohesion, will and decision making ability through psychological operations, electronic warfare, and deception activities combined with physical destruction of his propaganda capability and command and control capability. Secondly INFO OPS are aimed at the local population and key leaders to give behavioural instructions and counter insurgent propaganda.¹⁴⁸ Influence considerations in the planning of the clear phase also play a vital role in making sure that the use of kinetic force does not contradict messages disseminated (words and deeds); this is to avoid negative second and third order effects in the subsequent hold phase.

Hold. The phase primarily consists of defensive activities in order to ensure that areas freed from insurgent control remain so. The emphasis in this phase should be on the host nation govern-

(145) AJP 3.4.4., 2010, point 0559 to 0562.

(146) Todd, Paul and Glenn, 2007, p. xiii.

(147) Mackey and Tatham, 2009, p. 14.

(148) The reverse has also been seen. In Afghanistan in operations in and around Helmand province ISAF has in 2010 ceded the operational and tactical surprise by publicly stating when and where ISAF would clear areas. This send clear messages to (and therefore shaped) both indigenus populations and the Taliban insurgents.

ment, its security forces and their ability to control the area. In this face, INFO OPS play a vital role in explaining the clear phase and the intentions for the future, all the while showing tangible results. Also in conducting rumour control to avoid a tactical success becoming a strategic failure, if the insurgents “narrative” gets to be dominant. In this phase force posture (PPP) plays an important role in showing what has been told – “words and deeds”. Also the promotion of host nation security forces and employing these forces in the dissemination of messages, doing recruitment campaigns, and the creation of Key Leader Networks are important INFO OPS tasks in the hold phase. INFO OPS in the hold phase should therefore be aimed at both maintaining effects achieved in the clear phase and at starting to shape or frame the subsequent build phase.

Build. The phase primarily consists of stability or consolidating operations with a focus on the ability of local government and host nation security forces to deliver results supported by the COIN force. INFO OPS will be focused at promoting the legitimacy of the host nation authorities, often through host nation security forces distribution of messages. INFO OPS will also be involved in supporting capacity building efforts to include for example Host nation “Army Information Dissemination Operations” (AIDO). INFO OPS and especially Public Affairs in cooperation with CIMIC can also be involved in the creation of a host nation information infrastructure and the training of local journalists. There still has to be a big focus on PPP and KLE.

It can be argued that there is furthermore a “Completion and Transition Phase” following the “clear – hold – build” approach in which the local authorities are in charge and where the COIN forces act more as advisors and continues capacity building programmes. The phase can also be used for the COIN forces’ preparations (shaping) to enter a new, adjacent area still controlled by the insurgents.

In the shaping and clear phases especially deception, electronic warfare and Psychological Operations (leaflet drops, loudspeaker operations, radio broadcasting, key leader engagement through special forces, and so on) will be dominant, along with continuous considerations on the perceptual or cognitive effect on all audiences of the use of kinetic force. The focus in the hold phase, however, shifts to presence, posture and profile, civilian-military cooperation and key leadership engagement. Psychological Operations will still play a vital, but more of a supportive, role. Radio broadcasting, dissemination of printed products, and PsyActs will still be used, but there will be an added focus on Face-to-Face communication and support to key leadership engagement. In the hold phase communication per proxy will be increasingly important along with the utilisation of a newly created local information infrastructure in order to get a “local face” on the messaging. In the build phase there will be an even larger emphasis on local communication.

Way Ahead

Having looked at how to implement Tactical INFO OPS in COIN, operationalised on the “clear – hold – build” approach, and all the things behind Tactical INFO OPS, it is time to look at some suggestions to the way ahead, based on lessons identified throughout the paper.

- Writers, thinkers, scholars and doctrine developers must stop inventing new terminology for INFO OPS every 12 months. For an example the US name change from PSYOP to MISO (Mili-

tary Information Support to Operations)¹⁴⁹. Even though the intentions are good and they only want to keep up with the lessons learned from theatres of operations, it confuses every new generation of leaders graduating from Army Academy, career courses, Defence College, or functional courses (for example. in INFO OPS or associated capabilities). It creates different levels (or generations) of command with different understandings of INFO OPS and how to utilise INFO OPS in COIN (and other operations). Future doctrine should, besides coming up with a more or less enduring set of definitions, focus more on principles for effectively integrating INFO OPS disciplines with traditional combined arms.¹⁵⁰ This to make it as natural as fires, logistics, and signals to commanders and planners. It is therefore not sufficient to simply incorporate influence into military doctrine without establishing structures and educational programmes to facilitate effective and practical application.¹⁵¹ Furthermore doctrine and TTPs must address and explain how a company, battle group or brigade can deliver tactical non-kinetic effects and how soldiers are to execute “influence”, and achieve the “information end state / effects” in the commanders intent.

- The entire area of INFO OPS should be further professionalised giving soldiers, non-commissioned officers and officers the possibility to become specialists and subject matter experts in for example PSYOPS or intelligence support for influence (target audience analysis). At the same time the personnel should retain the possibility for a vertical career, giving the functional area more visibility also in “peace time”. Not as it is now where most “influence positions” only are two to three year assignments at best and, to make matters worse, where “influence positions” in missions often are assigned “individual augmentees”.
- Meaningful change in the view on INFO OPS will, however, not occur until commanders at all levels take responsibility for Influence both in regards to education and training, planning and execution of operations.
- Incorporate the philosophy of COIN operations and tactical INFO OPS and its techniques and capabilities in all pre-mission training; and also incorporate the influence education and training preconditions into all normal education and training so that the basic concepts of influencing are not new when a force starts preparing for a COIN operation. This means adjusting the training of our leaders and soldiers according to the modern information environment in general, and not just when they are trained for operations other than full scale war. A full scale war would most likely move into stability or even COIN operations anyway, looking at the contemporary operation environment trend.
- Find ways to tackle the challenge of the on the one hand working under the direction and guidance from an overall narrative with a top-down information strategy, and on the other hand the tactical level authority and flexibility in execution of Tactical INFO OPS which ground commanders need.
- At the tactical level significant effort should be made to ensure a larger degree of continuity

(149) OSD, 2011, p.2.

(150) Larson [et al.], 2009, p. xxii.

(151) Mackey and Tatham, 2009, p. 6.

in the application of INFO OPS across unit rotations, including plans and programmes and knowledge development. A common database across rotations and functional areas (e.g. CIMIC, PSYOPS, HUMINT etc.) would not only enable deploying units to monitor developments in the mission area, but could also foster the development of the institutional memory needed to achieve the desired level of continuity.¹⁵²

Conclusion

This paper has discussed a series of aspects of the tactical implementation of INFO OPS in COIN, covering the information and operating environment, target audiences, desired effects, and delivery through Tactical INFO OPS. The paper has furthermore discussed the employment of different techniques and capabilities, and all the things behind that forms the preconditions for successful use of INFO OPS, especially education and training in its broadest sense, leadership, intelligence and planning.

Where it concerns the tactical level, it cannot be stressed enough that INFO OPS should be an integral part of all plans, operational phases and activities in COIN. In short INFO OPS in COIN is about how the counterinsurgent should protect the local population against the insurgents and create a perception that the insurgents doesn't pose a threat neither to the local population, nor the supported government and its security forces that are the alternative to the insurgency. At the same time the counterinsurgent must avoid becoming the like the insurgents himself in the eyes of the local population. It is also about how the counterinsurgent should not lose focus on the persuading of the local population while struggling with the insurgents, lest the counterinsurgent be sucked down into an "anti-insurgent" kind of warfare instead of COIN operations. In order for this to work the counterinsurgent at the tactical level must work under the direction and guidance of an overarching plan (comprehensive approach), including the military as well as the political, economic and civilian lines of operations.

Concurrently with the tactical activities there are also strategic information activities that need to be taken into account and have an impact not only on the tactical situation but on the entire campaign.

Taking as a truism Thomas P. O'Neill's statement that "all COIN is local"¹⁵³ then successful tactical INFO OPS are a direct strategic enabler in the greater context of the comprehensive approach in COIN operations.

As argued throughout the paper COIN is as much about, if not even more, influencing perceptions, will and behaviour as it is about influencing (read *destroying*) enemy capabilities through kinetic action. But even though COIN operations are conducted locally or tactically they have strategic implications and must be conducted on the backdrop of the strategic plan, to include a coherent narrative and an information strategy, to drive the Tactical INFO OPS.

Most importantly, people are the Centre of Gravity and their "perception becomes reality", and with that we are back to General Sir Gerald Templer and his emotional (Hearts) and cognitive (Minds) components of perception and why INFO OPS, especially Psychological Operations, are a key factor in COIN operations.

(152) Larson [et al.], 2009, p. xxi.

(153) Flynn, Pottinger and Batchelor, 2010, p. 12. (originally he said "all politics are local")

Closing Perspectives

The fundamental elements in COIN operations as argued in this paper have in some form or other been a historical part of these kinds of operations for a long time. The cases of Burma, Malaysia and Vietnam, Iraq and Afghanistan, are some of the more familiar. These cases cover the past to the present, but what about in the future? What perspectives do we see in regards to COIN operations and INFO OPS in the future?

Looking at the operations in Iraq and Afghanistan they are both COIN operations, but it could be argued that the similarities more or less ends there. The background for the conflicts were different, and therefore also the strategies including the “ends, ways and means” at the strategic, operational and tactical level. The approach to, and focus on intelligence and operations in the two theatres has been different, and rightly so, and therefore the approach to INFO OPS has also been different.

In the short run, it is likely that NATO or NATO countries will continue to engage in low intensity conflicts, with their own characteristics in other parts of the world, for example Africa has been named continuously. There is nothing to indicate that NATO or its member nations are about to embark on full scale war in order to survive. This assumption leads to another, namely that the future use of military forces will be mainly in stability operations of some form. Perhaps not labelled as COIN operations but as peace support or stability operations, but the operations will most likely be conducted “amongst people” and in the modern information environment, and the COIN’s constraints on planning and execution of military operations will still be valid, if not more. INFO OPS will therefore also be a vital and necessary part of modern military operations in the future, also when we are no longer in Afghanistan.

References:

Adams, Mark W G (2009): Cognitive Operations for Strategic and Operational Effect: UK Military Influence Activities in the 21st Century. In Defence Academy Yearbook, Defence Academy of the United Kingdom.

AJP-01(D) (2010): Allied Joint Doctrine. NATO. (NATO/PfP UNCLASSIFIED)

AJP-3.4.4. (2010): Allied Joint Doctrine for COIN. NATO. (NATO/PfP UNCLASSIFIED)

AJP 3.10 (2009): Allied Joint Doctrine for Information Operations. NATO. (NATO/PfP UNCLASSIFIED)

AJP 3.10.1 (A) (2007): Allied Joint Doctrine for Psychological Operations. NATO. (NATO/PfP UNCLASSIFIED)

Amend, Kurt (2010): COIN Principles for the Diplomat. Published by Elsevier Limited on behalf of Foreign Policy Research Institute. Spring 2010. Page 215 to 231.

Bryder, Nana, Andersen, Steen Bornholdt (2009): Forsvarets sproglige og interkulturelle beredskab. I Militært Tidsskrift, 138. Årgang, nr. 4, December 2009, pp. 423 to 438.

CALL (2006) - Centre for Army Lessons Learned: "Southern Afghanistan COIN Operations – Tactics, Techniques and Procedures". CALL Handbook, no. 07-6, October 2006.

Cassidy, Robert M. (2009): War in the Information Age. Review Essay in Parameters, Winter 2009-10, page 177 to 122.

Coffey, Luke (2009): Detainee Operations in COIN Operations – Lessons form Afghanistan 2005 – 2006. Small Wars Journal, <http://www.smallwarsjournal.com>.

COMISAF (2009): ISAF Commander´s COIN Guidance. ISAF Headquarters, Kabul, Afghanistan, September 2009. http://www.nato.int/isaf/docu/official_texts/COIN_guidance.pdf (29/3 2010)

Dauber, Cori E. (2009): YouTube War – Fighting in a world of cameras in every cell phone and photoshop on every computer. Strategic Studies Institute, November 2009. www.strategicstudiesinstitute.army.mil

DCDC – Development, Concepts and Doctrine Centre, UK Defence Academy (2010): Army Doctrine Paper – Operations in the Land Environment, draft as of February 2010.

Dilegge, Dave (2007): "Hearts and Minds", *SWJ Blog*, 21. October 2007. [www.smallwarsjournal.com/blog/2007/10/\(26/3 2009\)](http://www.smallwarsjournal.com/blog/2007/10/(26/3%2009)).

Ferguson, Barbara (2010): Arming Marines with Operational Culture. In Militært Tidsskrift, 138

årgang, no. 4, januar 2010. Page 439 to 441.

FKODIR 147-0 (2008), Forsvarskommandoens direktiv for Informations Operationer, 2008.
(Danish Defence Command directive on Info Ops)

FKODIR 147-1(2008), Forsvarskommandoens direktiv for Psykologiske Operationer, 2008.
(Danish Defence Command directive on PSYOPS)

Flynn, Michael T, Pottinger, Matt and Batchelor, Paul D. (2010): Fixing Intell - A Blueprint for Making Intelligence Relevant in Afghanistan. http://www.cnas.org/files/documents/publications/AfghanIntel_Flynn_Jan2010_code507_voices.pdf (2. februar 2010)

FM 3-05.301 (2003): US Army Field Manual - Psychological Operations Tactics, Techniques and Procedures. December 2003.

FM 3-05.302 (2005): US Army Field Manual - Tactical Psychological Operations Tactics, Techniques and Procedures. October 2003.

Galula, David (1964): COIN Warfare – Theory and Practice. London, UK: Praeger Security International, 1964.

Gowing, Nik (2009): Skyful of Lies ´and Black Swans – The new tyranny of shifting information power in crisis. In RISJ Challenges. Reuters Institute for the Study of Journalism, RISJ 2009, University of Oxford.

Halverson, Jeffry R., Goodall, H. L., and Corman, Steven R. (2011). Master Narratives of Islamist Extremism. New York: Palgrave MacMillan.

Hampsey, Russell (2010): Rediscovering the Art of Psychological Operations in the Afghan COIN. In Small Wars Journal. www.smallwarsjournal.com

JP 3-13 (2006): US Joint Publication on Information Operations (IO). Department of Defence (DoD), 13 February 2006.

Kelley, John Robert (2009): “Between ”Take-offs” and ”Crash Landings””, *Handbook of Public Diplomacy* (ed. by Nancy Snow & Philip M. Taylor). New York: Routledge, 2009.

Kilcullen, David (2006): ”Twenty-Eight Articles – Fundamentals of Company-level COIN”, In Marine Corps Gazette, Summer 2006. http://turcopolier.typepad.com/sic_semper_tyranis/files/twentyeight_articles_edition_1.pdf (24/03 2009).

Kilcullen, David (2009): The accidental Guerrilla – Fighting a Small War in the Midst of a Big One. Hurst & Company, London.

Krieger, Mark P. (2007): We the People Are Not the Centre of Gravity in an Insurgency. In Military Review, July – August 2007, pp. 96 to 100.

Labarre, Frederic (2009): Effect-Based post-conflict reconstruction and stabilization. In: The Comprehensive Approach – Challenges and Prospects. Royal Danish Defence College Publishing House, Copenhagen, 2009.

Lamb, Christina (2006): “US Radio Ramshackle wins over Afghan locals”. *TimesOnline*, 22. October 2006. <http://www.timesonline.co.uk/tol/news/world/article608976.ece> (26/3 2009)

Larson, Erik V., **Darlek**, Richard E., **Kays**, Dalia Dassa, **Morgan**, Forrest E., **Nichiporuk**, Brian, **Dunham-Scott**, Diana, **Thurston**, Cathryn Quantic and **Leuschner**, Kirstin J. (2009): Understanding Commanders’ Information Needs for INFO OPS. RAND Corporation.

Liborius, Søren (2010): Sprog og kultur – Når soldaten ikke kan tale (sit eget sprog). I Militært Tidsskrift, årgang 138, nr. 4, januar 2010, page 516 to 522.

Mackay, Andrew and **Tatham**, Steve (2009): Behavioural Conflict – From General to Strategic Corporal: Complexity, Adaptation and influence. The Shrivenham Papers, Number 9, December 2009. Defence Academy of the United Kingdom.

McKenna, Sean and **Hampsey**, Russell (2010): The COIN Warrior Waging Influence – Hints for the COIN Strategy in Afghanistan. In Small Wars Journal special 2. June 2010. www.smallwarjournal.com

Mitchell, William (2009): The Comprehensive Approach dilemma: No Unity of Command – No Unity of Effort. In: The Comprehensive Approach – Challenges and Prospects. Royal Danish Defence College Publishing House, Copenhagen, 2009.

Mitchell, William (2010): Swinging the Tomahawk – The Role of Cultural Experts in War Fighting. I Militært Tidsskrift, årgang 138, nr. 4, januar 2010, page 442 to 462.

Moir, Nate (2008): Influencing COIN operations through PSYOP. Paper under the Van Deman Program at U.S. University of Military Intelligence, August 2008, www.universityofmilitaryintelligence.us (26/3 2009).

Murphy, Dennis M (2008): Fighting Back: New Media and Military Operations. Centre for Strategic Leadership, United States Army War College, Pennsylvania. www.carlisle.army.mil/usacsl/Studies.asp.

Murphy, Dennis M (2009): Talking the Talk – Why warfighters don’t understand. In IO Journal, April 2009, pp. 18 to 21.

Nissen, Thomas Elkjer (2007): The Taliban’s Information Warfare. RDDC Brief, Copenhagen. Royal Danish Defence College, 2007.

Nørgaard, Katrine & **Holsting** (2006): Vilhelm, Internationale operationer i Fokus. København: Forsvarsakademiet, 2006.

OSD – Office of the Secretary of Defense (2011): Directive OSD 12401-10 on Strategic Communication and Information Operations in the DoD. Pentagon, 25 January 2011.

Ringsmose, Jens (2007): Nye krav til Vestens soldater i det 21. århundrede. Nyhedsavisen, 10. april 2007.

Ringsmose, Jens & **Thruelsen**, Peter Dahl (2010): NATO´s COIN campaign in Afghanistan – are classical doctrines suitable for alliances? UNISCI Discussion Papers No 22, January 2010.

Roca, Raimundo Rodriguez (2008): "Information Operations during COIN Operations – Essential Option for a Limited Response", Athena Intelligence Journal, vol. 3, no 1, 2008.

Rosin, Randolph (2009): To Kill a Mockingbird – The Deconstruction of Information Operations. Small Wars Journal, 2009. www.smallwarsjournal.com

Rowland, Lee and **Tatham**, Steve (2010): Strategic Communication and INFO OPS: Do We Really Get It?. Special Series 10/08, Advanced Research and Assessment Group, Defence Academy of the United Kingdom, September 2010.

Seese, Gregory and **Smith**, Paul N (2008): Measuring PSYOP Effectiveness. In Sepcial Warfare, November – December 2008. Volume 21, Issue 6. United States Army John F. Kennedy Special Warfare Center and School, Fort Bragg, N.C.

Smith, Rupert (2005): The Utility of Force – The art of war in the modern world. Penguin, Allan Lane. London, England.

Sullivan, Michael D (2007): Leadership in COIN: A Tale of Two Leaders. In Military Review, September – October 2007.

Tatham, Steve (2008): Strategic Communication – A primer. Sepcial Series 08/28, Advanced Research and Assessment Group, Defence Academy of the United Kingdom, December 2008.

Terence, Daly (2006): "Classic COIN – The key to victory against today's insurgents". Marine Corps Gazette, December 2006.

Thruelsen, Peter Dahl (2009): The Comprehensive Approach in Helmand Province – From a military perspective. In: The Comprehensive Approach – Challenges and Prospects. Royal Danish Defence College Publishing House, Copenhagen, 2009.

Todd, Helmus; **Paul**, Christopher; **Glenn**, Russel (2007): Enlisting Madison Avenue – The Marketing Approach to Earning Popular Support in Theatres of Operation. RAND Corporation, 2007.

www.forsvaret.dk/hok/

www.cnn.com

The author's interviews with commanders and key personnel within Info Ops, PSYOPS and CIMIC from Danish Battle Groups deployed to Iraq and Afghanistan between 2003 and 2010, as well as briefings and end of tour reports from these deployments.

-- # --