Professional Journal of the South African Army

Editor:
H.R. Heitman
Telephone 012 347 1929
Mobile 083 675 0615
Telefax 012 347 1179
E-mail heitman@iafrica.com

Postal Address:
254 Pleiades Avenue
Waterkloof Ridge
Pretoria, 0181 South Africa

Editorial Committee:
Major-General L. Rudman
Colonel S. Zeeman
Lieutenant-Colonel Annelize Rademeyer
Telephone 012 355 1902
Telefax 012 355 1414
E-mail sso@saarmycom.co.za

Postal Address:
SA Army Journal
(Corporate Communications)
Private Bag X981
Pretoria, 0001 South Africa

Design and Reproduction:
Bushbaby Communication

Printing:
Sherino Printers
Atlas rd Boksburg
# CONTENTS

## Editorial

<table>
<thead>
<tr>
<th>Page</th>
<th>Title</th>
<th>Author(s)</th>
</tr>
</thead>
<tbody>
<tr>
<td>2</td>
<td>National Security Policy, Strategy and Doctrine and the Department of Defence’s Responsibilities</td>
<td>Colonel Bob R. Janssen</td>
</tr>
</tbody>
</table>

## Warfare and Armed Conflict

<table>
<thead>
<tr>
<th>Page</th>
<th>Title</th>
<th>Author(s)</th>
</tr>
</thead>
<tbody>
<tr>
<td>12</td>
<td>Lessons learned from African Insurgencies: Implications for South African Army Intelligence</td>
<td>Major C.S. van der Spuy</td>
</tr>
</tbody>
</table>

## Doctrine, Strategy and Operations

<table>
<thead>
<tr>
<th>Page</th>
<th>Title</th>
<th>Author(s)</th>
</tr>
</thead>
<tbody>
<tr>
<td>25</td>
<td>Asymmetric Strategies as Strategies of the Strong</td>
<td>© 2011 Michael Breen and Joshua A. Geltzer</td>
</tr>
<tr>
<td>30</td>
<td>Cultural Intelligence as an Enabler</td>
<td>Major A.J. de Vos</td>
</tr>
<tr>
<td>38</td>
<td>Cultural Intelligence: The SA Army in Peace Operations</td>
<td>Pte Katlego Mashishi</td>
</tr>
</tbody>
</table>

## Other Armies

<table>
<thead>
<tr>
<th>Page</th>
<th>Title</th>
<th>Author(s)</th>
</tr>
</thead>
<tbody>
<tr>
<td>44</td>
<td>A Proposed Service Delivery Philosophy for Army Support</td>
<td>Col Dries van Jaarsveld</td>
</tr>
<tr>
<td>48</td>
<td>High Mobility Forces of the German Army</td>
<td>Dietmar Klos</td>
</tr>
</tbody>
</table>

## Risks and Opportunities for Security and Connectivity: Cyber Issues for Central Africa

<table>
<thead>
<tr>
<th>Page</th>
<th>Title</th>
<th>Author(s)</th>
</tr>
</thead>
<tbody>
<tr>
<td>52</td>
<td>Risks and Opportunities for Security and Connectivity: Cyber Issues for Central Africa</td>
<td>Major Raoul Nanci Yossi</td>
</tr>
</tbody>
</table>

## Book Review

<table>
<thead>
<tr>
<th>Page</th>
<th>Title</th>
<th>Author(s)</th>
</tr>
</thead>
<tbody>
<tr>
<td>58</td>
<td>Counterinsurgency in Africa: The Portuguese Way of War 1961-1974</td>
<td>John P. Cann</td>
</tr>
<tr>
<td></td>
<td>Strategy: The Logic of War and Peace</td>
<td>Edward N. Luttwak</td>
</tr>
</tbody>
</table>

## Enfilade

<table>
<thead>
<tr>
<th>Page</th>
<th>Title</th>
<th>Author(s)</th>
</tr>
</thead>
<tbody>
<tr>
<td>60</td>
<td>Remarks by Secretary Gates to North Carolina ROTC Students</td>
<td></td>
</tr>
</tbody>
</table>

## Remarks by Secretary Gates to North Carolina ROTC Students

2

25

44

48

52

58

60
From the Editor’s Desk

Readers may wonder why this issue of the Journal does not cover Bangui, even though that is now already six months in the past as this editorial is written. The reason is simple: While the basics have been well covered by debriefs and even in a short e-book, there is actually a lot to be learned from this deployment, and it will be better to cover it later and perhaps in a series of articles by different people looking at different aspects, once everyone has looked beyond the immediate lessons and digested some of the longer-term implications.

As editor I will, however, allow myself some initial comments here:

• Regardless of what may have been written in public articles, and even if some of it was true, there was a good strategic reason to deploy: The Central African Republic forms a large portion of the northern border of the DRC and the entire western border of South Sudan. The DRC is an SADC state that we are attempting to help stabilise. Instability in the CAR will spill over into the Equateur province of the DRC and cause problems for the DRC’s eastern neighbours – Uganda in particular – and for stabilisation efforts in the North Kivu province. South Sudan is, like the CAR, contiguous with the DRC and a major security problem along its western border will also impact on its border with the DRC. To use a basic military term, both the CAR and South Sudan are, in effect, within the ‘area of influence’ of anyone wanting to stabilise and protect the DRC. In fact, there are already indications in press reports of spill-over from the chaos in the CAR.

• The initial deployment was exceedingly small, partly for political reasons and partly for reasons of inadequate force levels and airlift capacity. But the announcement that some 400 South Africans would be deploying in Bangui, where there were already some 600 French troops and troops from several Central African states does seem to have been a factor to cause Seleka to pause and opt for negotiation in the interim, rather than simply regroup and drive into the city. That bought time.

• When Seleka did resume their attack, however, the Central African force was no longer visible, the CAR Army had evaporated, and the French commander was in a difficult position with – at that point, some troops having been withdrawn in January – only some 400 troops to protect the airport and the embassy, and round up 1 200 or so EU civilians.

• That left the SANDF contingent out on a limb. But those troops fought as well as any in history under an exceptional group of officers and NCOs, and performed their primary mission – protect or extract the SANDF training team – despite immense odds. Their performance in Bangui will save us casualties in the future: Other African rebels have taken note, and will be reluctant to engage South African troops. Some, indeed, already know that from previous contacts in Burundi, the DRC and Darfur.

What we need to do now, is understand that Bangui will not be the only situation of this type that will fall to the SANDF: There will be short-notice missions, and there will be missions in situations where intelligence is vague at best; and there will be both smaller operations, an SF hostage rescue for example, and larger ones that need to be conducted on a ‘come as you are’ basis. We need to think about that and prepare for it – and let us please hear from our readers on that subject: You are the ones who will have to conduct those missions, so it is you whose responsibility it is to study and analyse Bangui and come up with ideas – type and strength of force; command structure; weapons and vehicles; etc.

And let us remember that those who fought at Bangui did us all proud: Some gave their lives; some were badly wounded; all were exhausted; and all will have had family members fearing for them. Give them the respect they have earned and hear them out when they tell what they experienced and perhaps suggest how to do things better. There are very few soldiers in the world today who have been through an experience like that, and it is our duty to learn from them.

And let us pack away our negativity: Yes the Defence Force and the Army face real problems – but no army’s soldiers could have fought better. We may not have been there ourselves, but we can take a quiet pride in the fact that we serve the same Army as these soldiers.
This paper proposes to answer the question of what are the responsibilities of the government departments regarding South Africa’s National Security Policy irrespective of whether South Africa has an implicit or an explicit national security policy? The paper provides a discussion on the concept of security, including how matters or issues are securitised. It then discusses the responsibilities of the government departments regarding the planning and contingency planning to prevent matters of becoming securitised or ensuring that these matters become desecuritised.

Introduction

Jacques Chirac once said “Peace can never be taken for granted and the first responsibility of any government is security.”

The South African Government has been developing its national security policy, strategy or doctrine for quite some time. The reason for referring to the document as a “policy, strategy or doctrine” is that there is some debate as to what it should be called.

A number of countries do not have an explicit national security policy, strategy or doctrine. This is not always because they lack the expertise to compile one, but perhaps because they are better informed than those who do. Rear Admiral R.A.S. Hauter once said² that if you make known the country’s acceptable limit of tolerance to the enemy, the enemy will test your resolve. In risk management language one would refer to South Africa’s risk appetite.³ Do we really need to have our enemies testing our resolve? What will they test?

The South African National Defence Force has had the challenge of developing the defence policies and strategies according to Government guidelines that are usually not detailed enough to perform this task. This has been the situation since before World War Two. In 1937 Major General Van Ryneveld⁴ complained that the General Staff had had to endure a period of ten years without a clearly defined State Military Policy. He described the situation as follows:

Whatever the causes may have been – public hope that the millennium [of peace] had arrived resulting in indifference and lack of money for military requirements, political prejudice, uncertainty caused by new inventions, etc. – the fact remains that for the last decade, the General Staff has been faced with the grave handicap of not having any clearly defined State Military Policy.
The axiom that service training makes better citizens has at least afforded some guidance … but for clear planning, a more precise definition of the object of our defence organisation and training is required than is implied in the [Defence] Act.

A ray of light is now being let in and however faint it may be, it immediately provides a part at least of that indispensable aim without which all our military preparations are nebulous.

The policy now emerging is to think and plan in terms of bush fighting efficiency, and even to the laymen it must be clear that with nothing more than this apparently vague definition of policy, it now becomes possible to decide on matters from puttees versus leggings to guns versus howitzers.5

The question that one needs to ask is whether it is the responsibility of the politicians to provide guidelines for each of the government departments in such detail that no questions will remain. Not even White Papers or Ministerial guidelines are in such detail. It is therefore necessary for the officials of government departments to analyse the government’s intention in order to formulate the detail for that specific department to infer what the South African National Policy contains applicable to them enabling the preparation of its own security planning including contingency planning.

The intention of this paper is to elicit debate (or promote creative stress), to critique certain matters of the current processes of compiling the South African National Security Policy and to suggest further options.

When studying national security, one can view it from an academic or a military practitioner perspective. This paper will try and discuss it from both perspectives.

The question one needs to answer is: what are the responsibilities of the government departments regarding South Africa’s National Security Policy irrespective of whether South Africa has an implicit or an explicit national security policy?

Conceptual and terminological considerations

- **Distinguishing between policy, strategy and doctrine**
  The question is whether the national security document is to be called a policy, a strategy or doctrine. The problem is that even though a national security strategy is called a strategy one should ask whether that is the correct terminology. In the next part the difference between policy, strategy and doctrine will be explained.

History indicates that policy covered the administration of the state, be it at town level or at central state level. Administration covered functions such as finances, war and legislation, with the main emphasis on the finances.6 Perhaps the most authoritative definition of policy is the one by Easton: “the authoritative allocation through the political process, of values to groups or individuals in the society.”7 Politics is also defined as “the science of who gets what, when and why.”8 Ranney makes a distinction between the policy process and policy contents. He explains the policy process is “the procedures by which policies are made” and policy content is “the rules, regulations, and other courses of action that governments take.”9 Hanekom adds a number of other types of policies which he explains are different phases of policy, namely policy demands, decisions, statements, outputs, and outcomes. He describes them as follows: “policy demands – representing community needs that necessitate action by authorities; policy decisions – the decisions made by the authorities and which result in action; policy statements – i.e. making the authorities’ intentions public; policy outputs – what is actually done;” and “policy outcomes – results of the steps taken to satisfy demands.”10 Anderson defines public policy as “a relative stable, purposive course of action followed by government in dealing with some problem or matter of concern.”11 He explains that the action is in response to a specific purpose and is in response to specific policy demands made by private citizens or public officials on government. Policies may be positive or negative, meaning it could require action or prohibit action. Public policy could be proclaimed in law and then it would be authoritative and enforceable, or it could be issued as guidelines as is the case of a “white paper,” in which case it would be an imperative but not be able to enforce legal sanction when omissions occur.

Vickers, with regard to policy, explained it as follows:

In government and business, a distinction is often drawn between policy making and executive decisions - the first being designed to give direction, coherence, and continuity to courses of action for which the decision-making body is responsible; the second designed to give effect to the policies thus laid down12.

I have described policy making as the setting of governing relations or norms [values] rather than in the more usual terms as the setting of goals, objectives, or ends13.

Betts indicates that there should be linkages between the various levels of policy and strategy as well as between the two concepts. He explains it as follows:

Considering examples at different levels of analysis is reasonable as long as the focus remains on the linkages in the hierarchy of policy, strategy, and operations, where the logic at each level is supposed to govern the one below and serve the one above. A scheme for how to use a particular operation to achieve a larger military objective, or a foreign policy decision that requires certain military actions, are both strategic matters at different levels in the chain between means and ends. Strategy fails when some link in the planned chain of cause and effect from low-level tactics to high-level political outcomes is
Booth once remarked, “Strategy is a deadly business”\(^\text{16}\); with a strategy? decisions in order to achieve a certain purpose. What then is Policy therefore is a course of action and to guide future means.\(^\text{14}\)

J.C. Garnett explains defence policy as follows:

In retrospect … policy is revealed by series of decisions, and in prospect it is revealed by general statements of purpose. … The term ‘policy’ needs to be able to embrace both what is intended and what happens in the implementation of the intention. It ought to be identified not by its goals but by the actual behaviour attempting to effect the goals. Policy, therefore, is best thought of, not as a series of finite decisions, but as a flow of purposive action over a period of time. It incorporates what governments have done and what they are trying to do.

Whatever definition is accepted it is clear that policies involve decisions – decisions about what to do and about how to do it. …\(^\text{15}\)

Policy therefore is a course of action and to guide future decisions in order to achieve a certain purpose. What then is a strategy?

Booth once remarked, “Strategy is a deadly business”\(^\text{16}\); with the habit of business management, every sports commentator, economist and even psychologist using strategy in their fields of expertise, the problem today is that there is no clear conception on what strategy is. The word appears to have lost its original meaning to the soldier of today, if one believes all the misuses of the concept of strategy the concepts needs to be re-examined. A number of definitions will be provided to indicate what the meaning of the concept strategy is when referring to it.

Carl von Clausewitz defined strategy by distinguishing between tactics and strategy when he explains:

Strategy is the use of engagements\(^\text{17}\) for the purpose of the war [own emphasis]. The strategist must therefore define an aim for the entire operational side of the war that will be in accordance with its purpose. In other words, he will draft the plan of the war, and the aim will determine the series of actions intended to achieve it: he will, in fact, shape the individual campaigns and, within these, decide on the individual engagements. Since most of these matters have to be on assumptions that may not prove correct, while other, more detailed orders cannot be determined in advance at all, it follows that the strategist must go on campaign himself. Detailed orders can then be given on the spot, allowing the general plan to be adjusted to the modifications that are continuously required. The strategist, in short, must maintain control throughout\(^\text{18}\).

If one studies the explanation of Clausewitz’s definition, strategy becomes more than just the simplistic number of battles to attain the aim of the specific war. He explains strategy to be even more than campaigns, as all the battles that will be required are to contribute to the attainment of the aim of the war. It means that the strategist will have to re-plan each time to ensure that the various campaigns still are directed towards attaining the aim.

The greatest contribution Clausewitz made to the science was to place war in context. He explained that war consists\(^\text{19}\) of three remarkable characteristics, first, it consists of violence, secondly, chance and thirdly, it is subject to political control. He explained that “war is an instrument of policy”\(^\text{20}\) or put in another way, military force is the continuation of government’s policies by other means than social, economics or diplomacy.

André Beaufre’s definition of strategy is as follows:

It is therefore the art of the dialectic of force or, more precisely, the art of the dialectic of two opposing wills using force to resolve their dispute.\(^\text{21}\)

Strategy is … a thought process which, complex though it is, should be able to point the way in practice towards achievement of the ends desired by policy and, even more important, eliminate those glaring errors of … in recent history\(^\text{22}\).

The essence of strategy … is the struggle for freedom of action. The basis … of strategy, therefore, is the preservation of one’s own freedom of action (security) and the ability to deprive the enemy of his freedom of action (by surprise or initiative)\(^\text{23}\).

Strategic thinking, however, is a mental process, at once [simultaneously] abstract and rational, which must be capable of synthesizing both psychological and material data. The strategist must have a great capacity both for analysis and for synthesis; analysis is necessary to assemble the data on which he makes his diagnosis [prognosis], synthesis in order to produce from these data the diagnosis itself – and the diagnosis in fact amounts to a choice between alternative courses of action\(^\text{24}\).

Beaufre, therefore, describes strategy as a much broader concept as did his predecessors. The reason for this is that he builds on the definitions of previous thinkers such as Clausewitz and makes the concept of strategy a subject with many facets. For this reason one is amazed by the simplistic description of strategy by Maxwell D Taylor who defined strategy in 1981 as “objectives, ways and means,” which Lykke amended to “ends, ways and means”\(^\text{26}\). Reducing strategy to an equation is to
reduce it to mathematics, for which Clausewitz criticised Antoine Jomini. This explanation detracts from complexities such as described by Clausewitz and Beaufre, whose descriptions of strategy cannot be reduced to an equation or to a simplistic rational process. In practice, this definition is used to a large extent, contributing to the misconceptions surrounding the concept of strategy. Fourie’s definition for strategy is: “Strategy is a method of using coercion to create an untenable situation for an opponent.”

Why do some people refer to a national security doctrine? Firstly, the national security policy is called a doctrine in some countries, e.g. the East-European countries. However, these days some of the national security policies are called national security concepts. Although the Russians these days call their national security policy a “concept,” it was described previously as a doctrine as can be seen from the following quote by Marshal Grechko:

The concept of doctrine… encompasses teaching, a scientific or philosophical theory, and a system of guiding principles and views. Accordingly, military doctrine is understood to be an officially accepted system of views in a given state and in its Armed Forces, on the nature of war and methods for conducting it, and on preparation of the country and the army for war. At the very least military doctrine answers the following basic questions: What enemy will have to be faced in a possible war? What is the nature of the war in which the state and its armed forces will have to take part? What goals and missions would they face in this war? What armed forces are needed to complete the assigned mission and in what direction must military development be carried out? How are the preparations for war to be implemented? What methods must be used to wage war? … all of the basic provisions of military doctrine stem from actually existing conditions, and above all, from domestic and foreign policy, the socio-political and economic system, the level of production, the status of means for conducting war, and the geographic position, both of one’s own state of that of the probable enemy. … The theoretical basis of Soviet military doctrine consists of the following: Marxism/Leninism; military science, and, to a certain degree, branches of social, natural, and technical sciences related to the preparation of armed struggle, as well as to other forms of struggle – economic, ideological, and diplomatic. Military doctrine, in its turn, has a reverse influence on military-theoretical thought.

An example can also be found in a current situation where the “coalition of the willing” was used in Iraq, rather than a North Atlantic Treaty Organisation consensus approach, is called a doctrine. Doctrine is also found in the White Paper on Intelligence, where the following is said: “The national security doctrine must promote the creation of a societal environment that is free of violence and instability. It must engender, within the context of a transformed judicial system, respect for the rule of law and human life.” Doctrine is therefore broader than just the teachings of the armed forces or, stated differently, it can be seen as a fixed strategy for set situations.

National security therefore should be seen as policy rather than strategy. A strategy can be devised later should an opponent of government be identified that require to be countered. From here on, national security policy strategy or doctrine will be referred to as a “policy.”

• **The concept of security**

Most definitions in the social sciences are written from the perspective of a certain approach or paradigm and do not always define the whole spectrum that a specific definition should describe. There are many definitions, each with its own advantages or shortcomings and it is not the purpose of this paper to analyse these definitions in much detail. Each can be written according to its own approach, from realist to constructivist. Conceptualising security will therefore be discussed from another perspective.

Similarly Richard Wyn Jones and Sarah Tarry analysed the definition of security from the perspective of deepening, broadening and extending the concept of security. Wyn Jones indicated “in addition to criticising the attempt to draw a rigid distinction between the subject and the object, Horkheimer’s critique of ...” isolating particular security “… practices from its totality of which they form part...” is not desirable. By broadening the concept of security he tries to incorporate both the non-military issues and the referent object that move away from the statist paradigm. Extending the concept of security is to extend the concept from the statist with a view to incorporating the security of the individual, groups and multinational institutions. Michael Howard once explained that one could study military history from three perspectives, namely width, by observing what has changed and what has not. In studying history in terms of depth one would look at a single campaign and explore it not only through official histories, but also from memoirs, letters, diaries and other literature. Lastly he explained that military history should be studied in context as one could only understand each campaign by understanding the complexity of the societies within which it was fought. In the next section a small selection of the current conceptualisations of security will be discussed.

• **Traditional concept of security**

The realism approach is reflected in Stephen Walt’s statement “equates security with peace and the prevention of conflict through military means.” This was predominantly the approach before 1990 when the enemy was easily identifiable as being one side or the other in the Cold War. Ian Bellany defined it as: “Security is a relative freedom from war, coupled with a relatively high expectation that defeat will not be a consequence of any war that should occur.”
In this conceptualisation, security is the domain of the state which relies on the military to secure sovereignty and is written in the context of Clausewitz's dictum, where strategy (or war) is subordinate to the country's policy or politics. Deepening the concept of security

Security can be both a subject for study, and an object or a goal to be achieved. Deepening the conceptualisation of security also involved looking past the pure realist way of approaching the subject of security. In other words, the theorists attempting to deepen the concept of security looked further than just the military being involved in ensuring security. This deepening of the concept of security also recalled the dictum of Clausewitz who indicated that war or its strategy was subordinate to political activities, which is in line with the view of Ken Booth and R.B.J. Walker who stressed "the relationship between notions of security and deeper assumptions about the nature of politics and the role of conflict in political life." Booth went further and indicated that security needed to be emancipated. By this he meant that there should be an absence of a threat or, put differently, there must be the freedom of choice. This included freedom from war, "poverty, poor education, political oppression and so on."

- **Broadening the concept of security**

In the eighties the concept of security was broadened to include human security. Wæver explained that this included the following: "The security of individuals can be affected in numerous ways; indeed, economic welfare, environmental concerns, cultural identity, and political rights are germane more often than military issues in this respect." Buzan also broadened the concept of security as follows:

The security of human collectivities is affected by factors in five major sectors: military, political, economic, societal and environmental. Generally speaking, military security concerns the two-level interplay of the armed forces and defensive capabilities of states, and states’ perceptions of each other’s intentions. Political security concerns the organizational stability of states, systems of government and the ideologies that give them legitimacy. Economic security concerns access to the resources, finance and markets necessary to sustain acceptable levels of welfare and state power. Societal security concerns the sustainability, within acceptable conditions for evolution, of traditional patterns of language, culture and religious and national identity and custom. Environmental security concerns the maintenance of the local and the planetary biosphere [e.g. environmental degradation and global warming] as the essential support on which all other human enterprises depend.

This is even broader than just military action in ensuring the security of the state or its sovereignty.

Another example of the broadening of security can be found in the wording of article 55 of the United Nations Charter, which reads as follows:

With a view to the creation of conditions of stability and well-being which are necessary for peaceful and friendly relations among nations based on respect for the principle of equal rights and self-determination of peoples, the United Nations shall promote:

a. higher standards of living, full employment, and conditions of economic and social progress and development;

b. solutions of international economic, social, health, and related problems; and international cultural and educational co-operation; and

c. universal respect for, and observance of, human rights and fundamental freedoms for all without distinction as to race, sex, language, or religion [own emphasis].

This includes the matters of social development and human security, economics and international relations.

The White Paper on Defence in South Africa also broadened the concepts by stating:

Security is an all-encompassing condition in which individual citizens live in freedom, peace and safety; participate fully in the process of governance; enjoy the protection of fundamental rights; have access to resources and the basic necessities of life; and inhabit an environment which is not detrimental to their health and well-being.

At national level the objectives of security policy therefore encompass the consolidation of democracy; the achievement of social justice, economic development and a safe environment; and a substantial reduction in the level of crime, violence and political instability. Stability and development are regarded as inextricably linked and mutually reinforcing.

At international level the objectives of security policy include the defence of the sovereignty, territorial integrity and political independence of the South African state, and the promotion of regional security in Southern Africa.

The term “securitisation” was developed to facilitate expanding the conceptualisation of “security” beyond the military realm. Waever introduced the concept by asking: “What really makes something a security problem?” He discusses it as follows:
...(A) major focus of “security studies” should be the processes of securitization and de-securitization: When, why and how elites label issues and developments as “security” problems; when, why and how they succeed and fail in such endeavors; what attempts are made by other groups to put securitization on the agenda; and whether we can point to efforts to keep issues off the security agenda, or even to de-securitize issues that have become securitized?50

What then is the difference between securitisation and a political issue? Essentially Wæver explains that for something to be securitised, it might imply the use of military force, whereas a political issue can be solved by other means, such as diplomacy.51

- **Extending the concept of security**

Waever indicated that national security was the security of the state.52 The state in turn could also have its problems as indicated by Deon Geldenhuys who indicated that “(s)state decay can take on at least three different forms: in a soft state, corruption is endemic; a weak state is characterised by deep internal cleavages, and a failed state suffers from the collapse of official institutions and law and order.”73 Buzan, however, indicated that “the term 'national security' suggests a phenomenon on the state level, the connections between that level and the individual, regional and system levels are too numerous and too strong to deny.”74 In other words the concept of security includes human security, military protection of the state, but it is now extended to include matters such as anti-corruption, good governance, and security not just for the state, but also for the individual and in the region and the world.

- **Contextualising the concept of security**

Ken Booth and Peter Vale studied the effect of security studies within the perspective of Southern Africa. This study interrogated force postures as well as the effect of migration on regional stability.55 The regional arrangement is also discussed in Chapter 8 of the United Nations Charter.56 The outcomes of these studies are not analysed here but rather the issues of contextualisation of security not just for a country, but also for the individual, the group, the region but also for the international community. The context should also consider the time within which matters or issues of security are considered.

Betts explained:

One danger in strategic studies is missing the political forest for the military trees. That danger was greater during the cold war than now. The opposite danger – that defining security broadly will squeeze out work on the military aspects – is greater now.57

This is not only true for strategic studies but also for security. A balance is still to be achieved between all the elements of security and not ignore matters such as the military. After all the concepts have been discussed it might be good to venture a definition of national security.

- **Defining security**

In examining the responsibility of government in respect of national security one could study the state’s implied responsibilities as contained in the concept of statehood. The constituent parts of a “state” according to the Montevideo Convention of 1933 are: “a population, a territory and a government, which could even enter into relations with other states.”58 Statehood is the fact of being a state and of having the rights and power of a state, implying both de jure and de facto recognition of a specific state to be sovereign. Relating the parts of statehood to security, the state’s regime is therefore responsible for, amongst others, the provision of security for its population, territory, and government. One could therefore define national security by combining the constituent part of a state with that of Mandel59 who defined the purpose of national security. The definition then reads as follows: “National security is the pursuit by government of a psychological and physical condition in which there is protection against an immediate or future threat endangering the sovereignty, the survival of the government and its regime, the territorial integrity, their citizens, or their way of life. A condition in which the individual citizens live in freedom, peace and safety; participate fully in the process of governance; enjoy the protection of fundamental rights; have access to resources and the basic necessities of life; and inhabit an environment which is not detrimental to their health and well-being.”60 Trying to incorporate all elements of security could make this definition even much longer. A shorter definition for security could be “curbing of threats to ensure survival.” This survival should be viewed much broader than just trying to exist in the future for the state and the individual, but should also include its liberation from a struggle of just existing to becoming a fully independent, progressive and sustainable.

In layman’s language, security can be defined as: freedom from threat,61 freedom from fear and want,62 from hazardous impact, from indignity (social security), and freedom of choice. Another way is to describe insecurity by indicating the threats, e.g. a threat to survival, a threat to existence or freedom, a threat to self-determination (a sovereign state) or development, a threat of being expelled, or a threat to one’s identity or values.63 Although this discussion above tried to expand the concept of security, there are much more elements to it than mentioned above, because other international relations approaches such as collective security has not been explored and must not be ignored when considering what government department responsibilities may be.

- **The usefulness of an explicit national security policy**

One must consider that a national security policy could be an explicit written document or it can be an implied policy. An implied national security policy can be made known through various methods in South Africa, such as the government Programme of Action, the Presidential Priorities or even what Waever called a “speech act.” The latter would then be communicated by the State of the Nation address or a similar type of occasions. If a national security policy is an explicit document it may have the following advantages or disadvantages.
• **Advantages of having a defined national security policy.**

Having an explicit national security policy ought to ensure that every government department is clear on what is expected from them regarding their responsibilities. An explicit policy could also indicate the intentions of the government regarding bilateral and multilateral matters.

An explicit national security policy may create the impression that each government department does not have to define its own risks or vulnerabilities as the national security policy has already done this and therefore the responsible department does not have to think for itself. This in itself could be viewed as a weakness of a very comprehensive national security policy.

• **Disadvantages of having a defined national security policy.**

A national security policy may be a unilateral document and would not necessarily take into account the view points of the bilateral or multilateral partners. In South Africa’s case, this might not be a problem as the government is very serious about African Unity through the consolidation of the African Agenda. This, however, is not always true for all countries as can be explained by an example from the 2006 United States of America National Security Strategy. “The goal of our [United States of American] statecraft is therefore to help create a world of democratic, well-governed states that can meet the needs of their citizens and conduct themselves responsibly in the international system. This is the best way to provide enduring security for the American people.” In this case, the United States of America has very noble intentions but is prescribing to the rest of the world what should happen in other countries. In other words, it is assuming the role of a supranational organisation. The United Nations is not even a supranational organisation as it is only an international organisation. Even though the United States of America is not a supranational organisation, the wording above appears as if it perceives itself as being powerful enough to accomplish the task.

The explicit public national security policy of a country only provides an abstract of the more comprehensive classified document that is only meant for the eyes of certain government officials. No country will provide the classified documentation, as it could jeopardise its relations with other countries. The problem could then be that it becomes an imperative for foreign countries to start hunting for a copy of the classified document, as they may perceive some devious intent by the government against their specific government.

The explicit national security policy may be parochial (protection of the specific government department’s “turf”), depending on the lead department responsible for compiling of the document. This has happened in the past in South Africa and could happen again. In this case, the guidelines for the one department may be sufficient, but not for all other government departments.

The document could become outdated within a short period of time, due to the fast changing security environment. The acts of terrorism perpetrated on 11 September 2001 in the United States of America have changed its conception of national security and has had the effect of making acts of terrorism a securitised matter. This can be seen through the efforts of the United Nations Security Council where the securitisation of the acts of terrorism, for example, has had the effect making it of international concern. The explicit national security policy could also become outdated due to new matters being securitised.

African unity could also have an effect on the national security of South Africa, as one ally could become a target for terrorism and dragging all its allies into the same mould. This can be seen where acts of terrorism have spread to a number of countries involved in any North Atlantic Treaty Organisation’s operations or where the country is allied to the United States of America.

The constantly changing national policy as contained in, for example, the Government Programme of Action, white papers, policy statements by politicians, etc, could also force a change to the content of the national security policy, which will then require redrafting of the national security policy. The problem one has to consider is the time required to redraft and produce a new national security policy.

Opponents or enemies to South Africa’s security could test the resolve of the government and the citizens of the country when limits are set as to what type or level of conflict will not be tolerated. This could evolve in a similar situation to that of the United States of America and the United Kingdom. The question may be whether South Africa will specify these limits within their explicit public national security policy.

It is clear therefore that a country does not actually require an explicit national security policy as one has more advantages with an implicit national security policy. The reason being that an implicit policy provides fewer problems regarding security, and that each government department would concentrate on its own responsibilities or shared responsibilities, in areas where the specific department is a specialist.

**Responsibilities of government departments regarding national security policy**

Irrespective of whether the government has issued an explicit or implicit national security policy, the government departments will have to perform their own analysis of future actions required. This will ensure that they zoom into matters pertaining specifically to their own field of expertise or their “core business.”

• **Defining a threat**

The defining of a threat is part of making an issue a political issue or securitising the issue. The defining of a threat could also be done by instruments other than an explicit national security policy, for example through a separate national threat document.
Possible expected threats, taking the responsibilities of the state as a framework: Threats to the democratic order of South Africa (including the Constitutional order and the state); threats to the people of South Africa (such as violence, disaster, disease, and economic threats); threats to the territorial integrity of South Africa (such as protection of the country’s resources and infrastructure, which may include a military threat); or threats to the regional and global harmony. As can be seen from the examples, they are not all military threats.

• **Subsequent actions**
The problem for this discussion is not the process of identifying a political issue, securitising an issue (a matter becoming a security issue), desecuritising an issue (a matter stops being a security issue) or even non-securitising an issue (a matter not becoming a security issue, possibly through diplomacy), but rather what should a specific government department do in the case a matter becomes a security issue or risk that requires responses. The government department is to react by defining the threat or vulnerability. It could accept the threat to, or vulnerability of a specific threshold, or share the threat by making use of other government departments or multilateral organisations. The government department could institute active measures (combatting the threat or reducing the risk or vulnerability) and passive measures (preventing the threat or avoiding the risk) to mitigate the threat that may influence the national security of South Africa, or perform consequence management after an act compromising the national security has taken place.

Should the state be required to take extraordinary measures to counter a threat, and the contingency planning is in place, the specific government department will be in a position to react at very short notice. In South Africa the tendency is not to militarise issues, but rather to keep them the responsibility of the appropriate government department. An example of a matter being demilitarised over the past few years is the National Crime Prevention Strategy. In any case, the responsibility of the government department should be to prevent a matter becoming a political issue, or being securitised (non-securitised) or, when it has been securitised, to desecuritise the specific matter.

• **Risk management**
As already indicated a government department has to react to political or securitising issues that may influence the national security of South Africa. In order to be able to plan for these eventualities, the government departments will each have to perform specific tasks within their own departments.

• **Requirements of government departments regarding national security policy.**
Each government department is to determine what the government’s intention is regarding specific political or securitised issues that may become its responsibility. They will have to perform the complete sequence of policy analysis which could contain the following steps: policy demands, formulation, enactment, output, implementation and impact.

The specific government department will have to compile a position paper on the specific perceived policy and obtain ministerial approval for its interpretation. These position papers could also be forwarded to the inter-ministerial committees (or Clusters). In response to these issues the specific government department will then draw up its plans or contingency plans and obtain approval for these plans through the Cluster committees. This will prevent a course of action being taken at short notice without the consent of the national executive.

An example where contingency plans were communicated too late to the national executive was the “Schlieffen Plan” that caused the mobilisation act of Germany to become the First World War, instead of just threatening the Russian and French coalition. The intention of the Kaiser was to mobilise the armed forces; in other words to call them up as a show of force to threaten Russia. The armed forces, however, interpreted the mobilisation as a declaration of war, including the initiation of a war on France first and then to switch over to the Russian front within a very short period of time, all calculated to minute detail on train schedules. The reason for attacking both fronts was because they were allies and the Russians would take longer to move their forces to threaten Germany. The Kaiser, however, changed their plans on short notice in order not to infringe Dutch neutrality, but to use only Belgian territory. This detailed the finely scheduled plans to move the armed forces by rail.

• **How government departments compile an abstract for their own department from the implied national security policy**
Even in the case of an explicit National Security Policy having been promulgated, the government departments will still have to compile their own abstract of the National Security Policy, because in most cases, the National Security Policy will not address all government departments in detail. The abstract will therefore have to consider what the government’s intention is in the situation should a matter be securitised.

• **Possible areas that may be made a political or securitised issue (within each government department’s responsibility)**
The abstract would also have to specify all the contingencies that need to be addressed by the specific government department. These would then have to be addressed by the department’s plans or separate contingency plans.

• **Contingency or mitigating plans to address vulnerabilities**
Plans or contingency plans should be prepared, controlled, updated and approved to be in line with identified threats and securitised issues. These plans will have to consider all the possible reactions to the specific situation to mitigate the security risk or vulnerabilities.

Approval of contingency plans will have to be obtained from the Cluster Committees. The planning elements and the plans of officials will have to be published in order to have the specific
official know his or her responsibilities. These contingencies will also have to be staff tested (or rehearsed) in order to test their feasibility and contingency plans will also have to be updated as required.

Conclusion

The purpose of this paper is to indicate the responsibilities of government departments irrespective of whether South Africa has an explicit or an implicit national security policy. This is done by questioning the conceptualisation of security and indicating what should be done by the government departments in this regard.

The problem with the conceptualisation of security is that it is a concept that is contested or is in the process of being developed. At first, security was very narrowly defined as being the responsibility of the armed forces, but these days everything that causes conflict can be ascribed to a security problem. The difficulty is what to include and what should be excluded. The complexity of security is that it may include matters ranging from poverty, conflict within the family, or war. It is therefore difficult in practice to confine security to a limited number of issues, which does not make the job of the government department any easier.

The government will have to consider a structure within the Cluster Committees with responsibility for national security. The committee will have the task of ensuring that each government department comes up with its own suggested issues that may be securitised or risks that may be unacceptable to government. The committee will then be responsible for ensuring that the various government departments have sufficient and viable plans to counter risks and vulnerabilities or issues that may be securitised. This will ensure that risks are avoided, reduced, shared or accepted. The Committee must ensure that each government department is able to deal quickly with any fast evolving security matter. The contingency plans should ensure all potential events are addressed and that the surprise and possible associated costs or losses are thereby reduced. Should certain issues overlap the responsibilities of more than one government department; the Cluster Committees should identify the lead department and ensure that these issues are addressed by multi-departmental committees.

Each government department must analyse its own responsibilities and mitigating actions to support South Africa's national security. This must be done irrespective of an explicit or implicit national security policy. These contingency plans are also meant to highlight the requirement of each department to ensure that they are sufficiently prepared to take decisions at short notice, having already considered the most probable contingency.

These contingency plans will also have an impact on each government department’s policies, strategies, doctrine and budgets. This means that these policies, strategies and doctrines must be updated to comply with the requirements of South Africa’s national security policy. In the case of most of the government departments, these policies, strategies and doctrines that have been revised, will have to be staff tested (through exercises or rehearsals) to ensure their viability.

It is clear from the arguments above that it does not matter whether South Africa has an explicit or implicit national security policy; each government department still has responsibilities regarding national security. Over and above the responsibility of the state to protect its citizens, ensure growth and development of the country, it also has the responsibility of planning for matters or issues that may become securitised or could be prevented from being securitised. These efforts will have to be coordinated through the Cluster Committee system as part of normal government business. The latter is responsible to ensure early warning systems are in place to provide early warning of matters or issues that may be securitised.

NOTES

1. Jacques Chirac, NATO in the New World, in Mail & Guardian, December 1 to 7 2006.
4. General Sir Pierre van Ryneveld was the founder of the South African Air Force in 1920, became Chief of General Staff in 1933 and retired in 1949.
7. Cloete and Wissink, op cit, p. 11.
17. Engagements in the original German is “Gefechts”, which could also be translated as battles.
22. Ibid, p. 133.
27. Fourie, D.F.S., Strategic studies (Honours), Only study guide for STUSTO-S (The study of strategy), Pretoria: University of South Africa, 1992(1976), pp. 12 to 23
34. Ibid.
44. Ibid.
48. O. Waever, Securitization and Desecuritization, in R.D. Lipshutz (Ed),
Lessons learned from African Insurgencies: Implications for South African Army Intelligence

Major C.S. van der Spuy

Background

“The problem is that you cannot prove yourself against someone who is much weaker than yourself. They are in a lose/lose situation. If you are strong and fighting the weak, then if you kill your opponent then you are a scoundrel... if you let him kill you, then you are an idiot. So here is a dilemma which others have suffered before us, and for which as far as I can see there is simply no escape.” (van Crevel, 2007)

It is evident that insurgency is assuming a new profile in the 21st Century. Insurgents present government and intervention forces with complex problems involving an elaborate mix of political, economic and social dimensions. The shift towards transnational terrorism and decentralised structures adds to this dilemma. An analysis of various counterinsurgency strategies will reveal that well-developed and decentralised intelligence structures, interlinked with the police and other role players are the keys to success. This paper will examine the lessons learned from various African insurgencies, including those experienced in the South African context, in order to determine the requirements for intelligence gathering during counterinsurgency in terms of doctrine, force design, training and technology. It suggests that the South African Army is not structured to meet the requirements for counterinsurgency both in the internal and external dimensions. It highlights the shortcomings in intelligence training and contends that the South African Army has the experience and knowledge to conduct counterinsurgency, but that its doctrine must be updated and implemented. Specialist knowledge must be reincorporated into training and the taboo surrounding counterinsurgency is to be abandoned in order to be successful.

The paper commences with a definition of insurgency and counterinsurgency as a precursor to the discussions. This will be followed by an analysis of the change in insurgency from the colonial to the contemporary era with a look into African insurgency trends. Lessons will be extrapolated from these discussions, which will serve as a basis for the intelligence requirements in future counterinsurgency operations. The South African Army’s intelligence capability for counterinsurgency will then be analysed with these requirements as a basis.

Defining Insurgency and Counterinsurgency

Insurgency can be defined as a strategy adopted by non-ruling groups within a state to obtain political objectives when they are unable to do so through conventional means. Insurgency is, therefore, the strategy of the weak, and is usually characterized by protracted, asymmetric and psychological warfare, which mobilizes the population. The end result is to discredit the existing government and turn the tables in order to gain the upper hand and build legitimacy. Insurgents may have the aim to overthrow the government and obtain power, which is known as revolutionary insurgency, or they may have more limited objectives, which may include separation, autonomy or a change in policy. (Metz and Millen, 2004: 2)

There are a number of strategies used by insurgents in the past. One of the most well known strategies is Mao Tse-tung’s protracted popular war strategy. This strategy followed a phased approach, which begins with the development of popular support in the rural areas. As the movement becomes stronger, a guerrilla warfare stage is entered and, when the government is weakened by further social, political and military means, the insurgents cross over to conventional warfare. Few insurgencies, however, move into this stage. Another approach is that used during the Russian Revolution (1917). This strategy called for a small group of elite revolutionaries which would conduct subversion of the political and social structures. A military-focused strategy, on the other hand, requires that the insurgents use predominantly military force to seize power, and finally there is the urban approach, utilized by the Irish Republican Army, which entails the use of terrorism against the
Counterinsurgency (COIN) is a term that has been used in conjunction with stability operations, irregular warfare and military operations other than war to name a few. Despite this conceptual turmoil, counterinsurgency is simply the actions taken by government forces or their allies in order to overcome an insurgency. (Baker and Jordaan, 2010:33) Smith has termed this as a ‘war amongst the people.’ This ultimately means that modern militaries no longer face tangible enemies, but rather opponents that are nestled within the population. (Smith, 2007)

There are three major approaches to counterinsurgency. The first approach involves the winning of hearts and minds (WHAM). This is an approach aimed at gaining the trust and support of the population through political, social and economic development. The second approach is more coercive and is, therefore, primarily military focused; communities are punished if they are found to support the insurgents and this ultimately leads the community to weigh the relative costs and benefits. Counterinsurgency forces that face manpower shortages, however, tend to opt for the imperial approach. This is the strategy of building enemies for the insurgents. Regardless of the approach used, counterinsurgency remains a difficult task, as indicated by van Creveld above, and must be applied according to the unique circumstances at hand. (Baker and Jordaan, 2010: 34)

Evolution of Insurgent Conflict

The Global Experience

There are a number of differences that have surfaced in the conduct of insurgency in the post cold war era. Large-scale conventional war between states is unlikely for the moment. Globalisation; the failure of states to meet the needs of their population; the erosion of political, social and economic structures; as well as the manifestation of organized crime; have made insurgency strategically important and on the rise. (Metz and Millen, 2004: 1)

Insurgency during the 20th Century can largely be seen as a form of proxy conflict between the superpowers, namely the United States of America and Russia. There was no direct confrontation between these powers due to a possible nuclear breakout, with the result that their battles were played out in the Third World. (Metz and Millen, 2004: 10) The end of the Cold War, however, meant that the support, training and ideology that had previously sustained insurgencies were no longer available. Support for insurgencies will still be obtained externally and the motivation factors will remain the same, but some will be more intricate (Figure 1). With this large support base removed, insurgencies have to derive other means to generate income. The solution to this problem has been adoption of crime as a means to gain such support. This has a two-fold effect, namely it removes the need for external sponsors as well as the need for popular support, eroding the active involvement of the people. (Metz and Millen, 2004: 10; Hammes, 2006: 20) The reduction in the importance of popular support ultimately leads to greater use of violence against civilians. Metz has termed this commercial insurgency. (Metz, 1993: 1, 13; Malaquias, 2001: 317)

While insurgencies were important during the Cold War due to their use for superpower rivalries, insurgencies are even more important in the contemporary context due the link to transnational terrorism. This is not a new phenomenon, as insurgents have long used terrorism as a means to intimidate supporters of the government. What makes it distinguishable, is that it is used in a strategic way. (Metz, 2007: 7-8) Insurgents use terrorism as a form of long-range power projection which may deter counterinsurgency support from states that have little vital interest in the conflict.

The protracted people’s war, as described in the previous section, presents a particular difficulty when trying to apply it in the contemporary world, because the social, political and economic conditions that could be used to foster nationalism, are not that visible in present times. What makes this notion more complicated is that insurgents, particularly in Africa, no longer face foreign government but rather an indigenous one. The result is that it becomes increasingly difficult to harm the reputation of these governments, and the insurgent groups signify only a minor part of the population. (Davidson, 1981; O'Neill, 1990)

Adding to the difficulty in its application, is the fact that governments are now becoming stronger technologically and militarily, and have thus developed greater counterinsurgency competencies. The increased ability of governments in terms of transportation, information processing and detection capabilities, somewhat diminishes the advantage of large rural areas and inaccessible terrain. In some cases, even without these capabilities, there is an absence of large populated territory and favourable and accessible areas. Another possible factor that might play a role results from the increased technology and transport abilities of the government - the attraction of many people to urban areas, resulting in a draining of the rural support base. This calls for a totally different strategy altogether. By the end of the 20th Century, counterinsurgency had evolved to such an extent that it was effective in combating insurgents. (Davidson, 1981; O’Neill, 1990) Insurgents, rather than isolating themselves in rural areas, will now embed themselves in the urban environment, with the initial stages of the strategy forming and taking place within the city itself. (Metz and Millen, 2004: 12; Khalil, 2011; Hoffman, 2007: 5)

Steven Metz argues that insurgent ideologies have changed. Ideologies based on radical Islam are on the rise, while there are only a few remaining Marxist insurgencies. These and other ideologies such as Pan-Arabism and Pan-Africanism have not been successful, and new ideologies based on ethnicity and religion are emerging. These, however, are not really new but
are accompanied by fewer constraints, which is attributed to the absence of the supervision of the superpowers. (Metz and Millen, 2004: 13; Metz, 1993: 8; Pearson and Laitin, 2001: 4; Hoffman, 2007: 6) He has coined this phenomenon as a ‘spiritual insurgency’, which is the rejection of the ‘social, economic and political system associated with that regime.’

It was mentioned before that insurgents turn to crime to support their cause. However, in some cases obtaining wealth becomes an objective of its own. These insurgents may define personal meaning with possessions. Gurr has termed this as ‘relative deprivation’. This basically means that Third World societies are increasingly exposed to media through technology and are able to observe large-scale differences in the quality of life when compared to Western societies. This is seen in a material sense, and discontent is fueled as they have the perception that they are deprived and look to the government as the reason for their lack of such possessions. (Metz, 1993: 10; Malaquias, 2001: 317; Reno, 2009: 11)

One of the major changes in insurgencies is their metamorphosis towards networked structures. Today, insurgents are less hierarchical but more decentralized and operate in the form of webs or cells. This allows for great adaptability and is particularly suited to fast moving and high density information environments. Operating in this way, insurgents do not have an identifiable centre of gravity, and this is a difficult concept for the military that strives for a decisive target. There is no one cell that is more important than the rest. These cell-like structures are less rigid than the more classical models. (Metz, 2007: 12-13; Khalil, 2011; Crawshaw, 2007: 19; Hoffman, 2007: 8)

Support is obtained through a variety of linkages and alliances, which is made possible through greater interconnectedness through technology that would have not been possible in the past. (Metz, Rethinking Insurgency: 12-13; Hoffman, 2007: 8) Support is gained in the virtual realm and not only the physical, as demonstrated by the Zapatistas of Mexico. This removes the territorial connection and moves it into cyberspace. (Baker and Jordaan, 2010: 58; Arquilla and Ronfeldt, 2001: 185) Figure 1 serves to illustrate the changes in insurgent characteristics over time as well as the trend toward newer strategies.

African Insurgency Trends

Vrøy has highlighted a number of trends in African insurgencies. One is that they follow a nationalistic contour in which the ‘how’ of rule and ‘who’ rules are the focus. (Baker and Jordaan, 2010: 59) The desire for power and the weakness of states are the drivers for many African insurgencies. There may be dissatisfaction about government policies that may lead to an insurgency. (Baker and Jordaan, 2010: 60)

African insurgencies in some respects also host a mix of agendas. This is evident in southern Nigeria, where the Movement for the Emancipation of the Niger Delta (MEND) has both political agendas as well as those based on greed that is intertwined with ethnic factors, environmental insecurity and resource claims. There is a myriad of role-players, which range from gangs to criminal groups. In these cases, it becomes difficult to pinpoint the exact agenda, as there are so many to contend with. (Baker and Jordaan, 2010: 61)

Figure 1: The change in insurgent strategy and characteristics over time.
In line with Metz’s conceptualisation of spiritual insurgency, some African cases portray a defined ideological focus. This is exemplified by the Somali insurgency. In this conflict, the type of political rule is contested. This is of special note as this conflict has elements of piracy and possible terrorism at sea which makes it trans-national in nature. (Baker and Jordaan, 2010: 61)

The violence in Darfur, on the other hand, is characterised by politico-ethnic factors. Insurgent movements such as the Justice and Equality Movement (JEM) and National Movement for Reform and Development (NMRD) and the Khartoum government with their state-sponsored militias are in conflict. This conflict is different in that Sudan is bordered by Chad, which has its own insurgent threat. The result is that each country blames the other for aiding and hiding insurgent forces, which has also resulted in a large number of refugees, not to mention suspicion between the two states. (Baker and Jordaan, 2010: 61)

Lastly, it is noted that there is another party to the conflict in some African insurgencies and that is the various intervention forces. These include the African Mission in Somalia (AMISOM), the United Nations Organization Stabilization Mission in the Democratic Republic of the Congo (MONUSCO), the African Union – United Nations Hybrid Operation in Darfur (UNAMID) and the African Mission in Burundi (AMIB) that serve to complicate the situation by adding a peace mission aspect. It is asserted that these intervention forces, whether it be the United Nations (UN) or African Union (AU), actually make insurgency successful and worthwhile for non-ruling groups. The insistence by these organisations on inclusive conflict resolution means that insurgents are able to enter into national politics. (Baker and Jordaan, 2010: 62) The United Nations settlements will actually serve as an incentive for insurgencies and provide the means for a victory. (Metz, 1993: 1, 13)

**Learning from the Past**

**Lessons Learned from African Insurgencies**

Most of the European colonies had relinquished their power by the 1960’s. There was some resistance to insurgent movements, but no major counterinsurgency was conducted except in Kenya, Algeria and the Portuguese campaigns. The British learnt in the early stages of the insurgency of the Mau Mau in Kenya that disciplinary measures would only spur on the insurgency. The British subsequently called a state of emergency in October 1952. They embarked on a campaign to obtain attainable political objectives and punished those that tried to counter their efforts. This serves to illustrate the need for clear political objectives. (McConnell, 1999: 6; Baker and Jordaan, 2010: 76)

Potgieter states that good intelligence and an efficient intelligence collection capability are an essential first step in a counter-insurgency operation. This is due to the social and political nature of insurgencies. This requires good civil-military coordination as well as the use of informants, spies and pseudo operations in order to form an intelligence picture. (Baker and Jordaan, 2010: 76) The French campaign in Algeria (1954-1962) serves to exemplify this point. In the first two years in their efforts to combat the Front de Liberation Nationale (FLN), the French failed to predict the insurgent movement’s preparations for war as well as their conversion from politics to armed conflict. (Clark, 2006: 7, Mockaitis: 16)

The French were isolated in the capital city of Algiers and did not have strong police components on the interior. This meant that the insurgents were able to act uninhibitedly in the rest of the country. The situation however changed between 1956 and 1960 when the French changed their strategy, which led to the end of the insurgency. The following were some of the features used by the French during this period:

**Destroy Insurgent Infrastructure.** All police files were confiscated and a complete hierarchy of FLN was determined in order to re-establish government administrative management. (Clark, 2006: 8)

**Grid Surveillance System.** A system was introduced which divided the operational areas into grids which included tactical segments such as houses. A military unit was assigned a grid and the unit was responsible for surveillance, searches and cordons in that area. (Clark, 2006: 8)

**Census.** A population census was conducted and identification cards issued to residents. (Clark, 2006: 8)

**Border Protection.** The census was further reinforced with the construction of the Morice Line on the Tunisian border and the Pedron Line on the Moroccan border. Patrols were regularly conducted which prevented the flow of arms. (Clark, 2006: 8; Goetzke, 2005: 10)

**Indigenous Police Force.** The French created an auxiliary police force. These comprised mainly Algerian Muslims who were former rebels and had close ties to the insurgents. (Clark, 2006: 8)

The later stage of the campaign was marred by human rights violations, but the above-mentioned techniques proved invaluable in winning the fight. (Clark, 2006: 8)

The counterinsurgency conducted by the British in Sierra Leone (1991-2002) is seen as a model. One of the major reasons for the success of this campaign was the improvement in intelligence capacity. A military information cell was formed at the United Nations Mission in Sierra Leone (UNAMSIL) Headquarters in Freetown, which enabled threat assessments. It is also important to note that the ability of the British forces to deliver on promises in terms of development; maintaining a secure environment for the citizenry and conducting large scale disarmament programmes ensured their success. (Paul, 2010: 163; Roberson, 1995: 20; Evoe, 2008: 101)
Another important feature of counterinsurgency is to isolate the insurgent from the population. The fortified lines of the French can be seen as such a strategy. The British utilized identification cards, monitoring of suspicious individuals and resettlement, although resettlement was not on a large scale. Such large-scale resettlements did take place in Malaya and Algeria, but these were coupled with an improvement in living conditions. Psychological and political dimensions were incorporated and proved successful. Alternatively, the resettlement of the population by the Portuguese in Angola and Mozambique was not successful. This is due to the fact that it took people away from their ancestral land and led to a decline in economic activity. The social, political and economic factors must be taken into consideration when opting for resettlement. (Baker and Jordaan, 2010: 76-78)

It must be noted that South Africa has years of experience in counterinsurgency during the 1970s and 1980s. These were conducted against movements that were both internally and externally based. Internally it faced armed resistance from the African National Congress (ANC) and externally the South West Africa People’s Organisation (SWAPO) in occupied South West Africa. Although counterinsurgency was initially the domain of the South African Police (SAP), the military progressively became more involved. The following were characteristic features of the counterinsurgency:

**Destabilisation.** Destabilisation or ‘destructive engagement’ was conducted in the neighbouring states, which included sabotage, raids and assassination. Angola was kept unstable, with the aim of complicating support for SWAPO. (Baker and Jordaan, 2010: 87)

**Total Onslaught Mindset.** The ‘total onslaught’ mindset of the Apartheid government led to an increase in the deployment of the Army in support of the Police. This strategy was informed by Andre Beaufre, which stated that total onslaughts required total indirect counter-strategies, which combined military, civil and economic action whereby the military would play an auxiliary role. (Baker and Jordaan, 2010: 89-90)

**Reliance on Experience.** The South African Defence Force (SADF) relied less on theory but rather on experience when conducting counterinsurgency. They were a highly innovative force and learnt from their external experiences in Angola and Namibia. The local conditions provided the impetus for strategy and techniques rather than theory. (Baker and Jordaan, 2010: 90)

**Imperial Approach.** South Africa adopted an imperial approach to counterinsurgency. The independence of Angola, Mozambique and Zimbabwe provided opportunities to exploit enemies of Apartheid’s enemies. This entailed the recruitment of opponents to new regimes as well as COIN functionaries. The result is that multiple COIN operations could be waged against multiple insurgents. This strategy was adopted due to manpower shortages and was a widely used tactic. This has been signified as the core of the South African COIN experience. (Baker and Jordaan, 2010: 90)

**Area Command Units.** The SADF was able to reach all areas by means of an effective command unit system. There were provincial commands, which comprised of three to six group headquarters, which were in turn responsible for five to nine commando units. These units operated in support of the SAP, protected their assigned areas against insurgents, protected key points, collected intelligence and supported local authorities. They comprised local members with extensive area knowledge, which made them particularly effective. (Steinberg, 2005: 5; Baker and Jordaan, 2010: 91)

**Special Forces.** The Special Forces played an important role as a long range reconnaissance tool for strategic and tactical intelligence, offensive actions, sabotage as well as COIN. (Baker and Jordaan, 2010: 91)

**Military Intelligence Division (MID).** The MID played a central role in the South African campaign. The MID was divided into task teams for each of the external insurgent groups being supported, the National Union for the Total Independence of Angola (UNITA) and the Mozambican National Resistance (RENAMO), and internally it conducted actions under the code name ‘Operation Marion’ which provided support to the Inkatha Freedom Party. The SADF also operated under the Coordinating Intelligence Committee, which was a joint security forces organization, which aimed at identifying targets for eradication. Additionally, a COIN Intelligence Task Team was established, which comprised of the SADF, National Intelligence Service (NIS) and the SAP, and which carried out cross border operations. (Baker and Jordaan, 2010: 93)

**Principles for Success**

There is a myriad of literature on how to conduct counterinsurgency operations. The lessons learnt as well as theories formed from past counterinsurgency campaigns cannot be applied to all situations, as each insurgency has its own unique mix of political, social and economic factors. There are, however, some general principles that can be applied across most insurgencies. Using the cases above, which are only a limited overview, there are some general concepts.

Firstly, there must be clear political objectives. This is exemplified by the British in their campaigns in Sierra Leone and Kenya. Clear, unambiguous goals that remain constant no matter the changing circumstances led to success. These must be filtered to the lowest levels. (Moore: 21; Clark, 2001: 13; Cohen, 2006: 50)

Secondly, civil-military coordination is important. There must be unity in planning processes and procedures. There should be one overall commander implementing the government campaign, this commander can be military or civil as long as all differences in opinion can be resolved through one
channel. Military objectives must mirror the political objectives. (Great Britain, Ministry of Defence, 2009: 99; Clark, 2006: 15; Mockaitis: 16)

The third principle is that of integrated intelligence. According to Daniel Byman, “intelligence is the sine qua non of counterinsurgency”. It lays the foundation for a counterinsurgency operation. (Clark, 2001: 14; Crawshaw, 2007: 29) The intelligence required is more than simply determining insurgent locations and movement. It entails information relating to political, social and economic issues. It also includes the beliefs, perceptions and attitudes of the insurgents as well as those of the population and more importantly to determine changes in behaviour. Human Intelligence (HUMINT) is the defining concept in such operations. It requires careful coordination with other organizations and departments. (Hammes, 2006: 26; Moore, 22; Great Britain, Ministry of Defence, 2009: B-3-7; Cohen, 2006: 50)

Separating the insurgent from his support base is critical. The French by means of their fortified lines and the grid system achieved this. This removes the insurgent’s logistical and financial support. It also allows the counterinsurgents the opportunity to launch their own psychological campaign. There are many methods used to achieve this separation. They implemented curfews and an identification system, whereas the Portuguese made use of large-scale resettlement. Importantly this must be accompanied by an improvement in socio-economic status in order to be successful. (Great Britain, Ministry of Defence, 2009: 104)

Implications for Intelligence

If one is allowed a moment to reflect on the above discussion, there are a number of observations that can be made in terms of the conduct of intelligence operations.

The very definition of insurgency implies that the counterinsurgent will be dealing with a non-conventional force. The intelligence functionary who is trained to identify enemy targets based on a predetermined analysis of the enemy in terms of structure, doctrine and methodology, will find it difficult to analyse an enemy who ‘does not exist’. The enemy hides within the population, looks like a civilian and his primary weaponry consists of a cellular phone and laptop. These are difficult to pinpoint in the first place, and in the second, what actions can be taken against them?

Whereas the operations of foreign militaries are contained in doctrine that can be studied in depth and reasonable preparation can be conducted in this regard in force preparation training exercises, insurgents do not operate from manuals or doctrine, nor can their possible strategies be determined and ‘practiced.’ Insurgents operate from an array of political, economic and social agendas. Changes manifest constantly and the mix of agendas make it difficult maintain focus in a campaign. The ‘fog of war’ as Clausewitz defined, is just as apparent in contemporary conflict as in the traditional conventional wars that have been fought. Material used for preparation will be more socially and politically inclined, meaning that an in-depth analysis of history, social-economic dynamics, cultural intelligence and human behaviour is required.

Intelligence leading to the destruction of one component may not prove fruitful. Insurgents operate in cells. Destroying one cell means that there are a number more to continue with the mission. The solution may reside in the interception of the network and the interconnectedness thereof. Targets cannot be seen in isolation. Intelligence organizations need to adapt to this non-linear format. Surveillance will remain a useful tool and is timeless. Whether it is conducted on the tactical levels of day-to-day contact or through long distance surveillance using sophisticated technology will prove to be decisive assets in the fight against insurgents.

Terrorism is another component, which cannot be dealt with in a military way. As soon as the military is brought in, it is almost guaranteed that the insurgents will gain legitimacy. The fight against terrorism is an intelligence effort that is conducted ‘quietly’ and meticulously without any fanfare in close collaboration with the police. (Howard, 2002)

Intelligence Requirements

Human Intelligence

Routine contact with the population is a key source of information and intelligence. Educate the troops to be courteous and friendly and it will pay dividends.
There are a variety of means to gather HUMINT, but in most cases the best method involves the commonplace methods of police and intelligence work. Only a small amount of HUMINT is derived from clandestine methods. Some of the most common methods include:

Collection Through Daily Contact. This involves the daily interaction between the police or military forces and entails observant and conscientious reporting of personalities and incidents. These must be captured in databases from which attributes can be used for selection. (Clark, 2001: 14)

Cordon and Search. In this procedure, an area is cordoned off by the military and the area searched for a specific target, or the population is questioned to gain more intelligence. (Clark, 2001: 14)

Informants. Police and the military utilize informants. This is a valuable source of information. Their reliability must be accurately gauged and their identities protected. (Clark, 2001: 18)

Surveillance Operations. Surveillance can be conducted on fixed targets of known insurgent strongholds, or it can take place on known insurgents or acquaintances of insurgents. (Clark, 2001: 18)

Interrogation. This is a useful, however questionable practice. It should, however be conducted within the judicial prescripts of the host nation.

Organisation and Structure

The analysis on the differences between colonial and contemporary insurgencies highlighted the more network-based insurgencies. The tendency therefore is toward flatter, network centric structures that offer more flexibility. The time used for analyzing, processing and dissemination of information is less. Intelligence structures must take on the form of the insurgent structures. (Clark, 2006: 16) This may also include the skipping of command channels in order for the information to reach the appropriate levels. (Great Britain, Ministry of Defence, 2009: 140)

As the information from sources increase, there must be sufficient intelligence members to collate, analyse, process and distribute such intelligence. One of the most important aspects of counterinsurgency operations is that it is manpower intensive. (Great Britain, Ministry of Defence, 2009: 146) The counterinsurgency campaign must be large enough to cover the entire operational area. The deployment of police and military teams in strategic areas is known as the "oil spot" strategy, whereby they will systematically increase their web of informants, gain more information and thereby stifle the actions of the insurgents.

Technology

The vastly networked structure of insurgents means that they will make use of information technology in order to gain support. Counterinsurgency efforts, similarly, must conduct information campaigns in order to neutralize this capability. National databases of insurgents, activities and criminals must be developed with each civil and military organization tapped into it in order to contribute and retrieve information. (Smith, 14)

Sensors also play a vital role. Sensors that detect heat and movement can be effectively utilized. Visual, audio and signals can also be detected and identified. There is a downside to this kind of technology in that the insurgents may not possess the same level of technology, reducing the value of communications and signals intelligence. Unmanned Aerial Vehicles (UAVs) coupled with police informants on the ground can render important broad information. Information provided from open sources is another useful source. There is an abundance of data available particularly at the start of the campaign in terms of statistics and maps, which can be used to derive an intelligence picture. These technologies are not always available with the result that other techniques can be used, which includes those mentioned for HUMINT gathering as well as methods such as the French grid system and a census to distinguish the population from the insurgents. (Smith, 13)

Training

Members to be deployed for such operations must be properly trained. The functionaries that are going to conduct operations require adequate background knowledge of the mission. Most important is the training of specialists. These include the training of analysts, surveillance operators, image interpreters, source handlers, linguists and interrogators. (Great Britain, Ministry of Defence, 2009: 146)

Meeting the Requirements

We have noted that South Africa has experience in the conduct of counterinsurgency warfare. Structures were put in place, doctrine formulated and large scale and effective intelligence networks were utilized which were inherent in the force make up. However, after the move to democracy in 1994, the counterinsurgency capability began to stagnate and fade.

South African Army Strategy

After 1994, the Army assumed a conventional, non-offensive approach. COIN was seen as a taboo topic, something that was associated with the Apartheid regime. The basis for this policy framework was the 1996 White Paper on Defence. It outlined that the primary focus of the military would be defence against external aggression and that secondary functions would include border protection, support for the police and peace support operations (PSO). The secondary functions however are the
tasks that the South African National Defence Force (SANDF) is primarily involved in and the structure, training and equipment for this purpose is not adequate to the task. Currently the South African Army is active on the borders of 5 provinces, namely Limpopo, Mpumalanga, Kwazulu Natal, Eastern Cape and the Free State under the auspices of Operation CORONA (Figure 2). (Baker and Jordaan, 2010: 137; Le Roux, 2008: 100)

Figure 2: OP CORONA Deployments: 11 Sub-Units in total along the borders of Limpopo, Mpumalanga, Kwazulu Natal, Eastern Cape and the Free State. These deployments will increase to 15 Sub-Units in 2013 (http://www.nationsonline.org/oneworld/map/za_provinces_map.htm)

This does not mean that the SANDF has not recognized the change in the nature or threats. It is addressed in various strategy and policy documents. The Future SA Army Strategy document demonstrates the awareness that there is a need for flexible force designs, flexible approaches to operations as well as a flexible logistic supply. However, the main concern raised by Gossman is that these strategy documents do not pose COIN as a solution to these needs. This is due to the great sensitivity surrounding the topic. (Baker and Jordaan, 2010: 139-140)

**Doctrine**

With the transition, many of the Army’s specialists left the military to pursue a political or civilian career. The knowledge of these members who operated for both SADF and former insurgent parties were not gathered on a formal basis. (Baker and Jordaan, 2010: 140) COIN doctrine has remained ‘frozen’ and has not been updated since 1998. (Baker and Jordaan, 2010: 139) If these manuals are in the process of being updated, it has not been determined. Joint Operations, which has had the responsibility for developing doctrine relating to internal operations has not done so to this date. Until very recently, this responsibility has been placed in the hands of Director Document and Policy of the South African Army and a result is expected in the near future. If there is not doctrine for internal operations, there automatically will not be an associated structure.

The only SA Army Intelligence Doctrine relating to COIN is found in the Intelligence Management Doctrine: Conduct of Intelligence During Area Defence Operations. This doctrine was last updated in 1998. It contains an array of outdated concepts, which include intelligence operations, namely EXPLOR (an overt collection system conducted by the commados), RATIO (an overt collection network which is undertaken by Citizen Force members controlled by the Group Headquarters) and SEE KAT, which is an overt collection network by full time members. There is heavy emphasis on the commando system, which is no longer in operation.

**Structure**

The Army consists of conventionally trained forces. The specialized units that specialized in COIN were disbanded, and there is no light force capability except for the paratroopers. The commando system, which spanned the entire county, played a vital role in the COIN effort in terms of their intimate terrain knowledge, community links and self-sufficiency. This system was phased out in 2003. By 2009, the last commandos were closed down and in this time period, a security gap surfaced, as the police were never able to take over the role. This is the reason why the Army is systematically being deployed along the country’s borders. (Steinberg, 2005: 1; Baker and Jordaan, 2010: 142)

The Army is structured on a conventional basis. The structures to conduct intelligence in current PSOs and internal border operations are inadequate. This needs revitalization if intelligence is to be gathered in a COIN scenario. The smallest infantry unit that can operate is only 10 members. (Baker and Jordaan, 2010: 142) This needs to be smaller in order for them to operate more independently and to gather more intelligence. There are only 6 intelligence functionaries currently per sub unit deployed for Operation CORONA. There is an overwhelming need for a greater intelligence structure in these types of deployments. The problem, however, is that the manpower just does not exist to meet these demands. In order for an adequate intelligence structure, the Army strategy must include for the development of a second intelligence Regiment. The current standby arrangements do not allow for a greater intelligence component.

The discussion so far has not even touched on the surveillance capability of the SA Army Intelligence Corps. As a very well trained organization, this is a very scarce resource. Currently, the surveillance capability, which at this stage can only be deployed at Troop strength, is limited and can only be deployed to ‘hot spots.’ This capability has potential in a COIN situation due to the intelligence collation capability as a system to effectively process gathered information and distribute it to the relevant authorities.

**Training**

According to Gossman, troops are trained in COIN only during mission readiness training and according to the needs of that specific operation. The broader concepts and principles...
of COIN are not dealt with. In contrast to Gossman, formal training in COIN does take place, however it is conducted at the lower levels and is not found in later developmental courses of soldiers where the focus is conventional and to a limited degree on PSO.

Fighting in built up areas (FIBUA) is a specialist Infantry capability that enables soldiers to operate in an urban setting and is a step closer to meeting asymmetric demands. To this date more than 1 000 soldiers have been trained in this capability. (Baker and Jordaan, 2010: 142; Tlhaole, 2011: 21)

During PSO, the gathering of intelligence is a very touchy subject. All forms of covert intelligence gathering are illegal and, therefore, it must be derived from soldiers in uniform. Even the word intelligence is replaced with the word information, explaining the complexity of intelligence gathering. It is for this reason that the infantry soldier during his patrols acts at the intelligence functionary in these situations. He must not only fight the opponent but also follow up on insurgent attacks and not merely act in response to the attack. (Baker and Jordaan, 2010: 143)

These soldiers must be trained in intelligence gathering to augment the intelligence effort and provide effective, focused intelligence to the functionaries that are charged to collect and collate this information. In the domain of counterinsurgency, every soldier must see himself as part of the greater intelligence effort, a task which is no longer just the responsibility of the intelligence-trained members. Additionally, there is little understanding by Infantry commanders on the utilization of intelligence personnel. They are seen as a threat instead of as an important element providing the information driving operations. They are marginalized, with the result that intelligence functionaries are not given the necessary support to conduct information gathering, such as vehicles and logistical support.

Formal specialist training for intelligence members include:

- Surveillance Operators
- Tactical Questioning
- Operational Photography
- Model Building
- Tactical Aerial Photo Orientation

These adhere to some of the requirements necessary to conduct counterinsurgency operations, but there is a serious lack in training in HUMINT. There is no formal course that addresses this subject, nor is there any form of linguistic training. The handling of sources is also not dealt with in a formal way and there is the expectation that such skills will be developed from experience. The fact that the South African Army Intelligence Corps does not have the mandate to conduct covert collection does not mean that intelligence functionaries will not deal with sources. (Erwee, 2011)

At this stage, as Gossman has pointed out, intelligence COIN training is conducted as part of mission and combat readiness training. This is far from enough. It is conducted over a two-week basis and it is expected that members will have a firm grip on internal operations in this short time period. This is compounded by a few notable challenges, such as the age of the intelligence functionaries involved as well as their technical skills. Adding to the complexity is the fact that the training is only ‘re-training,’ as it is expected that member are trained in the various disciplines, while the structure in fact provides for corporals who are not formally trained in questioning skills.

The principles above stated that there is a serious need for civil-military cooperation. Our soldiers are not taught in this regard, and are expected to interact with members of the civilian population during internal operations. These concepts have still not been addressed in formal training. Soldiers are not taught the dynamics of operating in conjunction with the police and other agencies. More importantly, they are not taught the legal aspects that are part of this integration. Training in the legal aspects only surfaces during the mission readiness preparation, whereas it should be enforced during formal courses. According to Capt B. Erwee, instructor at the School of Tactical Intelligence, it would be beneficial, for instance, if members from the Tobacco Institute of South Africa, Defence Intelligence and the South African Police Service (SAPS) could brief the intelligence members as to what they can expect in terms of the crime situation and cross-border tobacco smuggling in particular.

Less conventional intelligence training has also been identified as important for intelligence operations and this includes tracking. Intelligence functionaries operating in the rural context require tracking skills in order to identify the number of people that cross the border as well as when they crossed. The capability exists to conduct such training; all that is required is the formalization into the mission readiness courses. (Erwee, 2011)
Technology and Equipment

The literature above points to the possibility that insurgents may use information technology to gain popular support. The implication is that information networks will have to be monitored and databases between agencies, police and military must be linked to have timeous information. Open source information is a method to gather information during the early stages of an operation. The Tactical Intelligence System (TIS) of the South African Army Intelligence Corps can provide a useful tool in the rapid collation and dissemination of information. The individual components of the system, which includes thermal imagers, ground radar and long-range cameras are able to operate independently, and allow flexible application suited to the tactical situation. The system is currently utilized in this format by the Surveillance Troop deployed in support of Operation CORONA.

UAVs are part of the long-term acquisition in the Intelligence Corps and once acquired, can have substantial potential in COIN operations. However, in order to conduct operations in a high technological context requires soldiers who have the requisite computer skills. This is a serious concern that has been identified in the recent internal deployments. The reporting system used on the border is conducted via a computer system designed by Defence Intelligence. There is a lack of computer skills of intelligence members. Members must be trained in basic computer skills in order to conduct basic communication with the Tactical Headquarters.

There are other shortcomings. There is a lack of skills in the utilization of the Geographic Positioning System (GPS). The problem cited here is that the equipment utilized is not the same as the equipment on which the members initially received training. It is, therefore, required that members are issued with the equipment during training so that they can learn on those pieces. Gossman also states that the equipment utilized during PSOs in the Democratic Republic of Congo (DRC) and in Sudan is inadequate. The equipment is not suited to the environmental conditions and the infrastructure does not allow the use of conventional equipment.

The above discussion highlights a number of challenges facing the SA Army and the Intelligence Corps in terms of its ability to conduct counterinsurgency operations. What can be said is that the South African Army is an experienced force when it comes to COIN operations. The overriding problem, which inhibits effective structuring and training, is the perception that COIN is a bad after-taste of the Apartheid era. Very important training programmes, such as informant handling, have been discontinued. These and other courses are very necessary for border operations and PSO. What is needed is a change in mindset to take the doctrine, which is readily available, to update it to make it applicable to the present day and implement it at all levels. The South African Army is rich in knowledge and if this resource is not tapped into soon, as Gossman points out, the South African Army will lose its counterinsurgency ability altogether.

Summary

It is evident that insurgency is assuming a new profile in the 21st Century. Globalisation; the failure of states to meet the needs of their population; the erosion of political, social and economic structures as well as the manifestation of organized crime have made insurgency strategically important and on the rise. Adding to this is the emergence of transnational terrorism. Insurgents are becoming increasingly networked and amorphous. They hide themselves in urban areas and utilize the media and technology to gain support. In this way, the population has come to matter less and are the targets for intense violence.

An analysis of various counterinsurgency strategies reveal that well-developed and decentralised intelligence structures, interlinked with the police and other role players are the keys to success. HUMINT is one of the most important methods of gathering intelligence and relies on sometimes mundane intelligence work. National databases of information must be linked and all departments must contribute to a central network of information that can be tapped into at any time. Specialist knowledge was found to be vital for intelligence functionaries, and includes the training of analysts, surveillance operators, image interpreters, source handlers, linguists and interrogators.

After 1994, the South African Army assumed a conventional, non-offensive approach. COIN was seen as a taboo topic. With this, doctrine has not been updated and various specialist training has been discontinued. The commando system, which was a very important intelligence gathering system, was systematically closed down. The knowledge and experience of previous South African insurgents and counterinsurgents was not tapped into, with the result that the structure and training of intelligence functionaries is lacking. Emphasis must be placed on altering the South African Army Strategy to cater for peace support and counterinsurgency operations. This requires a larger intelligence component.

Conclusion

South Africa has vast experience in COIN operations. This knowledge, however, has not been tapped into. A change in mindset is needed to update and implement COIN doctrine which is still very applicable to the current security environments that the South African Army is tasked to operate in. South African Army Strategy will have to plan to restructure forces in order to adapt to these asymmetric situations in which the Army will find itself. Intelligence is the driving force in counterinsurgency operations and it is not only the responsibility of the intelligence functionary or surveillance operator, but also the responsibility of every soldier on the ground. These changes must be implemented as a matter of urgency. Time is of the essence and it is running out.
Asymmetric Strategies as Strategies of the Strong

© 2011 Michael Breen and Joshua A. Geltzer
This article is reprinted with the kind permission of Parameters, the quarterly journal of the US Army War College.

Michael Breen is Vice President of the Truman National Security Project, a former Army combat arms officer, a member of Yale Law School’s Class of 2011 and a graduate of Dartmouth College.

Joshua A. Geltzer, also a member of Yale Law School’s Class of 2011, received his Ph.D. in War Studies from King’s College London, where he studied on a Marshall Scholarship. Geltzer is the editor-in-chief of the Yale Law Journal.

One needs merely to wade into the shallow waters of today’s deepest debates over American foreign policy to stub one’s toe against the notion of asymmetric strategies. Like the very strategies that it describes, the concept often seems frustratingly amorphous yet disturbingly omnipresent—and, most importantly, distinctly threatening to the United States.¹

This article takes the notion of asymmetric strategy seriously but re-conceptualizes it in a crucial way. The article questions the persistent identification of asymmetric strategies as strategies of the weak, instead revealing the many ways in which asymmetric strategies are becoming strategies of the increasingly strong. Consequently, the article also rejects the notion that asymmetric strategies can be deployed only against the United States, and aims to stimulate thinking about ways in which asymmetric strategies might be adopted for use by the United States. In the end, the article concludes that the American foreign policy community should cease thinking of asymmetric strategies as the exclusive province of weak non-state actors and, instead, should conceive of such strategies as even more important when intelligently wielded by strong state actors—including America itself.

The first part of the article isolates a definition of asymmetric strategy that, unlike many definitions proposed previously, defines such strategies independently of the actors that execute them: asymmetric strategies transform an adversary’s perceived strength into a vulnerability, often by revealing one’s own perceived vulnerability as a strength. The article’s second part employs that definition to reveal the ways in which asymmetric strategies are already being adopted by America’s adversaries, including states. The final portion of the article calls for new thinking about ways in which the United States might employ asymmetric strategies against its various adversaries.

The Concept of Asymmetric Strategies

Defining Asymmetric Strategies

Asymmetric strategy has been a crucial concept in the decade following 9/11, yet it remains devilishly difficult to define.² Numerous attempts to define the concept are so broad that they approach the definition of strategy itself, severely limiting any practical utility.³ For example, one foundational article on asymmetric strategy claims that “strategic asymmetry is the use of some sort of difference to gain an advantage over an adversary.”⁴ If this formulation is correct, it is unclear how asymmetric strategies differ from other strategies: “Emphasizing one’s strengths and exploiting an enemy’s weakness is what strategy is all about.”⁵

Other commonly used definitions are narrower, but conflate large differences in the relative strength of the parties to a conflict and the strategies that those parties employ. In other words, these definitions seem to suggest that asymmetric strategy is almost anything that a weak actor might do when faced with a much stronger opponent, especially if that action is somehow surprising or creative: “Asymmetric warfare is violent action undertaken by the ‘have-nots’ against the ‘haves’ whereby the have-nots, be they state or sub-state actors, seek to generate profound effects . . . by employing their own specific
Relative advantages against the vulnerabilities of much stronger opponents. Granted, the phenomenon being described here is of central concern to America in its status as the world’s lone superpower. The problem is that virtually any entity that the United States may fight, state or non-state, will be less powerful than America. If asymmetric strategy is simply what weaker actors do against stronger ones, then from America’s perspective asymmetric strategies are just good strategies against the United States: “Any military plan that avoids meeting the United States in a head-on, force-on-force, ‘fair’ battlefield fight is also considered to be ‘asymmetric.’”

We acknowledge that previous definitions of asymmetric strategy have been useful in describing the post-Cold War world of weaker but unruly adversaries confronting the United States. That said, we believe that strategists, soldiers, and scholars alike would benefit from a more precise definition—one that identifies asymmetric strategy as a conceptual category unto itself, independent of the weakness or strength of the actor wielding it.

Asymmetric strategies are roughly akin to the Japanese martial art of jujutsu, which is based on the idea that an opponent’s strength and energy may be used against him rather than directly opposed with strength of one’s own. When facing a taller or stronger opponent, for example, a jujutsu practitioner is encouraged to view the opponent’s advantages in height and muscle mass as exploitable weaknesses, as they tend to produce a high centre of gravity. Similarly, jujutsu practitioners use the very force that an opponent is able to put behind a punch in order to throw him to the ground, rather than blocking the blow and attempting to respond in kind.

Such an approach offers several advantages in hand-to-hand combat - regardless of the relative strength of the two opponents. This approach helps seize the initiative, as one’s opponent has the unsettling experience of having his own intentioned action and inherent power used against him. The strength of the jujutsu practitioner is greatly conserved, as it is largely the energy of the opponent that produces his downfall rather than any external force. Most importantly, jujutsu is fiendishly difficult to counter: how do you fight back against an opponent who consistently turns your own strength against you?

When properly defined and understood, asymmetric strategy is quite similar. In light of this understanding, we offer a definition of the concept: asymmetric strategies transform an adversary’s perceived strength into a vulnerability, often by revealing one’s own perceived vulnerability as a strength. Asymmetric strategy is an inherently relational art form – one that often exploits an opponent’s mistaken perceptions about both the asymmetric actor and himself. More importantly, it is available to any strategic actor, weak or strong. Sufficient skill and cunning are the only attributes that asymmetric strategy demands.

Asymmetric Strategies, More than Weapons of the Weak

Asymmetric strategies are typically conceptualized as weapons of the weak. Rod Thornton, for example, defines “the asymmetric adversary” as “the smaller, weaker protagonist.” Thornton’s voice is not alone in this regard: While asymmetric strategies have received attention since at least 1995, interest in the concept has quite clearly surged since the attacks of 11 September 2001 and focused American attention on adversaries whose limited capabilities make them appear weak, at least in a traditional sense.

It is not the inherent weakness of non-state adversaries that qualifies them as asymmetric actors. Consider Thornton’s description of the “three major characteristics of the ‘new’ terrorists that need to be considered: their increased degree of fervour, their increased ability to implement attacks, and their increased ability to cause mass casualties.” Not one of these is inherently an attribute of the weak. At any given moment in the Cold War, much of what America feared about its very strong adversary, the Soviet Union, was its increased fervour, its improved capacity to attack, and its enhanced ability to cause mass destruction.

Another set of authors exploring asymmetric strategies identifies what really seems novel about “global terrorist groups” and the threat that they pose to the United States: it is the fact that “America’s global economy, relatively porous borders, open source intelligence and information, and inadequate law enforcement resources allow access to a range of goods, services, and information that together can be developed into formidable weapons.” It is, in other words, not any characteristic of al Qaeda itself that made its attack on 9/11 a paradigmatic use of an asymmetric strategy. Rather, it is the inescapably relational manner in which the group transformed attributes of the United States normally viewed as strengths - for example, the country’s interconnected economy, open borders, and free flow of information - into devastating vulnerabilities. Al Qaeda accomplished this by making clever use of aspects of its own identity that the United States viewed as vulnerabilities, such as its small numbers, crude weapons, and limited training.

A weak non-state actor may have greater incentive to adopt such strategies in order to overcome a lack of options, but there is no reason that a strong state actor could not do the same. In the influential book Unrestricted Warfare, two Chinese People’s Liberation Army colonels argue that strategies currently identified with terrorist groups can and should be adapted for use by states such as China: “the new and old terrorists who consistently uphold the principle of resorting to every conceivable means are still the best teachers of each nation’s government.” Indeed, as the next part of this article will demonstrate, increasingly strong states are already using asymmetric strategies typically associated with non-state...
actors. Hence, the current tendency to identify asymmetric strategies with weak, non-state actors emerges from mere historical happenstance and conceptual confusion, rather than from anything inherent in the concept itself.15

While commentators focus on asymmetric strategies as the province of the weak, increasingly strong actors have begun deploying and employing these strategies, often to impressive effect. The next section examines how strong states such as China and Russia, or robust non-state entities such as Hezbollah, have attempted to transform their adversary’s perceived strengths into vulnerabilities by drawing on latent strengths of their own.

What “They” Are Doing to Us

Despite the prevailing focus on the asymmetric threats that non-state actors pose to the United States and its allies, increasingly strong states are also developing and employing strategies that seek to exploit apparent American strengths as latent vulnerabilities. This should not come as a surprise. Motivated perhaps by Thucydides’ explanatory triad of “fear, honour and interest,” rising powers such as China, Russia, and Iran feel the need to develop the capability to neutralize or at least mitigate American power.16 Given the position of economic and military dominance that America currently enjoys, states which may seek to coerce or deter the United States have an incentive to be creative. The rapid destruction of Iraq’s Soviet-inspired conventional military twice in little more than a decade conveys a clear lesson to would-be state challengers: “Don’t fight the United States unless you have nuclear weapons.”17

Even as they build more conventional capabilities, therefore, some states have chosen to develop strategies designed to exploit apparent American strengths as actual vulnerabilities. As is often the case, point of view is essential. For example, the networked, software-based wizardry that permits the United States to coordinate with astounding precision various air campaigns undertaken around the world from geographically remote command centres is undoubtedly a major American strength. In the eyes of an asymmetric adversary, however, the same capability may be viewed as a dangerous dependency that leaves America’s lavishly expensive military vulnerable to comparatively cheap cyberattacks. The relative strength of America’s adversary in such a formulation is immaterial—the strategy is asymmetric regardless of whether it is employed by a small group of hackers, a weak regional challenger, or a mighty global adversary.

It is no surprise, then, that a diverse array of states has begun pursuing asymmetric strategies against the United States. As they do so, a kind of parallel evolution is occurring. Over the past two decades, several increasingly strong actors have developed broadly similar asymmetric strategies. We outline several below to illustrate the central claim - that asymmetric strategies, properly understood, are already being employed by increasingly strong actors, including states, and not just by weak non-state actors.

Hybrid Warfare

Insurgency is perhaps the iconic asymmetric strategy and has proven highly effective at inverting the strengths of even the world’s most powerful militaries. States have long used insurgency by proxy as a means to harass an adversary; such tactics were common during the Cold War and currently are employed in a number of locations. As a strategy to be utilized directly by a state in a military confrontation with another, insurgency is typically far less attractive. An emerging but still quite nascent cocktail of tactics, techniques, and technologies is combining some of insurgency’s key asymmetric advantages with more conventional approaches to holding and controlling territory. Often referred to as “hybrid warfare,” this evolving approach to ground combat may soon present states with a viable asymmetric option against the United States.18

Insurgency undoubtedly presents a serious asymmetric challenge to even strong conventional military powers such as the United States. The strategy is asymmetric, according to our definition, in that it seeks to transform military advantages in mass and firepower into disadvantages by exhausting the foe in a protracted campaign while goading or misleading him into misdirecting force against the civilian population. Conventional military forces tend to orient on seizing and holding key terrain, and to focus their destructive energies on the dispatch of the opposing military force; meanwhile, insurgents orient on the population and their conventional opponents, routinely yield key terrain, and tend to focus their efforts on symbolic acts of violence that shift the balance of political power in their favour. In most formulations, the insurgency then capitalizes on favourable shifts in the political balance to alter the balance of military power to its advantage. If it is unable to accomplish such a shift, the insurgency simply continues to survive while draining its opponent’s will to fight, until the bloodied and dispirited conventional military withdraws from the conflict.19

For a non-state actor waging a campaign against a government, foreign or domestic, insurgency has proven an effective tool over the last hundred years. As an asymmetric strategy to be used by one state against another, however, it has serious limits. While insurgency is often a politically offensive strategy in that it frequently seeks to replace an existing government with another, it is largely defensive in geographic terms.20 Mao Zedong, the doctrinal father of modern insurgency, famously conceived of insurgents as fish swimming in the sea of a friendly population. Clearly, this approach requires the insurgent to have a claim to membership in the population in which he swims, or at least a powerful claim on that population’s loyalty.21

Even as a defensive strategy, insurgency is a matter of last resort for governments because it requires a government to allow a hostile force to invade and occupy its territory before the insurgency can even begin. Mao described his plans for insurgency against the onrushing Japanese army in just such terms: “The invader’s strategy must be one of lightning war. If
Hybrid warfare promises to partially rectify that flaw while retaining many of insurgency’s asymmetric advantages. In theory, hybrid warfare combines insurgency’s highly decentralized cell-based communications and leadership structures, light logistical footprint, and synergy with the civilian population with tactics intended to hold terrain and destroy, rather than just harass, the opposing force. Like insurgency, hybrid warfare is often based on a light infantry model that largely eschews big, conspicuous weapons platforms such as tanks and large-calibre artillery. Instead, hybrid forces employ man-portable anti-tank missiles, rockets, and mortars. The proliferation of accurate and inexpensive precision-guided munitions continues to make such weapons increasingly potent against conventional armoured formations, to the point that a decentralized but well-equipped infantry force capable of fading into the civilian population is also increasingly capable of standing its ground when attacked. Such a force presents few of the defensive weaknesses that tend to characterize conventional forces. For example, while the American military would typically target and destroy a conventional enemy’s communications and logistical infrastructure prior to beginning an attack, such infrastructure is difficult to identify and indistinguishable from civilian systems if the opponent is a decentralized hybrid force relying on close ties within the civilian population.

While hybrid warfare remains an emerging threat, some defence analysts believe that Israel’s experience against Hezbollah in Southern Lebanon in 2006 may reveal the shape of things to come. The conflict is of special note because the Israeli Defence Forces (IDF), largely equipped with American military technology and using American-style tactics, struggled to overcome the forces of an irregular adversary in Israel’s campaign to seize and hold ground. Hezbollah is itself something of a hybrid in that it is a non-state actor with roots as a terrorist and insurgent organization that also controls territory and fulfils many traditional state functions. During its 24-year history leading up to the 2006 confrontation with the IDF, Hezbollah appears to have developed an equally hybrid approach to fighting its highly trained, lavishly equipped conventional adversary. On the one hand, Hezbollah continues to emphasize a decentralized and autonomous insurgent-style cell-based organizational structure with virtually no logistical “tail” and frequently makes use of hit-and-run insurgent tactics designed for political provocation rather than military affect. At the same time, however, Hezbollah forces defended southern Lebanon in 2006 using an intricate series of prepared and concealed bunker positions designed and provisioned to sustain a lengthy defense, and employed a range of sophisticated guided weapon systems against Israeli targets on land and even at sea. Unlike traditional insurgents, Hezbollah fighters in 2006 consistently strove to hold ground against a determined attack by Israeli armoured formations, sometimes with success.

During Israel’s 33-day ground incursion, Hezbollah’s hybrid of conventional and unconventional warfare allowed it to inflict more Israeli casualties per Arab fighter than did any of Israel’s conventional opponents in the 1956, 1967, 1973, or 1982 Arab-Israeli wars. Given the similarities between the Israeli and American ways of war, this did not go unnoticed by potential adversaries of the United States. Iran, in particular, may have used the 2006 conflict as a test for strategies designed to defend against possible American invasion, and directly supplied much of Hezbollah’s arsenal. As one observer put it, “Hezbollah trains Iran, not the other way around.” Russia originally developed and manufactured the vast majority of Hezbollah’s high-end weapon systems, and Russian military planners no doubt paid close attention to their employment and effectiveness. China, meanwhile, is developing its own strategy for denying the western Pacific to American forces, in part by making extensive use of guided missiles deployed in a decentralized manner - an approach that it refers to as “Assassin’s Mace.” American observers have been quick to recognize the threat posed by such tactics.

Hybrid warfare potentially allows states to enjoy some of insurgency’s advantages while avoiding important costs,
especially the surrender of key terrain. Such a strategy presents an asymmetric advantage in that it allows an adversary to transform an opponent’s advantage in expensive, high-tech weapons platforms into a vulnerability, while at the same time converting apparent weaknesses in arms and numbers into strengths. In the aftermath of America’s entrance into Afghanistan and then Iraq, states seeking to defend their borders against possible American invasion, such as Iran and North Korea, have looked to nuclear weapons as their primary defensive option. In the near future, however, hybrid warfare may allow such adversaries to mount a more credible conventional defence against the American way of war.

Cyber Warfare

In recent years, cyber warfare has emerged as a serious challenge to the world’s most technologically sophisticated nations, including the United States. The decentralized and byzantine structure of the internet itself intensifies this threat, in that it is increasingly possible for state and non-state actors alike to develop and employ cyber warfare capabilities anonymously or through potentially oblivious proxies, making deterrence a difficult proposition. Given the potential to level the playing field by disrupting or disabling a more technologically advanced adversary’s capabilities and perhaps even to do so with plausible deniability, it is small wonder that states large and small have increasingly devoted resources to developing a capacity for cyber warfare.

The list of nations actively pursuing cyber warfare capabilities is extensive and includes a number of America’s potential challengers. China has developed official military doctrine for cyber warfare, trained large numbers of military officers to conduct offensive operations on the internet, and conducted an extensive series of exercises and simulations.33 Russia has developed a robust cyber warfare capability, partially in consultation with China.34 Russia also has demonstrated an enthusiasm for offensive cyber warfare over the past decade, conducting cyber attacks against Chechen sites as early as 2002.35 Using criminal gangs as proxies, Russia used cyber attacks to cripple Georgian networks prior to Russia’s conventional military attack in 2008, having seen the utility of such tactics in an earlier confrontation with Estonia.36 In both of these instances, it was the stronger actor, Russia, that adopted an asymmetric strategy. Iran, India, Pakistan, and North Korea are also known to be developing cyber warfare capabilities of varying sophistication and effectiveness, sometimes in coordination with criminal organizations.37

As several observers have noted, cyberspace is best understood not as an unprecedented forum for entirely new tactics but instead as a new venue where conflict will occur in forms roughly analogous to those seen on land, at sea, in the air, and in orbital space.38 In this new and evolving venue, just as in more traditional ones, we will see any number of strategies develop that mix and match direct and indirect approaches, as well as outright coercion and deception. Many cyber warfare strategies appear intrinsically asymmetric, in that the more highly developed and powerful a nation’s computerized infrastructure becomes, the more vulnerable the target nation is to the consequences of a successful cyber attack. However, recall that exploiting misperception is a central feature of an asymmetric strategy. As cyber warfare becomes a common feature of the global strategic environment, states that rely upon sophisticated computer networks will be all too aware of their vulnerability. In the near future, one can anticipate that computer networks will be viewed in the same light as aircraft carriers are today - powerful but vulnerable technological tools that must be zealously protected against attack.

As in other venues of human conflict, some small subset of cyberspace strategies will be truly asymmetric. It is probably too early in the history of cyber warfare to make definitive statements about which strategies will be employed, how they will evolve, and what asymmetric warfare in cyberspace will look like. We can, however, draw some very broad but useful distinctions.

Imagine an adversary that has developed a sizeable cyber warfare capability, employing large numbers of military and intelligence personnel and computers, and utilizes this capability to launch a large-scale denial of service attack on US military computer networks. Assume that the cyber attack is intended to cripple our command-and-control capabilities during an air and naval campaign that spans vast distances, allowing the adversary’s otherwise outmatched forces to mount a more credible defence. Although the attack would invert an American strength and render it a weakness in the broader sense, the means of attack is the rough cyberspace equivalent of an armoured thrust penetrating an enemy line on land - concentrated power applied against a carefully chosen weak point. Such an attack may achieve surprise and shock effect, but it is not asymmetric.

Contrast this type of attack with another hypothetical attack on American networks, conducted in order to achieve similar objectives. In this case, however, imagine the attack is carried out using a network of civilian, government, and military computers from around the world. In most cases the owners are probably unaware that the attack is even taking place - imagine this clandestine network is created and controlled by a group of individuals deniably employed by the attacking state. In this scenario, four or five people could strike a serious blow against the most powerful military in the world. Their perceived weaknesses are many; they are unarmed, they are few in number, and they have relatively few resources. Yet, those perceived weaknesses provide the attacker with the anonymity and deniability required to survive and execute their attacks. The effectiveness of this cyber attack emerges from its capacity to transform an apparent American strength – the technologically advanced, elaborately synchronized American military - into a weakness.
The potential for an attack along these lines is illustrated by the saga of the now-infamous Conficker worm.39 Like other worms, Conficker is designed to embed itself in a host computer without revealing its presence, making small changes necessary to defend itself and avoid detection, and then spreading to other systems. It also maintains regular communication with its unknown creator over the internet, and is capable of responding to instructions. The worm first appeared on November 20, 2008, and since then has successfully survived an unprecedented attempt to destroy it by a globally coordinated network of security experts. Today, the worm controls a botnet—or network of infected computers - likely consisting of millions of computers worldwide, mostly operated by entirely unsuspecting users. Such a botnet provides the worm and its controller with tremendous computing power, which could potentially be used to conduct debilitating attacks on even the largest and most secure networks in the world. For any organization, including a state, a stable botnet like the one that Conficker controls represents a powerful on-call offensive capability.

Conficker’s design and subsequent adaptations indicate that it was designed by a team of individuals possessing truly world-class expertise in a number of disciplines, including cryptography and software design. According to cyber security experts who have studied the worm, Conficker’s creators are “either incredibly sophisticated cyber criminals or a group that was funded by a nation-state.”40 Conficker’s creators remain anonymous, and it is not known whether the worm is controlled by a state. It may be significant, however, that the original version of Conficker was designed to avoid infecting any computer with a Ukrainian IP address.41

The combination of offensive potential and deniability offered by a capability like Conficker’s anonymously controlled botnet is simply too attractive for a state actor to ignore. Such capabilities represent some of the most dangerous and significant emerging threats to the United States and its allies, and are by no means exclusively weapons of the weak. Especially in combination with hybrid warfare and other asymmetric strategies discussed here, cyber warfare may offer America’s future adversaries a potentially transformational advantage. In the hands of a strong state actor with access to large amounts of intellectual capital and technical expertise, asymmetric cyber warfare could prove devastating.

Media Manipulation

Americans often view their country’s robust media as a strategic asset, and even adversaries have come to see the American media as strategically beneficial to the United States. During the Cold War, for example, the Soviet Union took great pains to restrict its citizens’ access to Western media, while the United States attempted to defeat Soviet censorship. The reverse, however, was not the case - Soviet media was utterly ineffective at influencing American audiences, and the United States made no serious attempt to censor it. Broadly similar dynamics persist today between the United States and several of its rivals, with the censorship of American media ranging from the extreme in the case of North Korea to more subtle measures in the case of China.

Some adversaries, however, have recognized that the American media may also be an American weakness under certain conditions. American media outlets pervade the globe, beaming an American viewpoint into households around the world; however, that same global scope and ambition on the part of US-based news outlets permit a foreign perspective on American foreign policy to reach American audiences. More importantly, American media coverage provides the American people with an often limited but highly visceral view of the immediate day-by-day impact of US policies, many of which require a long-term popular commitment to succeed.

This effect is particularly problematic for American leaders when the United States is engaged in armed conflict with a weaker opponent, a situation that America’s superpower status makes extremely likely. The problem is that a pronounced imbalance in strength produces serious moral and ethical issues for the stronger belligerent, whose strength, self-confidence, and will to fight are continuously eroded. Martin Van Creveld memorably compares this “paradox of strength” dynamic to a grown man confronting a small child who is attacking him with a knife - virtually anything that the adult might do, will appear to be either weakness or atrocity to an observer.42 When the American people observe their own military in such situations, they tend to react negatively.

Often, this dynamic is less a strategy employed by America’s adversaries than a simple fact of life. For example, reactions to graphic media coverage of devastating coalition air strikes
against retreating Iraqi troops in 1991 significantly contributed to a cease-fire that permitted much of Iraq’s Republican Guard to escape. As beneficial as this outcome was for the Iraqi regime, there is no evidence to suggest that the Iraqi leadership intended it to happen or even was aware that it was occurring. Similarly, China’s tight-lipped and centralized formulation of foreign policy enjoys certain advantages over Washington’s culture of frequent leaks, even without China actively doing anything to exploit this aspect of American policy-making.

Other actors, however, have been more deliberate in their attempts at shaping the coverage they receive in the United States. North Vietnam’s use of American celebrities as spokespeople to highlight alleged American atrocities is an infamous example, but more recent strategies have been both more subtle and more effective. Modern Iraqi insurgents have at times displayed a highly sophisticated understanding of the global media, arranging attacks to coincide with media coverage of the target area and even timing major strikes to take advantage of the American prime-time television schedule. Many of America’s military adversaries, including both the former government of Iraq and Iraqi insurgents, have shown an uncanny ability to direct television cameras to incidents involving civilian casualties. Iran, meanwhile, seems to have paid close attention to American media coverage and public opinion in its approach to its nuclear program, alternating between a conciliatory and defiant stance in order to avoid inducing a severe American reaction or making legitimate concessions. On the whole, what may once have been a rather unintended undermining of the United States through its media coverage seems increasingly to have become a deliberate strategic choice of American adversaries—and, in particular, an asymmetric choice that transforms a pillar of a free society into a shaky element of foreign policy formulation.

For a foreign state, manipulating American popular opinion related to foreign policy by influencing the media is certainly easier said than done. When the strategy does succeed, however, the results can be highly favourable to an adversary. For example, it was televised images of American casualties that led to an American withdrawal from Somalia in the early 1990s, not a military victory by Mogadishu’s warlords. Attempts to manipulate media coverage represent a potentially powerful asymmetric strategy, inverting the power of America’s influential media to affect Americans themselves.

What We Might Consider Doing to “Them”

The United States should prepare to respond to asymmetric strategies employed against it by a range of foes, from localized insurgencies to would-be regional hegemons. America should also consider doing something less reactive and more innovative: America needs to craft unique asymmetric strategies of its own. By and large, this has not been our approach to date. ”[T]he United States has virtually assured potential adversaries that it will respond to their actions only in particular, well-defined, reactionary, and very controlled ways.”44 In some ways, this is a consequence of America’s position as the primary guarantor of global stability. Yet the United States can move beyond its “symmetric” habit of mirroring and then outmatching opponents’ capabilities without compromising its global role.

Asymmetric strategies offer America a number of advantages. Asymmetric strategies tend to be economical, since they can side-step the need to match an opponent’s key capabilities with expensive capabilities of one’s own. Asymmetry often produces significant strategic surprise, at least temporarily permitting the user to seize and exploit the initiative as the opponent struggles to re-evaluate the situation. More fundamentally, an opponent’s discovery that his strength is also in some sense a debilitating weakness can lead to considerable confusion.

The uncertainty that asymmetric strategies tend to produce make them deeply unsettling to their targets, leading to confusion about the relative strengths of adversaries, the viability of existing defences, the utility of existing response options, and even the validity of the foundation of one’s own power. This power to unsettle and confuse a target may explain asymmetric strategies’ frequent association with terrorism, as the effects just described are precisely those terrorists seek when they launch their attacks. As we have seen, there is nothing about the motivations or relative weaknesses of terrorists that make them the exclusive or even most effective users of asymmetric strategy.

Just as a muscular and skilled fighter may employ jujutsu techniques to devastate a physically weaker foe, strong states may employ asymmetric strategies to achieve dramatic results against weaker opponents. Perhaps this is roughly what Thornton has in mind when he argues that “[t]here is much to be said for the idea that the powerful must become more like the weak in order to match their capabilities.”45 What we are proposing here is not that the United States emulate the particular ways in which the weak make use of asymmetric strategies. Instead, we propose that America develop unique asymmetric strategies of its own. These strategies will emerge from the unique capabilities of America itself, in relation to its adversaries. Crucially, they should be consistent with America’s moral character and position of global leadership.

As it confronts a global landscape increasingly populated with challengers weak and strong, the United States would do well to consider the advantages of the asymmetric approach. We do not suggest, of course, that there is an asymmetric solution to every strategic problem, nor that a given strategy is good or wise simply because it is asymmetric. The ongoing global embrace of asymmetry by state and non-state actors alike should give American strategists some indication of the potential benefits of such thinking. American power is indeed vast, but it is not infinite. As it seeks to husband its own power while confronting an array of increasingly muscular challengers, the United States would do well to turn its rivals’ strengths against them.
29


NOTES


2. It is important to distinguish between asymmetric conflicts, which are interactions whose asymmetry is a simple fact resulting from some sort of disparity between the clashing parties, and asymmetric strategies, which are deliberate attempts to shape interactions. The latter constitute the focus of this article.


4. Montgomery C. Meigs, "Unorthodox Thoughts about Asymmetric Warfare." Parameters 33, no. 2 (Summer 2003): 4-18; Steven Metz and Douglas Kiras, and Kolet, "Understanding 'Asymmetric,'" U.S. Military Strategy: The Definition, Background, and Strategic Concepts (Carlisle, PA: Strategic Studies Institute, 2001). Metz and Johnson, 1. Compare this similar, if more convoluted, definition, in Meigs, 4: "Asymmetry means the absence of a common basis of comparison in respect to a quality, or in operational terms, a capability."


8. Thomson, Asymmetric Warfare, 55. Thomson comes closest to this formulation, though - as already discussed - he offers other variations as well: "The turning of strengths into vulnerabilities is obviously what the asymmetric warrior is looking for."

9. Ibid., 3.


11. Thomson, Asymmetric Warfare, 27.


13. Thomson, Asymmetric Warfare, 4-5. Thomson notes that "it is useful to point out that asymmetric techniques can also be applied by the stronger power," and then underscores "the importance of the asymmetric threat today—from both state and sub-state actors." But see also page 76: "Asymmetric warfare operates from the weak state's perspective, not the strong state's. Why is the 'real threat' not from the strong state asymmetric adversary?"


15. In practice, of course, relative strength does sometimes correlate with targets of asymmetric strategies, as actors weak along traditional dimensions must look for creative ways to approach stronger adversaries if they are to have any chance at all of prevailing. But, in addition to there being no necessary relationship between the objective weakness of an actor and its decision to employ an asymmetric strategy, there is nothing inherent about relative weakness in the concept of asymmetry: instead, asymmetry is about revealing an adversary's strength as a weakness by drawing on one's own apparent weakness as a strength, even if one is, overall, the stronger party.


(accessed June 16, 2011). The term “hybrid war” is also occasionally used to describe conflicts involving both intra-state and inter-state warfare, rather than a fusion of conventional and irregular methods employed by a single belligerent.


20. Offensive state-sponsored insurgency by proxy, such as North Vietnam's campaign against the South using the Viet Cong, is another matter. It is worth noting as well that South Vietnam was ultimately defeated by a conventional military invasion, not by insurgent activity.

21. Kilcullen, The Accidental Guerilla. Che Guevara's expeditionary insurgent campaigns in Latin America, and al-Qaeda's strategy of embedding itself with local and regional insurgencies such as the Taliban, may present exceptions to this rule. However, both Che and al-Qaeda relied heavily on local interlocutors and overwhelmingly used local manpower in their campaigns.


23. Frank G. Hoffman, Conflict in the 21st Century, 8, 29. Hoffman defines hybrid warfare as a combination of conventional and irregular methods used by the same forces in the same battlespace, allowing for a much broader array of possible force structures and methods within his definition. While the most direct application of the concept is a decentralized, light infantry based model, other examples exist.


25. Ibid., 5. Tellingly, the 2006 war began when Hezbollah ambushed an Israeli patrol and kidnapped two IDF soldiers; Stephen Biddle and Jeffrey A. Friedman, The 2006 Lebanon Campaign and the Future of Warfare: Implications for Army and Defense Policy (Carlisle, PA: Strategic Studies Institute, 2008), 29.


27. Biddle and Friedman, The 2006 Lebanon Campaign, 35-36. This article provides an extremely useful "taxonomy" of Hezbollah's military behavior during the 2006 conflict.

28. Ibid., xv.

29. Andrew Exum, Hizballah at War, 7

30. Ibid., 6.

31. Andrew Krepeinovich, Barry Watts, and Robert Work, Meeting the Anti-Access and Area-Denial Challenges (Washington DC: Center for Strategic and Budgetary Assessments, 2003). "Assassin's Mace" itself is essentially a cocktail of mutually supporting asymmetric strategies, including undersea mining, cyber attacks and anti-satellite strikes as well as guided missile attacks.


34. Ibid., 107-119.

35. Project Grey Goose, "Project Grey Goose: Project Grey Goose-Phase-I-Report (accessed June 16, 2011). The term "hybrid war" is also occasionally used to describe conflicts involving both intra-state and inter-state warfare, rather than a fusion of conventional and irregular methods employed by a single belligerent.


37. Biddle and Chang, Cyber Warfare, 4-7


40. Ibid., 82.

41. Ibid., 77.


44. Barnett, Asymmetrical Warfare, 154.

45. Thornton, Asymmetrical Warfare, 148.
Cultural Intelligence as an Enabler

Major A.J. de Vos

Introduction

Cultural diversity is inherent within the South African landscape and South Africa holds this at the core of its existence with the expectation that respect for other cultures will form the fibre of South African society. Cultural diversity is so significant that respect for the various South African cultures has been codified in the South African Constitution (20:1). The South African National Defence Force (SANDF) also incorporated cultural tolerance in its Code of Conduct which states ‘I will treat all people fairly and respect their rights and dignity at all times, regardless of race ethnicity, gender, culture, language or sexual orientation” (21:1).” It therefore follows that the SA Army would be adept at cultural intelligence given the salience of cultural diversity within the society from which they originate. Unfortunately, cultural diversity does not necessarily equate with cultural intelligence.

A simple definition of cultural intelligence incorporates the awareness of, and the ability to interpret and bridge cultural differences and be effective across various cultural contexts. The application of cultural intelligence in modern warfare is not a new phenomenon but has been used with significant and sometimes surprising success within conventional and asymmetric warfare since the Persian Wars in the 5th Century BC. Cultural intelligence in the form of anthropological knowledge and the military have been linked for more than 100 years in the colonial power such as France, where anthropological studies contributed to the expansion and consolidation of the colonial powers during the empire age (2:65, 15:47).

In contemporary society, peace support operations have become the most widely employed means for managing conflict and contributing to its resolution and have also evolved to incorporate a plethora of tasks, necessitating the coordination of effort by multicultural forces and civilian agencies (6:142). Increasingly today’s operations also take place amongst civilians, with civilians having a significant impact within the operational theatre. Distinctions among role players and civilian communities have become blurred with no easily identifiable adversary against which to prepare forces in peacekeeping operations. Given the integral role that civilian communities play, the understanding of the host nation’s culture and the quality of the relations pursued will have a determining impact upon the attainment of the overall mission (9:567). Cultural intelligence therefore is essential for interaction between the components of a mission as well as interaction with affected communities outside of the mission. The South African Army has been committed to peacekeeping operations for over a decade with the current most notable contributions being to the
conflicts in the Democratic Republic of Congo and the Republic of Sudan (16:10).

The aim of the paper is to highlight the importance of cultural intelligence in peace support operations and will therefore commence by defining what cultural intelligence is before investigating what impacts cultural intelligence can have on peace support missions. The South African Army’s contribution and mission-ready training for the peacekeeping mission in Sudan will be utilized as a case study so that recommendations can be made for enhancing the SA Army’s sensitivity to cultural cues within the mission area and, thereby contribute to their efficacy in the peacekeeping mission.

**Cultural Intelligence as a Construct**

Culture is a complex concept embedded in many aspects of human life. Earley and Ang (7:63) liken culture to the “software of the mind”, being the set of programming unique to a community within a nation. Culture manifests itself in human behaviour, with differences serving to distinguish between particular cultural groups. Culture is acquired and transmitted through generations of society and, according to Matsumoto and Juang (14:10), can be defined as, “a dynamic system of rules, explicit and implicit, established by groups to ensure their survival, involving attitudes, values, beliefs, norms and behaviours, shared by a group but harboured differently by each specific unit within the group, communicated across generations, relatively stable, but with the potential to change across time.”

Culture is therefore a learned phenomenon that serves to shape the formation of one’s dispositions, perceptions and interpretations of events, and which determines motivations and appropriate and inappropriate behaviours. It provides guidelines for social and moral conduct which can be observed in unique behaviours, mannerisms, language and artefacts (26:9).

Language is a component of culture and the principle means by which we communicate with each other. Language and mannerisms have however been culturally adapted to suit the status and relationship between the participants and the context of the situation with differences in language reflecting cultural differences and serving to reinforce culture. It follows that because language and culture are intimately entwined; intercultural communication differs significantly from intracultural communication (14:264). Aside from the verbal language, non-verbal language also forms an important channel of communication which can convey or enhance meaning or contradict the verbal message being given. These non verbal cues hamper the receiver’s decoding of the message and could result in the message being interpreted differently from the manner in which it was meant to be conveyed (14:279). Uncertainty and ambiguity are inherent characteristics of decoding intercultural communication which in turn, makes conflict and misunderstandings inevitable.

Race does not equate to culture; people of the same race may be very different in their cultural dispositions, behaviours, attitudes and feelings (14:16). Just because one is born with certain biological or physical characteristics that conform to a particular race, does not mean that you conform to all the cultures embraced by that race. Culture is a learned behaviour, race is not. African descent does not imply cultural similarity across the African spectrum. Even with similar influences, such as colonialism, cultural differences do exist and should be recognised.

Van Den Bergh (26:18) identifies three strategies for overcoming cultural differences; the convergence theory (where one expects others to adapt to and emulate one’s own, dominant culture), the understanding of cultural differences (where a list of cultural differences and similarities is provided) or becoming culturally intelligent (the reshaping of one’s thinking and adjusting of behaviour to be more skilled and appropriate). The first two have inherent flaws which could hamper intercultural relations with the development of cultural intelligence being the favoured approach, being more holistic and integrative towards cultural differences.

Cultural intelligence is the ability to recognise, understand and adapt to new cultural contexts (7: 59, 22:40). Individuals in new cultural contexts need to create a new mental framework for understanding what is experienced and witnessed so as to generate appropriate responses for their current cultural environment. It consists of three components which combine to create intercultural competence – knowledge to understand cross-cultural phenomena, awareness to observe and interpret situations, and the adaption of behaviour to act appropriately. All three components need to be present for one to be characterised as being culturally intelligent (26:29; 7:62). Therefore, in the contemporary military context, the ability to effectively integrate cultural intelligence in modern military planning and operations, is a critical success factor (22:40).

The nature of social structures are shaped by culture as they grow and adapt and, therefore, many social interactions, including conflict resolution, can be aided through knowledge of cultural norms and practices (7:63). Insurgency forms of warfare, organisational structure and motivations are determined by and reflect the indigenous social organisation of the geographical region from where they originate and, therefore, timely cultural and social knowledge will assist in assessing, understanding and predicting enemy behaviour and structures (15: 43-46).

In counter-insurgency operations and peace-support operations, people remain the focus, with winning of the hearts and minds of the people central to operational success. However, before hearts and minds can be won, measures need to be initiated to understand and really know the communities in the operational theatre (2:67; 13:18, 12:9). Cammaert (5:27) stressed that, in successful peacekeeping operations, an understanding of cross-cultural issues is essential, not just of the local communities, but also of one’s allies. The cultural terrain should therefore be
viewed and developed similarly to the appreciation of military terrain in operational planning. This would greatly enhance the application of the Observe-Orient-Decide-Act (OODA) cycle, providing culturally aware commanders with control over the OODA cycle(19:1). Commanders would be able to move directly from Observe to Action as the Orientation and Decision components would already be pre-programmed due to cultural awareness. Cultural information should therefore be inextricably linked to the intelligence process (3:57-59) to allow for accurate analysis, interpretation, prediction and advice.

Cultural diversity in peace support operations

Because culture is dynamic, incorporating temporal and spatial variations, the cultural context and understanding of the mission activities change over the lifespan of the mission and are subjected to local nuances, introducing further differentiation within the mission area. Perceptions differ at the beginning and the end of a mission, assumptions differ between urban and hinterland areas – there is no single cultural experience during a mission’s lifespan, it is dynamic and can present with a kaleidoscope of experiences. A failure to recognise this, and conduct regular revision of cultural intelligence, will result in closed perceptions which can lead to the development of stereotypes (18:531).

The Impact of Cultural Intelligence on Peace Support Operations

Peacekeeping is a complex construct, involving a variety of tasks to be executed by peacekeeping forces. Cultural understanding can make positive contributions to these tasks and functions and make a difference at the strategic, operational and tactical levels. A misunderstanding of cultures at a strategic level could result in the introduction of mandates or policies which exacerbate insurgencies, at the operational level misunderstandings could manifest in negative public opinion and on the tactical level could result in endangering both soldiers and civilian communities alike (15:43-44).

Conflict Resolution and Protection of Civilians. A relationship of trust and interaction with local communities will ensure early warning for pro-active responses. “Cultural awareness will not necessarily always enable us to predict what the enemy and non-combatants will do, but it will help us to better understand what motivates them, what is important to the host nation in which we serve, and how we can either elicit the support of the population or at least diminish their support and aid to the enemy.” Until forces achieve a better understanding of local customs and politics, have a basic language ability and a greater comprehension of communities’ interests, the belligerent groups will retain their freedom of movement and the upper hand in...
the battle space (13:18). Knowledge of the population should therefore be considered as ‘key terrain’. Local issues could be resolved with prior knowledge of historical perspectives, emotive locations, key locations for economic reasons and tribal perspectives (5:26). Ethnoconflict theory could assist in this regard. This theory takes local assumptions and practices into consideration and prescribes the rules for conflict regulation within a particular society and can therefore serve to inform outsiders to the community as to the most appropriate strategies for intervention (6:145).

Peacekeepers will have to persuade belligerent groups to desist with conflict. Such persuasion necessitates cultural and situational awareness. Powers of persuasion are acquired through a high level of trust which has to be earned through actions and altered reality perceptions (22:44). Belligerent groups will not be persuaded to a course of action if the persuader does not understand the relevant language, motivations, fears and desires. The utilisation of an ethno-anthropological overview is an effective tool to develop comprehensive and accurate situational awareness (2:66).

Post Conflict Reconstruction. For post conflict reconstruction to be effective and sustainable, the institutions which are rebuilt need to reflect local interests and not impose outsider concepts upon local communities (15:45). A thorough and in-depth understanding of local communities’ requirements and incorporation of local participants in post conflict reconstruction planning is essential. This can only be attained through successful intercultural interaction and the development of trust relationships which are derived from cultural sensitivity.

Benefits of Cultural Intelligence

Cultural intelligence provides a number of benefits which enhance operational efficacy. These have been identified as follows:

- The incoming commander and unit will immediately possess the institutional memory of the people and area of operations (12:9). Armed with this knowledge, commanders will be able to identify and take advantage of opponents’ weaknesses and strengths and be able to ascertain the strengths and weaknesses of the local forces they may be required to train (2:68). In warfare, this thorough knowledge of the enemy and own forces’ capabilities endows battle confidence in that commanders need not fear the outcome of battle (15:42).
- Increased language capabilities extend effectiveness and task accomplishment (27:18) as relationships can be forged with local communities. Interaction with civilian communities promotes the development of Human Intelligence sources who provide crucial information for operational planning eg personalities, motives and intent (5:13, 13:23). The complete intelligence picture can be formulated to ensure that the right forces are deployed at the right time and place with the right equipment which in turn will ensure force protection and enhance the capability of the force to achieve its mandate (5:14)
- Understanding who the local authority is and who exerts control will assist in establishing and enforcing lines of communication with local political, religious and military leaders. An understanding of local moral values and codes of conduct will assist soldiers to negotiate with political, tribal and administrative authorities (2:68-69). These lines of communication will create familiarity with the meanings behind local symbols, avoiding Western interpretations and potential misperceptions and inappropriate responses (15:44)
- Interaction and knowledge of local cultural practices serve as force multipliers, enabling a small force to impose a stable and secure environment over a large area through interacting with and training local residents (2:68). The ‘culturally intelligent’ forces will be more effective in exercising control in their area of responsibility than other contingents without intercultural interaction, will reduce the necessity for the use of force, and will be better able to minimise unrest among people (13:23, 5:21, 3:64)
- Regular and committed interaction will serve to positively influence the communities to support mission objectives and to minimise the negative impact of military operations on civilian communities as well as diminish civilian interference in operations (3:61). This will enable more proactive initiatives and introduce a speedier reactive time with more effective responses (13:19)

The South African Army’s Force Contribution to United Nations African Union Mission in Darfur (UNAMID)

Sudan is a geographically vast country, incorporating great ethnic, religious and linguistic diversity. Loyalty in the country is divided amongst family, clan, ethnic group and religion, which gives rise to differences and tensions along ethnic, religious and linguistic lines. One of the contributing factors to the division and conflict in Darfur is between ethnic groups, split between herders and farmers (28:1). Distinctions of descent are also claimed with the Sudanese in the north claiming Arab descent whilst those in the south claim African descent. Groups may share a common language, cultural characteristics and common ancestry but still lay claim to a distinction between groups. Distinctions may then not be based on traditional criteria but something subtly and uniquely identified by the respective groups.

Sudan’s ethnic and linguistic diversity has been recognised as one of the most complex in the world. The last survey to provide detailed ethnic information, conducted in 1956, indicated 19 ethnic groups and 597 subgroups. A number of the smaller groups have, however, subsequently been assimilated into larger groups. Persons of Arab origin constitute the greatest proportion of the population but do not represent an overall majority in the demographic profile. Arabic is therefore the predominant language, recognised as the country’s official language, in conjunction with English in some locations (8:15).
Ethnic groups in Darfur originate from tribes of either African or Arab lineage. There are 36 main tribes and 185 sub-groups of African lineage and 32 main tribes and 119 subgroups of Arab lineage (25:1). Each of these tribes and sub-groups has differentiating subtleties which would have an impact on intercultural interaction.

A further conflict determinant is religion. Islam is the official state religion with more than half of the population being practicing Muslims. Other religions present in the country include Christianity and animist African religious practices (28:1).

UNAMID is a United Nations–African Union hybrid mission in the Darfur region and is one of the largest contemporary peacekeeping operations. As of 30 June 2012, it had a total of 22 445 uniformed personnel, 1 097 international civilian personnel, 2 919 local civilian staff and 471 UN Volunteers. Just under fifty countries contribute troops to make up the total uniformed complement, with the major troop contributing countries (TCC) being of African origin, as per Sudanese government stipulation (24:1). South Africa, as the 9th largest TCC, contributes 806 troops, 57 police and 12 experts (23:5). The South African Army contributes troops to this mission as part of the SANDF’s commitment to UNAMID, with the majority of SANDF forces forthcoming from the SA Army rank and file. From the above, given the plethora of different cultures present in the mission staff, as well as inherent to the host nation, it is apparent that cultural intelligence would be a crucial element in contributing to optimal efficiency and efficacy within the mission area to alleviate miscommunication and conflict from arising.

Forces deploying to Sudan have identified several shortcomings in the SANDF’s programme for mission readiness training, particularly when it pertains to knowledge of the human terrain. During mobilisation forces receive an introductory lecture on the causes of the conflict and the demographics of the country and a brief introduction to Islamic culture (1:199). These issues are addressed during a three hour slot allotted to Defence Intelligence to provide a country brief that includes background, current security development, geographical aspects and humanitarian developments. Due to programme and time constraints, only superficial aspects are highlighted (10:1). During the simulated exercise in mobilisation, lasting five days and consisting of computer-generated scenarios, some cultural and religious scenarios are gamed. Unfortunately a few scenarios do not suffice to constitute the full complement of cultural awareness, and neither are the appropriate responses formulated by cultural experts (11:1). Cultural awareness and sensitivity receive greater attention during Military Observer training. This training is, however, provided to far smaller groups, and the larger contingents could benefit, at least in the interim until an expert is identified and an institutional memory base established, from the same form of training.

Shortfalls in the mobilisation, in terms of cultural aspects, have been determined, and the issue could enjoy a more in-depth focus, to familiarise deploying elements with cultural and religious disparities unique to their host nation. Mobilisation staff (11:1) indicated that DOD Language Services have registered a project to ascertain how they could contribute to addressing some of the shortfall, but currently the SANDF does not have a country/ethnic/religious expert to brief and assist during mobilisation. A key identified deficit is the fact that the conflict in Darfur is simultaneously politically, ethnically and religiously based, and how deploying forces are expected to interact with the various groups in the country.

Given the insufficient attention given to cultural aspects, some serious cultural blunders have been made whilst deployed to Sudan. These include the usage of the wathu (places of spiritual cleansing) as urinals at the airport when no toilets where identified according to South African paradigms. The issue of dress codes also posed a cultural disparity; South African off duty dress consists of T-shirts and shorts but, in the Sudanese culture, this is perceived as disrespectful and is unacceptable behaviour. Race also played a role in some persons’ experiences – a white peacekeeper found that he could interact more easily with the different factions because he was African but was not a black African. Given the distinction between Sudanese Arab and Sudanese African groups and the subsequent tension between the two, Black African troops’ loyalty is instinctively placed with the Sudanese of African origin (1:200). Neither black African soldiers nor soldiers of Arab origin would automatically be perceived as neutral and their actions would have to indicate their neutrality to the respective parties in order to invite interaction.

**How Cultural Intelligence can be Developed within the SA Army**

In order to determine how substantial the cultural intelligence gap is, it is suggested that a cultural intelligence assessment be conducted of force elements earmarked for deployment prior to their departure for a mission area. This could then be correlated with a test conducted on post-deployment forces to ascertain how the deployment enhanced cultural awareness. An example
of such an assessment tool is provided in Appendix B (4:1) and can be utilised to develop a scale of cultural intelligence and to sub-divide the scale according to the rank structures. Once this assessment is completed, an overall score of Cultural Intelligence can be extrapolated to the SA Army, and one will need to introduce training to bridge the gap. TCC’s need to address the gap in cultural awareness and develop the capacity for their forces to use the cultural terrain to their advantage and utilise all operational opportunities provided. TCC’s should provide their deploying forces with information and guidance on how to approach populations local to host countries, to avoid committing of cultural faux pas and introducing breaches to intercultural communication (9:568). It should, however, be noted that not all ranks will experience the same frequency or level of intercultural interaction during deployment and preparation should be sensitive to the differences. The best manner of ensuring cultural awareness at all levels is to introduce cultural terrain considerations over the full spectrum of training and operations (3:58).

Cultural intelligence training will need to include training in all three components of cultural intelligence; knowledge, mindfulness/motivation and behaviour, and will, therefore, need to include cognitive, motivational and behavioural components. These are indicated in Table 1 below:

<table>
<thead>
<tr>
<th>Component</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Knowledge</td>
<td>Knowledge of the fundamental principles of a culture, flexibility and the ability to adapt one’s own view to complement a new situation. Strategic thinking about application of cultural knowledge</td>
</tr>
<tr>
<td>Meta Cognition</td>
<td></td>
</tr>
<tr>
<td>Cultural Strategic Thinking</td>
<td></td>
</tr>
<tr>
<td>Mindfulness</td>
<td>Observation and interpretation of certain situations, Energy and willingness to persevere despite the possibility of failure. Self-efficacy and self confidence.</td>
</tr>
<tr>
<td>Motivation</td>
<td></td>
</tr>
<tr>
<td>Behaviour</td>
<td>The ability to understand and execute the necessary actions(such as language, greetings and social conduct) with a reasonable level of proficiency.</td>
</tr>
</tbody>
</table>

Table 1: Components of Cultural Intelligence (26:31)

Countries such as France and the United States of America have created cultural training centres to develop operational culture capacity, which will allow the military to navigate in complex human terrains of deployment (2:65-67; 3:58). These countries can be used to benchmark programmes and development.

Mission experience remains the best source of learning how to deal with cultural differences. None of the contemporary South African Army deployments are new deployments and, as such, a body of knowledge exists within the forces that has returned from the mission areas. This knowledge needs to be tapped, consolidated and regularly updated, so that it can be utilised to prepare an anthropological study of the various communities with which the South African contingent comes into contact. This extraction of knowledge should take place during an After Action Review/Debrief that reviews the preceding rotation and identifies mistakes to improve the organisation and operational capabilities of the forces (2:71). The knowledge accumulated can be used for briefing subsequent rotations, and in developing future training doctrine to inculcate cultural intelligence throughout all levels of the SA Army. One can utilise the expertise available from those who have operated in the country before to give additional briefs based on their experiences. Instructors should have been to the country several times and be conversant in advising deploying elements how to interact with street vendors, local imams, what greetings to use, how to quickly identify dominant families in areas, how to bargain and how to follow the rules of hospitality. Integral to this, is that the forces be exposed to a basic introduction of the predominant language in the area of deployment, enabling them to deliver and understand key concepts in communication.

The Joint Operations Division should ensure that a good Human Intelligence orientation and training programme is incorporated in the pre-deployment phase so that the entire military component can be Human Intelligence information gatherers (5:21), thereby enhancing the information and intelligence capability of deploying forces. Pre-deployment exercises should also focus on cultural terrain perspectives to develop awareness (3:58).

An exchange of information during handover is a crucial and instrumental tool to advise incoming rotations on situational awareness, how to cope with the local tactical situation and provide important information about local society (2:70). An in-theatre cultural intelligence repository should be created, maintained and revised to serve as part of the “living” country brief. However, it should be cautioned that, despite the training and information which are provided, it is impossible to know a country, its people and its culture intimately, as there are elements that books cannot provide. It is, therefore, imperative that one should have a basic knowledge of other cultures, be aware of one’s perceptions of self and others, and be sensitive towards the perceptions that others may have of them (9:569). The SANDF will need to develop a reach-back connectivity to subject-matter experts in South Africa who can draw on government and academic sources to assist in analysis and interpretation and augment the utilisation by the commander (12:9, 3:59). This reach-back connectivity could be the curators of the institutional memory data base derived from after action reviews, debriefs, patrol reports, mission visits and research. A specific, standardised tool should be developed to understand local deployment conditions. The data collected by troop patrols should be collated and captured in a medium that all soldiers would be able to monitor and understand, with a possible solution in this regard being a geographic information system which can layer cultural data over physical geographical data.
Summary

Even to a culturally diverse nation such as South Africa, participation in peacekeeping confronts South African soldiers with unfamiliar practices and norms. An incomplete understanding of cultural differences could result in misperceptions and cultural tension. The nature of current conflict and the complexity of contemporary peacekeeping operations introduce a variety of cultural variables into peacekeeping and necessitate that participants are sensitive to cultural differences and adapt and adjust to develop cultural intelligence.

Peace-support operations are a global phenomenon, and success or failure in this sphere will resound in both the national and international media corridors, respectively promoting or ridiculing the relevant troop contributing country. Cultural intelligence can only enhance, not replace, traditional military skills, as the latter remain fundamental to peace-support operations. South Africa has been successfully engaged in peacekeeping activities for more than a decade, but gaps in preparation can be identified, and it is suggested that it is time to review the attention that cultural intelligence receives during training, pre-deployment, mobilisation and deployment phases. This will ensure that the SA Army remains culturally relevant in a dynamic environment.

Conclusions

If the current trend of executing military operations near or among civilian populations continues, success will be enhanced by a well-developed cultural intelligence capability that is integrated into training, planning, preparation, information collection, information analysis and operations. Defence forces will need to expand their focus on conventional military skills and operations to incorporate the development of cultural intelligence and human interaction skills, aimed to simultaneously undermine support for belligerent forces and act as a force multiplier for own forces.

The South African Army appears to fail to recognise the importance of cultural intelligence in the contemporary battle space. A possible reason for this could be attributed to our belief that we share the same ethos of African-ness with the community wherein we are deployed to serve. As already mentioned, race and common heritage does not equate to culture, and these differences could be costly to South Africans in terms of mission success and ultimately in terms of South African lives. Inadequate training and preparation leads to misperceptions.

Cultural intelligence serves as both an enabler and a force multiplier within the spectrum of the operations being undertaken. South African forces need to recognise the demands of the current battle-space and adapt accordingly. Cultural empowerment, as a key component of peace-support, will enable peacekeeping forces to win the hearts and minds of the people through peaceful means, as opposed to using the threat of firepower to enforce their will upon communities – the epitome of peacekeeping behaviour.

NOTES

10. Interview with a SANDF Lieutenant Colonel deployed in Sudan and currently responsible for presenting Sudan country brief at mobilisation.
11. Interview with a SANDF Lieutenant Colonel currently responsible for the mobilisation of SANDF forces for peace support operations.
The Twenty Item Four Factor Cultural Intelligence Scale

Mingle and help. That not only serves the purpose of a peace support mission, but builds mutual understanding and creates the basis for developing cultural intelligence.
The South African Army has over the past few years played a major role in Africa’s peace support operations. The Army has a responsibility to ensure that its participation in these operations result in sustainable, community-based, long-lasting peace, with minimum civilian and military casualties. The ability to know one’s enemy, his intentions and the terrain, more often than not, determines the success or failure of a mission.

The failure of the US intelligence community and armed forces to know, respect and appreciate the Middle Eastern Muslim community’s culture, religion and social settings led to a mission with disastrous consequences in Iraq and Afghanistan. A mission that would last for over ten years with no clear achievable objectives and rejection by the local population and ultimately global disapproval.

Introduction

The introduction of democracy and the destruction of Apartheid in South Africa meant a lot of different things to different sectors of society and industry. Immediately after the elections South Africa was confronted with a few continental security challenges, among others the genocide in Rwanda and the civil war in Somalia. Politically, as a continental super power and a new democracy with the necessary economic and military muscles it was seen as South Africa’s responsibility to intervene and stop the carnage.

As for the military, democracy meant a completely new role, a role that was to be largely defined by peaceful and humanitarian operations, instead of destructive counter insurgency and internal dissent repression operations. However, given the history of the nature of operations carried out by the then South African Defence Force (SADF) and particularly the army, it became clear that the new South African National Defence Force (SANDF) was not fully equipped and ready for the new role that would become its defining character and primary external role.

SADF members were highly effective and experienced in the fields of counter insurgency, and bush war, with troops whose skills and training was geared towards the containment of internal problems by force. The former Homelands came with their own armies with limited combat experience. The liberation movements such as the African National Congress (ANC) which came with its military wing, UmKhonto we Sizwe (MK) and the Pan African Congress (PAC) which also brought its own military wing, Azanian People Liberation Army (APLA), were mostly equipped with skills and knowledge of guerrilla and revolutionary asymmetric warfare.
This meant that the new SANDF was to become a huge and diverse force but with little or no experience in what was to become its future role. Peace Operations in a culturally rich and sensitive Africa.

The focus of this paper will be Peacekeeping Intelligence (PKI), with specific reference to the cultural dynamics of society. Why is it necessary to have a scientific study of cultural intelligence? The paper will show that cultural intelligence although usually ignored is a very important part of military strategy and tactics, and in modern military operations the knowledge of the ‘human terrain’ is more likely to determine the outcome of an operation and its long term effects.

The paper will, through the use of practical examples and known missions, attempt to prove that there exists a desperate need for soldiers to know and understand the socio-economic environment in which they operate; know the political, economic and cultural environments; and have a clear and comprehensive understanding of all social and non-military factors affecting the particular society.

It is in this context that the paper will argue in favour of cultural intelligence and provide facts to prove that the South African Army needs to invest more time and resources on cultural intelligence so as to build a lasting and community based peace. The objective of the paper, which is to prove the importance of cultural intelligence, will be achieved through the provision of a detailed summary of the history behind peace operations; this will be done so as to create a context and provide a theoretical framework from which the reader can understand the underlying logic behind the paper.

This will then be followed by introducing the reader to the art of intelligence and its cultural dimension. The last section of the paper will focus on the SANDF, and particularly the Army’s role in line with UN objectives in peace operations. Do we need cultural intelligence, if yes why do we need it and how is knowing the ‘human terrain’ going to be a help or detriment to us prior, during and post operations.

**Evolution of Peace Operations**

Over the past decades the term ‘peace operations’ has been used to mean and explain a lot of related activities, the nature of these activities evolving with time. During the cold-war era and before, peace operations were confined to monitoring cease-fire agreements already agreed upon by the contending parties, a typical example being the first deployment of United Nations (UN) observers to monitor the peace agreement between Israel and her neighbours in the late 1940s (Williams, 1995).

The evolution of peace operations meant that in keeping with its mandate of protecting civilians and ensuring global peace, security and stability, the UN had to look into the possibility of deploying lightly armed infantry combat troops into troubled and unstable regions, this development and the number of conflicts increasing at an exponential rate in Africa and elsewhere, paved a way for the emergence of new and advanced second generation peace operations in response to more complex international security challenges.

**Peacekeeping**

Peacekeeping is the second step after peace-making. This is the most common of peace operations; it involves the use of minimum military force to maintain the already existing agreements between opposing forces. Peacekeeping operations are normally characterised by clear rules of engagement, and these operations in their nature are not an end but rather a means to an end. Such operations are used to create a viable environment for a political and diplomatic solution to be found and implemented. The current deployment of South African troops to the Democratic Republic of Congo (DRC) and the Sudan, and previously also to Burundi are examples of peacekeeping operations (Williams 1995).

**Peace-Enforcement**

Peace-enforcement operations, on the other hand, involve the use of military force not to maintain an already existing agreement, but to end the conflict itself. This is achieved through military engagements with the contending parties. Given the nature of the UN as an international organisation with no independent war-making capabilities, these operations are normally carried by sovereign states unilaterally or in cooperation with another state (Williams, 1995).

The attack and ultimate overthrow of Colonel Gadafi’s Libyan regime by the US and her allies is one such example. For any one of the above mentioned operations to succeed, it is important for both the foot soldiers and the commanders to...
know what type of a peace operation are they involved in.

**South Africa in Africa’s Peace Operations**

Before 1994, South Africa actively deployed military force against its neighbours seen to be in support of the ANC and any other organisation standing against apartheid. The most notorious and successful being the deployment of 32 Battalion against the Popular Movement for the Liberation of Angola (MPLA) forces, and other liberation armies in Angola, and Namibia (the then South-West Africa).

In the eyes of many African leaders and people, South Africa represented a threat and a major challenge to the independence of Africa, the defeat of colonialism, and the defeat of what was seen as western influence and imperialism and the achievement of human rights, especially given its military might, economic muscles and support by the United States (US).

Upon assuming power in 1994, the new government saw it as a moral obligation to distance itself and prove to be different from the past government on issues of regional and continental social responsibilities. This meant the pursuit and promotion of human rights, support for neighbouring troubled countries and the promotion of peace and democracy.

South Africa occupied a high position on moral grounds in the international human rights platform due to having achieved a negotiated democratic order, and the implementation of programmes such as the Truth and Reconciliation Commission (TRC); it was, therefore, inevitable that at some point South Africa would be drawn into Africa’s conflict resolution, either as mediator or peace-maker. South Africa had the necessary economic and military resources required, and it was to a larger extent expected to “pay for the crimes” of the previous government (Southall, 2006).

**Intelligence**

Intelligence can mean a lot of things to different people; however, within a military context intelligence has its own special meaning. One of the world’s greatest war strategists of all times, Carl von Clausewitz (As cited in Christopher, Richard & Wesley. 2009) defines intelligence as “every sort of information about the enemy and his country, in short the basis of all our own plans and operations”. This definition however has its own loopholes as it describes intelligence as merely information about the enemy. The question still remains, what is intelligence and how does it differ from information.

Information can be anything, daily newspaper reports from the Daily Sun, Sowetan or Pretoria News can be considered information, News reports from SABC Television can be considered information, but would it be wise to classify this information as intelligence? That would mean journalists, and news reporters are intelligence officers which is obviously not correct.

Intelligence and information cannot be equated. It is true that intelligence involves information. But it is more than just information; it is a question of who collects the information; who or what is the source of such information; the manner in which it is collected and processed; who needs and uses such information; and for what purpose.

Taking all the necessary factors into consideration, intelligence can be defined as that which is dependent on confidential sources and methods for full effectiveness, performed by trained officers of the state for state purposes and consumption, with a specific focus on foreign subjects. In a nutshell intelligence is secret, state activity to understand or influence foreign entities (Christopher, Richard & Wesley 2009).

**Cultural Intelligence**

Generally, cultural intelligence can be defined as an analysis of social, political, economic, and demographic information that can provide an understanding of a society (Coles, 2005). Cultural Intelligence is again defined as the ability to recognise the shared beliefs, values, attitudes and behaviours of a group of people and to apply this knowledge towards a specific goal (Spencer, 2008). Within an African context however, cultural intelligence should be broader and seek to respond to the broad and diverse challenges facing Africa. Cultural intelligence cannot be of any use to the military unless it is timely, specific and, most importantly, reliable.

**The Need for Cultural Intelligence**

The ability to know one’s enemy and his intentions, more often than not, determines the success or failure of a mission. The
failure of the US intelligence community to know, respect and appreciate the middle eastern Muslim community’s culture, religion and social settings led to disastrous and lasting consequences in Iraq and Afghanistan during and after the ‘war on terror’, a war that would last for over ten years with no clear achievable objectives and rejection by the local population and ultimately global disapproval (Heinecken & Winslow, 2010).

The above mentioned event provides more than enough evidence to prove that there exists a serious and desperate need for the South African Army to have prior knowledge of what to expect before deploying troops on peace keeping missions. Cultural intelligence provides a foundation for the development and maintenance of successful military missions. Within a military context, cultural intelligence should be seen and understood as more than just demographic statistics. Unlike other areas of intelligence, cultural intelligence provides an understanding of how and why individuals and groups act in a particular way.

Conventionally, wars are known to be fought between nations over territory, economic reasons, political expansionism and lately regime change. Today however, things are different, the nature of modern warfare has transformed to an extent that only a few wars are fought between nations. Today’s wars are being fought within nations, and there exists a never ending new supply of civil wars motivated by ethnic, racial, cultural, religious and political differences among people of the same nation (Adebajo 2011).

Africa is home to a considerable number of known tribal, religious, ethnic and post-colonial political conflicts in the world. The ethnic cleansing in Rwanda, religious and racially motivated conflicts in the Sudan and Somalia, the civil wars fuelled by political rivalry in the DRC, the Hutu rebellion in Burundi and recently the Christian and Muslim rivalry in Nigeria, and many more, all in a period of less than 15 years (Adebajo 2011). Each and every one of the above mentioned conflicts might have arisen for one or more reasons, but the fact of the matter is that cultural differences played an enormous role.

Ethnic divisions and hatred, cultural superiority, religious and tribal animosity all created favourable conditions for violent confrontations (Carmel 1999). All of these and other divisive factors make it impossible for the South African Army to engage in successful peace missions and conflict resolution programs without a clear and comprehensive understanding of these regions, their cultures, traditions and customs.

The SA Army and the Need for Cultural intelligence in Peace and Stabilization Operations.

In March of 2003, the US and her North Atlantic Treaty Organisation (NATO) allies officially declared war on Iraq. The operation had the following as its primary objectives;

- Identify and defeat the entire al-Qaeda high command, with Osama Bin Laden and Abu Musab al-Zarqawi as high priority;
- Defeat Sadam Hussein and enforce a regime change;
- Identify and destroy all al-Qaeda training camps;
- Bring peace, stability and democracy to Iraq;

Most of the above mentioned objectives were achieved to a certain extent, particularly the first three. Largely due to the fact that the achievement of these objectives required military force. With the US and her allies being in command of superior forces and weapons, victory on their part was inevitable. Conventional military operations were quickly won (Coles, 2005).

What about the last objective? It is a well-known fact that up to this day, almost 10 years since the war began, there is still no peace in Iraq, democracy is still a dream that might never materialise; one cannot even begin to talk about stability. Lack of understanding of the local population and their culture was the primary cause of this failure of a mega proportions.

The success or failure of a peace operation is largely dependent on the relationship between peace keepers and the local population. This relationship can be influenced by a lot of factors such as individual and troop collective attitudes, personalities and, most importantly, culturally, ethnically, and racially motivated behaviour (De Brito, 1997).

Cultural intelligence must form part of the initial plan prior to the deployment of troops to troubled regions in Africa. The SA Army needs to know what the leaders and their opponents will think before they do, know their capabilities and limitations, know who makes decisions and what is it about their country and society that makes them different from the rest (Coles, 2005). General Anthony Zinni, former commander of operations in mission Restore Hope, stressed the importance of cultural intelligence (as cited in Coles, 2005) “It is important for the Army to know why they are at war and what is their desired outcome, their languages, their way of life, the needs and aspirations of the local population so as to win their minds and hearts, how far they are willing to go to achieve their stated objectives and all other social and non- military factors”.

Knowing your enemy as a commander and a soldier has always been the first principle of warfare. Although peace operations cannot be equated to warfare, the fact remains that peace operations are still military operations in need of military strategy and tactics whose success or failure depends on one’s knowledge of foreign cultures. Peace operations in Africa require a hands-on and practical management of post conflict cultural differences (Heinecken & Winslow, 2010).

Lack of cultural knowledge at strategic level in countries such as Burundi and Sudan, where religious, race and cultural intolerance are at the core of the conflict, can lead to the development of policies that can fuel an insurgency and derail the peace process. Many conflicts in Africa come as a result of failure to understand and tolerate different cultural groups (Donais 2012).
In the year 2000, a survey was conducted among senior and junior army officers in the SANDF on deployment in conflicts ridden areas in Africa. Almost all respondents stated that “We sometimes or always experience difficulties when interacting with civilian population, local authorities, local fighting factions and the media” (Heinecken & Winslow, 2010).

This is due to lack of cultural understanding of the human terrain of operation. Mission failures and unnecessary loss of lives make cultural intelligence an important element of strategy and not just another “expendable” casualty in the planning process. History and very recent events in Iraq, Afghanistan, Somalia, Bosnia, Sudan and many more have proven that a lasting and genuine peace can only be achieved if the peace makers and peacekeepers have a clear understanding of the conflict, its origin and its support structures.

**Major Challenges**

The SA Army does not have a comprehensive pre-deployment cultural education training program. Soldiers are given introductory lessons on the history behind the conflict, and a few lessons on basic terms for basic communication purposes. Most of the soldiers deployed on these missions lack the capacity to understand the complex ethnic, religious, economic and political dynamics behind these conflicts (Williams, 1995). Peace operations and armies in their own nature draw great interest from the international community and media. The idea of human rights and respect for diversity and foreign culture is very well respected internationally. It is, therefore, of critical importance that foot-soldiers on the ground be intellectually equipped with the ability to deal with issues that might arise in a manner that will not compromise mission success (Coles, 2011). Soldiers on the ground are the real focus point of international media and human rights organisations, not the strategic decision-makers who are not in the field. One wrong movement might turn international opinion against soldiers and ultimately ruin the entire operation.

Naturally, peacekeepers should be seen as objective and impartial, non-partisan and taking no sides. This is important for the success of a peace operation and drawing in the local community to be part of a home grown solution.

Impartiality and non-partisanship, real or perceived, cannot be possible unless soldiers deployed are familiar with the local cultural environment from all sides. Soldiers on the ground must be able to communicate with all the affected parties in their own languages, must have a thorough understanding and appreciation of local customs, and lastly must be familiar with the local political dynamics and social aspects of a society.

The last and important challenge is discipline. Armed soldiers in peace operations find themselves in a special and tempting position. During peace operations soldiers deal directly with the most vulnerable elements of society in times of conflicts; women and children (Williams 1995). The rape and abuse of women and young girls is a very prevalent practice during many peace operations.

Lack of discipline among soldiers with regard to how they treat the local population and conduct themselves has the potential of discrediting the credibility of an organisation, brings embarrassment to the entire force and country, and can tear the entire operation apart. The alleged poor behaviour of some South African troops on deployment, especially off-duty troops in Burundi and the DRC has been a great embarrassment for South Africa, resulting in giving the force a bad name and reputation (Mandrup 2008). Cultural intelligence should ultimately lead to the provision of specialised pre-deployment training programs that will assist in dealing with issues of ill-discipline.

**Lessons Learned from Peacekeeping in Africa**

In 1994 almost half a million civilian men, women, and children were killed in Rwanda. This tragedy occurred in spite of the presence of a UN Peacekeeping force. The performance of the UN force in Rwanda is still questionable to this day. Was the UN fully aware of the cultural complexity of this conflict? Was the force level right? Were the correct and appropriate units deployed? Were the soldiers aware of the cultural dynamics of Rwanda? (Malan, 1997).

[Image: Rwanda: Mass killings as in Rwanda and Bosnia are difficult for most people to comprehend, but are a vital illustration of just how far perceived cultural differences can drive people.]

It is important and necessary to study, analyse and understand the background to the conflict, social, cultural, political and economic dynamics of the society in question. A comprehensive analysis of these factors will provide an early warning system and assist the SA Army in determining the right time to intervene, the right units to deploy, and type of training to provide to both the commanders and the troops (Anyidoho, 1997).
DOCTRINE, STRATEGY AND OPERATIONS

Recommendations

The SA Army must develop a cultural intelligence collection and analysis capability which will not only provide the necessary pre-deployment information about the human terrain, but will also provide guidance and serve as a point of departure towards the design and provision of pre-deployment training programs. As an army we need to be able to recognise and appreciate the limits of our means and capabilities. The development of advanced cultural intelligence and situation awareness programs will enable the Army to have a reliable and accurate early warning system that will guide the Army’s actions prior and during troop deployments.

The SA Army’s contribution to peace operations should be based on rational and practical solutions that seek to address and resolve conflicts from their root causes. This can only happen if soldiers and their respective commanders are fully conversant with all socio-economic, cultural and non-military factors affecting both belligerent parties and the affected communities.

Unlike most world armies, the SA Army has an advantage due to diversity and continental cultural experience accumulated by many MK and APLA combatants during their years in exile. The Army needs to exploit such skills and knowledge to its advantage. Such members could be used to provide training and cultural awareness programs to new and young members to be deployed.

Conclusion

Somalia, Rwanda, and recently Iraq and Afghanistan, all present examples of what could be considered operational failure. In Somalia, peacekeeping forces were killed and their bodies dragged in front of international television eyes; in Rwanda masses of civilians were killed while the entire international community sat and did nothing, peacekeeping troops were deployed while it was already too late. In Iraq and Afghanistan military operations were quickly won by the coalition forces due to their superior air and fire power, but to this day there exists no peace or internal stability to talk about.

All the above mentioned operations have one or more factors in common. However it is important to note that they all failed to take into consideration the human terrain as part of the equation in their strategic calculations. Soldiers are faced with loyal and patriotic citizens in their host countries during peacekeeping missions; this calls for maximum participation and interaction between soldiers on deployment and the local population.

The reality is that, the SA Army will continue leading peace operations in Africa for many years to come. This calls for huge commitment and investment in the Army’s cultural and general intelligence capabilities. That will enable the army to engage belligerent parties from an informed, impartial and non-partisan position, ultimately creating a viable environment for a community-based and long-term peace.

NOTES

A Proposed Service Delivery Philosophy for Army Support

Col Dries van Jaarsveld
Officer in Charge Service Assurance Management at Joint Support Base Garrison

The reason for the existence of any Army Support Base (ASB) is that the support and services rendered must ensure that client units are enabled to perform their core functions and mandate. A philosophy for service delivery should provide guiding principles, which informs and determines strategy, plans and all decisions for the services offered and the way in which the services are provided (Santa Clara University, 2011: 2).

The essence of service delivery is that there is a service provider (ASB), client units and suppliers/contractors. The client has logistical related requirements, which is placed on the service provider (ASB), which obtains it from a supplier (being civilian organisations or military depots) and provide it to the client unit. Service delivery is backed by certain fundamentals i.e; structure through which services can be delivered; systems of service delivery (including processes); regulatory framework in which services must be delivered; attitude and performance of service delivery personnel and knowledge of the products and processes. The nature of service delivery is illustrated in Figure 1.

Regulatory Framework

Batho Pele as the South African service delivery philosophy and is based on eight principles (Kuye, 2007: 88). These principles are also captured in the White Paper on Service Delivery (RSA, 1997:5):

- Consultation: Users and consumers of public services should be consulted about the level and quality of the services they receive and, wherever possible, to be given a choice about the services that are offered
- Service standards: Users and consumers of public services should be told what level and quality of service they will receive so that they are aware of what to expect.
- Redress: All citizens should be offered an apology and solution when standards are not met and a speedy and effective remedy, and that any complaint will produce a sympathetic, positive response
- Courtesy: Users and consumers of public services should be treated with courtesy and consideration
- Information: Users and consumers of public services should expect full, accurate information about the services they are entitled to receive
- Openness and transparency: The public should expect to be told how national departments and provincial administrations are run, how much they cost, and who is in charge
- Access: All citizens have the right to equal access to the services to which they are entitled.
- Value for money: The public should expect that public services will be provided as economically and efficiently as possible

Understanding the Clients

Support Bases must have highly trained and attentive staffs that make it their business to know the clients’ business. As part of commitment to the clients units, the ASB must demonstrate personal attention to service. The ASB must understand the client business to be able to solve client needs, constantly monitor business processes and performance measurements, and ensure that clients receive the highest level of customer satisfaction possible. The business of an Infantry Battalion is vastly different to that of any support unit and the ASB must therefore know the core business of all the respective clients (Woloshuk 2010, 2).

Client care is non-negotiable and solving their problems, by providing expertise to streamline support and services and improve ongoing performance. The real bottom-line cost savings opportunities in every area of logistics and service provision must be identified by support bases and considered in their service delivery planning. This will enable the ASB to deliver cost savings and extreme administrative ease for clients and own organisation (ICC, 2008: 1).
The service provider will have to take into consideration the expected client outcomes in order to ensure expectations can either be met or negotiated to the satisfaction of both parties (UK, 2004:21).

**Service Description**

Determine and define standards for the level and quality of services provided. Service standards must be relevant and meaningful to all clients. Standards must also be precise and measurable, so that clients can judge for themselves whether or not they are receiving what was promised, eg by stipulating the length taken to authorise expenses, issue equipment and what services will in future be provided, etc.

Service standards should be captured in the service agreement (or memoranda of understanding) between the parties. However, publishing standards is not enough; performance against standards must be regularly measured and the results must be submitted to higher headquarters for scrutiny and assessment. It is also essential in order to track improvements in services from year (UK, 2009:6) to year, and to inform decisions about the levels to which standards should be raised in future.

Specific Service characteristics must include a description of the core values underlying the actual services that are offered to clients. (Woloshuk 2010: 2) Here the values of the SA Army should guide service providers. Where clients have little or no choice about the services they receive, information is one of the most powerful tools - sometimes the only tool - that they have to exercise their right to good service. This places an obligation on the service provider to provide in-time information regarding the progress of any service transaction at any given time.

Openness and transparency are fundamental to the public service delivery process. In terms of service delivery, the importance lies in the need to build confidence and trust between the ASBs and the clients they serve. Responsiveness is a core value of public service delivery. The key to implementing the responsiveness principle lies in being able to identify quickly and accurately when services are falling below the promised standard and having procedures and quality control measures in place to remedy the situation.

**Manage and Align Own Capabilities**

Like all successful organisations, the strength of the ASB should lie with its people. The ASB must be led by skilled and recognised leaders and experts in the field of logistics and service delivery. An ASB team should consist of skilled and experienced analysts, auditors, administrators, and commodity managers all focusing on the same, unifying goal: solving client needs, delivering high standard of service, and achieving bottom-line cost savings (ICC, 2008:1).

The ASB must constantly achieve increasing levels of excellence; for the clients and internally, so that bottom-line difference can be made for the long-term future. That’s why there must be a continuous re-investment in human resources and technological infrastructure. Staff must be developed to manage the various fields of expertise required to deliver excellent services to clients. It is essential to the success of ASB that the commitment, energy and skills of its people are harnessed to tackle inefficient, outdated and bureaucratic practices, to simplify complex procedures, and to identify new and better ways of delivering services. Performance appraisal must include an assessment of the performance of individual staff in contributing to improving service to the clients and rewards must be allocated accordingly (Bracker, 2010: 1, 2).

Aligning goals and resources is critical to the success of every service system or organisation. First the organisation must establish a service strategy that defines how value is created for the client, the service concept, which describes in detail the client requirements. When the ASB client base has been mandated, the unit structure must be aligned to the main functions of the base to serve the designated clients; assisting them to achieve their core objectives.

In the end, service delivery attitude will largely determine the perceptions of clients; therefore service provider staff will exert every effort to think of the client first, making prompt service to the client a priority over other work; take personal responsibility for providing service that is convenient, prompt, and efficient; live up to organisational commitments, keeping promises and admitting (and rectifying) mistakes; build long-term client relationships by anticipating, listening to, understanding, and meeting or exceeding our client’s expectations; bring energy to everything that is done - if a task needs to be done, it needs to be done well; tailor service to meet every client’s needs and provide service in a thoughtful and proactive manner, collaborating to meet client needs, solve problems, and implement effective solutions.

**Service Concept and Process**

The actual design of the service delivery process begins with the service concept, which provides the link between the service strategy and the service delivery process. The service concept describes in detail exactly what the clients’ requirements are, in term of how they perceive value, and how they are to be satisfied. The “what” focuses on identifying the specific needs of the allocated clients; the “how” focuses on establishing the organisation’s service delivery priorities that will allow it to meet those client requirements. In defining the service concept, management must also be attuned to the skills, qualifications and interests of the workforce.

The service concept encompasses four elements:

- The service operation – the specific manner in which the service is delivered.
- The service experience – the client’s direct experience with the service.
- The service outcome – the benefits and results for the client receiving the service.
• The value of the service – the benefit that clients perceive from the service in comparison to the cost of that service.

The Department of Public Service Administration has developed a service delivery model to analyse and review service delivery processes to stimulate innovation to enhance existing management processes. The analysis of service delivery processes can be done at the hand of the model as explained in Figure 2.

The service delivery process begins when the client first interacts with the service organisation or system and ends when the delivery of the desired service is completed and the client exits the process. The service delivery design system is a holistic concept, encompassing a number of elements – clients, service concept and the service delivery system – and these elements must be considered in an integrated way.

The service delivery process of the ASB has a certain generic value chain, based on the Porter Value Chain) as pictured in Figure 3. (van Jaarsveld, 2011:4)

**Service Assurance**

Service quality amounts to meeting and exceeding customer expectations. Service quality can also, be conceptualised as the difference between what a customer expects to receive and their perceptions of actual delivery. It is therefore, important, for employees to respond to the customer in a professional and helpful manner; always articulating a positive image of the organisation. This can contribute to the quality of service offered by the organisation.

Various gaps exist when measuring the quality of services. It is imperative to improve service quality by closing the gaps by creating service delivery improvement actions/plans. The quality
that a client perceives in a service encounter is directly related
to the magnitude and direction of the gap between the expected
service and the perceived service (Naidoo, 2004: 48).

Once the plans have been implemented and service delivery is
in process, progress needs to be monitored. This phase keeps
a check on progress, to ensure successful service delivery and
that service delivery remains aligned to the strategic objectives.
It feeds back into the planning phase to ensure continual
realignment, growth and development. A systematic approach
to quality measurement is required. Measuring client satisfaction
is relevant as a critical requirement for ASBs to improve service
delivery. In order to achieve an all-inclusive measurement of
service quality the ASB should measure the clients’ expectations,
of a specific service quality attribute and the clients’ perception
of service quality.

Utilise internal and external evaluation and audit tools/institutions
to indicate areas of poor performance within the regulatory
framework. The internal performance management system of the
DOD is an integral measurement tool to assess the performance
of the service providers by utilising client feedback into their
assessment results.

It is not enough to carry out a once-off survey and to assume
that they have bridged the “gap” to service quality. The existing
survey coupled to the quarterly performance against plan report
must remain the norm for client satisfaction survey. Measurement
should also include the monitor of complaints received and the
rate of resolved issues at front office/call centres (UK, 2009: 11).

When service quality has been measured, corrective action must
be taken to improve the current level of service delivery. This
requires continuous efforts to monitor the effect of any service
quality changes made, to narrow previously identified service
quality gaps, and to take further corrective action if necessary.
When the current status/ expected outcome of service quality is
realised, the next step is quality improvement (Naidoo, 2004: 34).

Conclusion

The service delivery concept is legally guided by the Batho Pele
principles, but practically it is mainly governed by attitudes of the
service providers and clients. It is imperative that service delivery
is properly mandated to avoid any misunderstanding on what
services must be delivered and what can be expected.

The service delivery philosophy should guide the process
and the service delivery strategy. Clear standards must be set
regarding the level and quality of services, focussing on the
specific requirements/needs of the clients and then utilise these
requirements in establishing service delivery priorities for the
service provider. High level of service delivery success depends
on sound relations between the service provider and clients.

Sustaining high level of service delivery depends largely on
measuring performance. These measurements must be used to
identify gaps between actual performance and client expectations,
which must be closed to ensure continuous service delivery
improvement in the organisation. This implies formalised service
assurance functions within an Army Support Base or other service
delivery organisations.

Article by Col Dries van Jaarsveld, Officer in Charge Service
Assurance Management at Joint Support Base Garrison

NOTES
Service: Seven Strategies for Success. (http://customerservice manager.com )
Service Reform Philosophies:with Particular Reference to the Nigeria’s
Servicom and South Africa’s Batho Pele Principles Journal of Public
Administration • Vol 42 no 5 • November 2007.
Police Service Community Service Centres. Tshwane University of
Technology, Pretoria.
5. Santa Clara University (2011). Our Service Philosophy. Santa Clara,
USA. Available at: http://www.scu.edu/is/service.cfm
Delivery Improvement Guide. Pretoria: Government Printers
Service
Public Service Delivery, Government Gazette No. 18340. Pretoria:
Government Printers
(HPCH): Improving Service Delivery Strategy.
initiated Integrated Financial Management System as a pilot project in
JSB Garrison (Paper for University of Pretoria Continuation Education).
12. Woloshuk, Constance (2010). How to develop a philosophy of service
delivery for non-profits. Available at: http://suite101.com/article/how-to-
develop-a-philosophy-of-service-delivery-for-non-profits.
The Army remains the core of the ground forces and the main source of forces for possible operational deployments by the Bundeswehr. That will bring missions that cannot be carried out without forces specifically orientated and trained for such tasks.

Until now, these forces were grouped into the Special Operations and Airmobile Divisions. The new Army structure will see these forces reduced in strength and grouped into a High Mobility Division. This force previously comprised two airborne brigades with four parachute battalions and supporting elements; a modern air-mobile brigade of a light infantry regiment, two attack helicopter and one transport helicopter regiments, as well as three additional medium and light transport helicopter regiments. In the new Army 2011 structure this division will have only about half that combat power, although the Special Forces Command will remain in its current form.

The new division will be faced with some real challenges and special operations, although it will no longer have to handle all special operations; at least not to the present extent. Thus, for instance, one result of practical operational experience is that operations against irregular forces will in future be conducted by all forces with infantry capability, including mechanised infantry. Also, depth operations are of lesser relevance in the context of likely deployments for conflict prevention and crisis management.

The new high mobility division will house the Army’s capabilities for special and special forces operations, for air-mobile operations and mixed heliborne operations. The Special Forces Command retains its present structure and its mission set, among others rescue and evacuation operations, special reconnaissance, covert operations and countering terrorist threats. The 1st Airborne Brigade will hold the airborne forces of the Army, primarily two parachute regiments, an airborne reconnaissance squadron and an airborne engineer squadron. The latter two units will have a similar mix of capabilities to the equivalent units in the other formations, but with lighter equipment. The Army Aviation component will comprise two transport helicopter regiments with NH-90s and one attack helicopter regiment with the Tiger.

Once the capabilities transfer from the Airborne and Special Operations Divisions has been completed and the Air-Mobile Brigade has been stood down, the various responsibilities will be reassigned within the High Mobility Division.

Air-mobile, airborne and helicopter operations in the context of stabilization missions will be commanded by the division headquarters, or detached headquarters elements.
Crisis response, evacuation and hot extraction operations will be commanded by either the division headquarters or that of the Airborne Brigade.

The Airborne Brigade will command air-mobile operations and have elements specially trained to support operations by the Special Forces, as well as providing infantry for sustained stabilization operations.

The helicopter regiments will cover the range of army aviation missions, from transport to air assault operations, independently or in the context of the Division’s operations.

This division will provide readily available forces that are rapidly deployable over tactical or strategic distances and able to be formed into highly mobile and powerful combat groups that can be optimized to meet the demands of varying missions.

Paratroops

Drawing on operational experience, Army 2011 will increase the ratio of combat to support troops, and particularly the proportion of infantry and mechanised infantry. The strength of the paratroop force, however, will be reduced, from twelve paratroop companies to ten and from four support weapons companies to two.

The Airborne Brigade will include Parachute Regiment 31 that, with six parachute companies will, somewhat stronger than the previous parachute regiments. This regiment will be focused on military evacuation and hot extraction operations, as well as supporting the Special Forces Command. Parachute Regiment 26, with only four parachute companies, will be focused on airborne and airmobile operations. Each regiment also has a light medical company and a light supply company. The paratroops can also provide the Army’s contribution to early entry operations.

The parachute companies are similarly organised to other infantry companies, with three rifle and one weapons platoon. The latter has sniper, automatic grenade-launcher and anti-tank sections of three teams each. The anti-tank sections are equipped with the MBDA Milan, but will receive the Eurosipe LR as ‘light multi-role capable guided weapon system’ (supplied by a consortium of Rheinmetall, Diehl, BGT Defence and Rafael). The platoons comprise a command team and three sections. Each section is an integrated system of ten soldiers and a range of equipment including sixteen infantry and light anti-tank weapons. It can operate as two manoeuvrable elements, each led by a sergeant, enabling it to carry out independent tasks effectively.

The parachute companies are similarly organised to other infantry companies, with three rifle and one weapons platoon. The latter has sniper, automatic grenade-launcher and anti-tank sections of three teams each. The anti-tank sections are equipped with the MBDA Milan, but will receive the Eurosipe LR as ‘light multi-role capable guided weapon system’ (supplied by a consortium of Rheinmetall, Diehl, BGT Defence and Rafael). The platoons comprise a command team and three sections. Each section is an integrated system of ten soldiers and a range of equipment including sixteen infantry and light anti-tank weapons. It can operate as two manoeuvrable elements, each led by a sergeant, enabling it to carry out independent tasks effectively.

Each parachute regiment also has a heavy weapons company of six platoons, to support the parachute companies or form a ‘Schwerpunkt’. Each of these companies has:

- An anti-tank platoon with TOW (later Spike LR) on the light tracked Wiesel 1 vehicle;
- Three gun platoons with 20 mm armed Wiesel 1s;
- A mortar platoon with eight 120 mm mortars mounted on 2-ton Wolf vehicles;
- A tactical fire support platoon of four joint fire support teams.

The headquarters and supply company of each regiment includes a pathfinder platoon, for reconnaissance of DZs, airfields or vital terrain, and a canine platoon with dogs trained to detect hidden persons or explosives.

The equipment of the parachute regiments is generally light. Some 400 Mungo ‘operational vehicle for specialised forces’ from Krauss-Maffei are used mainly as command vehicles and section carriers. The Mungo is air-transportable, can operate off-road and can accommodate ten soldiers or up to two tons of cargo or equipment. Its armour protects against light infantry weapons, hand-grenades, anti-personnel mines and shrapnel. The air-transportable light tank, the Wiesel 1 from Rheinmetall, serves as the paratroops’ weapons carrier, while a number of Wiesel 2 are used as command vehicles. The Wiesel 2 may also be selected as replacement for the existing Wiesel 1 vehicles. Both models can be transported inside a CH-53 helicopter. The
existing Rheinmetall 120 mm mortars on Wolf carriers are due to be replaced from the middle of the decade. The mortars are meanwhile being converted to the R1 tube with an obturation ring to allow the use of Austrian ammunition or a later new generation of ammunition. The hardware of the MRT86 portable militarised computer will be adapted accordingly.

The innovative Gladius ‘Infantryman of the Future – Expanded System’ will immensely enhance the effectiveness of the infantry and mechanised infantry. The prime contractor is Rheinmetall, with a large number of sub-contractors. The system comprises a range of improved equipment and will improve command and control and effectiveness, be lighter and require less electrical power. Many different infantry and anti-tank weapons can be used, radio systems will provide for voice and data communications, and the section vehicles will be equipped to serve as the interface to the new Army command information system. Each core system is structured for a section of ten soldiers. The first thirty systems have already been acquired for use in Afghanistan and a further sixty will follow before the end of 2013.

**Army Aviation**

The mission of the Army Aviation Corps remains largely unchanged in the context of the air mobility of the Army: Tactical/operational air transport is the traditional and most demanding task of Army Aviation, allowing transport of personnel, wounded, materiel and supplies over short and medium distances without dependence on fixed land infrastructure. The new light transport helicopter NH-90 will be employed in this role in the Army and to support other elements.

The CH-53 medium transport helicopters, previously operated by two Army Aviation regiments, were transferred to the Air Force at the beginning of the year. They will be required to support many of the air-mobile missions of the Army. Command and reconnaissance tasks will in future fall to the NH-90 in place of the Bo-105, which is to be phased out.

The German Army distinguishes between **airborne operations**, mainly by paratroops and also using transport helicopters, and **air mechanised operations**. The latter are a specific mission of Army Aviation, in essence an aerial extension of anti-tank defence, albeit in an entirely new dimension and quality. This task falls to the Tiger attack helicopter and the NH-90, the latter fitted with the relevant mission packages.

The Tiger with its wide range of weapons will be effective against a multifarious threat spectrum, and can be employed independently or jointly with systems of other services. The next step towards the future of the air mobility of the Army is ‘air-supported operations’. This will see Army Aviation forces, transport and combat systems, well-armed infantry and organic or attached combat and mission support elements combined under single command to achieve the required combat effects. With the air-mobile brigade originally intended for this role no longer to form part of the new Army structure, such operations will be commanded by the High Mobility Division.

This will enable the Bundeswehr to quickly focus combat power, establish or quickly relocate ‘Schwerpunkte’ or surprise opposing forces in their depth areas, in the context of operations of varying intensity and also, if required, in operations against irregular forces.

Another task of Army Aviation and the CH-53 medium transport helicopters is cooperation with the Special Forces and the parachute elements supporting them: Transport and insertion unobserved by the opposing forces; combat support by Tiger attack helicopters, command support, reconnaissance and aerial resupply are among the missions of Army Aviation.

The Army Aviation Regiments have been redesigned for Army 2011. Instead of the previous flying and technical battalions, the regiments will be organised into squadrons directly under the...
regimental headquarters. Attack Helicopter Regiment 36, with 32 Tiger attack helicopters, will conduct nap of the earth and low altitude combat missions, with the focus on air-mechanised and airmobile operations. The regiment, and also its sub-units, will conduct operations independently or in cooperation or in support of combat and combat support forces and Special Forces. It will work together with transport helicopters.

The core of the attack helicopter regiment are two squadrons of each 16 Tigers in four flights of each four aircraft. The three other squadrons of the regiment will provide the technical and logistic support.

The multi-role Tiger will greatly increase the Army’s ability to bring precision fires to bear in a wide range of operations. It is all-weather and night capable; is protected by a combination of armour, a mast-mounted sight and a self-protection system; and has a range of 700 km and an endurance of about five hours. It has modern navigation and weapons systems, and will use a mix of four weapons: Air-to-air Stinger missiles; a 12.7 mm gun pod for close-range tasks; 70 mm unguided rockets with various warheads for use against area targets; and the long-range PARS-3 fire-and-forget anti-tank missile with an imaging infra-red seeker, which can be fired individually or in salvos of up to four missiles at ranges up to 6000 m. Its HEAT warhead with a precursor charge makes it effective against tanks, bunkers and similar targets.

The Bundeswehr is acquiring 57 Tigers, of which 40 are included in the Army 2011 structure. Thirty have been delivered, of which eight are being used at the joint training centre at Le Luc in France. Eight others have been fitted for operations in Afghanistan, and four more will be similarly fitted by the end of 2013. Four of these Tigers are in Afghanistan. Still to come is the acquisition of the PARS-3 and of laser-guided 70 mm rockets.

82 NH-90s are on order, with 72 going to the two regiments and ten to the training centres of the Army. 28 have been delivered, and 12 are being converted to the Forward Air Medivac role, four of which are being used in Afghanistan to support ISAF operations.

The NH-90 can be fitted for various roles by installing the relevant mission packages, among them command and control, reconnaissance, suppression of enemy air defences during air-mobile operations (usually in cooperation with Tiger attack helicopters), and for search and rescue and the classic transport mission. In the latter role the NH-90 has a payload of 2.5 tons and can sling-load up to 4 tons. It has a range of 800 km and an endurance of 4½ hours, with two long-range tanks taking it to 1 260 km. The normal crew is three, and it can transport up to 16 troops or 12 stretcher patients. Virtually all systems are digital.

Looking Forward

The importance to the Bundeswehr of the high-mobility forces of the new division is obvious, providing powerful force elements that are quickly available and have special capabilities. The Special Forces, Airborne Forces and Army Aviation will make a major contribution to the effectiveness of the Bundeswehr in missions worldwide, also in difficult terrain and the urban battlefield, and against various threats.

The new division will be stood up between 2014 and 2016/17, in parallel with performing the missions assigned to its various elements during that period. It will combine in one formation all the elements that operate “in or from the air”, with training, exercises and operational experience being focused on quickly developing the required cohesion. The same applies in the case of the new 1st Airborne Brigade.

It will not be easy for the new smaller force to ensure the maintenance of the multitude of important capabilities, and the new High Mobility Division and its troops will require both consideration and support, including the provision of the equipment still be to delivered or to be acquired.
A growing number of cyber-security incidents has taken place in African countries. These include anonymous calls and/or e-mails for blackmailing, web defacement of government sites long service interruptions of websites, due to system failure or insufficient equipment, frequent scamming plots originating from the sub-region, and smuggling of animal and natural resources facilitated by the Internet.

Unfortunately, these incidents have shown that African governments are inadequately prepared to exercise authority in the cyber domain. This situation has forced some governments to legislate on the matter, but the laws are far from complete or enforceable. Many steps are still needed for these laws to become enforceable, like penal procedures, specialized law-enforcement personnel, specialized infrastructures and software. Lacking a sound cyberspace security strategy, Central African countries will likely allow vulnerabilities to continue to grow to the point that their cyberspaces will become safe havens for criminals and terrorists.

In the same manner in which it is growing around the world, cyberspace is growing in Central Africa—along with threats. Governments cannot disregard enforcing their authority in both physical and cyber space. There are some measures being taken to improve the presence of government in cyberspace. However, there is too much to be done with not enough means, from knowledge acquisition (basic, intermediate and expert education), to building infrastructure and to creating and enforcing regulations.

Most of these efforts are designed to make cyberspace operational. On the other hand, additional initiatives concerned with securing the whole system and giving governments more control have been ignored and put off to be worked out in the future.

Central African militaries, whose basic roles are to guarantee their countries’ sovereignty, seem unprepared to fulfill their missions in the cyber realm. Opening this debate within the Central African military community is a good first step towards filling this gap.

Increasing cyber-security can lead to numerous positive spillover effects.
Public trust in the Central African cyber domain will bring local economic entities to invest in the electronic-business sector. Similarly, increased confidence will attract more international financial transactions and increase Central Africa’s competitiveness. Limiting the amount of criminal acts in the regional cyber domain will diminish the negative perception of the region in the world, thus increasing its attractiveness, or soft power.

An efficient cyber strategy that integrates a regional vision would help overcome the financial barrier to infrastructure investment. In the militaries of Central Africa, where the acknowledgement of cyberspace and cyber-security is still in its infancy, debate on the matter will be quite beneficial, as it will help military planners define adequate future directives in order to counter and preempt cyber threats in a more globally integrated fashion.

In the Economic Community of Central African States (ECCAS) region, the existing reality of cyberspace is quite complex, although very limited. The overall index of cyber readiness for the region is evaluated as a two on a scale of one to seven, which places the region in the very bottom of the world list.

**Infrastructures**

From the infrastructure perspective, cyberspace in the Central Africa community is at the brink of a tipping point.

The year 2012 was the promised year of accomplishment for many projects in all eight countries of the ECCAS sub-region. These projects aimed to connect partners to international undersea optical-fiber cables, followed by the interconnection of regional capitals in a Central African backbone, and finally by the interconnection of major cities through high-capacity communications links.

The present telecommunication infrastructure landscape is dominated by wireless technology, either for distribution to the local population or for the interconnection of distant cities. Mobile telephony and mobile services are highly developed, especially in urban areas, although the rural sector does have an acceptable level of mobile penetration as compared to landline services.

Surprisingly, and thanks to the portability of information and communications technology (ICT), the ECCAS sub-region is now benefiting from all the existing telecommunication solutions offered around the world. The miracle of competition has led to the introduction by mobile-phone companies of 4G, 3G, GPRS and CDMA networks for the population.

Internet access, when available, remains insignificant from a global world perspective and is still expensive due to the reliance on satellite for bandwidth access in many ECCAS countries.

The absence of local Internet-managing infrastructures like Internet eXchange Points (IXPs) contributes to a high cost for Internet access. Projects backed by the World Bank are underway to fill the gap, namely, the Central African backbone, the WASC optical-fiber link, the African telecommunications satellite RASCOM and many others.

**The Military’s Role**

In the physical realm, the military and, in a broader sense, the security apparatus, have always been among the principal assets that guarantee the existence of states.

In Africa, they are considered to be the cradle of peace and development. The security forces provide protection to government institutions and enforcement and dissuasive arms
for the respect of laws. They also provide for the protection of national integrity from inside and outside threats.

In some countries of the ECCAS region, they even provide direct contribution to social and economic development. For all these reasons, the role of the security apparatus in the physical realm is obvious, but in the cyber realm, the reality of this role is still undefined. Despite the use of military and other security forces to protect critical communication infrastructures, based on their recognition as national security assets, and despite the participation of the military in frequency-management boards, the relation of the military to cyberspace is tiny.

In fact, the militaries in Central Africa are merely ICT consumers; use it as a performance enhancer. But the actual role of the security apparatus can be more important. Indeed, in the developing context of cyberspace in the ECCAS region, the roadmaps ahead of the states are very dense.

Priorities are multiple and cover infrastructure, education, laws, business, and security—the latter not being addressed until the final stage, leaving the newly created cyberspace vulnerable to diverse forms of dangers. Up front, in parallel with all other efforts, the security apparatus has to take the lead and bring their experience with crime and instability in the physical world into the nascent cyber realm, making sure that networks, information systems, and laws will not have to be rebuilt because down the road they fail to meet security requirements.

The experience of the military regarding secrets protection can be necessary to help identify or define priorities on what to protect immediately when moving to online capabilities.

An immediate sector that the military can take advantage of is intelligence collection through the numerous collection tools available online.

From another perspective, the military, although not connected to cyberspace, is immersed in ICT that is embedded in various weapon systems. In a context where countries lack expertise in security matters in cyberspace, it can be economically effective to employ the military potential, which is easy to adapt and disciplined, to protect and design countermeasures against cyber criminals.

In a more statutory sense, the police and national gendarmerie, which enforce law and order in the physical realm, should do the same in the cyber realm, as they are the ones with whom citizen complaints are filed.

The security apparatus is a government’s means for exercising authority. It has to be present also in the cyber realm. This presence means possessing the forensic and active and defensive capabilities necessary to give power to the state.

**Technology**

As far as technology is concerned, military organizations in Central Africa exist in a global sociopolitical and economic context where they are very important actors. Thus, they are affected by the technological breakthroughs that might be suitable for the region. But like all armies, they experience many difficulties in the assimilation (or innovation) process.

Overall, the militaries in Central African deal with technology in a submissive way, rather than being leading actors. Nevertheless, as soon as a technology is incorporated, they usually are quick to master it and excel in its utilization.

These acquired abilities are generally not used to their full potential. Some military corps of the region, such as the engineer and signal corps, put their expertise to the service of nation building and can be used as models for the whole military organization to help develop a sub-region that is striving to get out of its socioeconomic stagnation. One of the sectors where this contribution will certainly be welcome is information technology and cyberspace, where the security aspects are not yet implemented.

**The Cyber Community of Central African States**

The Economic Community of Central African States is an organization that already exists and possesses functioning organic structures. In a context where actionable resources are rare and scattered across the community, and because the cyber realm is said to be without borders, one can hypothesize that collaboration built upon existing assets that promotes the sharing of cyber resources and capabilities within the region would be a good point of beginning. Such cooperation will help to create a strong cyber environment conducive of the confidence and trust necessary to tip off a Cyber Community of Central African States (C3AS).

One fundamental truth of cyberspace is that it is universally accessible—thus the idea of a borderless realm. This concept brings up the need to cooperate as the first variable of success especially in Central Africa where no country pretends to have all the resources or capabilities required to prevail. Given the fact that when a cyber resource is available online it can be useful to all in the region, and having an existing community of states where the pillars of regional cooperation are established, the countries of ECCAS should put together their resources in a mutual agreement and create a formal C3AS. Such a cyber community will strengthen the basis for Central African cyberspace and make it better prepared to face the challenges that come with it. Overall, countries in the region face the same sort of problems: poor infrastructures, education and regulations.

At the infrastructure level, interconnecting all regional networks will bring multiple advantages. First, those countries without access to undersea cables for high-speed access to the Internet will be connected through their neighbors. Second, an interconnection through high-speed links will make it possible for countries of the region that possess core ICT infrastructures
Interconnection will also bring access to knowledge by linking regional universities or training centers. With regard to security, a mesh grid of interconnected networks of ECCAS countries will reduce the likeliness of a state being isolated from cyberspace due to a disagreement with neighbors who were network-access providers.

The Central African Backbone (CAB) project, which is now finishing the interconnection of three states of the sub-region (Cameroon, Chad and the Central Republic of Africa), and in its latter phase will interconnect the rest of the countries of the region while providing core infrastructural facilities like IXP, PKI and server farms, constitute a sample of the model envisioned in the C3AS concept and is to be encouraged. Other projects of this nature have to be developed to create a solid core for the C3AS. In that manner, as for the energy sector, the Central African region (Democratic Republic of Congo, Cameroon and Gabon) disposes of a tremendous energy potential that can be developed and shared through an interconnected energy grid. This gives the region an opportunity to solve its energy gap, a good thing for ICT development.

At the information-systems level, virtual environments and delocalization of resources are technologies that have been proven robust against attacks aimed at one geographically located information system. Therefore, through a collaborative endeavor, countries in Central Africa could develop multiple data-center environments - a sub-regional computer cloud - which if interconnected could help build cheaper distributed information systems that are robust and resilient to the benefit of all its members. Such a regional computer cloud will present tremendous economic advantages, as it will help reduce the amount of traffic out of the C3AS sphere, thus having an impact on the contractual bandwidth for external transaction. A Central African cyber community will only be possible if there is a common desire to make it happen. This is to say diplomatic efforts have to be paramount. Indeed, the decision makers of the ECCAS region have to come to together and put in place a global strategic plan that will set the path to a C3AS. The framework of the economic community (ECCAS) constitutes a background that only needs to be reinforced and strategized. In that respect, there are many contacts that exist between the different administrations in charge of ICT, but these exchanges remain just a forum for discussion and opportunities, not a community where members see themselves as engaged in the same struggle. This forum of exchanges between ICT leaders has to evolve into a decisional structure in charge of all the ICT strategies of the sub-region, defining directives, regulations, and laws to be enacted by the parliaments. In that sense, all the countries of the sub-region must harmonize their legal framework on ICT and have a comprehensive strategy of development. The less advanced will benefit from the achievements of the other members, and the most advanced will benefit from the elimination of unstable areas within their vicinity.

As noted earlier, education constitutes one of the strongest pieces of ICT development; in the ECCAS region, the countries are not at the same level in that matter.

A collaborative initiative will facilitate access to training infrastructures to all members at a relatively low cost. The few universities available that become centers of excellence for regional training and research for the promotion of ICT may help create adequate training programs and technological solutions for the local needs of the population. Another aspect crucial in this collaborative initiative is law enforcement.

The growing trend of cyberspace crime, which for now revolves around scams and identity theft, calls for an intensive
collaboration between law-enforcement agencies (exchange of information, continuation of investigation, training and expertise sharing).

The potential gain from a cyber community in Central Africa is significant.

Indeed, when one considers that the region possesses a population of nearly 114 million inhabitants, mostly youth - who are grand consumers of ICT - developing a robust, resilient and secure cyber environment can generate revenues for the states and economic gain for the population, not to mention the quality of life that comes as a bonus.

The reluctance of foreign companies to sell or provide some category of service in Central Africa is a sign of mistrust. That is also true when it comes to electronic transactions within the region, where a lack of visibility on the means of recourses that consumers may have deters them from risking their money in cyberspace. The concept of a mutualisation of resources - human, intellectual, infrastructural, political and economic - in a common goal will create an environment conducive of trust. Generating confidence in cyberspace by promoting trust will fade away the various potential risks that exist in the C3AS, leaving a brighter future.

When it comes to social behavior, there are several criteria that presumably can help build trust and therefore contribute to shaping the behavior of a population. In the case of cyberspace, things are not so different; potential actors in cyberspace (or consumers of cyber products) will also be sensitive to these elements of trust. As presented by Piotr Sztompka P in his book Trust, the first element of trust one can think about is normative coherence; to the extent that people share the same values (morality, integrity, benevolence, skills level, etc.) and have the same expectations, trust will be easier to build. In the case of ECCAS, this is quite true; people in the region share similar ethno-cultural values, economic conditions and the levels of technology. It will be much easier for people in Gabon to understand what are the needs and expectations of their neighbors in Cameroon, the Congo, or Equatorial Guinea, and vice versa.

As a matter of fact, normative coherence is a criterion that is naturally given to the ECCAS, thanks to the common history of the people in that region.

The second element of trust is accountability. Obviously, everyone that engages his money online will need to be able to follow the trail and be able to react in case of any attempt to divert it from the original aim by the recipient. On that question, services offered in cyberspace by people located in the geographical area of the ECCAS will reflect a better impression of safety to costumers within the region than if the provider is miles away. The simple fact of being located within the region becomes an advantage.

Moreover, the establishment of uniform means of recourse within the C3AS will constitute a strong step forward in accountability when there are disagreements. In a community where laws are enforced properly, those that provide services will be constrained by the reality of retaliation in case of failure to comply with contractual commitments.

An educated population that understands how transactions in cyberspace work will be less reluctant to use it. The knowledge of this realm thus contributes to providing the population with the necessary confidence to counterbalance skepticism.

Many cyber businesses are run by young, computer-savvy entrepreneurs in the backyard and bedrooms of private homes; bringing more visibility to their activities in line with who they are, how their services are provided, and with whom they are affiliated, will give assurance or setback to potential clients.

These transparency elements can only be provided in an environment where cyber-service providers are encouraged to step out of the darkness and make themselves known to the public. Such encouragement to go official will be promoted by a global strategy for the sub-region.

The feeling of security also plays an important role in trust development. At the level of the state, the assurance that cyberspace will not be a source of political instability or social unrest can be a strong incentive for decision makers to consider the advantages that may exist in that realm. At the user level, the absence of negative experiences encountered by user gives them the impression of security, which overall favors confidence in cyberspace use. At a regional level, a fully meshed network grid contributes to reducing the risk of network disruption against one of the member states, providing each state with the perception of security, a perspective that urges each to adhere to the interconnection concept.
A C3AS environment that is trusted because of the existence of normative coherence, accountability, transparency, and security will be a perfect recipe for tipping the expansion of cyberspace in the sub-region. This will permit foreign investors to provide the necessary momentum for this realm to become a true instrument for development and peace by fighting poverty.

Where to Now?

At a moment where Central African region countries are moving towards cyberspace, with multiple efforts being done to bridge the numeric gap with the rest of the world, such as linking to high-speed broadband-transmission undersea cable and introducing information systems into the daily life of citizens in the administration and the private sector, there are many concerns regarding state control over this sprawling and boundless realm. Questions are asked about how cyberspace can change the daily life of Central African citizens, how the states can benefit, and what the risks of embracing the new reality are.

Because of the socioeconomic context of the ECCAS region and the political reality in many of its countries, the approaches to cyberspace are diverse, from indifference to pseudo grand strategy. These different approaches expose the region to the numerous risks that come with cyberspace and hinder the advantages that states could derive from it. For the states of the Central African region to find their way out of a time of much tragedy and enjoy the benefit of the power of cyberspace, they need to put their assets in common to form a Cyber Community of Central African States that will gives them a strong basis from which to withstand the beast.
Some readers will immediately shy away from this book, feeling that Portugal lost its war and was, in any event, a colonial power that deserved to lose. That would not be right for anyone who claims to be a professional soldier: The profession of arms is too important and too challenging for such a glib attitude; we need to study conflicts and learn from the successes and failures of all sides. Also, hard as some might find it to believe, Portugal had effectively defeated the insurgencies in Angola and was not doing that badly in the other territories.

The South African Army is going to be involved in peacekeeping, peace-enforcement and stabilisation operations in various parts of Africa for some time yet. The latter two are not much different to counter-guerrilla or counter-insurgency operations in their nature, so it is important to study such operations. And it is particularly important to study operations conducted by a small country in theatres far from home, which is precisely the situation that South Africa faces today and that Portugal faced in the 1960s and 1970s. Also, much as the SA Army has had to ‘rethink’ from simple deterrence and defence to expeditionary operations, so the Portuguese had to reinvent themselves from a military centred on the defence of Europe as part of NATO, to one conducting counter-insurgency campaigns far from home.

The Portuguese went about it in a very professional way indeed: They studied what other defence forces had done or were doing, sent officers to attend their courses and to study their doctrines at first hand, analysed what they learned, adapted it to their situation, and then reinvented and restructured themselves to meet the challenge. On the way they also showed a clear understanding of the nature of insurgency and counter-insurgency and an ability to think ‘out of the box’.

All of this is very neatly set out by John Cann, and set out in a fashion that is easy to read and easy to digest and refer back to.

John Cann is a retired US Navy captain. That has perhaps made it easier for him to look at Portugal’s counter-insurgency campaigns in a more dispassionate way than might an army officer, every army having its own firm views. Also, his naval background gives him the strategic understanding of the difficulties of fighting far from home, something army officers do not always grasp. He holds a doctorate from Department of War Studies at King’s College, University of London is a former professor at the US Marine Corps University and on the staff of the Institute of Defense Analyses.

If you are involved in any way in planning our participation in peace support operations or expect to be deployed on such an operation, and have time to read only one book this year, this is the one to read.
Another book that has been around for a while, but one that deserves to be re-read by any officer or civilian in the business of defence strategy or military planning – or to be read a first time for those who missed it previously. Edward Luttwak has been teaching strategy since the 1970s and has a refreshing habit of seeing things differently – uncomfortably so in some cases – to many other writers in this field. In this edition, for instance, he takes issue with the entire concept of peacekeeping, arguing that in many cases all that such an operation will achieve, is to prolong the conflict. Looking at the history of peacekeeping it is hard to argue with him on that point.

He also restates the point already raised by Napoleon and Von Clausewitz among others, that victory can be dangerous for a defence force: “With victory, all of the army’s habits, procedures, structures, tactics and methods will indiscriminately be confirmed as valid or even brilliant – including those that could benefit from improvement or even drastic reform”. He uses the example of the Israeli’s after 1967 to make the point, their dramatic victory in that war leading directly to initial operational defeat and final politico/strategic defeat in 1973 and, some of the lessons still unlearned, to the stalemate in Lebanon in 1982.

South African officers should take heed: Former SADF officers believe the campaign in southeast Angola in 1987/88 was a major conventional undertaking and brilliant success, while former MK officers like to believe the mythology of the ‘failed’ attempt to capture Cuito Cuanavale. Both are wrong: The SA Army of 1987/88 so bungled its logistics that it required weeks and even months to restock the single brigade that was deployed after an action by one or two battalion groups; and had it had instructions to capture Cuito Cuanavale, it would have done so from the west, where other SA Army elements were on the loose operating quite freely against Swapo and against the Fapla supply line from the main base at Menongue. There is a similar misunderstanding on both sides of the intent and effect of the Cuban deployment of their 50th Division in southwest Angola. We need to study the realities of this campaign to learn from it, not what we would like to believe happened.

Luttwak also warns against too much faith in technology, for instance in the belief that modern anti-tank weapons will enable light forces to stop and defeat heavy forces – one of the myths that grew out of the initial fighting in the Sinai in 1973 – and the belief that air power alone can achieve decisive results.

You will not always agree with Luttwak, but he will make you think, and that is worth the time spent reading – and re-reading to absorb his arguments properly.
Remarks by Secretary Gates to North Carolina ROTC Students

Comments by Robert Gates, former US Defence Secretary, might seem an unusual choice to place in the Army Journal. But what he had to say on this occasion, seen against the background of his career, is something every military leader should take to heart. To put him in perspective: Gates served as an officer in the US Air Force, and then served for 26 years in the CIA and National Security Council, rising to Director of Central Intelligence, before moving to academia, where he rose to head a major university. He then returned to public service as the Secretary of Defence, serving two very different Presidents from 2006 to 2011. So his words to the ROTC students come from someone with an interesting and relevant background.

"As someone who is now working for his eighth president (President Obama), I can say that leadership is something that I have observed and thought about for a long time. And so I’d like to share just a few thoughts with you about that.

I’ve come to believe that very few people are born great leaders. When all is said and done, the kind of leader you become is up to you based on the choices you make. I’d like to talk about some of those choices and how those choices will be shaped by the realities of this dangerous new century.

I would start with something that I tell all the new generals and civilian executives that I meet with at the Pentagon. It is a leadership quality that is really quite basic and quite simple, but it’s so basic and so simple that too often it’s forgotten. And that is the importance, as you lead, of doing so with common decency and respect towards your subordinates.

Harry Truman had it right when he observed that one of the surest ways to judge someone is how well or poorly he treats those who can’t talk back.

The second fundamental quality of leadership is doing the right thing when it’s the hard thing. In other words, integrity. Too often we read about examples in business and government of leaders who start with the best of intentions and, somehow, go astray.

I found that, more often than not, what gets people into trouble is not the obvious case of malefæscence, taking the big bribe or cheating on an exam. Often, it’s the less direct but no less damaging temptation to look away or pretend something didn’t happen or that certain things must be okay because other people are doing them.

And deep down, if you look hard enough, you know that’s not true. To take that stand, to do the hard right instead of ignoring the easier, more convenient or more popular wrong requires courage. Courage comes in different forms. There’s physical courage on the battlefield. But in addition to battlefield bravery, there’s also moral courage, often harder to find.

In business and universities and the military, in any big institution, there is a heavy emphasis on building teams, teamwork and collaboration. And the higher up you go, the stronger the pressure to smooth over rough edges, paper over problems, close proverbial ranks and stay on message.

The hardest thing you may ever be called upon to do is stand alone among your peers and superior officers, to stick your neck out after a discussion becomes consensus and consensus ossifies into group thinking.

The moral principles of leadership I’ve just discussed are timeless. They apply to any military leader in any generation. So do a range of other choices you’ll face as you develop into the leader you aspire to become.

I refer to those relating to the kind of judgment, wisdom, mental skills, intellectual attributes, if you will, that will be most needed to be successful as a military leader in the 21st century.

Another piece of it that I think is important and something for you to think about as you go through the military ranks, it’s important to have irreverent people around you. People who aren’t afraid to poke a little fun. People who can criticize.

I think it’s very dangerous to surround yourself with people who tell you what a wonderful person you are because that - I’ve seen too many people go down that road, and it’s always disastrous because you’re not and, sooner or later, you’re going to find that out.

I’ve always liked the expression “taking the job seriously but not yourself - and I think it’s also very important to remember where you came from. I mean, one of my lines is that when I was a brand-new second lieutenant, I did what my sergeant told me. And between the two of us, we did my job pretty well.

So it goes back to the original point about the need for flexibility and adaptability, and the honesty to admit to ourselves that our record in predicting conflicts that we will be in is perfect. We haven’t gotten one right.

So we better face that reality and be prepared”.

It is perhaps worth adding that, in reply to a question, he remarked “and I read a lot of history”.
