INFORMATION OPERATIONS, THE NATO PERSPECTIVE

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

ABSTRACT

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

INTRODUCTION[1]

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

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

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

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

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

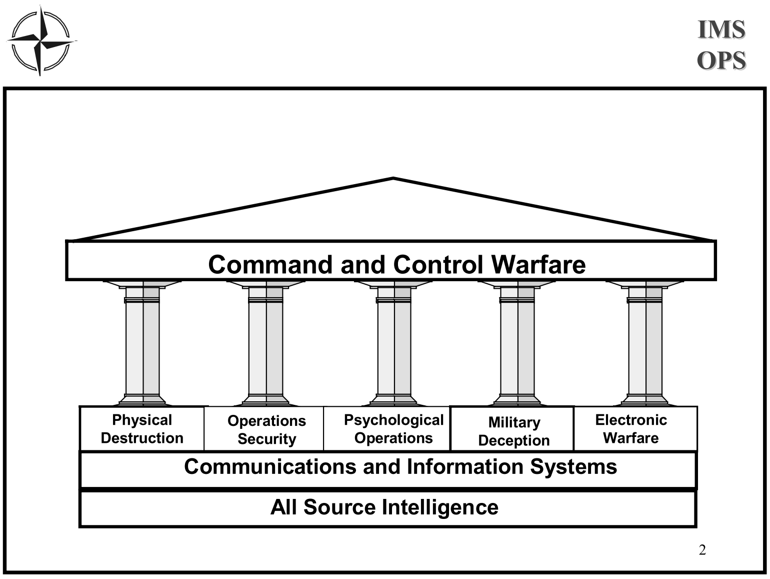
Before we delve too deeply into Information Operations, I would be remiss if I did not mention the strategy that led to the development of Information Operations, a strategy which was executed to near perfection by the Allies in the Gulf War. That strategy is Command and Control Warfare (C2W). Please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

DEFINITION OF C2W

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

C2W Pillars and supporting structure

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



IMS
OPS

Command and Control Warfare

Physical Destruction
Operations Security
Psychological Operations
Military Deception
Electronic Warfare

Communications and Information Systems

All Source Intelligence

2

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

Spectrum of conflict

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

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

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

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

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

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

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

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

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

WHAT DOES ALL THIS REALLY MEAN?

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

PSYCHOLOGICAL OPERATIONS.

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

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

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

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

IMPLEMENTATION

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

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

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

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

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

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

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

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

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

INTELLIGENCE

The next, and final, environmental change which I will discuss is a bit easier for us in the military to understand and relate too, because we deal with it on a daily basis, that is Intelligence. The planning, execution and assessment of effective Info Ops activities is virtually impossible without the proper intelligence. This presents NATO with a particularly difficult problem to solve, as the Alliance does not possess organic capability to collect and process the data required for developing intelligence. Additionally, there is no joint Military/Political intelligence apparatus in place in NATO. And to top it all off, the intelligence requirements for Info Ops are different from those traditionally found in the military.

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

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

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

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

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

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

WAY AHEAD

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

CONCLUSION

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

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