Information Operations during Counterinsurgency Operations: Essential Option for a Limited Response

Raimundo Rodríguez Roca

Athena Intelligence Journal
Vol. 3, No 1, Article 4
14 de febrero de 2008
www.athenaintelligence.org

Athena Intelligence
Advanced Research Network
on Insurgency and Terrorism

ISSN 1998-5237

Athena Intelligence Journal
Vol. 3, No 1, (2008), pp. 23-44

Information Operations during Counterinsurgency Operations: Essential Option for a Limited Response

Theory of Operational and Tactical Employment of Information Operations: Combination of CNO, CMO, PSYOPS and PA.

MAJ Raimundo Rodríguez Roca

February 14, 2008

Abstract:

The importance of Information in the XXI century has become a fact that nobody can deny.
The relevant role of the Information in societies can be observed as well during the development of conflicts where western forces participate. That is one of the reasons why controlling information flow arises as a significant requirement.

The purpose of this article is to present a theory of operational and tactical information operations (IO) employment, as limited and non-lethal effects during counterinsurgency operations (COIN), with an important role to support area control. Firstly, this study will mainly focus on four integrating elements of IO: psychological operations (PSYOPS), civil-military operations (CMO), public affairs (PA) and computer network operations (CNO). Secondly, a practical case of IO execution will be simulated and a concept of operation will be developed.

It should be noted that the approach presented herein is from a Spanish Army perspective. As we will appreciate in this article, the knowledge and managing of IO and the employment of CNO as a tool to empower PSYOPS, CMO and PA activities is of extreme significance and it will become essential to understand and to face the scenes of future conflicts and new wars.

Keywords: Counterinsurgency operations, Limited response, Information operations, Infosphere, Cyberwar

.

Major Raimundo Rodríguez Roca holds a diploma in General Staff by the Spanish Army and by the US Army Command and General Staff College. He has been assigned in the Special Operation Command, the Joint Command and the Research Division of the Spanish Training and Doctrine Command. He has participated in military missions in Guatemala (1997) and Kosovo (2003). E-mail: rrodro7 @ et.mde.es

Introduction to theory

In recent times, information aspects have become increasingly more important during the development of conflicts where western forces participate. Expressions such as "non-casualty war" or "minimal collateral damage" are widely used. New terms have emerged such as "information warfare" to allude to other terms as diverse as cyberwar, psychological warfare, public information, etc. Controlling information flow arises as a significant requirement. However, experience from past conflicts has revealed the impossibility to achieve a total dominance over information and its dissemination. In spite of this, there is still some room during military operations to achieve a certain degree of control at the origin of information[i]. Information superiority will constitute an objective to pursue during the development of operations, although it will be progressively more difficult to achieve due to the global availability of new technologies. Faced with the difficulty to compete for complete control, the solution resides in cooperating, sharing maximum information and gaining legitimacy to combat an adversary's information.

The asymmetric enemy[ii] will use technological capabilities offered in the private market that might not necessarily be sophisticated but display a great conceptual advance.[iii] Furthermore, this enemy will use the most effective weapons within its reach to elude our strengths and take advantage of our weaknesses. One of these weapons will be information, an element difficult to counteract and crucial to gain the population's support and approval. Our own forces in theater must "know what to do"[iv] and "how to face" the new adversary's way of operation. The execution capabilities of the force will require a wise employment of new methods to exercise some degree of control over the information and the civilian population. The enabling tool in a limited and non-lethal form will be information operations (IO)[v].

IO can be generally considered as "the set of coordinated actions undertaken to affect adversary systems and information-based processes while protecting one's own."[vi] However, in actuality, its field of action goes beyond mere information processes; that is to say, it is aimed towards decision making processes. Right here is where IO can be considered as those elements as a whole and in a coordinated manner may affect information and the civilian population. The latter is always susceptible of being influenced, if not manipulated, through media or digital information and direct communication. Therefore, IO actions underlie two types of effects often difficult to differentiate: those effects on information and those on the civilian population.

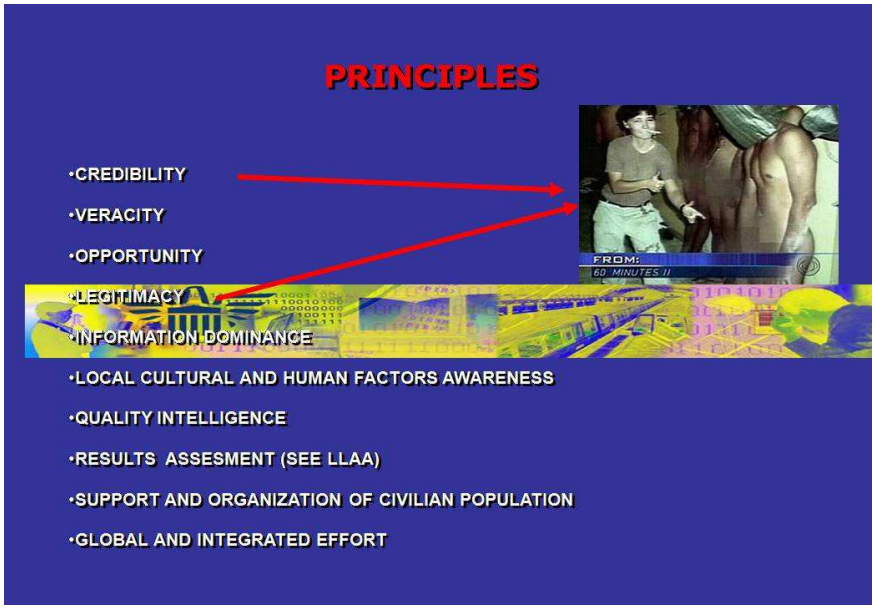
The purpose of this article is to present a **theory of operational and tactical OI employment**, as limited and non-lethal effects during counterinsurgency operations (COIN), with an important role to support area control. This study will mainly focus on four integrating elements of IO: psychological operations (PSYOPS), civil-military operations (CMO), public affairs (PA) and computer

network operations (CNO)[vii]. The latter represents an emerging military doctrine in the information age albeit in its early stages[viii].

Nevertheless, IO constitutes much more and integrates many other aspects. In fact, both US[ix] and Spanish Army[x] doctrines consider that some elements addressed in this paper are not totally contemplated as part of IO. This study will not explain what IO is or individually analyze the four selected components, since this is already done in many doctrinal or conceptual development publications. Instead, IO is presented as a decisive form of tactical warfare where its elements are discussed as a "whole," as coordination of interactions that collectively have a higher weight when delivering an effective response and *effects over both information and population*. In doing so, a higher degree of information control could be exerted, as well as an integration of capabilities that will facilitate legitimacy to counteract enemy information activities. It should be noted that the approach presented herein is from a Spanish Army perspective.

Hereafter, the elements selected to develop this operational and tactical theory will be first framed and linked while outlining the principles[xi] and techniques for its employment. Secondly, a practical case of IO execution will be simulated and a concept of operation will be developed. Lastly, in addition to the conclusions, some necessary capabilities for a Brigade-type force are included to implement the operational and tactical theory presented herein.

Figure 1. IO Principles



Changing the logic of Operations

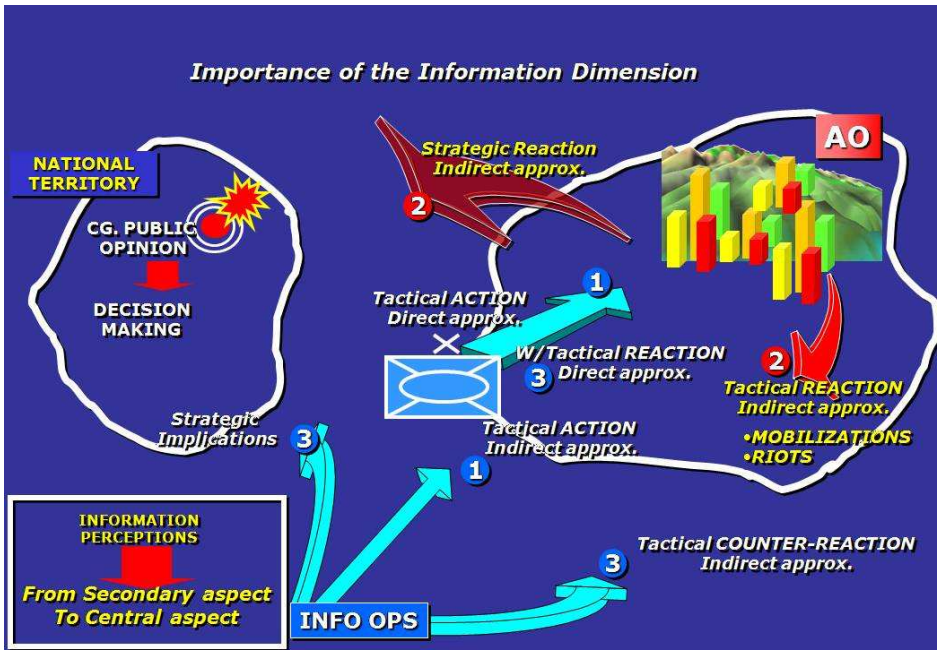
The operations logic of regular armies, organized in an analogous (symmetric) form on the battlefield following predictable guidelines, leaves way to another logic where the imbalance between adversaries imply that one side (non-regular asymmetrical force) will use a different combat system not subject to the same rules and restrictions. Therefore, operations will be directed by an *asymmetrical action,*

reaction and counteraction logic. Lastly, this logic is shown in terms of insurgency versus COIN.

The asymmetrical actor or insurgency will seek to cause effects on the public opinion through the employment of guerrilla warfare, subversion, terrorism, information manipulation, mass mobilization or intimidation. One's own forces will try to counteract with war professionalism, technology, economic and humanitarian assistance, respect and support from indigenous cultures within the theaters of operation, etc. In addition, one's own forces must also act with legitimacy during the development of operations to gain the support of the local population as well as their own. Although it might seem paradoxical if the adversary manages to affect the rational and emotional dimensions of the civilian population, it may also influence societal perceptions limiting the actions of their political leaders and even conditioning military operations in the theater. Therefore, operations are not limited to physical lethal effects caused during traditional combat since they also include a broad spectrum of lethal and non-lethal effects[xii]. Traditional combat will only comprise "one part" of the force's way of operation to achieve the desired effects. The "other part" is based on effects attained "with and over" information and perceptions of the population which will also become a central aspect of the conflict.

Normally, the operations of a force within the theater are materialized through ***actions*** with two components: one is constituted by direct approximation usually with physical characteristics[xiii] and the second component is an indirect approximation, less tangible, non-lethal, and centered on information[xiv].

Figure 2. Logic of Operations



However, the adversary's response to that force will not be situated at the same level, but rather, will conduct ***reactions*** through a direct approximation with a noticeable strategic character outside the theater, aimed against one's own public opinion, seeking to cause an effect on decision makers. In addition and simultaneously, it will carry out tactical reactions in the forces' area of operations (AO), employing all procedures within their reach, such as manipulation of the civilian population through mobilizations, riots, etc.

The ***counterreaction*** of one's own forces in the AO will be centered again in both aforementioned components. Nonetheless, when trying to obtain information dominance, we cannot lose sight of the strategic implications that our counterreaction could cause in the public opinion among one's own national population.

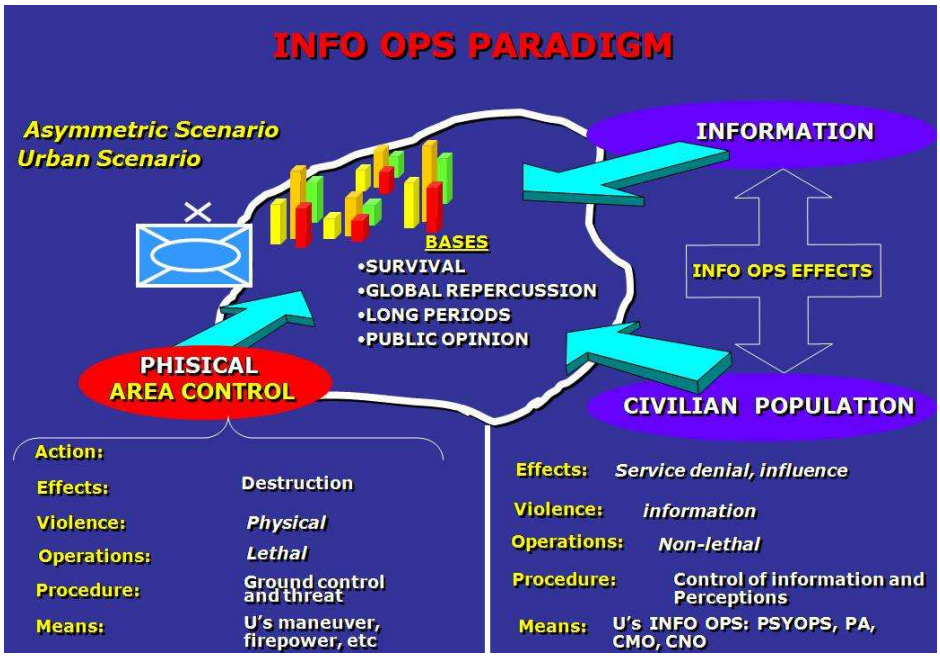
Operation Characteristics

Lessons learned from recent conflicts, such as Afghanistan 2001 and Iraq 2003, revealed that the way in which operations are conducted are as important as the results obtained after their conclusion. During the execution of operations, the intent will not be merely to seek a general physical destruction of the enemy, but to achieve a succession of wide range effects. A desirable operational outcome is short in duration and sufficiently effective and decisive which causes minimal damage. This way, it will be perceived by the theater's civilian population and one's own nation's public opinion as necessary and inevitable, although limited. In fact, IO activities must concentrate on the contribution to that limitation. It is necessary to control the level of damage caused during operations. Providing a controlled and limited response to the actions of an asymmetrical adversary not subject to any physical or legal restrictions is a requirement to maintain legitimate actions and the support of the civilian population, both locally and at home[xv].

Paradigm of IO

As a complement to the required actions to gain control of the AO[xvi], preferably with physical dominance, there are other actions that affect the civilian population which pursue cognitive and information dominance[xvii]. Such "other actions" contribute to counteract the enemy's methods of action[xviii] as well as to quickly and decisively affect their bases of intervention[xix] with a limited character by: (1) destroying their ability to survive by wearing down their persistence, (2) limiting global repercussion of their actions through restricted control of media, (3) limiting the extension of the conflict in the area by debilitating the enemy's will to survive and not offering opportunities to explore, (4) fighting to maintain the support of the local and one's own public opinion by forbidding the adversary from obtaining legitimacy in their actions before the public eye[xx].

Figure 3. IO Paradigm



Effects on the information and the civilian population are incumbent of the IO scope and configure its own *paradigm*, comprised of different elements: various degrees of violence and type of operations, effects, procedures and means. The degree of *violence* will not be applied in the traditional physical way known as "violence in the use of force," but rather in the information domain or "violence in the use of information[xxi]," that is to say, in everything that affects any aspect of information whether digital, published (in media) or any other type. As a result of this, operations will have a non-lethal character whose efforts are more focused in achieving influence and denying certain services than in destroying.

Procedures, understood as ways to execute assigned tasks, will be directed to control information and perceptions, creating the possibility of a range of operational and tactical options with "different lethality" that could be used by military forces. Lastly, the *means* to be used will be functionally integrated in what can be labeled as "information units": psychological operations (PSYOPS), civil-military operations (CMO), public affairs (PA) and others units that in the near future could be named CNO units[xxii]. This latter unit could be employed as an authentic "maneuver unit"[xxiii] whose value may reach such a magnitude that the commander will maintain direct control of its employment since it provides great flexibility[xxiv].

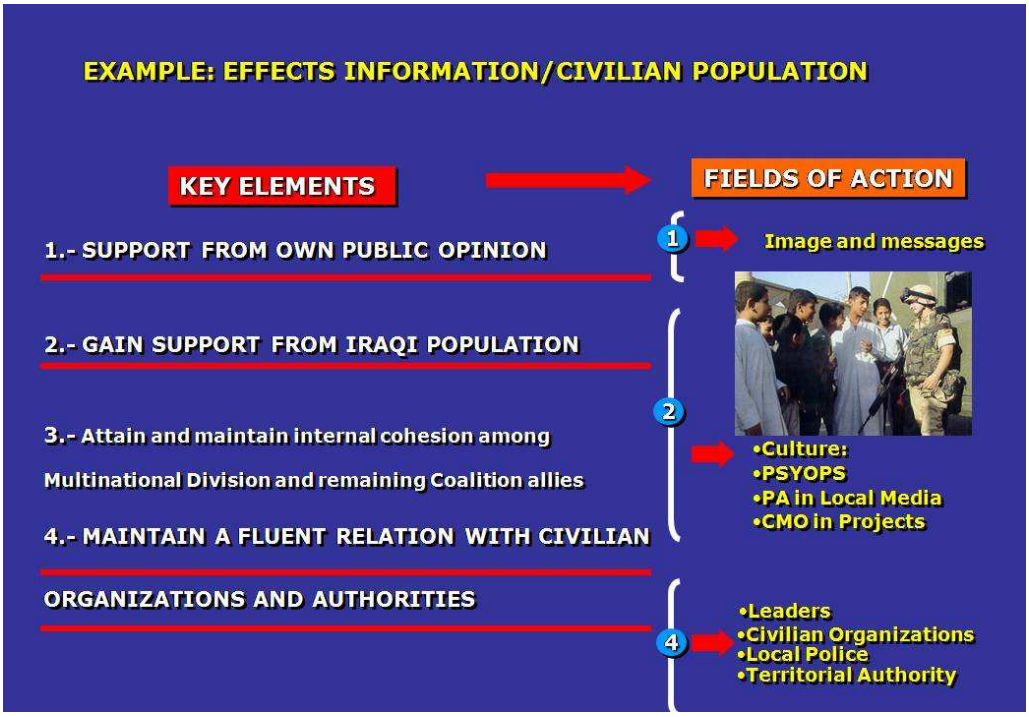
The Spanish Model: Lessons on Efficiency

In order to illustrate the aforesaid, the recent Spanish experience in Iraq provides an excellent example.

The key objectives indentified to accomplish their mission in the area of operations were as follows: obtain support from Spanish public opinion, gain support from Iraqi population, achieve and maintain internal cohesion within the Multinational Division and remaining Coalition allies, and maintain a fluent relationship with civilian organizations and authorities.

Three of these objectives have a direct relationship with the **Information dimension** or, if preferred, with those elements whose scope aim to influence perceptions. Therefore, to successfully achieve said objectives, the performance was centered on: (1) disseminating favorable images and messages through social media, (2) Maintaining a respectful attitude towards the local civilian population and their culture, (3) Combining simultaneously PSYOPS and PA actions through local media as well as conducting infrastructure projects lead by CMO teams, and (4) Contacting local actors (i.e. political and religious leaders), civilian organizations, Iraqi Police chiefs, Coalition Provisional Authority, etc[xxv].

Figure 4. Example: effects information/civilian population

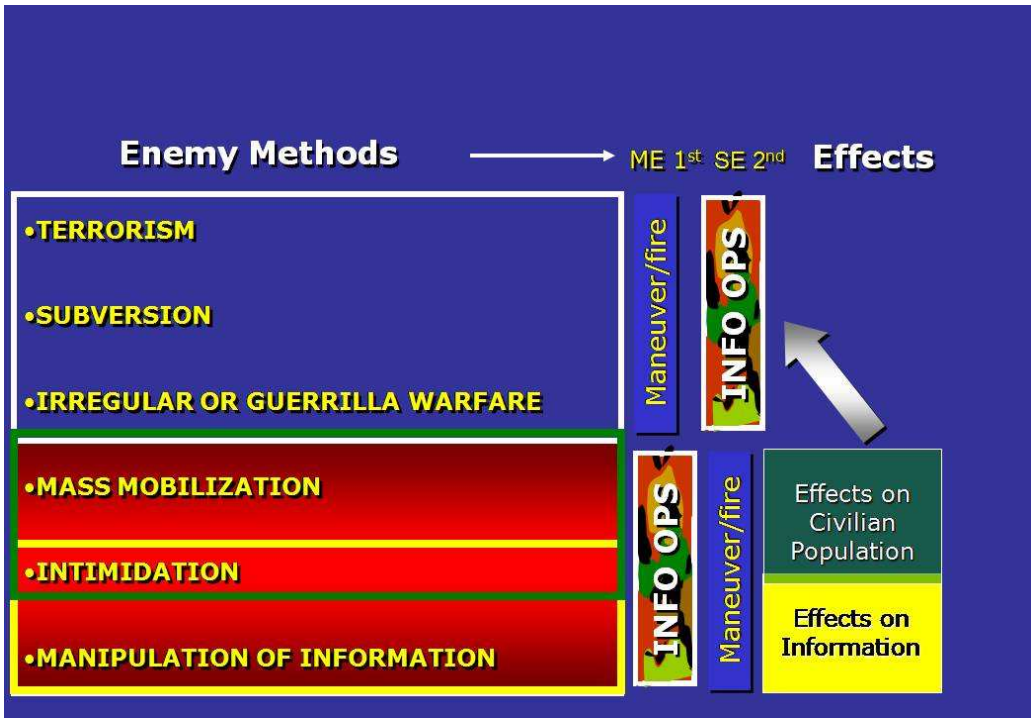


Own Effects Versus Adversary's Methods

Methods employed by the insurgency will require a response in which the effects over the civilian population and information are going to represent a fundamental role. Nevertheless, when addressing *terrorism, subversion and irregular or*

guerrilla warfare, the main effort will be carried out through physical control. Here, the information dimension and IO will be a counterpart to the physical dimension: maneuver, fire support, mobility, etc. However, when the enemy employs methods for *mass mobilization, intimidation and information manipulation*, the main effort will be developed by units and means dedicated to IO[xxvi].

Figure 5. IO main effort.



In order to counteract mass mobilization methods, our force must implement non-lethal limited effects on the civilian population. When trying to react against *information manipulation*, actions will focus on information processes and systems, as well as on the cognitive dimension of perceptions. *Intimidation* will require a balanced combination of both types of effects.

An effective response to the *mass mobilization* method first requires attacking the adversary's cohesion at its strongpoint[xxvii]. Simultaneously, it is necessary to maintain legitimacy in the response to an adversary's violent provocations and, also, to reach the civilian population as rapidly as possible through CMO projects and humanitarian assistance to prevent unconditional support to hostile elements.

In regards to *intimidation*[xxviii], it will only be possible to neutralize the fear caused by the threats of large human casualties by discrediting the adversary, building trust in our response capability and maintaining internal cohesion with other civilian elements in the area of operations, such as NGO's, international organizations, local authorities, etc.

In order to combat *information manipulation*, PA and CNO actions must make a great effort to illegitimate the impact of any opposing propaganda from those who

pursue public awareness. Simultaneously it will be necessary to fight to protect ourselves against their defamations and not to fall into traps that illegitimate one's own actions. Effects on civilian population and information are broken down into a series of activities[xxix]. When said activities are related and reach a proper degree of homogeneity, they can be grouped by function[xxx].

Figure 6. Activities

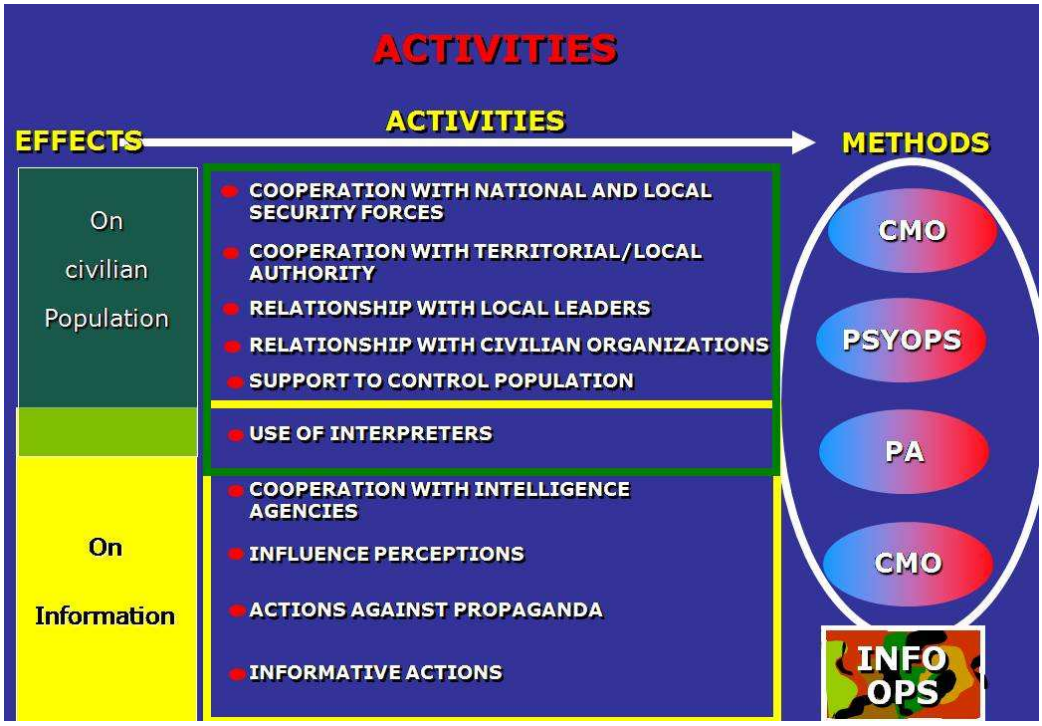
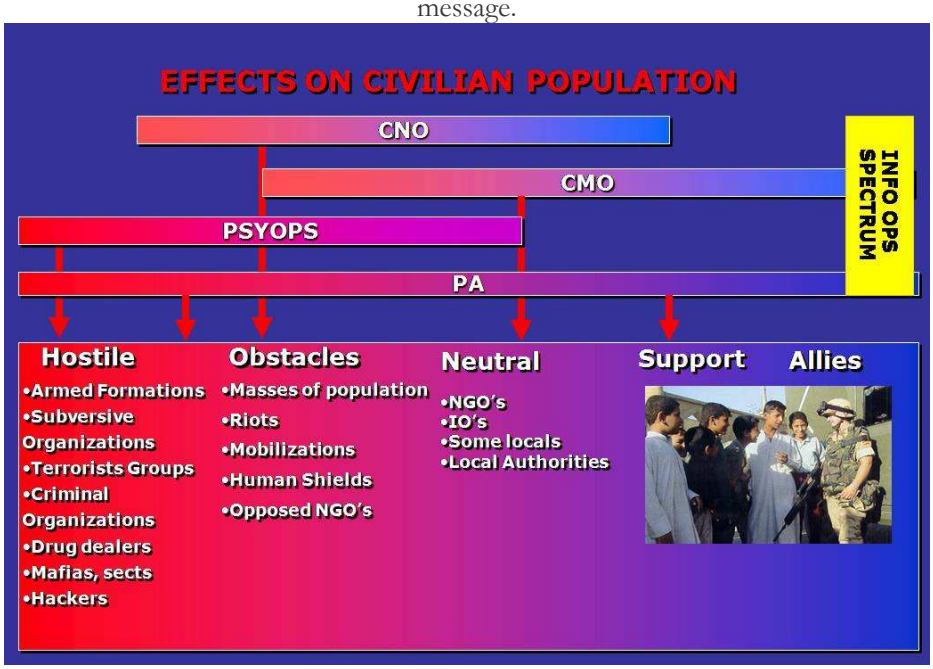


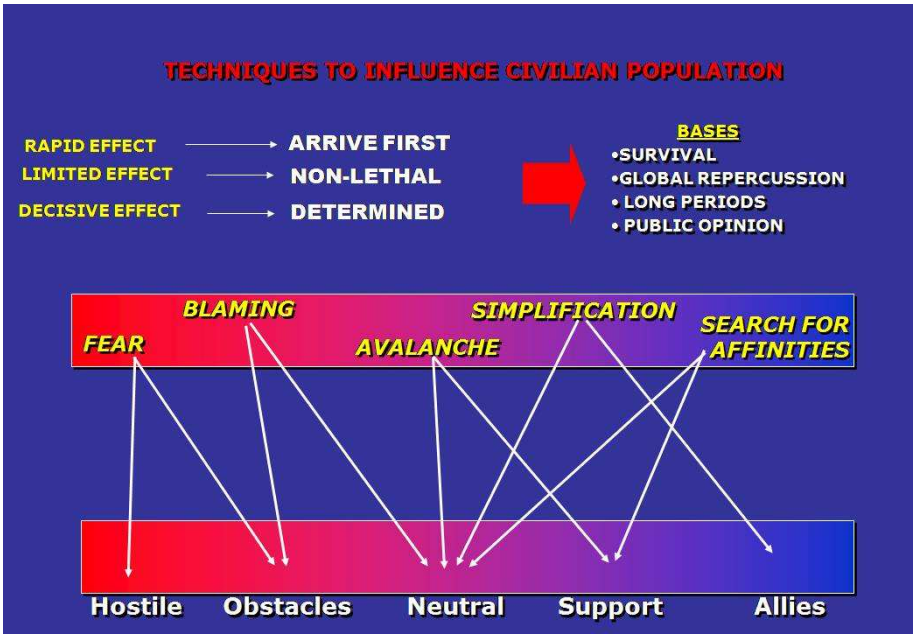
Figure 7 depicts the main scope of action for each IO component. The red vertical arrows indicate the main effort for each component. In the case of public information subjects, it must be considered that their action is permanent and affects several target audiences with the same message.



The Taxonomy of INFOSPHERE and Cyberwar

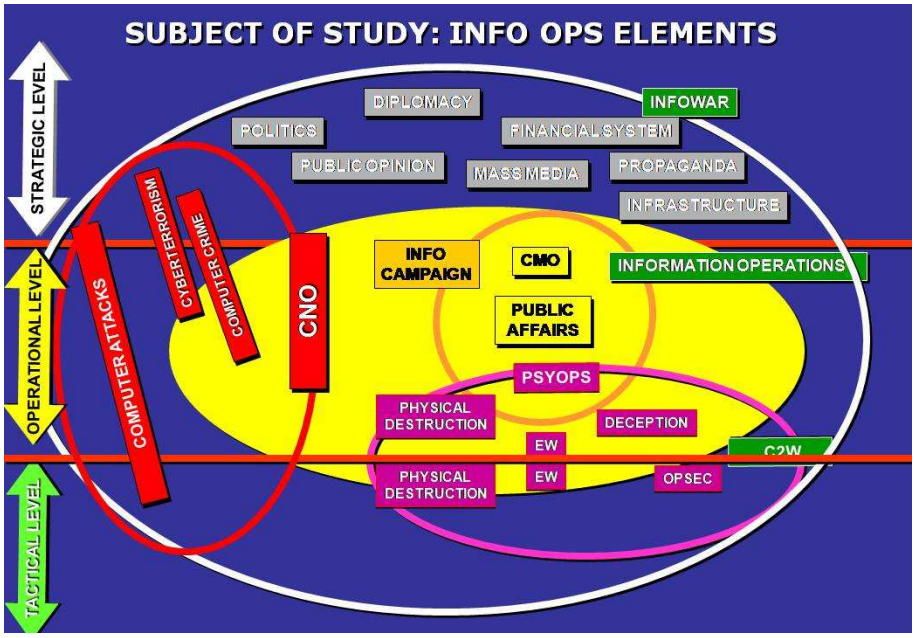
So, why are these four main components of IO selected from the broad spectrum of the information sphere? We find the answer in the "hearts and minds" battle. This means the fight to gain control over the "emotional and rational". The four elements pointed out in the previous section are considered to have a higher influence in the perceptions of the population, and therefore, in support to controlling the AO[xxxi].

Figure 8. Techniques to influence civilian population



The information sphere (INFOSPHERE) has been expanded through the times[xxxii]. First, it was called "Command and Control Warfare". Soon, it evolved into the military concept "IO" that included elements of the information campaign. The sphere of everything that affects information has been functionally extended until reaching strategic and political levels, forming the denominated "information warfare"[xxxiii]. In addition, a new element that has implications at all levels of combat operations has been added: CNO.

Figure 9. Information Sphere (INFOSFERA)



CNO represents one of the recent and more direct aspects derived from information and knowledge warfare. It has the potential to obtain information on "who knows what," "when," "where," and "why." The more identified areas are those focused on attacking information systems to render them unusable, corrupt them by unleashing computer viruses and introducing wrong data or simply to steal information. During cyberwar, the attacks may be isolated or caused by hackers, but also made by an organized group against specific objectives "to interfere with or destroy the enemy's information systems whether a country or an armed force."[xxxiv]

CNO provides unlimited possibilities even within the operational and tactical framework of IO. However, its use will also have to be regulated by combat principles. Manipulating enemy perceptions, creating confusion by covertly altering official declarations and broadcasts, frightening leaders, or another kind of deceiving communications, in principle do not violate the laws governing war. However, manipulating the enemy to the point that their citizens and leaders become deranged or using propaganda and videos that have been distorted or altered to carry out deceptive transmissions could be considered illegal[xxxv].

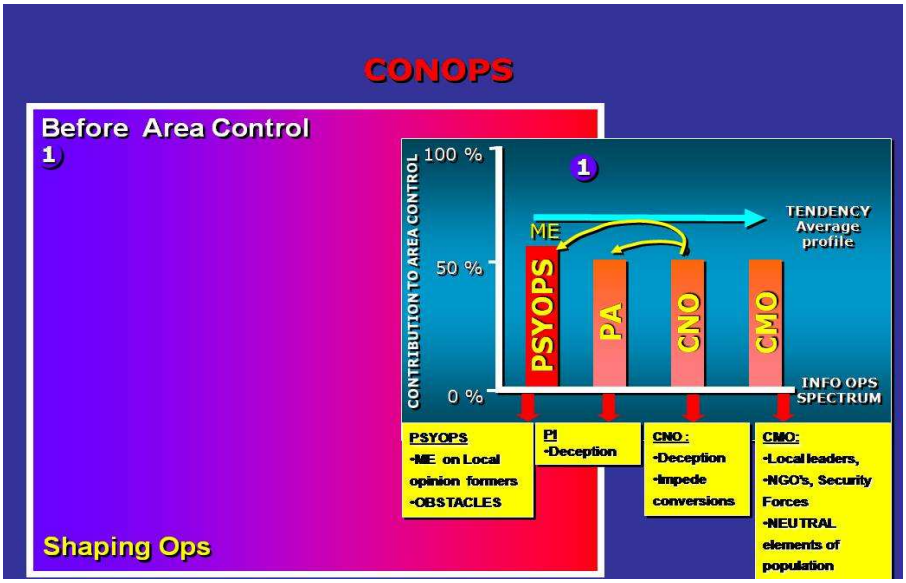
IO Execution

Having explained a general concept of IO, next it will be required to explain the "know-how" for a force to execute IO to support the physical control of the AO[xxxvi]. The *mission* would have to be oriented to support the control of the area of operations by: (1) achieving information dominance, (2) conducting non-lethal effects on the civilian population directed to influence their perceptions, (3)

executing measures to protect one's own capabilities and control informative actions of the adversary's civilian population[xxxvii].

The general intention of IO should pursue contributing to achieve a fast, limited and decisive operation while maintaining the support of the international community and obtaining the support of the local population and its leaders. IO during the control of the AO should contribute to a safe and stable environment to obtain the support of the local population and its leaders while showing a clear resolution to subdue the adversary. The key to success is maintaining the initiative (moving ahead and arriving first) in media information activities directed within the AO as well as one's own home country. The aim would be to reach the desired final result, maintaining area control while preserving legitimacy in actions, information dominance and influence on most of the population.

Figure 10: CONOPS.



The concept of operations[xxxviii] to support control in the AO would be developed in four phases. *Before area control*[xxxix]. Shaping and support operations would begin, directed to configure the battle space, as well as to provide protection and support. During this phase, the integration of the four IO components would contribute an average profile to support area control while the main effort (ME) would be developed by PSYOPS focused on opinion formers and the "obstacles-type" population[xl]. *During area control*[xli]. Decisive operations will be developed. The importance of IO would decrease as a support action. The ME of IO would be in charge of public information, directed to the entire spectrum of the population, offering a transparent and global vision to maintain legitimacy during a time when the intensity of "physical" actions would have increased. *During the main action*[xlii]. The highest point of intensity and lethality during the decisive operations would be reached and IO would continue maintaining a low influence profile in the ME. *After*

area control[lxiii]. During this time of transition and maintenance of control, IO would recover the main role and the ME would become CMO activities.

Combination of efforts and activities before area control. (See figure 7)

Figure 11

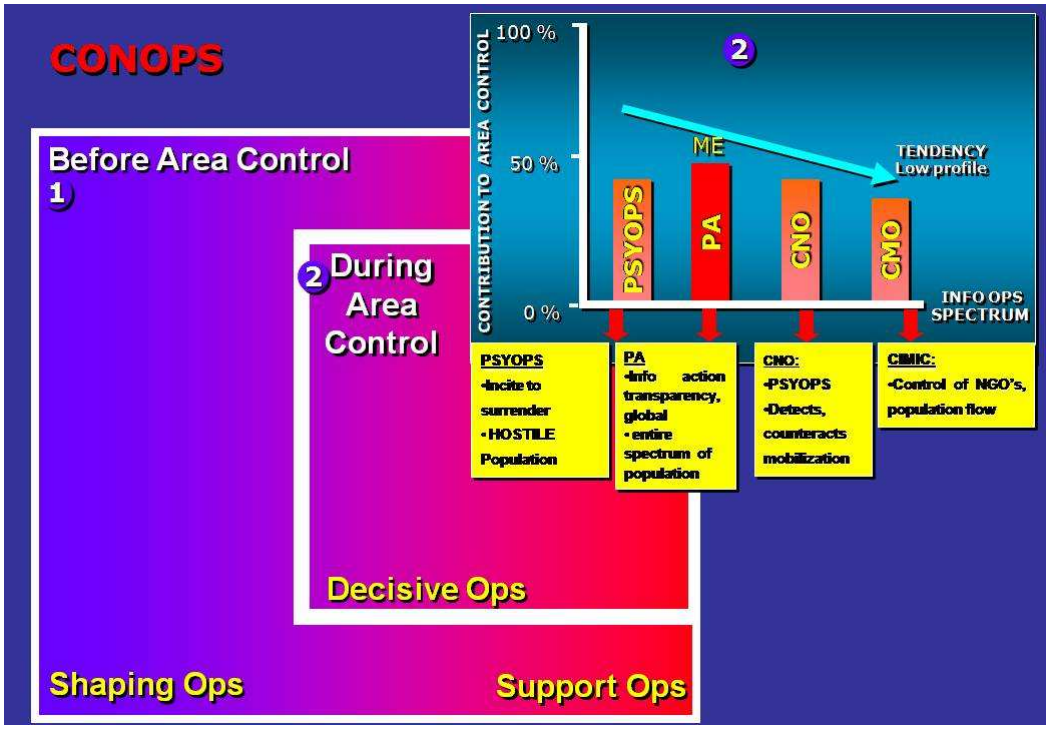


Figure 12

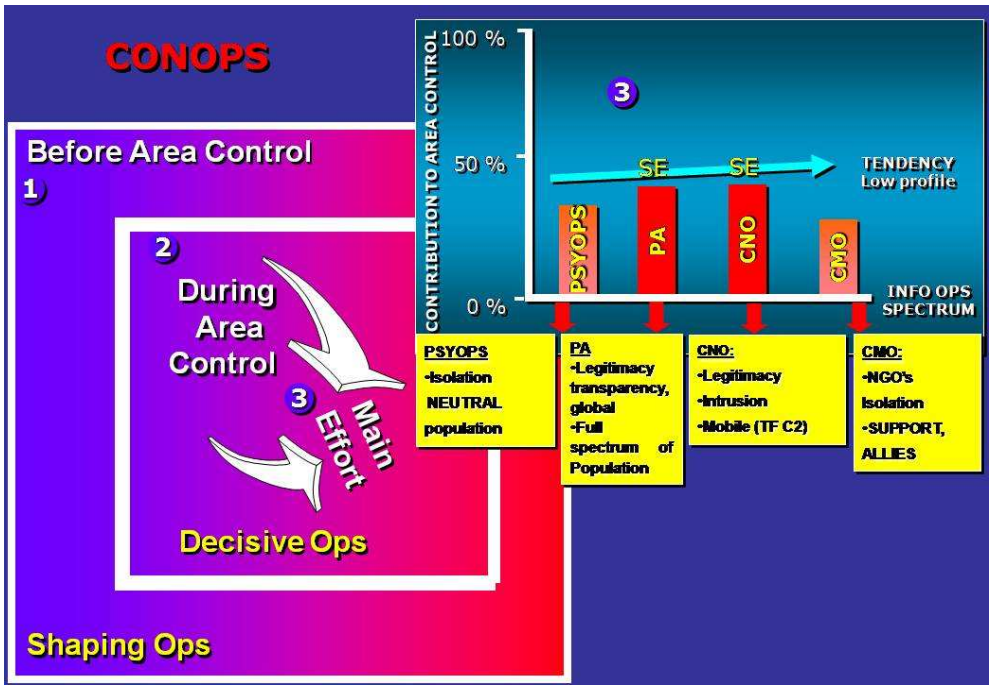
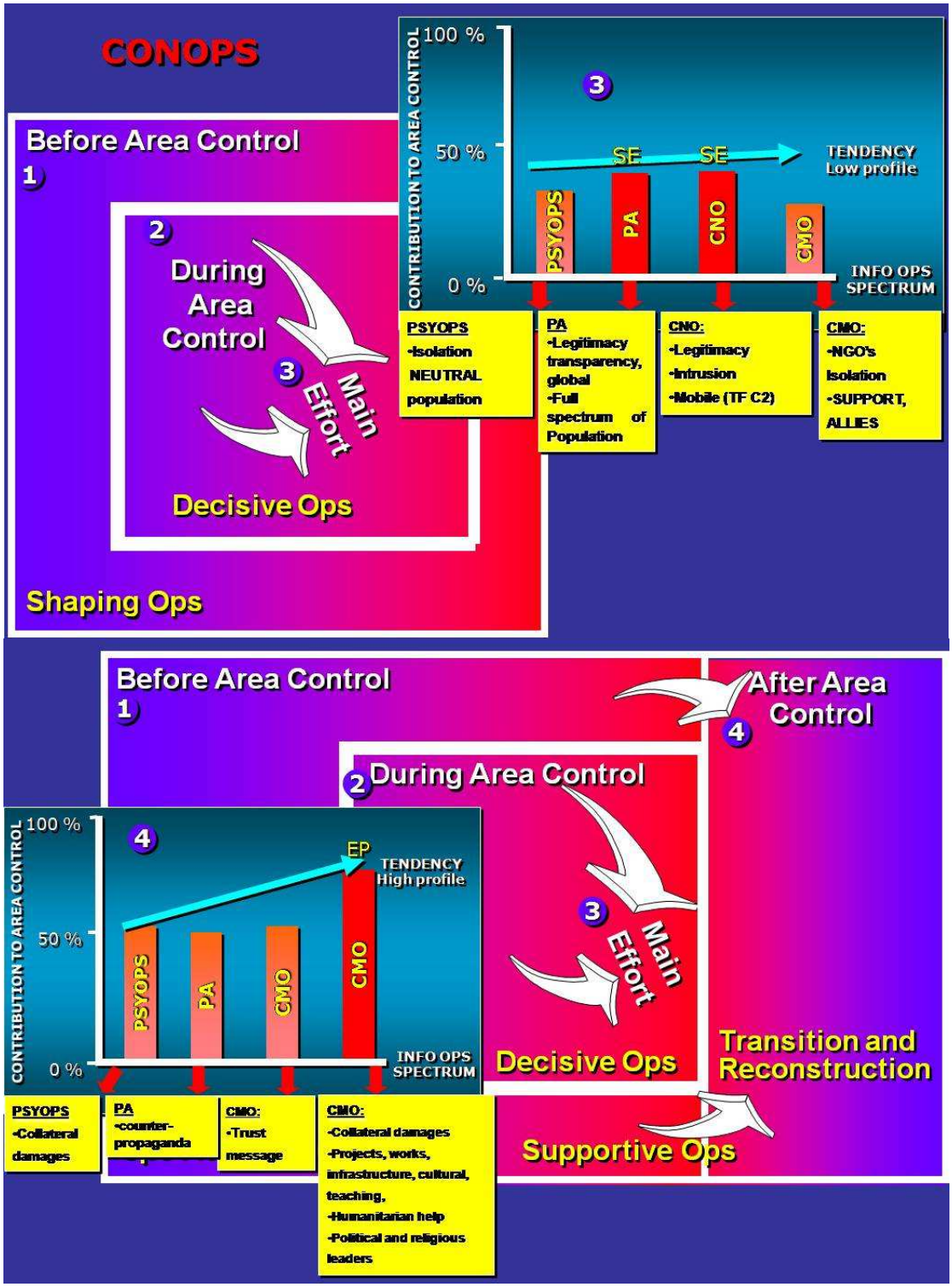


Figure 13



Conclusions

The information and perceptions of the population are leaving their traditional secondary role to become one of the main aspects of the conflict. The contribution of IO as a non-lethal and limited option of operations is essential and must be driven. The model theory of employment developed herein intends to bring a

solution to stimulate commanders at different levels to bear in mind and dominate all the possibilities offered by the information dimension to successfully deploy effects on information and the civilian population.

The true value of IO resides in the planning and integrated execution of PSYOPS, CMO, PA and CNO. The predisposition to act jointly and wholly albeit the different messages from PSYOPS, CMO and PA since they can be directed towards different audiences, will be crucial to maintain coherence and avoid contradictions. Its use as a "whole," constant support and mutual reinforcement are key. Pondering the importance and role developed by each of these elements according to the evolution of the situation will express the capability of the command.

It is adequate to consider the convenience of functionally grouping the units that develop the activities from CMO, PSYOPS, PA and together with NCO elements into Battalion-size "IO units" at Brigade level. These units would considerably expand the array of "options of use" for the force's combat units within a Brigade. This would provide flexibility to the commander, especially during stabilization operations[xliv]

The most remarkable capabilities would be those that allow us to: (1) Influence local and international public opinion through one's own dissemination on radio and TV with products directed to local and international audiences in their own languages;(2) gain access, deny service and maintain a constant flow of information through cyberspace-based services; (3) Rapidly restore information when jeopardized, corrupted or destroyed;(4) Assign CMO equipment and interpreters in direct support to battalions when required by the conditions of isolated activities of these units, and (5) simultaneously maintain other teams providing general support to the Brigade's ME.

The capabilities of verbal communication must be empowered by having an ample range of highly qualified interpreters previously hired in one's own country[xlv]. Cyberwar is a recent element that is progressively incorporated in the development of operations. It is convenient to establish the bases to have adequate capabilities with sufficient notice. Cyberwar is an inevitable extension of the battle space, but still plays a supporting and reinforcing role to other activities. It is evident that both state and non-state ac

[1] As a result of the experience gained from previous conflicts, U.S. and UK established a system of accreditation for war correspondents. Approximately 700 journalists were integrated into Coalition units. For the first time, technological advances allowed correspondents to present the news to their audience in "almost real" time from the place where combat was taking place. Although this allowed public opinion to witness live aspects of a conflict never seen before, the criteria on "what to show" and "what not to show" was left to the media's discretion. The organizations dedicated to the relations with the media and press information centers in the home nations and the AO coordinated the process. However, contrary to what some believed, not all media processes were under the control of the Coalition forces. Some media organizations unfolded journalists who worked outside the Coalition forces. This situation entailed serious security problems and several

journalists found themselves caught and trapped in the battle with tragic consequences in some instances.
R. Rodríguez R. *Fuerzas Terrestres en la Guerra de Irak: Una aproximación al Campo de Batalla Futuro*. 2003 Hernán Pérez del Pulgar Award. Spain. November 2003.
[2] Also depicted in some doctrines as non-conventional current enemy
[3] High Concept, Low Technology Idea.
[4] Know-how.
[5] INFO OPS or IO. The term INFO OPS is usually used in NATO doctrine.
[6] There are numerous definitions of IO and all of them bring differentiating variations of meaning. Some of the most complete definitions are transcribed next. ARRC (NATO), current NRDC-UK, 18 Sep 00: "actions taken to influence perceptions of decision makers as well as certain key audiences to support political and military objectives by affecting adversary information, processes-based information, C2 systems and CIS, while simultaneously operating and protecting one's own information and information systems". NATO MC 422, 26 Feb 02 "actions coordinated to influence adversary decision makers to support joint objectives of the Alliance, through affecting their information and information processes and systems, while exploiting and protecting one's own information and information systems."
[7] "Information and Knowledge. The services made strides both in the ability to move information and translate information into knowledge, but they did not attain the goal or capacity to wage network-centric warfare. Equally important, although the services made concerted efforts to wage information operations, gauging the success of those efforts remains elusive partly because the data is still unclear, but also because the concept remains immature."*On Point, The United States Army in Operation Iraqi Freedom*. Center for Army Lessons Learned. http://www.globalsecurity.org/military/library/report/2004/onpoint/intro.htm
[8] The methodology applied was based on the use of qualitative, quantitative and comparative procedures. Most of the investigation was carried through secondary sources, since there is plentiful bibliography on the subject. Also, many short reach consultations to civilian and military experts were made, and some experiences during recent conflicts were compared to include Spanish National Forces operations.
[9] Joint Publication 3-13 Information Operation. Joint Chiefs of Staff. 13 February 2006
[10] DO1-001. *Empleo de las Fuerzas Terrestres*. 17 October 2003. (Spanish Army Doctrine).
[11] IO Principles. There are some basic ideas that usually govern the successful actions of forces that can be deduced from the lessons learned from past conflicts. Its knowledge does not constitute a *sine qua non* condition to impact the enemy although, without a doubt, if neglected they might help the asymmetric adversary to take advantage of our weaknesses.
Anthony H. Cordesman. The Lessons of Afghanistan. CSIS. August 12, 2002, Anthony H. Cordesman. The Lessons of the Iraq War. CSIS. July 2, 2003.
Credibility, veracity, opportunity, legitimacy, information dominance, awareness of local cultural and human factors, support and organization of the civilian population, as well as an integrated and global effort are *principles* to take into account when applying procedures of "other measures to control the AO." A common aspect that can be observed in all these principles is the importance of maintaining a quality in the messages that are disseminated. This quality must derive from intelligence verified through diverse sources. Since it is impossible to develop all aforementioned principles for obvious space restrictions, two are deemed to be key: *moral legitimacy* and *information dominance*. *Moral legitimacy* is not a safe and permanent value; public opinion and other powers may grant it and deny it depending to occurrences. All actors will try to guarantee the conditions that increase the legitimacy of their actions before the public opinion and their governments. The struggle to impose a specific story that justifies one's own position and illegitimize their adversary's is an especially attractive mechanism for those asymmetric actors who do not have any possibility of an armed confrontation.
Manuel R. Torres Soriano. La *Lucha por la Legitimidad en la Sociedad de la Información*. *Revista Ejército*. January-February 2004. No. 754
Searching *information dominance* to affect the enemy perception of the situation and their decision making process, as well as to protect oneself, is a crucial principle as well.
Figure 1. IO Principles

[12] Effects Based Operations. Bingham, PT. Seeking Synergy. Joint Effects Based Operations. JFQ, spring 2002. United Stated Joint Forces Command. Also «Effects Based Land Operations and the Manoeuvrist Approach: Tradition and Transformation». Presentation to RUSI Conference. October 2003. Effects- based operations is a concept still in the development process by different Armies. The aim is to achieve a new package of military capacities through the integration of kinetic means (mainly lethal) and non-kinetic means (non-lethal) to reach the desired military effect. In actuality, the new concept emphasizes the importance of IO. It includes approaches that go beyond attacking a target and first order effects. In fact, it includes the entire spectrum of direct and indirect effects after the application of instruments of power, such as diplomatic, military, economic and psychological measures.
Also, Commander's Handbook for an effects based Approach to joint Operations. US. Joint Forces Command. Joint Warfighting Center. Joint Concept Development and Experimentation Directorate. Standing Joint Force Headquarters. 24 February 2006.
[13] Maneuver, fire supports, mobility, countermobility, protection, etc.
[14] Figure 2. Logic of Operations.
[15] The duty of preserving legitimacy in actions and not abandoning the local population despite prevailing hostilities will demand from multinational and joint forces to avoid extensive and unnecessary damage in lifeline civilian infrastructure. Hatred is an element that can be easily exploited by local asymmetric enemies. Hatred or resentment will not arise spontaneously; it will derive from the direct or indirect damage infringed to their own existence, to their own ideas, their own form of life, their social situations or any other type. Excmo. Sr. D. Felix Sanz Roldan. Asymmetric conflict. XI International Course of Defense. Jaca, Spain September 2003. Damages in transport and communication infrastructures, energy and electricity plants, energy reserves and basic industry should be avoided as much as possible. In order to suppress the enemy's ability to resist, it will be necessary to employ non-lethal methods in conjunction with the traditional methods that cause lethal effects. At the political and strategic level or operational and tactical IO scale, the elements that constitute information-based warfare will play a significant role when achieving non-lethal effects during limited operations and will promote a general support from the civilian population.
[16] Effects expounded by LTC Pablo Arredondo and MAJ Eugenio Castilla Barea [Spanish Army]. Lecture: Area Control during Asymmetric Conflicts. DOCEX 04 CDES. Paris, 8 June 2004.
[17] DO1-001. DOCTRINA. *Empleo de las Fuerzas Terrestres*. Chapter 17. *El conflicto Armado Asimétrico*. 17 October 2003.
[18] LTC Francisco Jimenez Moyano and MAJ José Luis Calvo Albero [Spanish Army]. Lecture: Enemy Activities. DOCEX 04 CDES. Paris. June 8, 2004.
[19] Ibid. Enemy Intervention General Bases.
[20] Figure 3. IO Paradigm.
[21] Quiao Ling nad Xianqsui. Unrestricted Warfare. Beijing:PLA literature and Arts Publishing House, February 1999
[22] Or even Cyberwar Units
[23] This terminology is used since it is the most popular at the unofficial level and used in numerous forums. The correct term to express the idea underlying the sentence will be «combat units» included in DO1-001. October 17, 2003.
[24] Excmo. Sr. Alfredo Cardona (General, Spanish Army) A. Symposium on Iraq. Spanish Army War College. May 2004.
[25] Figure 4. Example: effects information/civilian population
[26] Figure 5. IO main effort.
[27] Normally, there will be a strong support in concrete sectors of the civilian population.
[28] Specially through the threat of employing weapons of mass destruction (CBRNE)
[29] Figure 6 . Activities.
[30] The functional grouping of homogeneous activities can be broken into four main components: CMO, PSYOPS, PA and CNO. These elements also are organized into an extensive functional classification that falls under the IO scope. Hence, the methods employed by the enemy can be counteracted through the *"four-way operating order,"* although not exclusively, where each element will

play a higher or lower leading role based on the conflict method or combination of methods chosen by the adversary as well as the required intensity of the response.

Effects on the information are necessary to counteract digital or media information that is not under the control of one's own authorities and might directly or indirectly influence the (successful or failed) development of operations. Freedom of information is possible through the control of propaganda and disinformation with the effective use of IO. Consequently, a great part of the success of the effects on information will first require timely anticipation to "arrive in time" or, better yet, "arrive first" so the adversaries' systems will not obtain, attempt to disseminate, or worse, actually disseminate information (or mainly disinformation) to a global audience. This "anticipation" translates into achieving an initiative that allows one to be ahead of the game while providing "freedom of action." Secondly, effects on information require an "iron will" that must emanate from higher echelons and provide credibility. Morality in our action will provide veracity and a moral impulse to our forces. Said motivation is known in military terms as the *"will to win."*

In order to conduct effects on the civilian population, the understanding of the local culture is an essential aspect that embodies the key to success. Connecting in a cognitive way with the populations in the theater will mean to sway the balance of their support and recognition to our side, but overall means a safeguard against the asymmetric adversary's influences and attempts to win over supporters. It is exactly in that field where CMO activities constitute a tool of extraordinary value to provide veracity to our actions, obtain the support of the population and counteract the effects of the enemy's subversive publicity. A broad and incisive psychological and propagandistic, but at the same time subtle, campaign that affects the local population and public opinion world-wide will be executed by PSYOPS elements and supported and driven by CMO, PA and CNO. This will be the way to adapt the means and forms of employment to establish limited and non-lethal assignments. The control of information flows within cyberspace will allow us to follow up on our adversary's intentions and contribute to the general purpose of IO. Therefore, in order to be efficient when conducting effects on the civilian population, it will be necessary to know how to determine the necessary IO resources and how to effectively use the available ones; that is to say, the *"capability of execution"* will be crucial.

Communication capability is a decisive aspect for the force to gain the confidence and support of the local population. Verbal communication powers the collection of information and IO activities. The way the force efficiently and persuasively communicates with local leaders will be essential to achieve both political and military objectives. MAJ Angela María Lungu, US Army. Guerra.com. Military Review. September – October 2002.

Nevertheless, the forces that develop IO are usually limited by the number of local interpreters. The degree of penetration of the messages will be determined by the ability of the interpreters available. Their role is fundamental and it will be necessary to count on a good network for both effects on information and on the population. The Lessons of the Future. UK DoD. 2003.

However, having a suitable number of interpreters will not be enough; their quality will be a fundamental requisite as well. When most interpreters are of local origin, negotiations, aid distribution, contract allocation, text translation, contacts with authorities, etc., are conditioned by their opinions. Therefore, in order to maintain a quality capability, it will be necessary to hire the interpreters from one's own country.

Excmo. Sr. Alfredo Cardona. Symposium on Iraq. Spanish Army War College. May 21, 2004.

Effects on the civilian population will have to consider a spectrum of the civilian population articulated in five categories according to the degree of hostility against our own forces (listed from most to least severe): hostile, obstacles, neutral, supportive and allies. It will be necessary to act on the entire spectrum in a synchronized and, in many instances, simultaneous manner.

In most cases, the force in theater faces armed asymmetric actors (terrorists, warlords, etc.) that are intermingled with the civilian population. This is the reason for denominating a sector of the civilian population as a hostile target audience in the high scale of the spectrum. In actuality, the hostile category will be a sector of the population comprised of the most diverse type of "asymmetric combatants" more so than the civilian population, strictly speaking.

Figure 7 depicts the main scope of action for each IO component. The red vertical arrows indicate the main effort for each component. In the case of public information subjects, it must be

considered that their action is permanent and affects several target audiences with the same message.

Most importantly, the proper combination of IO capabilities requires a joint function where the effects of the four objective components of this study are coordinated and integrated. Although messages from PSYOPS, CMO, PA and CNO may differ (since they are directed toward different audiences), it will be important that they are coherent and do not contradict each other. It is crucial that each subject and objective reflects and supports the general purpose, and that the informative programs are integrated within all the programs of any particular information. This way, the consistency of the main and complementary messages will be assured.

[31] Figure 8. Techniques to influence civilian population.

[32] Figure 9. Information Sphere (INFOSFERA).

[33] Information Sphere. Dimension that compiles all that is related to information whether electronic (digital) or media (public opinion, published…). In this dimension are included propaganda actions, counterpropaganda, political actions, public opinion, cyberwar, media, IO, all the components of the command and control war, etc. *Concepto para el Combate. «Espacio de Batalla»*.EME.2002

[34] However, that is not the only and exclusive potential of cyberwar. What was described above is a denomination equivalent to the physical dimension in the controlled area of operations, just to draw a parallel. Moreover, there is another less spectacular way of cyberwar that underlies the attempt to damage or modify what a targeted group of population knows or believes to know about themselves and the world. Cyberwar can focus on the general public opinion, certain groups or both. In fact, cyberwar offers endless options to asymmetric actors that must be counteracted from within the same cyberspace domain by one's own forces. For example: propaganda measurements, psychological campaigns, political or cultural subversion, sabotages or interference on local media, infiltration on database and computer networks (NGO's, OI, etc), dissident movements. They can also be employed to hide identities, collect financing funds, as a command and control mechanism, as recruiting tool, to compile information about a potential objective, to steal information or to manipulate data, to send hidden messages and propaganda, to obliterate business (subversion of business), to mobilize diaspora, foreign combatants groups or others, etc. All these activities fall under the IO scope. The application of cyberwar through CNO, in combination with PSYOPS, CMO and PA, constitutes a multiplying factor of capabilities. Using PSYOPS via the internet means isolating targeted audiences, for instance, to prevent certain populations from receiving certain products through the internet.

The internet offers endless opportunities without breaking any laws. During operations, the force will be able to use the internet in an offensive way to assist activities to control the area of operations, to invalidate the effects of the enemy's propaganda and the disinformation generated by hostile groups as well as to influence neutral factions.

The support that CNO will provide to CMO will be centered on the expediency to interact with NGO's, international and local organizations, religious and political authorities, etc. Thanks to the possibilities of computer science, all NGO's have the ability to communicate internationally and interact with foreign populations. The possibility to keep in touch through this medium fosters awareness on their movements and feeds network contacts.

The contribution to public information is also elevated. The reinforcement of diffusion, the greater timeliness in the publication and the counteraction of hostile messages, constitutes some of its best applications.

[35] MAJ Angela María Lungu, US Army. Guerra.com. Military Review. September – October 2002.

[36] The generic "how-how" would be determined by different elements that characterize the planning: mission, purpose, desired final result and concept of the operation.

[37] Mainly in the events of mass mobilizations, intimidation and information manipulation.

[38] CONOPS.

[39] Figure 10

[40] See figure 7. Combination of efforts and activities before area control.

[41] Figure 11

[42] Figure 12

[43] Figure 13

[44] Stability and Reconstruction operations. FM1 The Army. HQ Department of the Army. June 2005.
[45] Not technically, but in terms of reliability as well.

BIBLIOGRAPHY

ARRC (NATO), current NRDC-UK, 18 Sep 00: NATO MC 422, 26 Feb 02

Arredondo, Pablo (LTC, Spanish Army) and Castilla Barea, Eugenio (MAJ, Spanish Army). Lecture: Area Control during Asymmetric Conflicts. DOCEX 04 CDES. Paris, 8 June 2004.

Cardona, Alfredo (GEN, Spanish Army). Symposium on Iraq. Spanish Army War College. May 2004.

Cordesman, Anthony H.. The Lessons of Afghanistan. CSIS. August 12, 2002, Anthony H. Cordesman. The Lessons of the Iraq War. CSIS. July 2, 2003.

Commander's Handbook for an effects based Approach to joint Operations. US. Joint Forces Command. Joint Warfighting Center. Joint Concept Development and Experimentation Directorate. Standing Joint Force headquarter.24 February 2006.

*Concepto para el Combate. «Espacio de Batalla».*EME.2002

DO1-001. *Empleo de las Fuerzas Terrestres*. 17 October 2003. (Spanish Army Doctrine).

Effects Based Operations. Bingham, PT. Seeking Synergy. Joint Effects Based Operations. JFQ, spring 2002. United Stated Joint Forces Command.

Effects Based Land Operations and the Manoeuvrist Approach: Tradition and Transformation». Presentation to RUSI Conference. October 2003.

Experimentation Directorate. Standing Joint Force Headquarters. 24 February 2006.

FM1 The Army. HQ Department of the Army. June 2005

Jimenez Moyano, Francisco (LTC, Spanish Army) and Calvo Albero, José Luis (MAJ, Spanish Army). Lecture: Enemy Activities. DOCEX 04 CDES. Paris. June 8, 2004.

Joint Publication 3-13 Information Operation. Joint Chiefs of Staff. 13 February 2006

Ling, Quiao and Xianqsui. Unrestricted Warfare. Beijing:PLA literature and Arts Publishing House, February 1999

Lungu, Angela María, MAJ US Army. Guerra.com. Military Review. September – October 2002.

On Point, The United States Army in Operation Iraqi Freedom. Center for Army Lessons Learned. http://www.globalsecurity.org/military/library/report/2004/onpoint/intro.htm

Soriano, Manuel R. Torres. La *Lucha por la Legitimidad en la Sociedad de la Información. Revista Ejército*. January-February 2004. No. 754

Roldan, Felix Sanz. (GEN, Spanish Army). Asymmetric conflict. XI International Course of Defense. Jaca, Spain September 2003.

R. Rodríguez, R. *Fuerzas Terrestres en la Guerra de Irak: Una aproximación al Campo de Batalla Futuro*. 2003 Hernán Pérez del Pulgar Award. Spain. November 2003.

The Lessons of the Future. UK DoD. 2003

Athena Intelligence Journal: Instructions for authors

- The manuscripts can be sent to the following direction publications@athenaintelligence.org
- Papers on radical Islam, Jihadist Terrorism, Counter-insurgency and Counter-terrorism from a rigorous and original dimension will be welcomed
- Once received, an anonymous copy of the analysis will be sent to two referees for its evaluation. The positive or negative answer will be formulated in a term of two weeks from its reception

Norms of presentation:

- The paper can have a **maximum extension** of 14000 words.
- They must be written to one space, in Garamond letter type size 13 and with a space of separation between the paragraphs.
- The paper can include graphics and charts inserted in the text.
- Each article should be summarized in an **abstract** of not more that 100 words
- Five **key words** must be included and a **short bio** of the author is required (no more than 50 words)

References:

- References must be at the end of the text.

Articles:
Shaun Gregory, "France and the War on Terrorism", *Terrorism and Political Violence*, Vol.15, No.1 (Spring 2003), pp.124–147

Book:
Peter L. Bergen, *The Osama bin Laden I Know*, (New York: Free Press, 2006)

Book Chapter:
Mohammed M. Hafez, "From Marginalization to Massacres. A Political Process Explanation of GIA Violence in Algeria", Quintan Wiktorowicz, (ed.) *Islamic Activism. A Social Movement Theory Approach*, (Bloomington & Indianapolis: Indiana University Press, 2004), pp. 37-60