OBJECTIVE METHOD FOR ASSESSING THE INFORMATION IN CONTEMPORANY INFORMATION OPERATIONS

Captain Assistant Professor Sorin TOPOR, PhD[*]

The general theme of the present work is based on some reflections resulted from studying the impact of terrorism on military science in the "global information era". It is known that one of the priority objectives in the modern military operations is achieving information superiority, especially in the main effort directions. Should this mission be transposed in a strategic objective, then the information interest direction may become a priority domain over which international domination will be pursued. We consider that the impossibility to identify the relevance level of the information may lead to real social catastrophes, of which disinformation or misleading information to the public would represent the effects easiest to undertake by mankind.

In this work we will propose an alternative method to assess information referenced on the general pattern of information operations.

Keywords: *Information operations, Intelligence, Management.*

Nowadays more and more people speak about "the need to secure something". That "something" may be a real, material objective (e.g. a building, group of buildings or any other objective with material limits possible to touch), and also a virtual one (e.g. a theory, strategy, environment, etc., elements which cannot be strictly delimited in the physical environment). Knowing this "something" represents the capacity to understand the reality in which it exerts its existing functions, under a systemic approach, all efforts to adapt

[*] Capt. (Navy) Associate Professor, PhD, "Carol I" National Defense University, Bucharest; topor.sorin@unap.ro

“something” to the progressive conditions will generate information for itself and also for the elements it relates to in establishing the place, role and prospects. These considerations fully justify the statements that “*information means power… information is a weapon*” and that “*in modern world everything is translated in information*” [1].

Information represents the perfect tool to ensure an unconscious dependence of the population on the society values based on knowledge. The military structures, as part of the civil society, identify this reality by creating and using information technology in information capabilities of forces’ command and control, the effect inventing and modernizing interoperable patterns, which succeed, from a huge amount of outdated information, to get useful estimates for the decision-making processes. Nothing prevents us from considering that if this pattern can function within a specific microclimate, such as a military organization, it will not work in a bigger “lab”, as the civil society. It is strange that in contemporary literature, specialized in training or retraining, most works teach us how to persuade others to do what we want and how to make them accept our idea as being more attractive while convincing them that they themselves created it.

Starting from these premises, in the present work we intend to identify some landmarks to establish a framework for predicting the value of information.

General pattern of information operations

Our scientific approach will have as starting point the military concept of “information operation”. This concept is widely debated, in academic or non-academic environments, for which a series of norms included in doctrines and specific regulations have been designed. NATO line documentations define information operations as:

“… co-ordinated military activities within the information domain to affect information and information systems to achieve desired effects on will and capabilities of adversaries and others in support of mission objectives while sustaining own information and information systems.” [2]

As it can be noticed, regardless of the type, dimension and kind of information society, the international conflict aims to obtain the desired effects for reaching the target, through coordinated activities executed against the information and information systems of the opponent, the final end being affecting his will and information capabilities. In other words, information operation means the act of obtaining and maintaining control over the information environment through perception modifying methods, information flow influencing, and modifying information parameters.

Therefore, information *could or could not* reflect reality. Control over the opponent's perceptions will be accomplished only as soon as information would outline a favorable image of the dominant side, being a sequence of reality or "an artificial reality".

NATO concept of information operations is based on a series of coordinating and integrating principles, classified on specific information parameters on which they exercise their function, components which, essentially, hold the same persuasive aims over:

1. the human element - represented by the enemy's staff: commanders, opinion leaders, other decision factors, troops, civilians who support the enemy, etc.
2. Automated sensors and all information processing elements, such as: receivers, automated command equipment, hardware included or not in the weapons, communication equipment, decision assisting equipment, etc.
3. Information networks - respectively components which ensure communication: components of communication and computer networks (conductors, transmitters, maintenance equipment), intra and inter-systemic information flows, other elements which allow information exchange and communication between leaders, between leaders and the public, between forces in lead or cooperation.

The in-depth study allowed us to identify some general aspects which fit in the general principles of any conflict. We can enumerate:

- In any type of military act the information operation is a function of a force structure. Planning of information operations is drafted by the planning structure in a command or a temporary structure with counseling or support duties for mission planning;

- In a command, at any hierarchy level, information operations are organized, planned and executed focused on objectives and not in relation with the available amount of force and means or estimated enemy force;
- The command intention and operation conception are key elements to which objectives, targets and priorities are subordinated;
- The specific actions of information operations must be synchronized and integrated in the command processes at all hierarchy levels and adjoining leadership.

Their integration must be accomplished in two directions, namely: 1. horizontal-information operations must be coordinated with and integrated in similar activities, planned strategically, operationally and tactically; 2. vertical activities specific to information operations must be integrated in any military act whose development may produce a certain message. (Any action must contain a message and suggest information, especially for the decision element of the adversary).

We can state, on a real basis, that regarding information operations, the elements based on which a classification which has as reference the conflict escalation point differ substantially. Thus we can distinguish three types of information operations, namely:

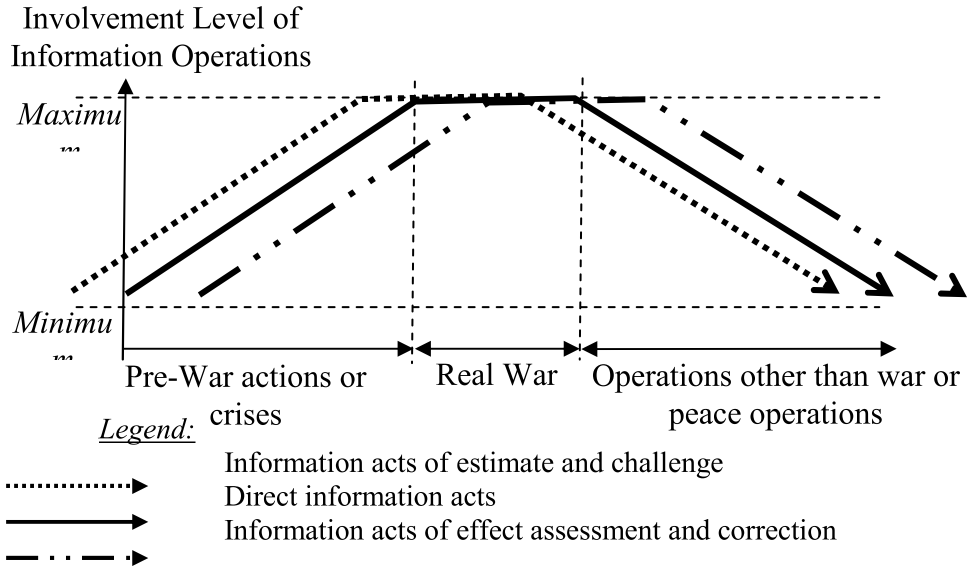
-Information operations preceding the conflict;

-Information operations executed during the armed conflict;

-Information operations performed post-conflict and in an environment of relative peace.

Periods and acts when one of those prevails are difficult to separate due to the specific objectives of each stage. In addition, we have to understand that their typology differs, mainly, regarding information demand and processing patterns (i.e., limitation of redundancy level and information mining). All these aspects demand a certain period of time, a situation which does not allow realizing a strictly defined time pattern, transition from a stage to another being extremely ambiguous.

We consider that only from the development point of view can we accept as general classification pattern for information operations the one showed in picture 1 in which the basic reference is given by the conflict escalation curve.


Involvement Level of
Information Operations
Maximum
Minimum
Pre-War actions or crises
Real War
Operations other than war or peace operations
Legend:
Information acts of estimate and challenge
Direct information acts
Information acts of effect assessment and correction

Picture1 – Interdependency of information operations on their typology and conflict escalation curve

We consider that, as a rule, during pre-conflict or crisis stage, information operation objectives are concentrated on the adversary's deterrence to initiate any type of actions which may have effect on own or allies' information system. Carefully designed, coordinated and executed, these information operations may contribute to crises priming, consolidation for diplomatic relationships, as well as economic, military, social and other activities of support, eliminating the cause of military involvement.

During the war, information operations support any type of action of own forces and prepare future schemes, completing the panoply of activities in the operational information environment. The specificity of this type of operations is determined by gaining advantage over the adversary's decision making process, by holding control over the available time. In this respect, ending the OODA loop (observe, orient, decide and act) before the adversary is materialized in introducing new information in his information systems, a situation which will make him continuously resume the OODA loop, at the level of observation and orientation in the event he is searching for optimal action. Continuous re-initialization of the decision making process equals a firewall over information flows through which the adversary has to start action. In other words, a well organised and executed information operation will paralyze all driving elements of the adversary's structures, regardless of how well he thinks or how well prepared he is to perform a certain maneuver.

In the third stage of the conflict, together with settling peace and restoring order, information operations must support ceasing of military force development and actions of its retreat from the conflict area. In this situation the information operation will represent the key element in small conflicts. As a rule, information operations of this type focus on influencing the perceptions of the adversary and his supporters in order to adopt favorable attitudes towards the implementation of the new policies necessary to maintain peace. Through the reality demonstrated by the contemporary combat area we may conclude that *the power granted by information constrains the execution and exercise of physical power.*

To apply these conceptual patterns a specific technology of information operations is required of which, by far, that of communication can be noticed. That is why together with the implementation of global communication technologies, physical power does not represent the essential indicator for the armed forces. The power of information allows, by using small and extremely flexible structures, but with fast access to connect to various information flows, to get fast control over any surface on earth. Thus any force located anywhere on the planet may become invisible not in the sense of the principle of physics, but by cultivating the perceptions of its presence necessity to ensure individual and collective security.

Since ancient times, peasants used to take refuge in walled cities which offered safety against invaders. It did not matter whether the fort could be subject to long sieges or to systematic bombing, a situation in which people were extremely vulnerable by being increasingly wounded, ill or starving; the population under siege lived with the feeling that the soldiers would protect them. Historical sources show that most of the people hidden in woods or underground huts could escape from being captured if the enemy chose to confront the adversary in the final battle.

The illusion of security offered by the fort walls is still present today; the modern man adores to be tricked even if he fully understands reality. In these circumstances, how the vanity of a commander is not to be satisfied when he has the perception that he understands everything without a thorough judgment of the situation and to be given the information that he wishes for. The study of all wars can offer enough relevant examples, in which the end of a battle was decided the moment when the commanders misjudged the realities of the battle field.

Nowadays we can notice the tendency of modern armies to use automated means in direct confrontation, which work according to well defined algorithms and do not allow the decision making process to be affected by human emotions. But the number and diversity of these modern sensors does not change the above mentioned theory. Using any contemporary technology of collecting information other than quantitatively will only raise the fort walls, as well as the security perceptions, until the attacker innovates something or implements a new weapon. In addition, the necessity to be aware of the real situation and its dependency on the sensors' higher quality is real, but we cannot help asking ourselves: *How relevant is that piece of information delivered by own sensors?*

What is relevant information?

As a rule, it is considered that holding more relevant information brings along a higher value of the information product or even of the decision itself. We consider this conception, although very spread in the military environment, as wrong, especially in today's information operational environment. The error is induced by the uncertainty caused by the information relevance degree. The present conception used mainly in military commands accepts the variant that information becomes relevant when linked to certain objectives in an investigation.

Our opinion is that information becomes relevant when has the power to argue or deny at least one theory of the investigation in question. To justify this approach we present two theories, namely:

1. *The information which confirms or supports a hypothesis is not relevant*. Psychologically speaking, an element of decision tends to be influenced by the evidence supporting the initial information, satisfying the belief underlying the above mentioned theories.
2. *The lack of information about a hypothesis may represent the relevance of it*. To understand this theory, we have to introduce the pattern of information double processing. This essentially maintains that a piece of information can be processed simultaneously by several receivers able to perceive it correctly depending on their instructions in the field. Thus an information structure will be correctly assimilated, the information adding extra quality, while an individual will report the information to his system of assessment determined by his previous instruction. However, both ways of information processing will determine actions generating new information. Thus, after a certain period of time, it can be noticed that a single piece of information initiates two complex, totally different action processes. According to this algorithm/pattern, we can notice that the lack of information on the specialised channel may determine a high level of hypothesis relevance by avoiding the information "cascade" with misunderstood or distorted information.

The method that we are suggesting, namely that one should not look for information to support the theory in question and to argue against it is supported by the level of experience of the information system in the field. A long experience will cause the information filtering along the information flows to be more complex and repeated due to the correlation to other indicators which support the hypothesis in question. In other words, the multitude of apparently inexistent information becomes relevant information necessary to a correct assessment of a situation. Without the method of debating and questioning information the real information would not be distinguished in the multitude of global and globalised information characteristic in the contemporary information environment.

In addition, we must admit that real information in contemporary military operations is extremely hard to identify due to the complexity of the protection measures. Once identified, it can be processed in almost real time, the generating element being located, intercepted and neutralised fast.

The information assessment meant to establish its relevance should be based on two stages, namely:

- A first stage should be generating hypotheses. To do this, very useful are the simulating devices based on the "game theory". No matter how large the number of hypotheses, depending on the initiators' creativity degree, contemporary computer technology allows to solve any problem whose virtual reflection corresponds to significant patterns of the situation under analysis.
- The second stage comprises negation of each hypothesis based on solid information. An advantage of this task is using experienced people who possess strong knowledge. These experts should be able to cover a very large number of fields, be human and not belong to the respective information system. The request that the experts be human and not information algorithms is supported because only the human being has emotions, uncontrolled and logically unexplainable reactions. History has many times witnessed that, and there have been moments when commanders made a difference through illogical decisions at that moment, but which changed the course of wars. On the other hand, an information programme holds a number of routines which, no matter how fast and performant, are limited to conditions not previously estimated. All this, completed with the lack of the sense of belonging to the analyzed system will make the resulted product able to identify as many logical errors of the analyzed hypothesis as possible.

Conclusion

We estimate that one of the immediate results of such an approach will cause the emergence of new information assessment techniques. This idea is based on using the techniques of debating the proof with solid arguments for which data mining methods should be used.

The advantage and novelty of using this method resides in the fact that it is not necessary to wait for the information operation to end and to the lesson learned stage to prove that someone was wrong when elaborating a decision or during a scenario analysis.

In addition, the advantage of using this method may offer new prospects and alternatives to the initial estimates. These hypotheses test by comparing them with counter proof takes a long period of time depending on the magnitude and effects of the information operation. In this respect, we consider that at tactical level the time for using such a method will not be very long considering the targeted objective and the constraints imposed by the mission received.

Though, we conclude that using this method at the operational and strategic levels may lead to eliminating collateral damage, neutralizing insurgent ideologies, as well as containing any threats to critical infrastructures.

BIBLIOGRAPHY

Volkoff, Vladimir, *Tratat de dezinformare, De la Calul Troian la Internet*, Bucureşti: Antet, 2000, p. 165

Information Operations – Analysis Support and Capability Requirements, RTO Techincal Report, TR-SAS-057, 2006, p. 11.

Tsang, Steve, *Serviciile de informații şi drepturile omului în era terorismului global, Geopolitica Lumilor secolului XXI*, Bucureşti: Univers Enciclopedic, 2008.

Maior, George Cristian, *Un război al minții, Intelligence, servicii de informații şi cunoaştere strategică în secolul XXI,* Bucureşti: Rao, 2010.

Feyerabend, Paul, *Against Method, Outline of an anarchistic theory of knowledge*, http://www.marxists.org/reference/subject/philosophy/works/ge/feyerabe.htm