INTEGRATED INFO-KINETIC OPERATIONAL SYSTEM A SOLUTION TO COUNTERACT COMPLEX THREAT TO PEACE, CRISIS OR WAR

Ilie BOTOȘ
General (r)
ibotos65@gmail.com

Abstract: This article seeks to illumine different aspects pertaining to a possible solution to the problematic of conflict and especially information warfare, namely an integrated info-kinetic operational system-based approach to counteracting complex threats to peace, crisis and war. In the introductory part we will look at and clarify important preliminary notions such as information warfare and information operations. Then, the concept of integrated decoding matrix will be debunked, as an important part of the proposed solution. In the second part, we will approach the concept of integrated operational matrix and its benefits, reaching in the end the conclusions sustaining the integrated info-kinetic operational system as a pertinent tactical response to conflict and war.
Keywords: war, information warfare, integrated decoding matrix, integrated operational matrix.

INTRODUCTION

In order to be able to discuss a possible solution to the complex problematic of conflict and war, some preliminary notions will firstly be clarified.

Information warfare includes various activities such as psychological operations, deception and misinformation in civil and military matters, electronic warfare, physical and information attacks, and a range of defense activities and programs. It is important to emphasize that information warfare is a construction that runs throughout the spectrum, from peace to war, to enable the effective application of the responsibilities of the forces (United States Air Force, 1998). As a working definition, information warfare represents the set of actions taken to achieve information superiority, in support of the national military strategy, by damaging the opponent's information capabilities and information systems, maintaining and protecting their own systems and information (Libicki, 1995). The information war represents the totality of the actions carried out at tactical, operative and strategic levels in time of peace, crisis, escalation of the crisis and conflict, in which information-related means are used to reach the desired objectives and finalities (Power, 1996).

Information warfare exists at the convergence of intelligence activities and processes, support activities, core processes, command and control processes. (Jensen, 1994).

Information operations are actions taken to influence decision-makers in support of the pursuit of political and military objectives by affecting each other's information, information-based processes, control-command systems and information and management systems, at the same time exploiting and protecting their own. information and / or information systems ". There are two main categories of information operations: defensive and offensive, depending on the nature of the actions involved (NATO, 1999).

One of the effects of information technology is the creation of virtual space as a new dimension in which war can be waged. The virtual space has inseparable basic elements: the armed forces, the nation and the international community. All levels of command and control can be attacked and must be defended accordingly. At all levels, man is the one who has the final decision-making power. This makes the concept of influence an option and a danger. Modern states face a dilemma: on the one hand, digitalization is a natural evolutionary stage towards which modern societies tend and, on the other hand, these advances create new and serious vulnerabilities.

NATO understands that information is a strategic element in any field. And for this reason, a specific risk management policy is needed in terms of information quality. We are in the process of examining how we can maintain an effective level of connectivity and interoperability in hostile situations. Our concept in this regard is that this issue must be developed in collaboration with all structures in the field of defense, security, law enforcement and justice in close cooperation with the civilian sectors, all based on transparency and interoperability between allies. It is necessary to continuously analyze the level of development of the information systems and the degree of dependence on them at the social body level.

The EU, NATO and the UN need to further develop their own legislation and collaborative mechanisms to be able to react in real time to information attacks. This suggests that information aggression against individuals and organizations is seen as a matter of civil and criminal law, but rules need to be integrated and refined to allow a comprehensive investigation of the full spectrum of threats to military capabilities, influence on the perception of the masses, the use by terrorist entities or organized crime groups. The evolution of threats in recent years reveals a multispectral combination of them that aiming a large number of targets in a well-structured synchronization matrix. The promotion of international security and defense policies is achieved through a complex of means involving military, intelligence, counterintelligence and security in fields of economic, energy, food, health, humanitarian, etc.

The manipulation of information by exploiting all the means offered by the written press, television and social media offers the possibility for hostile factors to prepare their field of action for complex operations that include: espionage networks, forces for clandestine special operations, agents of influence, operational support groups. On the other hand, hostile entities can use the capabilities of cybercrime groups, cross-border organized crime, terrorist groups, and more and more contractors in private military companies to camouflage the origin of operations.

INFORMATION DECODING MATRIX

In the following, as part of a proposed response to the problematic of war we will analyze the notion of information decoding matrix.

First, the amount of information that an experience gives with two equally achievable results reveals its operative and operational value. Structuring this process, we have:

I = information

Pe = probable event

Po = probability of occurrence and manifestation of an event.

Re = a reference event already produced.

The internal information transmission system is based on the particularities of the nervous system as a whole. External information follows the route from the source to the receiver via a channel.

S----------C----------R

There may be parasitic information factors at both the source and the channel or the decoder matrix of the receiver. Also, under the influence of negative emotions, major perceptual distortions can occur. Information can undergo substantial changes that can turn it into amorphous information or, more seriously, into toxic, manipulative information. There are also influences that do not change its active substance, its operational value. The formula for evaluating information is as follows:

Iov = Rri-Pi+Pvd

Iov = information with operational value;

Rri = relevant real information;

Pi = parasitic information;

Pvd = possibilities to verify and document the information parasitic level.

Recent research, however, highlighted the fact that the formula is more complex, involving two new dimensions that better outline the process:

Iov = Rri-(Sci+Epi) + Pvd where:

Sci = represents subjective conditioned information, the external stimulus being bound by an association of emotionally charged information, existing at the level of the subconscious of the human individual. Depending on the context, subjective conditioned information may have added value to the initial information or be an element of distortion of reality.

Epi = External parasitic information, either as a result of a qualified parasite, intoxication, disinformation, manipulation, or as a result of multiplication of information with the addition of false information, due to erroneous perceptions of intermediate human sources.

The characteristics of the information carrier in relation to its emotional influences as well as the expectations, internal constructions and the expectations of the receiver are likely to influence the quality, quantity and operational relevance of the information.

The value and relevance of the information is not in direct ratio to the size of the carrier signal. Once the signal is received, the information is distributed across different segments where it is subject to specific processing. These processing elements are part of a synergistic, correlated and integrated operational process in the nervous system, depending on the content of the reference matrices.

The reference matrices are architecturally structured and loaded with information in consonance with the beliefs, ideologies, principles and education that structure the personality

of the human individual. We are talking here about the working memory subjected to states of consciousness, subconscious, latent memory, to which is added the whole spectrum of tensions existing at the instinctual unconscious level and the mechanisms of reflex processing of information and, in addition, somatic reactions specific to the autonomic nervous system, especially those of the sympathetic nervous system.

THE CONCEPT OF INTEGRATED OPERATIONAL MATRIX

Going further, let us now look at the concept of integrated operational matrix. The social body must be a system with innate capabilities for continuous development and self-regulation, which is equally subject to conditioning of human component and internal and external environmental pressure.

The informational capabilities of a state generate a very complex system of systems that includes technological support, human intelligence combined with artificial intelligence organised into three components:

- hard power – the use of military and economic means to gain power;
- soft power - is the ability to co-opt rather than coerce by shaping the preferences of others by attraction and persuasion
- smart power – which represent a mix of hard and soft power strategies

What is needed is to integrate, analyze, exploit all the information for decision making processes and those necessary to ensure the optimal functionality for whole components of social body. Vulnerabilities to misinformation are exploited by the hostile entity at all levels of the information start at the level of the mechanisms of the individual s perception influenced by beliefs, expectations and representations along with education and are modulated at the level of groups, organisations and social networks.

Operational information fusion cell (OIF) consists of:

- storage and transport of information;
- elements of technological support;
- capabilities of fusion and integrated analysis;
- means of coding and dissemination to decision makers and operation.

The characteristics of interdepartmental network of integrated intelligence circuits:

- -flexibility, plasticity and calibration, principles that must underlie the adaptation of the informational components of the social system to sudden changes in social balance;
- -the reorganisation of the information system represent the ability to change existing structure, functions and connections in response to environmental challenges. This reorganisation can be described at many levels ranging from the tactical (basic operational cell) to operational circuits & networks) and strategic level (system of systems);

- -informational plasticity means the ability of the system to restructure itself with the change in the dynamics of the spectrum of threats;
- -system flexibility & plasticity mediates the transition from classical learning to automatic responding (optimal state of action; early warning system; automatic response reaction).

Development of mechanisms for early assessment of the risks of info-emotional manipulation of public opinion by means limited to the information war.

Functional connectivity between operational fusion cells, informational circuits, informational network and intelligence systems into integrated informational operational system. This functional connectivity modulate the informational flow in the whole system, increased level of synchronization between specialized components which is very important for the cognitive process and knowledge management.

Structural and functional correlates of cognition macro scale level:

All functions of the integrated information operational system, especially awareness and knowledge management imply a dynamic balance between segregation and integration, resulting in a perpetual functional and structural organisation of the whole system. Critical dynamics is considered to operate at the edge of phase transitions meaning that the operational fusion cell and the networks operates near a critical point posed between a phase where the activity is enhanced (supercritical phase) and a phase where activity collapses (subcritical phase).

Subcritical phases are characterised by strong coordination between systems elements but without fluctuation, in which operational fusion cell are locked into fixed interactions, while supercritical phases are characterized by chaotic fluctuation with low coordination which leads to lack of stability.

Operating under criticality means optimal information processing with a balance between stability and flexibility.

The calibration of the reaction to a certain operative situation is achieved by accelerating the conversion from voluntary (cognitive programs/knowledge management) to automatic program during peace, crisis or war. Through them the early warning system (EWS) , the fast and stable entry in the optimal state of action (OSA) and the spontaneous triggering of the automatic kinetic response (AKR) are activated.

Integrated Operational System benefits:

a. increasing the level of awareness, knowledge management and calibration of the dynamics of informational flow;
b. increasing the level of self-regulation depending on the evolution of threats;
c. increasing the level of ergonomics and the economy of resource consumption by applying the principles of smart power;
d. increasing the level of resilience to information manipulation of vulnerable groups;
e. maintaining a high operational level through the integrated operational application center.
f. continuous upgrading of the field of sensors and information sources in parallel with the alert and response system and consequences management system and their testing for specific condition of peace, crisis and war.

The Integrated Operational System acts in three main directions: prevention, detection and response;

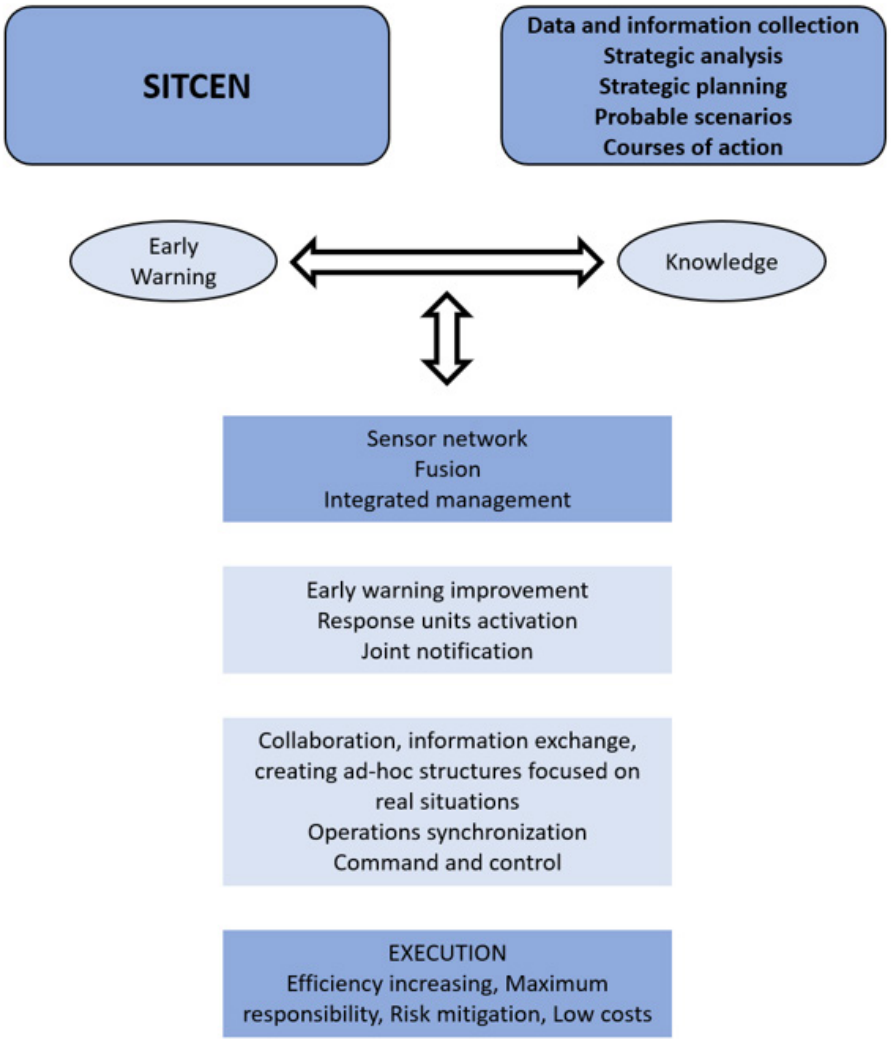

Figure 1. *NATO Situation Centre (SITCEN)*

Let us now look more closely at the three components (hard, soft and smart) identified earlier.

Hard Power Component includes:

- operational capabilities, forces and means of kinetic response (military, security, law enforcement);
- information mechanisms for collection and analysis at strategic, operational and tactical level;
- means of communication for ensuring the transport and storage of information and for the transmission of commands to kinetic mechanisms;
- calibration mechanisms.

Soft Power Component includes:

- software applications for selection, analysis and exploitation of information;
- mechanisms for analysis, knowledge, control, adjustment for awareness of multipolar threats, own and enemy vulnerabilities and for providing response options.

Smart Power Component:

- knowledge management;
- matrix of response operations synchronization;
- development of courses of action in operational applications for optimal calibration of circumscribed hard power and soft power in the face of complex multipolar threats;
- structuring the mechanisms of automatic response to critical crises and war situation,

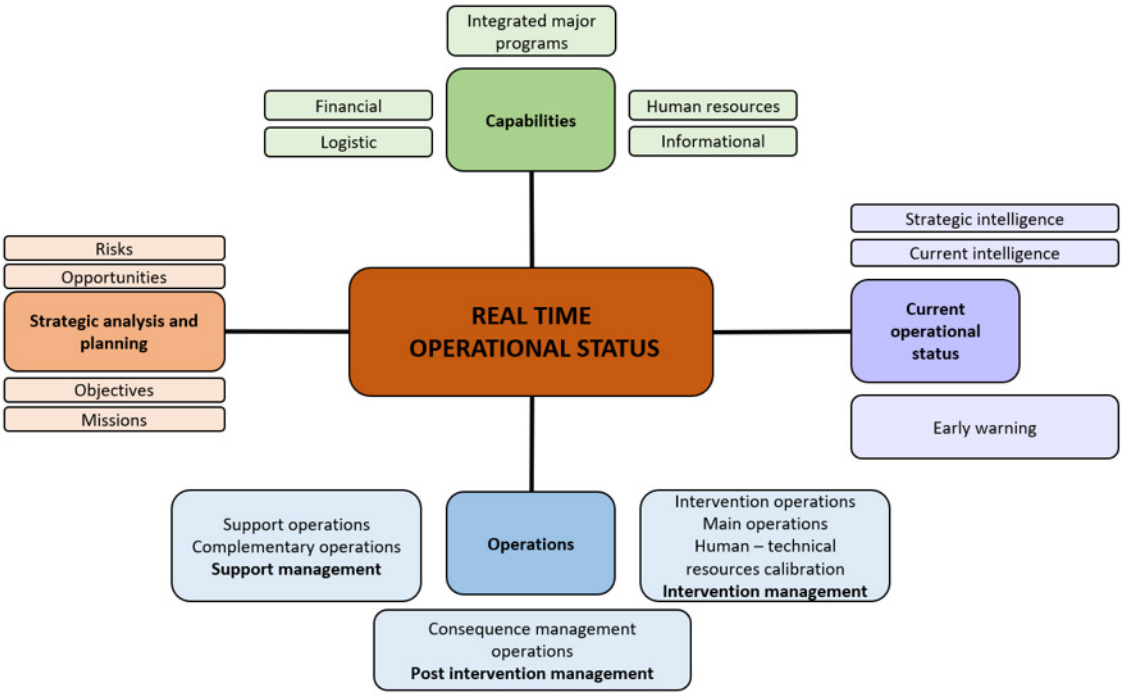

Figure 2. *Real time operational status characteristics*

The proposed approach to counteracting the problematics of conflict and war is based on the integrated operational matrix concept contains framework aspects organized in stages and on specialized circuits that contain:

- -policies, action strategies, operational aspects, action plans, operational applications, development of course of actions for peace, crisis and war; -ensuring the optimal response in real time;
- -adaptation mechanisms to ensure rapid and stable entry into the Optimal State of Action / Combat;

- -Integrated Early Warning and Alert System;
- -mechanisms for ensuring the automatic info-kinetic response to complex multipolar threats;

These operational tools are based on the ability to gather / collect information; analysis (prevention); self-monitoring (detection); self-adjustment (response); adaptation (balance).

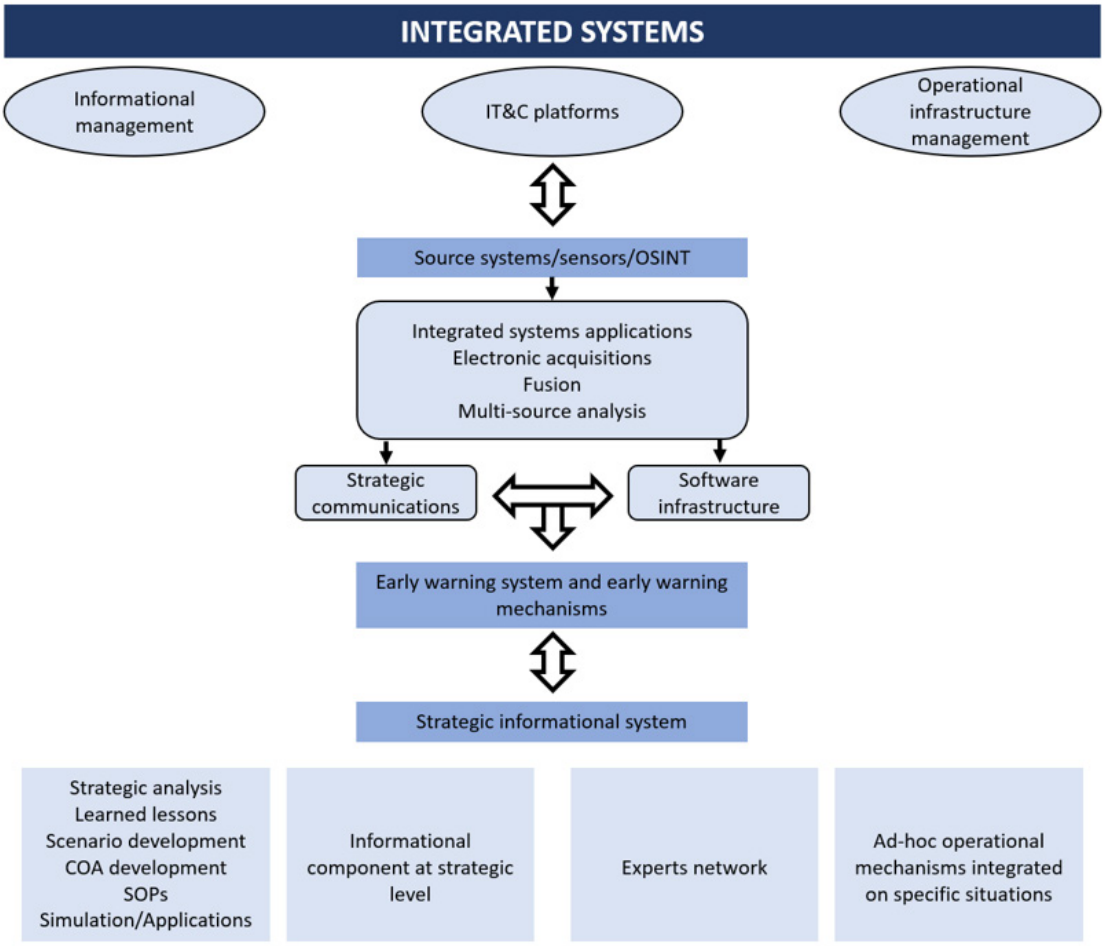

Figure 3. *Integrated systems approach*

Multipolar threats & vulnerabilities:

The hostile entity develops and infiltrates early vital elements capable of directing the behavior of the target social body in one direction or another through complex operational mechanisms with a wide variety of cover vectors (espionage, clandestine special operations agents, vectors of influence, support elements in the white area (institutions, state organizations, companies, media groups, influencers, etc.) gray (companies or dual entities with sight and clandestine activities, security companies or private military assistance employed in critical areas) or black (cross-border organized crime organisation , terrorist groups, etc.). Hostile entities use that cover tools and mechanisms to influence the decision and exploit the existential and emotional vulnerabilities of the population as a whole, targeting political, strategic, operational and tactical level.

CONCLUSION

By using the approach described in this article, namely the Integrated Info-Kinetic Operational System as a solution to counteract complex threat to peace, crisis or war there will be achieved: a proper organization and calibration of integrated countermeasures; disclosing of the mode of operation and means used by hostile entities; providing truthful information, relevant, conclusive and useful analysis and optimal measures to ensure, maintain and restore the balance of the social body in a critical crisis and /or war situation. As we have shown, this is an integrated approach based on the operational matrix concept which may be employed in different conflict and disruption situations.

REFERENCE LIST

Jensen, O. E. (1994). Information Warfare: Principles of Third-Wave War, Airpower Journal, 8(4), 35-43.
Libicki, M. (1995). What is Information Warfare?. National Defense University Press, ACIS 3. Washington, D.C.
NATO (1999). MC 422 Information Operations Policy, 12th of January 1999.
Power, R. (1996). CSI Special Report on Information Warfare, Computer Security Journal, 11(2), p. 63+.
United States Air Force (1998). Information Operations. Air Force Doctrine Document 2-5, 5 August 1998. Available at: <https://www.globalsecurity.org/military/library/policy/usaf/afdd/2-5/afdd2-5.pdf>.

Ilie BOTOȘ
Is a Romanian 4 star general (retired – 2016). Prior to 2016, Ilie BOTOȘ was Secretary of State Public Security Department in Ministry of Internal Affairs and Secretary of State National Security Component led by Vice Prime-Minister for National Security Issues. Between 2006-2013 he worked for the National Defense Ministry (Deputy Director of Defense Intelligence General Directorate, Chief of Military Intelligence Directorate and coordinator of Romanian Army Special Operations Component then General Director of Defense Intelligence General Directorate: rank – General).

His military and law experience are completed with educational activities as a lecturer at the most prestigious Law Faculties in Romania: Cluj-Napoca and Bucharest, within the Forensic Investigation Department. He also coordinated master courses in criminal intelligence at the Lucian Blaga University of Sibiu.