

FEATURES OF INTELLIGENCE RESOURCES MANAGEMENT IN CRISIS SITUATIONS

Ilie PAUN

Ministry of National Defense, Romania

The emergence of security conceptual systems can contribute to diminishing the differences between security consumers and security providers and hence to the latter's transformation into security holders/guarantors. In this respect, intelligence is a field in its own right that can make an important contribution to this. Thus, intelligence in general, and its plethora of forms are a salient part of the arsenal of asymmetrical conflicts. Consequently, acquiring, holding or using information as part of intelligence is the major stake of the aforementioned antagonisms.

Key words: *intelligence resources management, crisis situations, intelligence.*

1. INTRODUCTION

Specialized literature focuses on a great variety of events and processes relevant for the analyses and studies on intelligence resources management. However, there is a deficit in the scope of these analyses in terms of framing the organizational approach they take within the wider international security environment.

An overview of the current security architecture and its underlying crises and conflicts highlights that there have not been major changes in the basic requirements of intelligence resources management. Thus, the latter's main goals have remained the same: safeguarding information and personnel, uncovering hostile intentions of third party state actors or non-state actors, identifying the structures and scope of activities of the parties involved in a direct aggression, crisis situation, conflict or espionage.

A salient part of intelligence resources management consists in the collection, evaluation, and dispatch of information to planners or decision making bodies with a view to having it modeled and employed in making decisions in the political,

diplomatic, military or other security adjacent fields.

One basic truth in this respect was formulated by the the great Chinese strategist, Sun Tzu [1] who states that knowledge (i.e. information) allows intelligent governments and military leadership to outspeed adversaries and to benefit from great accomplishments. Such a statement remains just as important and relevant nowadays as it used to be two hundred years ago since it emphasizes the need for on time information supply in increasing the efficiency of human actions.

The evolutions and transformations in the international security environment along with the effects of globalization have led to significant changes in the security paradigm and hence to a reconfiguration of intelligence resources management.

In terms of their forecast ability in the field of intelligence resources management, Western powers have failed to grasp in due time assertive approaches challenging the international security environment. For example, the Russian Federation of States reviewed its strategy and doctrine, and inherently, made large

investments in the military field, conducted large scale modernization of its fighting technology, used of coercion/force in managing political situations as it was the case of the intervention in Georgia or Ukraine and employs energy weapons. Similarly, Western states could not anticipate the creation of the Islamic State of Irak and Levant (ISIL), which sets a precedent in the system of international relations since it consists in the transformation of a terrorist organization into a state.

Since all of the above highlight an extensive field to be covered, this article is to only focus on the transformations from within the international security environment, the factors that influence it, and subsequently the intelligence resources management process and the possibility of a system approach to it.

2. FEATURES OF INTELLIGENCE RESOURCES MANAGEMENT

The complexity of the international relations framework, the numerous actors and their multifarious relations along with the globalization phenomenon can generate the “dismantling” of the classical international architecture of the XX century. Some arguments in favor of the above statement are: the transformation of ISIL into a state, as well as the constant effort of the Russian Federation to get and maintain a stronghold within the network of international relations through actions similar to those during the Cold War that unequivocally dismiss a unipolar international order and are directed towards reestablishing Moscow’s areas of influence. The Russian military intervention in Georgia and Ukraine has unavoidably impacted the region. Thus, Moscow’s unilateral decision to reconfigure Georgia’s borders, Crimea’s “integration” into the Russian Federation and the involvement of undercover Russian forces in maintaining the crisis situation

in Ukraine have all been generating numerous implications that trespass the Black Sea and Caucasus areas.

In order to prevent and counter such evolutions, the international community and, most specifically, the Euro Atlantic community has belatedly reacted by adopting a number of decisions both at the level of the European Union and at NATO level during the Wales Summit in 2014.

In this respect, the concept of “hybrid warfare” was delineated as “the use of a wide array of overt and covert military, paramilitary and civilian measures as part of a highly integrated architecture” [2].

With a view to evolutions and trends like the ones mentioned above, the intelligence community should adequately and efficiently react by taking into account the factors that influence states’ interactions within the international security environment and that are molded by the relations among states/establishments, states’ external policies, their geographical and political commitments, demographic, technological and economic trends, their political and military structures, as well as the trends of the late XX and beginning of XXI centuries in fields like culture, religion, ideology, media and online environment.

One of the few endeavors that aim at listing and cataloguing intelligence related agencies and services is the Intelligence Resources Program (IRP) [3] currently unfolding under the authority of the Federation of American Scientists (FAS). This is dedicated to identifying and classifying the information available on any agency or intelligence service acting at national or international level. However, its webpage is but a limited unofficial database that, in the absence of quantitative studies on intelligence communities, can be though used for research and information.

One of the features of intelligence resources management is the manner of reacting to the evolutions in the

international security environment when it comes to avoiding strategic downturns [4] caused by opposing forces/adversaries through prospective studies. There are three guiding criteria to evaluate this type of approach: the prospective nature, the goal of reducing uncertainty and the proven relationship with intelligence resources management.

An aspect that is barely approached by specialized studies concerns the cooperation among different intelligence services both at national and international level. Nationally, the efficient cooperation among intelligence agencies and services can yield the effective use of information and, consequently, meeting national interests by delivering on time information to the military decision making entities. Internationally, an adequate legal framework is required that also pays its dues to issues like the sensitivity of information exchange, confidentiality and, most importantly, unaltered national interest. In this respect, at international level, the coordination of intelligence efforts is based on agreements, protocols, programs and projects. In this respect, it is worth mentioning international security organizations like UN, NATO, EU that, even though they have specific technological means such as satellites (i.e. EU) or surveillance and reconnaissance systems (i.e. the NATO Intelligence, Surveillance and Reconnaissance System), do not have structures specialized in information collection. For these, they rely on the cooperation of national intelligence services.

From a methodological and institutional point of view, the features of intelligence resources management are still under the influence of two main factors:

- **The human factor**, namely the quality of the personnel from the intelligence structures and its impact upon specific processes, relations and products. This factor is the one that ultimately makes the difference between intelligence systems and the

real situation in the field. On example in this respect I the involvement of Turkish intelligence services in the efforts made to release the group of Turkish diplomats from the Turkish Consulate in Mosul detained by ISIL.

- **The technical and material factor** is related to the upgrade/update level of the systems in this area. The information system from within intelligence agencies and services can be a simple or a complex one and can rely on one or several types of resources. The features of source exploitation by employing specific technical means are reflected in the management system.

Another salient feature is represented by the transformations of the terrorist phenomenon from the so-called "traditional terrorism" to extremely violent facets of it that make totalitarian claims based on an exacerbated religious approach rejecting any other outlooks on world order. Hence, the religious arguments underpinning this new form of terrorism rely on „radically different value systems, mechanisms of legitimation and justification, concepts of morality and, world view" [5]. Some of the underlying characteristics of this new type of phenomenon are: symbolic and theatrical displays, violent and non-discriminatory targeting of prospective victims, and perception of self righteousness as a result of a rigid interpretation of religious principles.

The revival of religious argumentation highlights an inherent error: denying the intrinsic rationality of the religious subconscious. Moreover, the importance of religion within contemporary terrorism is rendered by exploitation of faith in a world that has no other systems of values to rely on.

An important role in collecting information as part of contemporary fight against terrorism is played by Civil Military Cooperation (CIMIC) entities operating in conflict areas. However, CIMIC personnel should not play the primary role

in intelligence gathering. In this respect, the motto of each and every modern CIMIS structure deployed in the operational field is: "CIMIC is not Intelligence". Failure to act accordingly leads to distrust on behalf of friendly forces and civilian population. As a result of its specific missions and functions, CIMIC structures can collect information on the operational area, population, resources, relevant organizations and likely hostility that could hamper mission fulfillment both before and during deployment. The capacity of CIMIC structures to interact with organizations or key entities (local leaders, civil organizations, etc.) amplifies their importance as a source of information with a major role in obtaining information superiority in the area of operations. A well employed instrument by the Romanian forces deployed in theatres of operations to achieve CIMIC related goals is KLE (Key Leaders Engagement). However, apart from its advantages, this instrument can only be used in ongoing conflicts.

The actions undertaken against the new facets of terrorism require operational awareness and precise knowledge, along with the involvement of special forces and elements belonging to the intelligence community, as well as high tech means such the Unmanned Air Vehicles. Remote control weapons are to be used further on especially during the peak of military operations. However, there are at least two reasons for which the likelihood of successfully waging war without troops' heavy reliance on roles anchored in fundamental virtues is a but a phantasmagoria.

First, the use of remote controlled weaponry fundamentally depends on the technological prowess of the adversaries. Until now, drones and similar technology have been intensely used in asymmetric warfare against enemies with no solid anti aircraft or submarine systems and hence with limited capacity to wage

cyber or electronic warfare directed against satellites or communications infrastructure. This is one of the counter arguments concerning a nation's decision to abruptly scrap its existing force structure or to exclusively rely on unmanned devices.

Second, asymmetric warfare conducted nowadays by the US in Afghanistan or in North Africa and that seem to frame the typology of future wars, is focused on two goals that can be hardly met by exclusively robot based weaponry. Closing a conflict through long term political agreements requires either direct control over the territory –and that can be achieved through the now traditional territorial occupation- or nomination of a new government. Territorial occupation is based on the presence of troops on the ground. A new government requires gaining political support of civilian population by winning their "hearts and minds" and that, in its turn, may incur a more significant foreign presence of civilian and military that can better meet the aforementioned desideratum than remote control systems.

The arguments above underpin the likelihood of future involvement of manned forces in theatre of operations. Consequently, the preoccupation concerning the transformation of fundamental virtues as a result of using military remote control systems may seem preposterous. However, as Codreanu and MacCuish point out, "The very words used to define the [asymmetric] environment are self explanatory in terms of the types of actions required. An environment defined under this acronym [i.e. VUCA] cannot but be: under the influence of rapid change (the volatility component), averse to pursuing stable long term solutions, of a complexity that makes it difficult to pinpoint every nook and cranny of a given situation and/ or to develop a comprehensive outlook... Thus, concepts like "value" and "competence"... should be more comprehensive but as long

as the guiding principles for the behavior of the organization and of the individuals that make it work are flexibility, adaptability, simplicity, tolerance to fuzziness while viewing challenges as opportunities to “juggle with”, ability to keep pace with the changes in the environment, capacity and willingness to do more with less, consensus focused decisions requiring that centralized and decentralized approaches meet half way.”[6]

Concerning the typology of current conflicts (namely, the terrorist actions of ISIL), the use of remote control systems to collect information is enabled or disabled by the technology of the adversary. Thus, if in the case of the expansion of the Russian Federation, the latter’s technical and military raise challenges to pursuing such a goal. On the other hand, when tackling actions like those of the ISIL, such technology can be successfully employed.

Planning military actions in a virtual environment cannot become an advantage in the counter actions directed towards the “new facets of terrorism” in the absence of cultural and sociological approaches to detecting and recognizing targets. Therefore, reorienting the strategy against religious terrorism becomes a priority and consequently, the human factor defined as HUMINT acquires momentum since it is the most important source of information within intelligence resources management.

Additionally, the lack of experience and poor training of personnel in espionage have led to serious malfunctions of the intelligence system. As a result of these, there is a deficit in valuable information gathered from human sources at all levels of the armed forces, as well as an increase in collateral damages adjacently generated by insurgent “hunters”. Lack of proficiency in foreign languages and in interrogation techniques contributed to situations like the ones in which the uncovering of the techniques employed by the US

military, as well as the detention of individuals raising suspicions in Abu Graibh and Guantanamo, and their unfavorable wide range broadcast in the media led to the inclusion of US techniques among similar practices of representatives of the “new archaic order”. The effect of violent interrogation practices was not the one intended, namely the fast retrieval of vital strategic information, but a failure in infiltrating among insurgents.

3. CONCLUSIONS

The international security environment is molded by the efforts of the state and non-state actors to gain access to resources, by the hegemonic tendencies of some of the players who are already or are to become great powers, as well as by the inherent strategic partnerships or coalitions.

Terrorism is one of the major factors influencing the international security environment and as such it has undergone major transformations triggered by religious fanaticism. One example in this respect is ISIL and its fierce attacks and executions in Syria, Iraq and Algeria. A rational analytical perspective on such events, anchored in a costs-benefits type of thinking, cannot grasp the goals serving such an approach. However, what stands to reason is that there is an intrinsic logic of religious terrorism.

A new power balance prefigured by the ascension of states like India and China, as well as by the hegemonic tendencies of Russia is to impact both directly and indirectly the regional and global environment, and, inherently, the Euro Atlantic intelligence community. Therefore, necessary transformation/adaptation measures become mandatory

Information resources management and the intelligence field are to still be equally under the influence of the human factor and of the technical and material ones. Moreover, specific situations that require a

symbiosis of the two and hence of the underlying efforts are to emerge.

On short and medium term states are still to be the main actors having access to resources and thus legitimating the field of information resources management.

From an institutional perspective, an excessive geographical and organizational development generates a wide information spectrum correlated with systematization attempts from a methodological point of view. However, the latter places constraints on the instruments to be used and imposes preserving secrecy and hence it yields negative effects in adequately supporting and developing the activities of the intelligence community.

Recent developments in the field of security pinpoint the fact that decisions under uncertainty, rational actions, group think or game theory are to play an important role in information resources management.

REFERENCES

[1] Sun Tzu (2003) *The Art of War*, Barnes & Noble Inc. New-York, p. 58.
 [2] Paragraph 13 from the Wales Summit Declaration issued by the Heads of States and Governments during the NATO Summit unfolded between 4 and 5 September 2014 in Wales, source: <http://www.mae.ro/node/28465>, last retrieved September 10, 2014.
 [3] <http://www.fas.org/irp/world/index.html>, last retrieved August 16, 2014.
 [4] Costinel ANUȚA, Studiile prospective și analiza de intelligence: de la managementul riscului la reducerea incertitudinii, (Romanian for Prospective Studies and intelligence analysis: from Risk Management to Uncertainty Reduction) in George MAIOR, Ionel NIȚU (coord.) (2013) *Ars Analitica*, București: RAO, pp.230-246.
 [5] Bruce Hoffman (1998) *Inside Terrorism*, Columbia University Press, p.87
 [6] Codreanu, A., MacCuish MILITARY ETHICAL META-KNOWLEDGE AND INDOOR TEAM BUILDING GAMES. FROM PROMISE TO PRAXIS, paper presented during the 4th Annual Euro-ISME Conference 2014 "Didactics of Military Ethics. From Theory to Practice", Koblenz, Germany.

[7] FM2-0, Intelligence, Headquarters Department Of Army, USA, March 2010JP2.0, Joint Intelligence, Defence Department, June 2007, last retrieved August 2014.

[8] JP2-01, Joint and National Intelligence Support to Military Operations, Washington DC, SUA, October 2004, last retrieved August 2014.

[9] JP 2-01.3, Joint Intelligence Preparation of the Operational Environment, Washington DC, SUA, 2009, last retrieved August 2014.

[10] Ilie, Marin (ed.) (2007) *Masa Rotundă "Sensuri ale managementului integrat al apărării"* (Romanian for round table on Meanings of Defense Integrated Management), Brașov, 23 July 2007, București: "Carol I" National Defense University.

[11] Nicolaescu, Gheorghe, Simileanu, Vasile (2005) *Restructurarea sistemelor informaționale* (Romanian for Restructuring information systems), București: Top Form.

[12] Savu, Gheorghe (2000) *Metode moderne de prelucrare și distribuire a informațiilor militare obținute prin cercetare, destinate conducerii strategice la pace și pe timp de război*, teză de doctorat, Editura Academiei de Înalte Studii Militare, București.

[13] Williams, Reginald J., Kendall, Rocky (2002) *Operationalizing Effects-Based Operations*, an EBO Methodology Based on Joint Doctrine, USA.

[14] Wilson, Michael - *Towards an Ontology of Integrated Intelligence and Conflict*, Decision Support Systems Inc, April 2001.

[15] <https://www.cia.gov/library/center-for-the-study-of-intelligence/index.html>.

[16] <http://www.ssu.gov.ua/sbu/control/en/publish>.

[17] <http://www.dia.mil/college/publications/>.

[18] <http://www.centerforintelligencestudies.org/>.

[19] <http://www.dtic.mil/>.

[20] <http://www.globalsecurity.org>.

[21] www.defenceandstrategy.eu.

[22] www.departmentofintelligence.com.

[23] www.nato.int.

[24] www.globalsecurity.com.

[25] www.foreignaffairs.org.

[26] www.mae.ro/node/28465.

ACKNOWLEDGMENT

This work was possible with the financial support of the Sectoral Operational Programme for Human Resources Development 2007-2013, co-financed by the European Social Fund, under the project number POSDRU/159/1.5/S/138822 with the title "Transnational network of integrated management of intelligent doctoral and postdoctoral research in the fields of Military Science, Security and Intelligence, Public order and National Security – Continuous formation programme for elite researchers" – "SmartSPODAS".