DOI: 10.53477/2971-8813-22-42

CHALLENGES IN USING IRS STRUCTURES IN UNCONVENTIONAL OPERATIONS IN THE CURRENT SECURITY CONTEXT

Cristian-Octavian STANCIU
Colonel, Professor, Ph.D., "Carol I"National Defence University
cristianstanciu73@yahoo.com

Valeriu-Adrian JIANU
Ph.D., "Carol I" National Defence University
adi_jianu_74@yahoo.com

Abstract: *The unpredictability of the security environment, amplified by the current conflict in Ukraine, the increasing presence of unconventional operations in modern conflicts, create the premises for a real challenge in the use of ISR structures in support of decision makers at all levels. The current Russian-Ukrainian conflict demonstrates the existence of a broad unconventional approach both before and during the conduct of classical military action. The acceleration of the deteriorating economic relations between the Euro-Atlantic states on the one hand and the Russian Federation on the other, but also the effects of the pandemic will contribute to the continuation of tensions between the two blocs, as these appear to have an economic, energetic, sanitary and social agenda to surpass the moment and redirect and channel their own resources towards solving problems of an internal nature.The definition of unconventional operations is a topic of debate for military theorists in all modern armies, the line between conventional (classical) and unconventional (non-classical) being increasingly difficult to achieve.For ISR elements, the combination of hybrid, asymmetric, network-based, mosaic-type information operations is a turning point in trying to change the paradigm of information support in all confrontational environments, in the current security context. The diversity of unconventional operations, the permanent emergence of new features and different approaches of some state or non-state actors, represent a real challenge for ISR structures, both from a national and allied perspective.*

Keywords: *Intelligence; Surveillance; Reconnnaissance; Unconventional operations.*

Introduction

Russia's invasion of Ukraine on February 24th will inevitably lead to a reconfiguration of the global and regional security paradigm, which will be accentuated by the revitalization of competition between both state and non-state parties, and creates the premise for maintaining it, at least for the short term of the unpredictability of the current security environment.

In the *National Defense Strategy of the country for the period 2020-2024*, reference is made to the tendencies to establish conjunctural alliances, with emphasis on the activities of state actors on a bilateral level. The same strategy shows that *"the exponential trend of developing emerging technologies (5G, artificial intelligence, big data, Internet of Things, cloud and smart computing)"* (Administration 2020) leads to increased measures of collection, processing, dissemination and security of information.

The hypothesis I started from is the need to understand whether in a security context unanimously accepted as extremely volatile, ISR structures at all hierarchical levels and in all categories of forces can adapt in a flexible and robust way thus to contribute in real time, with the necessary information support for military decision-makers.

For this, our study will analyze the main directions of action specific to ISR structures in the main unconventional operations using as research methods the study of NATO and national documents and doctrines, historical investigation, the method of observation.

Unconventional – in the current security context

On the one hand, the definition of unconventional operations is a topic of debate for military theorists in all modern armies, the line between conventional (classical) and unconventional (non-classical) being increasingly difficult to achieve. On the other hand, in the spectrum of unconventional operations, a close interdependence and interrelationship can be observed, so that the delimitation from the conceptual point of view is increasingly difficult. The initiator of unconventional operations is in principle focused on the outcome of the action and less on the type of action being taken to achieve the intended purpose.

The concept of unconventional warfare is not new, it is defined in American literature as a war that includes *"activities to allow a resistance or insurgency movement to coerce, undermine, or overthrow a government or power, occupant through operations carried out by or with an illegal, auxiliary or guerrilla warfare in a prohibited area. "* (JP 1-02 Department of Defense Dictionary of Military and Associated Terms 2012)

The war in Ukraine, the acceleration of the deteriorating economic relations between the Euro-Atlantic states on the one hand and the Russian Federation on the other, but also the effects of the pandemic will contribute to the continuation of tensions between the two blocs, as these appear to have an economic, energetic, sanitary and social agenda to surpass the moment and redirect and channel their own resources towards solving problems of an internal nature.

This "special military operation" defined by Russia shows that, both before and during the conventional actions, there are a number of unconventional operations tested during the military operations in Georgia and Crimea and revalidated in the current operations in Ukraine.

We can conclude that, at this moment, there is no unanimously accepted delimitation between military thinkers regarding the typology of unconventional operations. Therefore, in this approach we aimed to analyze from the ISR perspective the main non-classical operations identified so far and with a significant impact on the conduct of combat actions, namely: network-based operations, effects, operations specific to information warfare, hybrid, asymmetric, mosaic operations.

ISR structures in support of unconventional operations

By definition, network-based warfare is a concept that *"generates increased combat power through the informational integration of sensors, decision makers and performers, in order to know the theater of operations, increase driving speed, accelerate the pace of operations, intensify lethal effects, emphasizing protection and achieving a certain degree of self-synchronization".* (Alberts D. 2000)

In this type of operation, ISR systems are fully integrated, by complementing technical sensors on certain platforms with human sensors to create a "system of systems" capable of transforming information superiority into decision-making superiority. However, technical limitations, differences in interoperability, insufficient knowledge of the opponent and surprise elements can hamper the actions of SRI structures.

According to the definition, effects-based operations have the role of *"producing effects that impose the desired political results"* (Saunders-Newton D. 2002) and represent the classic principle in military science called the principle of "economy of forces and means" with the help of tools through which *"those who are experts in the art of war subdue the enemy army without a fight."* (Tzu 2004)

In order for the effects to be as expected, the decision makers have the appropriate, necessary information in terms of the actions of the ISR structures. In this type of operation,

ISR structures rigorously substantiate the informative preparation of the operational environment and represent an essential part of the targeting process, with both valences: lethal or non-lethal.

Actions taken to achieve *"information superiority in support of the national military strategy by degrading the opponent's information and information systems, while positively influencing and protecting one's own information and information systems"* (Vizitiu C. 2008) can be defined as actions specific to the information war.

Direct examples of information warfare are present today in the war in Ukraine, where the struggle for information superiority is evident. For ISR structures, the challenge of this type of operation is given by the ability to collect, centralize, analyze and exploit information primarily from open sources. We see today, a general infusion of news, on media or social media channels, whether they are real or not, the purpose of some being misinformation or misleading. In order for the information to be true, the elements of ISR are engaged in an extensive process of analysis and dissemination based on the "need to know" principle.

According to some authors, in military conflicts in which not only military forces are confronted, but also other structures, such as non-military, mixed, military-civilian, asymmetries predominate. (Ghe. 2021) If conventional operations aim to concentrate forces at the dominant point in order to execute the attack quickly and achieve victory in a short time and with minimal losses, asymmetric operations aim at dispersing forces, concealing actions, prolonging the duration of actions, time becoming a real weapon in this type of operation. (C., The future of conflict - asymmetric and hybrid operations 2012)

In asymmetric operations, the civilian population having an essential role for SRI structures, the main challenge is determined primarily by the contribution of HUMINT in information support. To this end, the preparation of ISR elements in the field must be carried out in peacetime, with the increased involvement of specialists in the field. Therefore, we consider it necessary to prepare the elements of ISR in the interaction with the population in different social environments. Therefore, the human sensor in this type of operation can be superior to the technical one, through a specific training in the field of human intelligence.

NATO has defined hybrid threats as threats that are launched by *"adversaries who have the ability to simultaneously use conventional and unconventional means to achieve their goals,"* (Bi-SC Input to a New NATO Capstone Concept for the Military Contribution to Countering Hybrid Threats no.1500/CPPCAM/FCR/10-270038 2021) and in the first analysis of the European Center of Excellence to Combat Hybrid Threats, inaugurated in 2017, the current security environment is characterized as *"an era of hybrid threat."* (Lehaci N. 2019)

The direct example of the hybrid type operations used by the Russian Federation can be found in recent history both in the war in Georgia, but especially in the purpose of annexing the Crimean Peninsula. We find the same approach in the self-proclaimed independent regions of Donetsk and Lugansk.

For the ISR elements, the challenges in this type of operations are multiple, as the scope of hybrid warfare is extremely varied, and to understand it requires a detailed analysis of the concept of PMESII (political, military, economic, social, infrastructure, information). For this, we support the exchange of information between the categories of forces, but also inter-institutional, through a synchronized matrix at national level, both from a military and non-military perspective.

For example, American theorists have proposed, in the case of the hybrid threat, the complex IPB that describes six stages (Pike T. 2022): defining the operational environment; description of the effects of the political, cultural and social system; evaluation of majority social groups; estimating the interactions between social groups; assessment of population behavior.

In response to the Chinese and Russian anti-access and areal interdictions (A2 / AD) systems, US researchers have launched the "mosaic" concept of warfare, which aims to "bring together all the individual battle platforms." *to establish a complete picture of a quick and decisive victory against any aggressor, as well as to develop an appropriate package of skills."* (Ioniţă C. 2021)

Today, scientists are developing innovative concepts such as machine learning artificial intelligence systems called Generative Pre-trained Transformer 3 / GPT-3. (Ioniţă C., The latest technological developments in the mosaic war 2021) Some theorists also mention expert systems, such as the "AMUID" system (provides real-time information, integrates all information received through research reports, assists the commander in battlefield analysis) and the "ANALYST" system. (Able to investigate critical situations in the area of operations). (Stanciu C. 2016)

In order to meet the challenges of this new type of war, IRS structures are required to maintain the level of procurement in line with operational requirements. The development of technology is causing rapid reactions in the approach to endowment with smart means, as the acquisition of systems may be too late and may be inefficient in relation to information requirements. Therefore, we believe that today it is necessary to purchase less expensive systems but in as large a number as possible and in the shortest possible time to equip and streamline ISR structures.

We can conclude that the diversity of unconventional operations, the permanent emergence of new features and different approaches of some state or non-state actors, represent a real challenge for ISR structures, both from a national and allied perspective.

Conclusions

In the recent conflicts, and especially in the current war in Ukraine, we have witnessed an increase in all types of unconventional operations, operations performed before or during classical operations, following their evolution even after the end of combat-type actions. Unconventional operations hinder the actions of ISR structures, structures trained to support decision-makers, especially in conventional actions.

Starting from the general characteristics of the listed unconventional actions, we can conclude that a doctrinal reform is needed in the conceptual paradigm of ISR, so that expertise especially in the fields of collection disciplines (such as HUMINT, IMINT, SIGINT, OSINT, etc.) be a permanent concern in the area of preparation of structures from all categories of forces.

The cooperation of ISR structures in the ground forces with the naval and air forces and the exchange of information, in order to avoid redundant, outdated or unnecessary information, as well as to avoid clutter of repetitive information, can be achieved by intensifying joint training, in particular continuously throughout a year of training.

On the other hand, the integration of national ISR systems into alliance ISR systems can help increase interoperability and the level of expertise between existing capabilities.

At the same time, we propose the co-optation of experts in the analysis of information for the capitalization of the entire information cycle, by setting up support cells affiliated to the organic ISR structures on the national territory.

Inter-institutional cooperation between SNAOPSN structures and ISR structures belonging to the Ministry of National Defense can be carried out in large-scale exercises carried out on the national territory with the interconnection of existing sensors and systems so that the information reaches the beneficiary in the shortest time.

The current experience of supporting refugees in Ukraine demonstrates the inter-agency capacity to use information for the benefit of the structures involved, but also the importance of involving governmental or non-governmental organizations.

From an endowment perspective, current historical experience shows that certain ISR systems can provide the information support needed by decision makers, and better systems can have lethal effects on a superior adversary in terms of their capabilities.

Bibliography

Alberts, D. 2000. *Network Centric Warfare*, 2nd Edition,

Ioniţă, C., C. *The latest technological developments in the mosaic war, Strategic Impact Magazine, no.1/2021.*

JP 1-02 *Department of Defense Dictionary of Military and Associated Terms*, 8 November 2010 (as amended through 15 August 2012).

Lehaci N., T. 2019. *Intelligence Component in Combating Hybrid Threats*, Ed. UNAp, Bucharest.

Saunders-Newton D., Frank B.A., *Effects-Based Operations: Building the Analytic Tools*, Defense Horizons, no.19/2002, Washington DC.

Stanciu C. 2016. The future of conflict - asymmetric and hybrid operations, Ed. UNAp, Bucharest.

Sun Tzu. 2004. *The Art of War*, Antet Publishing House, Oradea.

Visit C., I. 2008. *Electronic Warfare, Modern Aspects*, vol. 2, Military Technical Academy Publishing House, Bucharest.

Web Sources:

Bi-SC *Input to a New NATO Capstone Concept for the Military Contribution to Countering Hybrid Threats* no.1500/CPPCAM/FCR/10-270038, available online at http://www.act.nato.int/images/stories/events/2010/20100826_bi-sc_cht.pdf, accessed on 31.03.2022.

Văduva, Ghe., Is war knocking on our door? available online at www.iss.ucdc.ro/studii-pdf/bate războiul la uşă, accessed on 31.03.2022.

Pike, T., Brown E., IPB Small Wars Journal, 2016, available online at http://smallwarsjournal.com/jml/art/complex-intelligence-preparation-of the – battlefield-in-ukrainian-antiterorism-operations, accessed on 31.03.2022.