DE GRUYTER OPEN

Land Forces Academy Review
Vol. XXIII, No 1(89), 2018

REDEFINING DOCTRINE CONCEPTS IN MODERN MILITARY ACTIONS

Mihai-Marcel NEAG
"Nicolae Bălcescu" Land Forces Academy, Sibiu, Romania
mmneag@yahoo.com

ABSTRACT

The mosaic approach to conflict requires redefinition of some doctrinal concepts that can influence the way in which the response to the risks and threats to the state of security, the future of military actions and the acceptance that the technological development will be a factor for the success of the wars future.

The issues addressed could be important elements in the architecture of a possible future strategic concept of integrated use of the basic elements of national power - diplomatic, informational, military and economic. At the same time, the results of this theoretical approach can contribute, as a reference point, to proposing viable and innovative doctrinal and operational solutions to counteract aggressions to national security, regardless of their nature or origin.

KEYWORDS: operational environment, military business revolution, doctrinal concepts, joint operation, asymmetric war

1. Introduction

The doctrinal concepts have the role of explaining, justifying and arguing the positions and attitudes of the military leaders towards the manifestation of the contemporary military phenomenon, of prospecting the directions of the development of the military system in which they operate and of proposing directions of action. Their elaboration is influenced by the specific conditions in the operational environment, the level of knowledge of the contents and the forms of manifestation of the risks, the threats and the vulnerabilities of security, as well as the requirements imposed by the technological progress.

The events that characterize the current security environment have confirmed that insecurity, uncertainty and unpredictability persist. It is therefore necessary to rethink the geopolitical and geostrategic environment in terms of the interests, diversity of conventional and unconventional, asymmetric and hybrid threats, actors involved, and reconfigure new strategies to effectively manage these complex situations.

The operational environment, as a component of the security environment, is increasingly dynamic and tends to diversify and amplify crisis situations and conflicts. The integration of information, virtual, psychological and media space into the operational environment diversifies the sphere of conflict through the emergence of new doctrinal concepts.

There is a change of paradigm at the level of military art, which has the role of adopting a new vision in the elaboration of new concepts of efficient use of the structures of forces in the whole range of military actions at strategic, operative and

DOI: 10.2478/raft-2018-0003

tactical level, to be connected to the fields of the revolution in military affairs – technological, doctrinal and organizational.

The informational era provided the necessary framework for the revolution in military affairs, which in turn changed profoundly how to approach the conflict, in the conditions of diversification of threats, actors, strategies, tactics and means used in military actions. In this sense, the weak response to highly technologically advanced military actions was not to accept the situation but to find ways and means to compensate for its superiority and to eliminate the effects of the gap between cutting-edge technologies and information technology. Thus, the asymmetry emerged that compensated for disimetry and manifested itself in various ways in military conflicts. Typical forms of asymmetry are insurgency-counterinsurgency, war-guerrilla warfare, and terrorist war-the war against terrorism.

Another way to redefine conflict is materialized in the concept of information warfare/information operations. The concept of informational warfare/information operations opens a broad horizon of manifestation of non-kinetic actions, both in the physical environment, but especially in the informational, virtual, psychological and media space. The effectiveness of informational warfare/information operations is materialized in informational superiority, which generates decisional efficiency and strengthens the moral and actional component.

The hybrid war considered to be the war of the future is the expression of modernity that combines a wide range of conventional, unconventional, asymmetric and cybernetic strategies, tactics, methods and means to achieve military and military objectives. In this context, there are concepts associated with hybrid war defining composite war, proxy war and legal/legally war.

This mosaic approach to conflict requires redefining some doctrinal concepts on the future of military action and accepting the idea that technological development will be a factor in potentiating success in future wars.

2. Comprehensive Approach within the Legislative Framework and the Need to Redefine Some Doctrinal Concepts

Comprehensive approach is a process of interpreting and deciphering all the interests that occur in an operating environment to resolve crisis and/or conflict situations. This approach allows for a more credible engagement of civilian-military capabilities and offers the possibility of accurately determining the effects of the operational trinomial environment (troops-population-opponent) in which the population element creates contexts difficult to predict.

The Lisbon Strategic Concept emphasizes the importance of making the Alliance more effective by addressing politically, civilian and military elements in crisis management (NATO, 2010, p. 6). Among the possible types of aggression towards the Alliance are explicitly or implicitly identified: nuclear aggression, terrorist aggression, criminal aggression, cyber aggression, resource aggression, space aggression and ecological aggression (NATO, 2010, art. 9-15). However, risks and threats based on "soft" media, from the field of information, psychological, media, cultural, religious, imagistic, symbolic, moral aggression, which can create vulnerability to the Alliance due to lack of coordination in the mentioned areas, are not addressed.

The national defense strategy of the country for the period 2015-2019, reflects the need to promote an *extended national security* concept. The strategy has an integrative and multidimensional approach in which the defense dimension combines and balances with a number of other

dimensions – public order; intelligence, counter-information and security; diplomacy; crisis management; education, health and demography (Presidential Administration, 2015, p. 5). These issues are motivated by ensuring convergence with European security principles. It is stated that national security objectives aim at "developing capabilities to combat asymmetric threats" (Presidential Administration, 2015, p. 9) and admit *"the difficulty of delimiting the classical threats from asymmetric and hybrid threats"* (Presidential Administration, 2015, p. 11).

The strategy recognizes that the inter-institutional response to crisis situations is affected by the precariousness of resources and the incoherence in managing the various types of risk. This vulnerability becomes even more important if we refer to the interoperability capability of the various state institutions that have to act in case of asymmetric and hybrid threats (Presidential Administration, 2015, p. 16). It is accepted as action directions *"the development of capabilities* necessary to react in case of asymmetric and hybrid threats", "*identifying and counteracting hybrid asymmetric actions"* and *"developing the security culture"* (Presidential Administration, 2015, pp. 18-21). The responsibility for counteracting unconventional or hybrid threats rests with information, counter-information and security, and to a lesser extent it is involved in defense, an aspect that does not create a solid legal framework for close inter-institutional cooperation at peace, as well as crisis and war.

In the *White Paper of Defense*, a level of ambition is formulated which states that *"the Romanian Armed Forces must be able (...) to plan and conduct a strategic defense operation on the national territory, of a common type, until the deployment of the main allied forces"* (MoND, 2017). In order to accomplish the missions, the document proposes as a solution the development of specific capabilities in peacetime, but the mechanisms for transposition do not identify, as no priorities are identified.

The Military Strategy of Romania states unequivocally: *"The military strategy defines the strategic and operational principles and concepts that ensure the achievement of the national military objectives and the established missions"* (MoND, 2016). Strategic and operational concepts, in the sense of this strategy, describe how armed forces are committed to achieving the set goals. In this context there is a need to clarify some doctrinaire concepts, especially as the directions for achieving a lasting transformation of the military body explicitly support the development of the concept of counteracting the hybrid war.

Between the theoretical support of concepts and the provision of the necessary capabilities to support military action there is a fault that may be a vulnerability of the moment, but which can be overcome by further clarification of existing theories and by reorganizing what we now have.

3. Asymmetric War

In the international security environment, marked by conflict, uncertainty and diversification of the threats and actors involved, the effect of the military revolution was to create the first breach in the armed struggle by transforming symmetry into disimetry (disproportion), so that the existing technological gap puts the opponent in the inability to act effectively. In this way, the concept of *disproportionate warfare* emerged, ensuring informational, decisional and actional superiority and guaranteeing success in the whole range of military actions.

This was the context in which conventional warfare, through the integration and interconnection of cutting-edge technologies and information technology, turned into super-technologically and ultra-fast conventional warfare, war-based warfare, a war that

supports the effect. Types of wars based on advanced technologies have embraced the concept of dysmetric (disproportionate) warfare in which a party totally dominates the other party involved in the conflict and provides the necessary conditions for achieving the proposed goals with minimal losses and within a short period of time.

The dysimetric war has overturned the paradigm of the balance between the actors involved, reduced uncertainty, generated dominance in the full spectrum, secured the initiative and freedom of action for its own forces, and restricted the possibility of an appropriate response from the opponent. Thus, the response effect in the manifestation of the advantages of the revolution in the military field, concerned the following aspects taken into account by the stakeholders:

- accepting disproportionality and losing conditions by failing to meet the proposed objectives, which is hard to accept for US and NATO opponents;
- re-launching the arms race, allocating the necessary resources for the doctrinal, organizational and technological development of the military dimension, which implies a budgetary effort that is often difficult to bear;
- asymmetric reaction by exploiting the opponent's vulnerabilities and reducing the technological advantage across the spectrum of confrontation.

If disimetry is the consequence of reaping the benefits of the military revolution, asymmetry is the result of the weaker reaction, which, through atypical strategies, methods and procedures, attempts to compensate for the superiority of the opponent and to eliminate the effects of the gap between cutting-edge technologies and information technology.

In this sense, the asymmetric war contains a set of atypical, irregular actions that compensate disproportionality, thus defeating defeat and disregarding the rules of the classic game. Thus, I appreciate that asymmetric war has its origins in disimetry, which in turn is generated by the technological gaps existing in the security environment, which is vulnerable to informational age societies and permanently confronts the state of conflict. This systemic approach to conflict provides us with the theoretical and methodological framework in which we appreciate that the first breach in symmetry, in proportionality, was made by the military revolution that generated disparity, disproportionality, and the second breach aimed at canceling the benefits of disimetry through strategies, asymmetrical, atypical and irregular tactics and techniques.

In this context, I believe that by the disimetry the victory was facilitated by the performer, but it gave rise to the asymmetry in which the weak exploits the vulnerabilities of the strong one, imposing its own strategy and its own rules that do not respect the classical principles of conduct of the conflict. Therefore, *"asymmetric actions are complexly complex, usually by non-state actors, carried out in a hostile operational environment, with long-term consequences and seriously eroding the institutions and values of modern societies"* (Văduva, 2007, p. 13). Technological performances of developed countries that have stepped into the informational era demonstrated in military conflicts have prompted opponents to adopt the asymmetric approach, ie to abolish the benefits of superiority in full spectrum and to exploit the vulnerabilities of the adverse side.

In the asymmetric war, it faces two unequal forces, both by the military means at its disposal and by the way they are used. Asymmetric warfare is developing continuously, both in physical space, in the electromagnetic and virtual environment, appreciating the vital role of information in generating knowledge to transform the superiority of the opponent into weakness, exploiting vulnerabilities and generating large losses.

As conflicts become asymmetrical without complying with the rules and principles of the armed struggle, some dilemmas are created that address the following aspects: the need to adapt the strategy to the methods and procedures of the opponent to counteract asymmetry with atypical processes; the use of conventional and unconventional (special) forces to neutralize asymmetric actors; the flexible use of diplomatic, economic, informational and military instruments of power, and the consideration of the civilian population, which becomes an important actor in the conflict equation (Ghigiu, 2011). Effective solving of these dilemmas will allow for a correct approach to asymmetric conflicts by understanding that not neutralizing or destroying asymmetric actors, their bases and infrastructure elements is the main element of success, but defeating their will to fight and gaining support from the population become objective which must be met.

Asymmetric conflicts have transformed the conventional war based on cutting-edge technologies and information technology, namely, on disimetry, into new types of wars, war in the middle of the population, limited war, irregular war, low intensity war, preemption war, war against terrorism, insurgency war, guerrilla, military operations other than war, etc.

This panoply of war concepts, given by asymmetry, directs the conflict in the sphere of continuous warfare, in which reactions are based on violence, nonviolence, terror, cyber attacks, atypical actions designed to maintain a state of uncertainty that affects the morale of the opponent and to make it bearable losses. In this context, the insurgency-counterinsurgency war, the guerrilla war-guerrilla war and the terrorist war – the war against terrorism are asymmetric reaction forms.

4. Information Warfare and Information Operations

The information warfare is a product of an informational era that exploits the technological developments recorded in the peak areas represented by communications, electronics and computers. If information was characterized by widespread use, including in the military, advanced scientific research, and information technology, the information warfare as a beneficiary of these achievements uses information as a target-oriented weapon (objectives).

The information warfare integrates a set of offensive and defensive actions that aim to achieve informational superiority, maintain decision-making, and potentiate their own actions. The informational warfare that supports the communications and information system, ie the information infrastructure, is carried out in order to influence, affect or neutralize the information and information systems of the opponent, while protecting and capitalizing on its own information-based systems.

In this context, the dual character of the definition of the concept of information warfare, expressed as follows:

- for the adversary – affecting, influencing or neutralizing information and information systems in order to affect the will, to make erroneous decisions and reactive action;
- for their own forces – protection of information and information systems, valorisation of information products through the achievement of informational and decisional superiority, maintenance of the initiative and proactive action.

Depending on the aim pursued (Mureşan, 2004), information warfare is carried out for information (achievement of domination, superiority, knowledge and understanding) through information (information cycle, decisional efficiency) and against information (protection, anti-

manipulation measures). Thus, there are relevant aspects of the information warfare oriented towards knowledge and especially the understanding of the situation, preventing the opponent from knowing and acting in a timely manner and distorting reality, forcing him to operate with erroneous data and information. These aspects call for *"the creation of an impenetrable, active, flexible, interoperable and offensive information system that ensures information superiority through kinetic and non-kinetic actions"* (Frunzeti, 2012, p. 11).

In this context, I appreciate that information warfare, as a dimension of military action based on information and information technology, falls into the category of non-kinetic, non-contact strategies, and is also an intermediate between conventional and unconventional operations.

Within the information society, estimating the strength and viability of the national security system without considering information systems and how information is exploited is a major risk because the center of weight of the actions tends to move from the material dimension to the information dimension. There is a distinction between the phrase "the war of the informational era" and the "information warfare" in the literature. The Informational Age War uses information technology as a means of achieving a time and force saving in military operations and affects all combat activities. By contrast, information warfare sees information itself as a special domain, as a powerful weapon but also as a lucrative goal. The information is still technology-independent. Nevertheless, the information age technology transforms a theoretical possibility into a real fact: direct manipulation of information available to the opponent.

The essential features of the informational war that highlight its extremely complex nature are: difficulty in specifying opponents; the absence of geographic and/or temporal boundaries; the multitude of targets; the lack of rapid ways of remedying the consequences it produces; the use of relatively simple, cheap and widespread technology; the difficulty of establishing clear and precise responsibilities for domain management; relatively low costs of informational operations in relation to the results that can be obtained; increased handling possibilities; the disappearance of the differences between command levels.

If information warfare is a general concept that includes capabilities for influencing actor's behavior and affecting or neutralizing information and its functional systems in various fields of activity, information operations (INFO OPS) are the applicative part and express ways of planning, preparation, execution and evaluation of a specific action to achieve a particular goal. The essence of the concept of information operations lies in the ability of one's own system to achieve and maintain informational superiority across the spectrum of military action and integrates objectives, effects, activities, functional areas and specific capabilities.

Informational superiority means the ability of a system that integrates information technology to collect, process and disseminate a continuous flow of information and information products while distorting or forbidding the ability of the opponent to do the same. In other words, information superiority supports maintaining and capitalizing on its own initiative and freedom of action through permanent knowledge and understanding of the situation, while uncertainty is induced to the adversary as an accepted state in the governing system and its strength. The functional areas of INFO OPS include (Zecheru and Saracu, 2015, p. 29): psychological operations (PSYOPS), Operational Security (OPSEC), Information Security (INFOSEC), diversion operations (MILDEC), Electronic Warfare (EW),

Physical Destruction, operations in computer networks (OCN). Related fields of INFO OPS are public information/public relations (PI/PR) and civil-military actions (CIMIC).

If we exclude physical destruction, INFO OPS falls into the category of non-kinetic actions aimed at influencing target groups, distorting information and annihilating the opponent's information systems without using physical force. During the war, INFO OPS will support any form of conflict approach and prepare the adoption of future kinetic actions, thus completing the panoply of activities in the informational operational environment. Being a new environment, devoid of laws and binding rules for all users, circulating and storing information through its infrastructure has begun to raise real problems. Taking into account all the above mentioned, it can be stated that the cyber war is the most complex and multilateral form of attack on information in order to acquire informational superiority. Its main purpose is to ensure the separation of the actions of the committed forces, institutions and the civilian population.

5. The Hybrid War

The term "hybrid war" is a concept that does not have a unanimously accepted definition, but some states are reviewing their military doctrines or security strategies. In military language, the *hybrid* phrase is used to encompass the increased complexity of current operations and the multitude of actors involved (Department of the Army, 2011). In the concept of NATO, "hybrid war" is a concept that refers to an extended range of hostile actions, in which the military force is only a small part, and which are executed in concert as part of a flexible strategy with long-term goals (Hotnews, 2014). Thus, the operational environment becomes the place where various types of conventional, unconventional, asymmetric actions are combined, with regular forces, special forces, and irregular forces (insurgents, fanatical and religious factions, mercenaries).

This made it possible to move from the cyclical approach of military action to the mosaic approach, which takes into account an amalgam of situations and confrontations at the intersection between conventional, unconventional and asymmetric. From this perspective, anticipation and technological development are decisive factors in the preparation, deployment and modeling of military action. Also, the future of the armed struggle will be marked by the combination, integration and greater interconnection of its levels, the types of actions currently taking place, systems and technologies, ie hybridity.

The complex and confusing nature of hybridity has proven to be particularly difficult to integrate into classical threat assessment methodologies for military planners and analysts. The forecasting and evaluation of a hybrid threat has become difficult due to the complexity and wide range of capabilities that the opponent can use, as well as the reluctance of some to this concept. This does not mean that hybrid threats are impossible to predict. Unlike asymmetric threats targeting non-state actors, hybrid threats are orchestrated by state actors using third party services (terrorist groups, organized crime, guerrilla formations, anarchist, non-governmental organizations, news trusts, political parties) to promote their own interests (Popescu, 2014).

In the literature, the concepts associated with the hybrid war, which include *the composite, proxy and legal war*, are being used more and more often, which demonstrates the complexity, intensity and magnitude of conflicts now and especially in the future.

Composite war is defined as an armed conflict triggered by the use of conventional forces, and various non-conventional

capabilities were subsequently used. By comparing the concepts of composite war to hybrid warfare, the complexity of the latter, in the sense that the hybrid warfare combines conventional, unconventional, asymmetric and cybernetic strategies, tactics, processes and capabilities, as a rule, simultaneously for the fulfillment of political and military objectives.

The proxy war is the conflict in which a state actor tries through a third party to impose its interests within another state. The proxy war, that is, the war waged by third parties, is aimed at transforming the indirect aggressor state into a sponsoring state, and the interstate warfare in an intrastate conflict, wanting to interpolate international law on masking aggression.

The legal/juridical warfare (lawfare) is a variant of hybridity that speculates the provisions of international law on aggression and subversion. Thus, the legal war becomes an instrument that makes it possible to use the law to support the legitimacy of military operations (through third parties) and abusive use of the law to undermine their actions or legitimacy.

This approach leads to the characterization of the hybrid war as a war without rules and restrictions, ie an unrestricted war that ignores and transcends international law in the field, the rules and principles of the armed struggle, and the limits imposed by the rules of engagement in the combat space. In the "hybrid war", essential are not only the military weaknesses, but rather the societal ones, ie the non-military ones, which the one that generates the aggression attempts to frustrate.

6. Conclusions

The current transformations of society, both military and civil, the evolution of the information society and the technological explosion, determine the emergence or transformation of some principles regarding the use of the system of ideas and solutions in the military field, requiring the redefinition of the existing doctrinaire concepts. It is a feature of the world in which we are developing mechanisms to detect the existence of hostile security policies and strategies, to avoid surprise and to prepare early countermeasures, both theoretical legislative, doctrinal, as well as institutional and operational.

Asymmetric warfare, informational warfare, and hybrid war are doctrinal concepts that originate in the disimetry generated by technological gaps in the context of non-conventional aggression supported by maneuvering forces. The logic of the redefinition of doctrinal concepts is determined by the legislative and doctrinal framework adopted in the light of the risks, threats and vulnerabilities identified the proposed objectives and directions of action as well as the ability to plan specific military capabilities in the medium and long term.

If the *Military Strategy* defines the strategic and operational principles and concepts that ensure the achievement of military objectives, being more a question of political will, the doctrinal concepts express a theoretical picture of a state of fact, based on a comprehensive approach to facts and events security of society at some point. Military doctrinal concepts call for a flexible and courageous approach to jump from classical war thinking to its new coordinates.

From this perspective, the importance of the correct understanding of the doctrinal concepts begins the process of rapidly adapting the conceptions and objectives of the military actions to its requirements by developing conventional means of credible discouragement and, in particular, by substantially rethinking the legal, doctrinal, institutional, technological and operational complex of non-conventional means of defense and national security.

REFERENCES

Department of the Army. (2011). *F.M. 3-0, C1, Operations,* Washington, DC: Department of the Army.

Frunzeti, T. (2012). Convenţional şi neconvenţional în acţiunile militare, *Impact Strategic, 4 (45)*, 6-14.

Ghigiu, A. M. (2011). Cine va domina secolul XXI? Noua structură de putere*, Impact Strategic, 3(40)*, 45-48.

HotNews.ro. (2014). *Ce este „razboiul hybrid" dus de Rusia in Ucraina si cum a fost el pregatit de zece ani sub ochii permisivi ai Occidentului,* available at: http://www.hotnews.ro/stiri-international-18014446-este-razboiul-hibrid-dus-rusia-ucraina-cum-fost-pregatit-zece-ani-sub-ochii-permisivi-occidentului.htm, accessed on: 05.01.2018.

Ministry of National Defense (MoND). (2016). *The Military Strategy of Romania, Modern Armed Forces for a Strong Romania in Europe and the World,* available at: http://www.monitoruljuridic.ro/act/strategia-militar-a-rom-niei-din-28-septembrie2016-for-e-armate-moderne-entru-o-rom- not-strong-n-europa-in-world-issuer-182367.html, accessed on: 03.01.2018.

Ministry of National Defense (MoND). (2017). *White Paper on Defense*, Bucharest: available at: https://lege5.ro/Gratuit/gi3dcmzzge3q/carta-alba-a-apararii-din-20112017/4, accessed on: 03.01.2018.

Mureşan, M. (2004). *Reflections on the military phenomenon,* Bucharest: Publishing House of National Defense University Carol I.

North Atlantic Treaty Organization (NATO). (2010). *Strategic Concept for the Defence and Security of the Members of the North Atlantic Treaty Organisation*, Lisbon.

Popescu, A. I. C. (2014). Observaţii privind actualitatea războiului hibrid. Studiu de caz: Ucraina, *Impact Strategic, 4(53)*, 124-138.

Presidential Administration. (2015). *National Strategy for Country Defense for 2015-2019*. *A strong Romania in Europe and the World*, Bucharest: Author.

Văduva, Gh. (2017). *Asymmetric War and the New Physiognomy of Armed Conflict*, Bucharest: Publishing House of National Defense University Carol I.

Zecheru, T., & Săracu, C. (2015). Aspecte privind operațiile informaționale în mediile operaționale în care se utilizează dispozitive explozive improvizate, *Impact Strategic, 3(56),* 28-36.