A NEW TYPOLOGY OF WAR –
THE HYBRID WAR

Mihai Marcel NEAG
“Nicolae Balcescu” Land Forces Academy, Sibiu, Romania
mmneag@yahoo.com

ABSTRACT
The complexity, diversity, physiognomy, the nature and dynamics of contemporary conflicts represent challenges that should be fully understood by the military in order to position themselves in a unified theoretical framework, with direct effects on the reporting capacity to them by timely actions, in the logic of the rules of the battles and the principles of the military action.

The war, be it ancient or modern, hybrid or not, is always complex and cannot be described by a single adjective.

KEYWORDS: asymmetry, hybrid threat, hybrid warefare, security crisis, integrated crises management

1. Introduction
In practice, any threat may be hybrid as long as it is not limited to a single war size or shape. When any threat or use of force is defined as hybrid, the term loses its value and brings about confusions rather than clarifying the reality of modern war.

The essence is that the opponents within modern confrontations use simultaneously conventional/unconventional, irregular, regular/explicit/hidden tools and exploit the whole arsenal at their disposal to combat the superiority that some or others hold in a conventional warfare. The hybrid threats are not confined to conventional tools but to the whole spectrum of modern war.

The term “hybrid” has emerged in 2005 and has subsequently been used to describe the strategy used by Hezbollah in the 2006 war in Lebanon. Since then on, the term “hybrid” has dominated the discourse about modern warfare and its future until the point in which it was adopted by military leaders and promoted as a basic concept for modern strategies of war.

2. The Complexity of the Environment of the War
The current war-type military actions and their essence – the armed combat, will evolve in relation to the non-state actors in tandem with technological development of the modern society based on knowledge and extensive information support, under the impact of the information revolution and as a result of multiple political, economic, legal or social determinations. The development of information technology influences and will decisively change the nature of future confrontations leading to the emergence of new doctrines and strategies, as well as other ways to conduct the war. Trying to define in a more precisely way the characteristics of future military confrontations, the military
Theorists introduced in the current vocabulary notions such as: integrated battlefield (space), expanded battlefield (space), multinational joint force, integrated operations, interdepartmental operations, effects-based operations, comprehensive approach in military operations.

The confrontation battlefield is in a continuous development and will remain an area of diverse types of conflicts characteristic to the information society, the information society type driving the transformation of the military confrontations which will be “in a very broad spectrum of actions and reactions, in a multidimensional space” (Mureșan, 2005). The multidimensionality of the space combat is circumscribed to a broad spectrum of military actions including the informational space, cyberspace, outer space, cognitive space or cultural – identity space, and the dynamics of changes in the international security environment, related to the use of armed violence has as effect the diversification of the types of conflicts.

The cyberspace has become an ideal environment for warfighting, and the military structures must be prepared to be able to respond to the threats that are generated in this environment. We can consider the cyberspace as a common global domain within the information environment, being made up of an infrastructure of interdependent information networks including telecommunications networks and computer systems.

The modern information environment is characterized by the increase of the amount of data and information necessary for planning and waging the warfare. The information about targets, about the forces involved in the operation, their overall condition, the material and environmental resources are provided to the deployment elements that may be located at great distances between them, given that they are obtained from the equipments that can be equally dispersed.

The threats extend into a space where “the enemies are no longer separated by an ocean but a firewall”, using “cyber rockets” (Sutherland, 2011) or new systems of weapons. It establishes that the state asymmetry is promoted which will result from the combined use of cyber war capabilities, anti-satellite or anti-missile systems and programs, augmented by the nuclear threat. The incidence of intrastate violence, with state actors, proxy/tertiary states or non-state actors will remain a permanent theme of analyses.

The unique feature of the new categories of risks and threats (international terrorism, proliferation of weapons of mass destruction, organised cross-border crime, cyber-crime, etc.) is represented by the fact that they cannot be highlighted individually as the new threat is, in general, unconventional, dynamic, non-linear and sometimes even random in incidence, without constraints or rules of engagement – in other words: asymmetric. At the same time, it does not have a doctrine of its own, it is difficult to quantify and project it and is supported by a variety of entities (if we are referring only to persons, then we can come across terrorists, religious fanatics, extremists and xenophobes and leaders of organized crime networks). The enemies of the past were predominantly symmetrical: static, predictable, uniform, hierarchical, rigid and resistant to change. The contemporary enemies are asymmetrical: dynamic, unpredictable, fluid, interconnected, self-organized, who constantly adapt and evolve.

The present military conflicts oppose individuals, groups and transnational groups, supported by states or international organizations that perform specific combat actions both locally in the conflict zone, as well as globally. We are dealing with different forms of violence, such as terrorism, insurgency, crime with targets focused on domains (cyber-attacks) and disorganization by intimidation or interference. The tactics, techniques and procedures continue to
improve in ways which bring opponents benefits and influence, including economic, financial and even diplomatic means. These forms of conflict are outside our perception about military actions, be them conventional or asymmetrical.

The military operations will be more and more dependent on other components and non-military capabilities; in addition to the intelligence community, they will involve a collaboration with the forces of the Interior Ministry, with other state or private structures, decentralized at the tactical level. The comprehensive approach will mean, in fact, a symmetrical, balanced response to asymmetrical, chaotic threats.

The term “hybrid threat” is a sophisticated amalgam of activities without restriction. A hybrid threat is characterized by decentralized leadership, military and non-military simultaneously used activities, a combination of traditional, asymmetric terrorist actions and of disruptive criminal methods, of complex environment operational conditions, all with the intent to use time and space to take the most appropriate decision for the given situation (Glenn, 2008).

“The hybrid threats agreed as representation at the level of NATO Allied Command for Transformation (ACT), are defined within the margin of a capability of one or more state actors, or of a group of non-state actors, to use a mix of actions (conventional and unconventional) in the battlefield and beyond its borders, with negative impacts on the decision-making cycle of the opponent in order to achieve the objectives” (Anghel, 2011, p. 58).

A number of criticisms show that there is insufficient evidence to support this idea. Others characterize the concept as a space for the activities of non-linear threat in an environment or the place of operational applicability of non-state actors.

War, this phenomenon, so complex and full of unknown, so unwanted by some and embraced by others, is one of the dilemmas facing humanity. That is why, nowadays, the conflict prevention is a topic on the agenda of international life, and its approach from positions that encourage concrete action is reinforced by recent positive or negative experiences in this field.

3. The Hybrid Warefare

A nebulous concept haunt the West since Crimea’s occupation by the Russian forces: the hybrid war, this misleading and inaccurate concept that has gained a rapid popularity (www.contributors.ro). The new form of manifestation of the conflict, brought into the hall of the God Mars, about which there are so many talks lately, got the name hybrid war to distinguish itself from other forms of known warfare forms. The phrase hybrid war is a concept that does not have a universally accepted definition, but after which some states revise their military doctrines or security strategies.

The primary source of the concept has been identified as being a document entitled “Unrestricted War/Unrestricted war-state” of colonel Qiao Liang and colonel Wang Xiangsui, drafted in 1999 and published by the PLA Literature and Arts Publishing House. The study deals with the subject of innovative thinking in order to find ways to fight off any opponents and capabilities. Thus, the first characteristic of the hybrid war was introduced: a war without rules and restrictions. Unrestricted and unlimited in the particular sense of the rules in use. (Chifu, 2015) The unrestricted warfare “ignores and transcends the boundaries of the battlefield and what is not the battlefield, between what is and what is not a weapon, between military personnel and civilians, between state and non-estate actors”. (Metz, 2014) The goal is to ensure equal opportunity to the weaker parties of the conflict.

The real use of the term hybrid war appears, for the first time, in the thesis for the degree of Master in Arts in the field of National Security Affairs of William J. Nemeth, Future War and Chechnya: the
Case for Hybrid Warfare (Monterrey CA the Naval Postgraduate School: June 2002). His thesis argues that countries are under a threat from the violence of desintegrating states, of the new unstable entities, characterised by a high level of violence inside those societies, with anarchic communities where traditional norms and rules are mixed with laws, norms and socio-political constructs. This, combined with modern technology, creates this hybrid society. The main result comes from the fact that this interference of the traditional and modern components leads to a special kind of creativity and innovation of the pre-state society in using modern technology and weapons, and this way of thinking creates surprise and capable tactics able to overcome the difference in power between two armies (Chifu, 2015).

If the content of the concept has been defined by the Chinese military as unrestricted warfare, if the name is due to William Nemeth, the parents of the hybrid war, as it is known today (Mattis & Hoffman, 2005). The essence of the definition resulted from trying to think as an enemy of the USA, and identifying niche solutions to fight against a superpower: modern technological combinations and unusual tactics used by opponents in order to obtain strategic advantages.

According to the authors the hybrid war is fundamentally an asymmetric, irregular warfare, using tools like guerrilla and terrorist tactics, criminal actions, cyber attacks, information operations, in a planned combination that might be able to affect the security interests of the certain state. Its impact seeks to affect different areas, which are thus transformed into some strategic domains, such as those related to the information operations carried out with the support of the favorable media. The objective consists in the alteration and transformation of will and support for the engagement into conflict of the target state, population or its leaders.

According to the NATO concept the hybrid war represents a concept that refers to an extensive area of hostile actions, in which the military force is only a small part, and which are simultaneously carried out, as part of a flexible strategy, with long-term objectives. The Statement of the NATO summit in Wales from September 2014, describes the hybrid war as “a range of paramilitary, military and civilian, direct and hidden [...] integrated actions” (www.hotnews.ro).

Russian mass – information means define the hybrid war as a military strategy which combines a conventional war, a small scale war and the cyber warfare. In another source, we find that in the “hybrid war” the actions are primarily undertaken in the information space and the one who will control this space will get the victory (Gîrneț, 2015). The clearest definition of this concept belongs to the Chief of the Staff of the Russian Armed Forces General V. Gerasimov, who wrote in an article in the weekly specialized journal – VPK – that war and peace become notions whose borders are more and more diminished while the ways of conducting the conflict have changed and imply “taking political, economic, information, humanitarian and other non military measures” together with the implication of the local population and under-cover forces (www.hotnews.ro).

According to Dr. Iulian Chifu, the concept of hybrid war means: “a combination of conventional, asymmetrical, irregular, economic, energy, cyber warfare along with a identity and information one, and a war through intermediaries, combined, in a very complicated and unstable form, with a limited war and, at the same time, with one without restrictions for the purposes of conducting capabilities of all kinds, without respect for any rules. The criminal capabilities together with the economic and information ones, the propaganda and irregular warfare through intermediaries, insurrection and terrorism, can be used in the
same theatre to achieve a specific objective in line with the realistic approach of Machiavelli, where **tous les coups sont bons**” (Chifu, 2015).

The concept of hybrid war fits into today's trend manifested inside all bodies and organizations of military type and tend to replace other concepts spoken about until recently. Thus, the new concept of the hybrid war seems to be the corollary of the very similar concepts, such as asymmetric warfare/conflict, unconventional warfare, effects-based operations, command and control warfare, information or network-based warfare, comprehensive approach to operations, integrated crises management, etc. No matter how we look at things and no matter how we try to identify the aspects of maximum novelty of the current security crisis or armed conflicts we find out that each of the techniques and methods used by the involved actors dates from older or more recent periods of the military history of mankind.

The hybrid warfare involves the use of a very comprehensive and nuanced variety of military activities, resources, programs and applications, dimensioned in such a way that they lead to a non-violent, persuasive maximization of the political and economic influence to reform the governments or hostile movements, as well as the reversal of the trend of the conditions of instability in the political, social and economic areas, characteristic to the collapsed or failed states. It also includes the full spectrum of the capabilities in the field of military information, unconventional weapons (including non-lethal ones), combat and support equipment, available at all times to be used if the opposing elements belonging to the regular forces or unconventional actors-insurgent forces, terrorist groups or other opposing elements – triggered hostile actions which constitute a direct threat addressed to the activities aimed to normalize the activity of the human community in that particular state (Bond, 2014).

On the other hand, from the analysis of the current events of specific geographical areas in which actions considered to be hybrid are taking place, it is necessary to notice that the objectives pursued by actors that are generators of instability are diffuse, indistinct and are unclearly outlined, and which in general, seek the establishment of a perpetual insecurity state among the local population and decision makers, by prompting the latter to adopt an unclear position in terms of foreign policy and an attitude of helplessness with regard to respect for the rights of the citizens of the area in question. By doing this, the hybrid war is very close to the concept of crisis, this being called in our particular case - a security crisis.

The principles of the hybrid war are clearly stated in a report drafted at the Joint Special Operations University and the Strategic Studies Department, MacDill Air Force Base, Florida/USA, according to which:

– a hybrid force acts, holds capabilities and configures itself in a unique way, depending on the context for which it was created.

– hybrid-type ideology determines the internal conduct of the organization.

– perception of the existing threat according to the potential opponent. This perception of the threat leads the hybrid-type force towards the abandonment of conventional military thinking, in order to ensure the long-term survival.

– correspondence between the capabilities of the hybrid-type force with those held by the potential opponent.

– a hybrid type force holds both conventional and unconventional elements. These items consist mostly in “accepted” military technologies and nonmilitary technologies, specific to the groups of guerrillas.

– the hybrid organizations rely on defensive-type operations.
the use of attrition tactics by the of hybrid type force (McCulloh & Johnson, 2013).

When discussing the hybrid war and its manifestation, there is a need for classification as a crisis phenomenon, the way it is treated in the military literature, that is, from the perspective of security crisis. The essential problem regarding the existence of threats of hybrid or hybrid war-types consists both in understanding the phenomenon and in finding solutions to counterattack this type of threat. Counterattacking the threats of hybrid type falls within a broader spectrum offered by the crisis management, a domain widely debated in the specialized military literature and which, at NATO level, has an effective response system to crises.

Therefore, a nationwide system of integrated management of security crises should be developed, covering all areas of national security. The setting up of a strategic executive structure of decision support should resolve the true implementation of this wish that is represented by the word integrated, from the commonly used expression, integrated crises management.

4. Conclusions
In order to attain the goals, the opponents of a conflict (state actors, proxy/tertiary states and non-state actors) will carry out activities that would result in a low and indistinct perception of their action in the environment of confrontation, the conflict aiming at continuously influencing the participants (and especially the population), activity which will be coordinated in a centralised way and carried out locally or decentralised.

In the hybrid war, not only the military weaknesses are essential, but especially the societal ones, namely the non-military ones, which the one who generates aggression is trying to capitalize: ethnic tensions, weak and corrupt institutions, economic energy dependency/etc. Based on these weaknesses, a hybrid war involves actions ranging from terrorism to media propaganda through irregular and unassumed warfare. A weak state is the favourite target of a hybrid war. Weak state refers to a state without strong institutions, with disengaged or even hostile citizens towards the state, economically dependent on potential enemies that are corrupted thus easy to infiltrate at the strategic decision level.

The hybrid warfare destabilizes the state and polarises the society, their gravity center being represented by the population. The opponent attempts to influence the policy makers by combining military means (large-scale exercises with troops or nuclear bombardment aircraft flights) with subversive actions (clandestine actions that avoid their assignment to the aggressor state).

In the future conflicts, the adversaries will induce various challenges to the ability and the operational capability of the opponent forces to fulfill its objectives, resulting in hybrid threats (which combine conventional, irregular and asymmetrical threats), simultaneously, in time and space.

REFERENCES


