IS HYBRID WARFARE A NEW MANNER OF CONDUCTING WARFARE?

Daniel-Cornel ŞTEFĂNESCU
"Henri Coandă" Air Force Academy, Braşov, Romania

DOI: 10.19062/1842-9238.2016.14.2.20

Abstract: *The current type of warfare - hybrid warfare - which humanity is apparently experiencing every moment, while being unaware of it, is no longer used by conventional techniques. It will never be announced by an official announcement. This form of war uses both conventional and, unconventional, undercover means, regular or irregular, with the support of more or less hidden governmental agencies and mass media. The virtual environment is the new battlefield, computer technology being a determining factor in conducting hybrid actions.*

Hybrid warfare has a complex and varied operation area, reaching all fundamental sectors of today's society: its economy, the ethno-cultural dimension, diplomacy, technology, media, strategic and operational segments as well.

Keywords: *instability, extremist groups, cyber operations, Hezbollah special forces*

1. INTRODUCTION

The current international environment is characterized by new threats resulting from the energy crisis, economic crisis, demographic conflicts, amplification of the non-military aspects, access to information, religious and ethnic separatism.

The technological revolution has transformed the war, giving it a new meaning, especially by the disappearance of boundaries between military and civilian actions. The new type of war, hybrid war, involves the use by states or non-state actors of conventional or unconventional warfare, and measures of political, economic, social, humanitarian, diplomatic and informational conjunction with the involvement of local people in taken actions. Non-state actors, sometimes represented by terrorist organizations or paramilitary receive weapons, money and even political support from states and take action for the accomplishment of their strategic interests.

During the last decades, the nature of conflict has changed a lot and at a fast pace, moving from conventional battles between armies of nation-states to irregular/ hybrid conflicts and instability.

2. HYBRID WARFARE - DEFINITION

Warfare is a social-historical phenomenon, a violent manifestation of conflicting political relations between large groups of people (classes, nations, states, coalitions of states), organized militarily, groups that pursue economic, political, territorial or religious goals[1].

Although hybrid warfare is an old concept, its study by scholars, especially theorists of the Western countries, began after the Second World War and focused on asymmetric threats against conventional superiority of Western countries.

The attacks of 11 September 2001 and the Israel-Lebanon war of 2006 played an important role in the evolution of hybrid warfare theories.

In the 70s, Evgeny Messner defined the new type of warfare (later on referred to as hybrid warfare) as an insurgent war, unreported, with the participation of the civilian population, as well, in which the rapport war - peace is unclear and where no one knows who signs for its ending[2]. This type of warfare will not require the deployment of large armed forces but it will be carried out by extremist groups that resort to terrorist tactics.

The Messner definition is taken over by Valery Gerasimov, Chief of Staff of the Russian Army, who, in February 2013, in an article issued by the Russian press, described the hybrid warfare as *"a war mixed with peace, where the conflict methods changed... while political, economic, informational, humanitarian and other non-military measures being involved to a greater extent. All of these can be supplemented by inciting the local population and by using armed forces in disguise"*[3].

Since 2000, the term *hybrid* has been used to describe contemporary wars, in which there is an increase in the complexity and lethality of violent actions carried out by non-state actors, and in the potential of informational (cyber) war.

Hybrid warfare is *"a combination of symmetrical and asymmetrical armed conflicts, in which the intervention forces conduct traditional military operations against enemy military and targets, while they simultaneously and decisively act to get control over the indigenous people in the theater of military actions, by stability operations"*[4].

Frank Hoffman argues that *"hybrid warfare incorporates a full range of different types of warfare, including conventional capabilities, irregular tactics and formations, terrorist acts, including generalized violence and coercion, as well as criminal disorder"*[5].

The former Secretary General of NATO, Anders F. Rasmussen, defined hybrid warfare as *"a combination of concealed military operations combined with sophisticated information and disinformation operations"*[6]. His successor, Jens Stoltenberg, described the hybrid warfare as the type of war that combines the power of unconventional means with cyber operations and information as well as covert military operations[7].

David Kilcullen, in the book "The Accidental Guerrilla: Fighting Small Wars in the Midst of a Big One," says that "hybrid" is best suited term to describe modern conflicts, conflicts that include a combination of irregular war, civil war, insurgency and terrorism[8].

Peter R. Mansoor (military historian) defined hybrid warfare as "a conflict involving regular and irregular armed forces (guerrillas, insurgents and terrorists), which may involve both states and non-state actors in order to achieve a common political purpose "[9].

In the hybrid warfare combat at the contact line disappeared, as well as that in trenches or fortifications, while complex methods of combat are employed, combining force categories (especially special forces), lethal and non-lethal means and conventional combat tactics with the unconventional ones. Frequently it manifests itself by terrorist attacks, assassination operations, information, disinformation and propaganda, by cyber attacks, by the use of media as a battle space, all actions being aimed at a justification in the international background and at weakening of the power of the enemy[10] (Fig. 1).

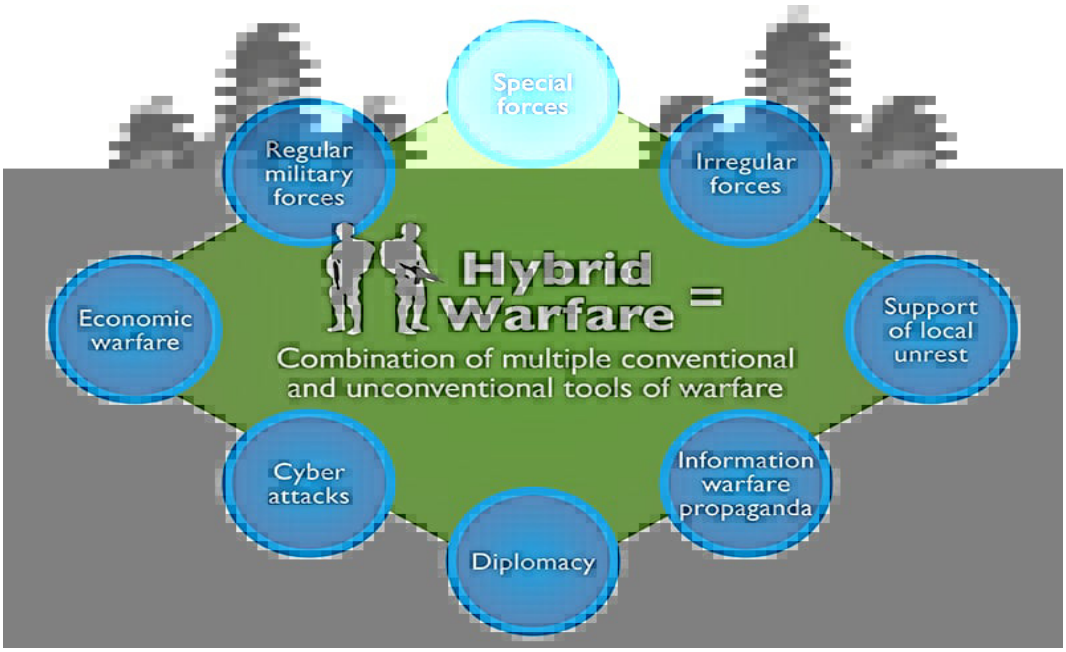

FIG.1. Hybrid war and its components [11]

The modern adversary uses conventional or unconventional means, covert, regular or irregular, and exploits all sides of warfare to counter its opponent's superiority in the conventional war. Conventional armies are used, preferably in the final stages of the conflict. Hybrid warfare is based on carefully combining the military kinetic action with operations meant to disunite, irregular activities, including information and cyber operations. They are often accompanied by intense activity of special forces, of mercenaries and of other paramilitary groups.

The 2006 conflict between Israel and Hezbollah militias represents the model of warfare that corresponds to contemporary definitions of hybrid warfare. Hezbollah fighters, trained and equipped with modern weapons and fighting technique (probably by Iran), surprised Israel by combining tactics of guerrilla with conventional military operations, employing last generation weapons (long range missiles, cruise missiles, sophisticated anti-tank weapons, UCAV) and modern communications systems (drones, satellites).

Low intensity conflicts, kinetic and non-kinetic threats to peace and international security, including cyber warfare, asymmetric conflicts of low intensity, global terrorism, piracy, transnational organized crime, demographic challenges, resources security, reduction of globalization and the proliferation of weapons of mass destruction were identified as the so-called "*hybrid threats*".

Hybrid warfare is conducted following a comprehensive strategy that involves combining long-term efforts in progressive steps, in such areas as political, economic, social, ethnic and religious, information and, finally, military.

3. DIMENSIONS, STAGES AND OBJECTIVES OF HYBRID WARFARE

a) The dimensions involved in running the hybrid warfare are:

- A political dimension resulting from the diversity of general interests or of objectives of establishing and exploiting the weak political points of the target state[12];

- An economic dimension - economic resources are especially employed as weapons in approaching a hybrid conflict. A state - dependant economically on potential enemy states, corroded by corruption, easily penetrated at the level of strategic decision, may be a potential target in hybrid warfare;
- An ethno-cultural dimension - the ability of a state/ non-state actors to exploit the existing ethnic and cultural tensions existent in the target state;
- A diplomatic dimension - able to develop an environment that will allow, through diplomatic means, the discrediting of the target state;
- A technological dimension – that includes the existence and the use of high technology in combat (anti-satellite weapons and cyber warfare against adversaries);
- A mass-media dimension – that reflects the ability of the aggressor to influence the people in the hybrid conflict deployment area. Weak states may be the favorite target of hybrid warfare, because the enemy can exploit people's discontent. Hybrid confrontation is "*a struggle beyond the physical aspects of the conflict, in which the manipulation of the media, the use of Internet and information operations integration with strategic communication programs are as important as the weapon systems on the battlefield*"[3];
- A strategic dimension – that requires complex actions, prepared in advance, diversified and constantly updated to create advantages over a possible adversary;
- An operational dimension - combining hybrid lethality of a conflict with irregular warfare[14].

The destructive component of the hybrid warfare is represented both by high-tech and crime, the latter being used to support hybrid actions or to spread disorder among the target nation members[15].

All of these actions are interconnected and overlapping in different segments, following one long-term strategy. The action begins in the information field, are pursued simultaneously in the economic-financial and social areas, and finally, if necessary, the military field is employed as well. The fight will take place on several spaces, with varied means, in most cases isolated and without any connection with other actions of the campaign. It will continue to be led by a collective idea, in the absence of a central command and control structure. These actions would circumvent international law by not taking responsibility for the action by either party, by denying the physical presence of the soldiers who violate the territorial integrity of an occupied country, by denying involvement in a cyber attack aimed at disrupting critical infrastructure or by influencing the minds of the people that should remain loyal to their authorities in order to preserve the integrity of their state.

b) Future hybrid conflicts may take place following the next steps:
- Weakening a country's economy through the aggressor's intentional actions;
- Collapse of the financial-banking sector or even pushing towards its total collapse;
- Involvement of the population in certain areas in social and economic life, to create widespread civil disobedience and disorder, used to justify political movements and insurgency;
- Support of the aggressor's actions by the local population both intentionally and as a result of fear of possible actions from the aggressor against them;
- Use of ethnic / religious minorities as an excuse for the outbreak of a conflict or its extension among all people of the area;
- A strong and intense international support, not always visible to the regular population;

- Use of unique symbols, very well known and easily to spot among the population in that area, as well as internationally ("little green men" present in eastern Ukraine, recognized by the local population and international environment as soldiers in the Russian regular armed forces);
- Assurance of personnel recruitment or fundraising to finance actions;
- Demoralization of the armed forces of a state or of government forces.

Hybrid warfare can be implemented through cyber attacks on citizens, whether civilian or military networks of a target state, facts that cannot be considered military operations, but which create a strong impact on the population. Use of cyber attacks in the full range of military and non-military operations produce strategic advantages over an unprepared opponent. Offensive cyber attacks are of three types: destruction, disruption or disinformation.

The objectives of a cyber attack are as follows:
- Loss / deterioration of the information integrity by its alteration;
- Loss / decrease in the availability, in the circumstance of the information systems being accessed by unauthorized users;
- Loss of confidentiality, where information is disclosed by unauthorized users;
- Physical destruction, where information from the systems is deliberately destroyed.

Cyber attacks are most frequently targeting critical infrastructure (financial services, manufacturing, telecommunications, transport and supply, electricity, water supply). Their conduct involves fewer people (but highly trained and equipped with the latest technology) and does not require a thorough check over the territory in which it is to be carried out.

Although most countries have invested considerable amounts of money in the development and operationalization of defensive cyber capacities, it was found that the cyber threat in the information environment is growing and it intends to transmit its effects from the civil society toward the military in order to damage national security.

Also, hybrid warfare involves actions related to information warfare. It consists of combat operations conducted in a highly tech battle environment, in which both parties use information technology, media, equipment or systems to obtain, control and use information[16].

Information warfare is based on three principles: gathering information, launching attacks and protecting assets. Some specialists consider that electronic warfare, information warfare and cyber warfare are synonymous.

CONCLUSIONS

Considering the technological development which takes place today and the global geopolitical changes, it is expected that future security threats will be more and more varied and lethal.

Future wars will involve all elements of national power in a continuous process of activities, from humanitarian missions, military operations up to stability operations, security and reconstruction, all of which will be conducted simultaneously. Wars will include hiring and simultaneous combination of conventional and unconventional means, lethal and non-lethal support units, combat equipment available for rapid deployment, terrorism, organized crime, cyber and electronic attacks, all conducted by the same aggressor.

Because of the diverse forms of materialization of hybrid warfare, a generalization of the counter-reaction to this type of warfare is not possible. In this respect, separate solutions for each challenge are required, the opponent (in most cases incomprehensible, elusive and irrational) concealing its intentions and actions through the involvement of paramilitary groups, separatists, pressure groups, militant states or Trojan-like type of states.

REFERENCES

[1] *** *Lexicon militar*, Editura Militară, Bucureşti, p. 563, 1980;

[2] *** *Ce este „războiul hibrid" dus de Rusia în Ucraina şi cum a fost el pregătit de zece ani sub ochii permisivi ai Occidentului*, 1 septembrie 2014, consultat în 09.09.2016, pe site-ul: http://www.hotnews.ro/stiri-international-18014446-este-razboiul-hibrid-dus-rusia-ucraina-cum-fost-pregatit-zece-ani-sub-ochii-permisivi-occidentului.htm;

[3] McCuen, John J., USA, Retired, Hybrid Wars, Military Review, March-April 2008, United States Army Combined Arms Center, Fort Leavenworth, Kansas, pp. 107-108,2008;

[4] Frank G. Hoffman, *„Conflict in the 21st Century: The Rise of Hybrid Wars"*, Potomac Institute for Policy Studies, Arlington – Virginia, December, p. 8, 2007;

[5] Stefan Grobe, *„Stoltenberg: NATO massively stepping up military presence in Europe"*, EURONEWS, 25.03.2015, http://www.euronews.com/2015/03/25/stoltenberg-nato-massively-stepping-up-military-presence-in-europe/;

[6] Kilcullen, David, *The Accidental Guerrilla - Fighting Small Wars in the Midst of a Big One*, Oxford University Press, 2009;

[7] Peter R. Mansoor, *„Hybrid War in History"*, in Hybrid Warfare: Fighting Complex Opponents from the Ancient World to Pressent, ed Wiliamson Murray and Peter R. Mansoor (Cambridge: Cambridge University Press), 2012;

[8] Marian Rădulescu, *Counter-hybrid warfare. Developments and ways of counteracting hybrid threats/war*, International Scientific Conference „Strategies XXI",vol. 2: p. 132. Bucharest: Bucharest „Carol I" National Defence University 2015;

[9] http://www.asianwarrior.com/2016/09/hybrid-warfare-the-next-generation-tool-unitedstates-russia-china-pakistan.html;

[10] Colonel Steven C. Williamson, *From Fourth Generation Warfare to Hybrid War*, U.S. Army War College, Carlisle Barracks, Pennsylvania, p. 15,2009;

T. R. Nail, *A disturbance-rejection problem for a 3-D airfoil exhibiting flutter*, Thesis, Virginia Tech., 2000;

[11] U.S. Joint Forces Command, *The Joint Operating Environment: Challenges and Implications for the Future Joint Force* (Norfolk, VA, November 2008), p. 39, 2008;

[12] Frank G. Hoffman, *Conflict in the 21st Century: The Rise of Hybrid Wars*, *op. cit.*, p. 27;

[13] Christopher O. Bowers, *Identifying Emerging Hybrid Adversaries*, Strategic Studies Institute, U.S. Army;

[14] Alexander, Dean, *Cyber Threats in the 21st Century, Solutions for Enterprise Security Leaders*; Sep. 2012, Vol. 49 Issue 9, p. 70, 2012.