HYBRIDITY – HALLMARKS OF A NEW WARFARE

Leszek ELAK

War Studies University

Abstract. The term 'hybrid', used in connotation with military domain, proved to be very popular at the beginning of the current century. It is linked with using other than military tools in combination with military pressure to influence security situation in other opposing nations. It is based on valid assumption that it is not necessary to use combat power in globalized world to impact other nation's internal situation, which could lead to their partial or complete subordination.
Keywords: hybrid, hybrid warfare, hybrid challenges, NATO, Russia, asymmetrical activities, war in Ukraine.

Introduction

In response to the phenomenon referred to as the „hybrid warfare", an army is also required to be prepared for non-conventional operations, below the threshold of war, propaganda campaigns, informational and psychological activities, exerting economic and social pressure. It needs to be pointed out that an opponent will use all the available means to antagonise the society, it will resolve to legal measures, weaken the trust to legal government and self-government authorities and undermine credibility of public institutions. The goal of all these activities is to affect the will and actions of leaders and change society's attitude towards its own country. It is worth to make the society aware that the hybrid conflicts are already a reality and we need to find our way and make effective decisions in this area.

Currently, it is required to take into account the issue of mass influx of displaced persons and population coming from the regions affected by conflicts that may lead to partial loss of control over state borders and disorganisation of internal security system and to partial breakdown of economic system. In relation to a growing threat, the armed forces troops will be deployed in problematic regions, receiving a series of tasks supporting civilian and Border Patrol actions. Securing state borders, protection and guaranteeing the basic living conditions for population, ensuring the functioning of managerial posts in public administration bodies, protection of important public facilities and performance of tasks for extra-military support of armed forces should be prioritised at the time of crisis.

In counteracting the hybrid warfare crucial tasks associated with reconnaissance, surveillance and patrolling the border area are among the responsibilities of the Territorial Defence Force. They also need to be used for establishing contact with local population and national minorities within a given territory. Protection of local population, securing the offices of local authorities and ensuring the capacity

of communication routes are the areas of extensive cooperation between the Territorial Defence and the Border Patrol. When fighting hybridity it is important to coordinate the tasks of operative forces with territorial defence troops, the Border Patrol and non-military forces at the time of crisis and war.

It is noteworthy that the concept of *hybridity,* which, in the context of security issues, may be explained as: "(...) a mixture of different methods – starting from the soft ones, such as informational war, cyberspace war, propaganda, psychological operations, up to the hardest ones, also with the military involvement. We deal with the soft ones on every day basis, which might be observed in actions by Russia aimed at intimidating the public opinions of other countries".[1]

In modern military conflicts definitions of hybridity vary: it is defined as „a combination of symmetrical and asymmetrical war".[2] We may speak of drawing a connection between three different sources of risk and unpredictable events in the form of: irregular activities (guerrilla); classic conflicts (but limited in scope) and asymmetrical threats.[3] It is „a logical combination of strategy and tactics with a purpose of mixing various types of military activities"[4] or otherwise presented – as a synergistic fusion of conventional and non-conventional forces in conjunction with terrorist acts and crimes.[5]

According to the definition by R.G. Walker „hybridity is a result of convergence[6] of rules of conventional warfare and special operations".[7] His definition fits the theory of Toffler, pointing out the increase of special operations significance in modern conflicts, referred to by the author as conducting „niche warfare". He also underlined the so-called demassification of world threats, replaced by multitudes of regional threats, yet exerting influence on a global scale. The special forces are best equipped to deal with them, as the author points out, they may be used "(...) in any type of warfare, from nuclear confrontation to tribal border skirmishes. (...)".

---

1 Based on the interview with the Head of NSB. Koziej: *Bezpieczeństwo Polski w kontekście walki informacyjnej, związanej z wydarzeniami na Ukrainie*, program publicystyczny *Racja Stanu* – TVP Polonia, date of publication 23.02.2015, available online: http://www.bbn.gov.pl/pl/wydarzenia/wypowiedzi-szefa-biura/6463,Szef-BBN-dla-TVP-Polonia-trzeba-wykorzystac-zainteresowanie-spoleczenstwa-sprawa.html?search=68766446 – downloaded in May 2015.

2 J.J. McCuen, *Hybrid Wars*, „Military Review", 2008, no. 2, p. 108 [in:] A. Gruszczak, op. cit., p. 13.

3 A. Gruszczak, op. cit., p. 13.

4 D.T. Lasica, *Strategic Implications of Hybrid War: A Theory of Victory*, School of Advanced Military Studies, United Army Command and General Staff College Press, Fort Leavenworth 2009, p. 11 [in:] Ibidem, p. 13.

5 F. Hoffman, *Conflict in the 21st Century: The Rise of Hybrid Wars,* Potomac Institute for Policy Studies, Arlington 2007, p. 14, online access: http://www.potomacinstitute.org, downloaded in November 2014.

6 Konwergencja – „zbieżność, tworzenie się jakichś zbieżności", *Ilustrowany słownik języka polskiego*, op. cit., p. 345.

7 R.G. Walker, *SPEC FI: The United States Marine Corps and Special Operations,* Storming Media, Monterrey 1998 r., p. 4-5 [w:] A. Gruszczak, op. cit., p. 10.

Generally speaking, *the hybrid warfare* is a fusion of classic military activities, both the regular and irregular ones (guerrilla warfare, sabotage, diversion, terrorist attacks) in combination with elements of informational warfare (propaganda, disinformation) and cyber warfare, as well as actions conducted in political, economic and cultural spheres.

It is noteworthy that the *concept of hybrid warfare* is an American take on modern warfare and constitutes an attempt to answer why the United States failed to use the position of global hegemony and take advantage of engaging with a considerably weaker opponent in the so-called peripheral conflict both in Iraq and in Afghanistan[8]. It is also a basis for taking up considerations over achieving the required efficiency of actions by regular state armed forces, equipped with cutting edge technologies in fighting against the so-called *silent enemy* – in most of the cases being a collection of loosely organised and poorly armed packs hiding among the civilians under the cover of globalisation, cultural diversity revitalisation and returning to the roots of their religion. As aptly pointed out by Michael Evans "(...) we are facing a strange mixture of pre-modern and post-modern conflict (...), with mosques and Microsoft programmes in the mix, (...)"[9].

In such a confrontation an opponent deprived of a state, with an extra-territorial, cross-border, network structure difficult to eliminate and allowing for communication within a given network and with global reach of disseminated values and principles is dangerous. Al Ka'ida is an example of such an opponent. Whereas a classic (state) opponent refers mainly to a nationalistic state, but also to traditional ethnic, clan or tribal communities, permanently inhabiting specific territories. Warfare hybridity may be therefore defined as[10]:

- applying variable methods of war activities, which may include asymmetrical activities along with irregular tactics;
- using mass-scale acts of terror and violence;
- crimes;
- all activities with the use of military and non-military means in an operation aimed at surprising the hostiles, consequently leading to taking over the initiative and gaining the upper hand by exerting psychological influence;
- utilising numerous diplomatic, informational and radio-electronic activities to take over the initiative in war activities;
- engaging in cyberspace operations, keeping the military and intelligence operations undercover as long as possible, coupled with applying strong economic pressure.

---

8 Ibidem, p. 10.

9 M. Evans, *From Kadesh to Kandahar. Military theory and the future of war*, „Naval War College Review", 2003, no 3, p. 137, [in:] ibidem, p. 11.

10 See M. Wojnowski, *Mit „wojny hybrydowej"*…, op. cit., p. 8.

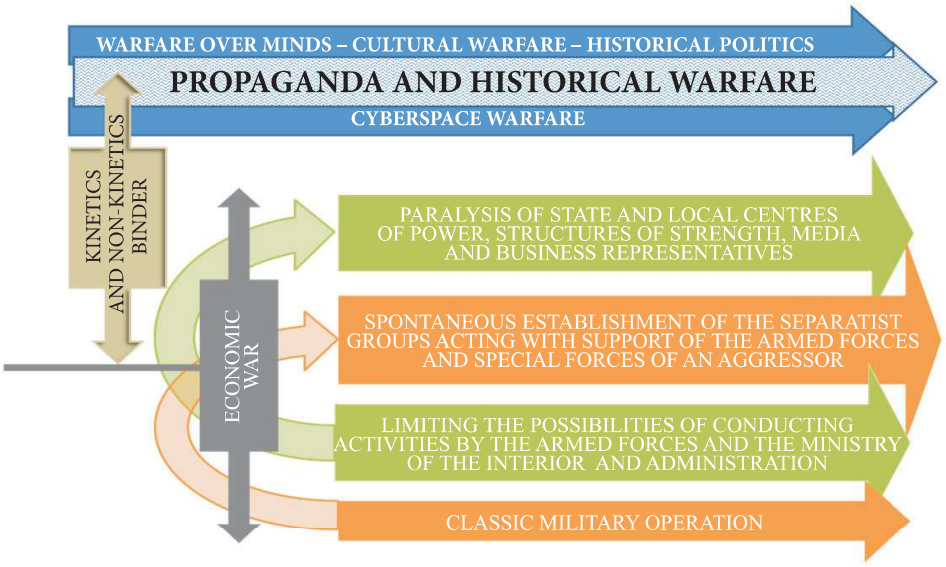

Fig. 1. List of hybrid threats
Source: Lectures by W. Michalski

According to W. Michalski the list of hybrid threats starts from cyberspace warfare, namely from:

- informational warfare with the use of media and propaganda apparatus;
- activities within informational and psychological structures;
- using historical politics to discredit state's credibility at an international scene;
- trolling;
- using social networking to collect information on certain individuals;
- threats of direct strikes on critical infrastructure;
- internet espionage (political, economic, military and technological);
- resource infiltration and copying (theft or replacement by deceit) of sensitive data;
- disruption of decision-making processes (including the election ones by affecting their outcome – in the case of their completion);
- penetrating into the ITC, power, industrial, road control systems – laying the ground for attacking the national, critical infrastructure;
- unexpected (devastating) cyber attack mainly on power sector;
- internet industrial espionage in the scope of access to military technologies;
- theft of officers' logins/passwords through a virus/Trojan fed to a system;
- breaking into and penetration of databases (access to sensitive information);

- infiltration of the integrated command and communication systems of the armed forces and military critical infrastructure;
- establishing false appearance of uninterrupted operation of the monitored systems;
- unexpected cyber attack on command, communication, transport and military infrastructure control systems.

Exerting influence on opinions and attitudes of society in a county affected by aggression is a final effect. Warfare over minds or cultural warfare is a process which is constantly ongoing. Poland has been attacked on numerous fronts for many years now, but with variable intensity. The historical politics of Russia is far more conservative and long-term oriented and strikes at the position of Poland at the international scene, resulting in some of the western media and politicians giving in to the Russian propaganda proclamations. In the propaganda and psychological warfare, the greater the lie the more easier for people to believe it. It is a harsher type of first stage of hybrid warfare, i.e. warfare over minds. The most recent example of immediate activities against Poland is a series of articles and reports on Polish politicians, or an attempt to discredit the Polish initiative regarding the Westerplatte ceremonies.

Next stage of the hybrid warfare is a fight in cyberspace, raging on constantly and being inextricably connected with two previous stages, since the warfare over minds and propaganda warfare occur in cyberspace. At this point, it is worth to mention the trolling, i.e. writing negative comments under anti-Russian articles or the entire media apparatus (Life News, Russia Today), which is very active also on the internet. Furthermore, cyberspace creates the opportunity to strike directly (paralyse) the critical infrastructure of a sate. It needs to be emphasised that cyberspace is a binder that joins non-kinetic stages of the hybrid warfare with the kinetic ones.

Another stage is a paralysis of state and local power centres, structures of strength, representatives of media and business. It is characterised by its role as an introduction to kinetic activities conducted through:

- placing the individuals acting for the benefit of an aggressor at the posts in state and local administration structures;
- infiltrating the armed forces, special services and decision-making circles of the Ministry of National Defence, the Ministry of the Interior and Administration and the strategic companies of the Ministry of Treasury;
- soliciting the approval of media representatives, attempts at taking control over them or downright establishment of such media;
- exerting influence on politicians or entire political parties (radical right-wing or radical left-wing) and sports fan communities.

The final outcome is disruption of functioning of administrative centres and state treasury companies crucial for defence. Paralysis of state and local power centres, structures of strength, representatives of media and business – preparation of this

stage is a very long process and constitutes an introduction to kinetic activities. Currently, there are serious threats in the form of placing the individuals acting for the benefit of an aggressor, or at least the persons sympathising with an aggressor, at the posts in state and local structures. Attempts at positioning such persons in the armed forces, special services and decision-making circles of the Ministry of National Defence, the Ministry of the Interior and Administration and the strategic companies of the Ministry of Treasury, including the armament ones, cannot be excluded. The last aspect applies to media representatives – from commissioning favourable articles, through constant cooperation with aggressor's intelligence, attempts at taking control over specific media or their downright establishment. Separate consideration needs to be devoted to exerting influence on given politicians or on entire political parties. In Poland the radically nationalistic and radically left--winged parties are the ones mostly susceptible to Russian influence (their leaders might be invited to meetings in Moscow under variable pretence – e.g. the Hungarian party Jobbik is coddled by the highest Russian authorities). It is also possible to set entire political parties from the ground up, to sponsor them and affect the political landscape in Poland through such parties. The sports fan communities (along with their leaders) might also be used by aggressor's intelligence to fire up social unrest, whether they are aware of this fact or not.

The next stage of the hybrid warfare is the economic warfare. At this stage we may observe a high level of threat posed by an aggressor undertaking the following:

- taking over the companies belonging to the Ministry of Treasury;
- destabilising the financial system (currency devaluing, stock exchange profiteering);
- imposing embargo and protective custom duties with the purpose of striking at Polish entrepreneurs;
- using crime and mafia structures to decrease state budget income (e.g. fuel mafia);
- discrediting the country at international exchange markets.

The final effect might come as intensification of economic dependency of a state and decreasing its credibility at financial markets.

The next stage of the hybrid warfare may be limiting the possibility to conduct the activities by the armed forces and the Ministry of the Interior and Administration, i.e.:

- overpowering the defence services of the military units;
- preventing from entering emergency areas or disrupting their entry;
- disrupting the military and material resource supply system;
- elimination of key personnel in command and in military units;
- high possibility of sabotage operations at weekends (or at night time);
- disruption of command and communication system of the military units stationed in different garrisons and facilities.

Another stage on the hybrid threats list is a classic military operation – despite the threat being minor, in its most critical scenario, an aggressor may repeat the Crimean variant in relation to one or to all the Baltic countries. Being the members of the North Atlantic Treaty Organization, these countries will expect a quick response from NATO – i.e. the Polish Armed Forces to react first. If there is no military reaction from the NATO states, an aggressor, as a matter of fact, will impair the Treaty credibility and will lead to its downfall, the consequences of which are difficult to predict.

Therefore, in light of the above, it needs to be pointed out that *the hybrid warfare* takes on a new meaning in perspective of Russian activities in the Crimea and in the eastern Ukraine. Crimean activities[11] showed skilful and effective use of the special services and forces, mobilised oppositional groups (irregular subunits) in the form of self-defence militia (Cuban Cossacks) coupled with coordinated activities in economic sphere (gas blackmail) and informational war – waged in various media and at the international political arena (i.e. activities by the minister Lavrov) to use the sub-units in regular forces, the so-called little green men, to maintain and solidify the reign over the seized territory in the final stage. The result of this confrontation between two state opponents was the capture of the Crimea with no bloodshed and starting an intensive political campaign at the international arena to justify and legitimise the applied means.

Encouraged by such a spectacular success in the face of passive Europe, Russia decided to take its next step by attempting to separate the eastern part of Ukraine (activities stated on 6 April 2014 in Donetsk) and incorporate it into the Russian Federation. However, in this case, the situation was more complex. Despite applying the same methods and means in its activities, faced with harsh response from Ukraine aided by the western countries, Russia had to apply more military resource in the form of equipment support at the initial stage of activities and, later on, reinforcing the separatists with the regular army sub-units, including the special forces (for example: utilising anti-aircraft BUK system[12] and shooting down the Malaysian aircraft flight MH-17 on 17.07.2014). In this instance, the activities involved bloodshed with casualties, not only among the fighting sides, but also among the civilians and bystanders, among which we may include the victims on board of the shot down Malaysian aircraft. *The hybrid war* by intensified application of military resource took on the shape of classic, local, military conflict (although a non-declared one) involving a wide use of armoured weaponry and artillery. However,

[11] 23.02.2014 – onset of the Crimea crisis by demonstrating support to BERKUT, coming back from the pacification of the so-called Euromajdan BERKUTU. 18.03.2014 – Russia annexing of the Crimea and Sevastopol. – Note by the author.

[12] 9K37 Buk (NATO code*SA-11 Gadfly*) – the system of guided ground-air missiles, developed by the USSR in 1979. Designed to eliminate targets hard to acquire, such as manoeuvring planes, choppers or Cruise missiles.

Russia, which, according to the international law, is not a side in the conflict, but is only deemed as a supporting country, is constantly engaged in the *informational war* and international-scale activities aimed at further destabilisation of Ukraine and its surrounding.

Nevertheless, such a modern and surprising approach of Russia to war validates the assumptions presented at the beginning of 21st century by Thomas M. Huber perceiving the concept of war as a *Compound Warfare*[13], described by the author as: "(…) simultaneous use of regular or main forces and irregular or partisan forces against an opponent (...)".[14] In other terms, it means an increase of military influence (combat capabilities) by applying both conventional and non-conventional forces at the same time. In his reflections on the issue, the author states that without synergistic command, with no network-centric management of military operations and with no proper combat area recon, in which the key role should be performed by intelligence agents, simultaneous use of regular army units and scattered irregular (special) forces will not be effective in combat activities.

Changes in the Russian way of conducting military activities were already spoken of by the general Valery Gerasimov on 26 January 2013, during the meeting of the Academy of Military Science members, summing up the work of Academy in 2012. In his speech, the general pointed out the fundamental changes in warfare law, introduced, among others, as a result of increased role of non-military resource applied to achieve political and strategic objectives. He emphasised that they have been repeatedly proven to be more effective than the used weaponry or classic military methods and frontal confrontations between large, military formations are becoming obsolete. The new types of warfare are mixtures of political, economic, informational, humanitarian and other methods of large-scale influence. Exerting a contact-free (distance) effect on an opponent is becoming the main method of achieving combat and operations objectives, and destruction of its facilities occurs throughout the entire territory. Differences between the strategic, operational and tactical levels, between the offensive and defensive activities, are becoming blurred.[15] He claims that: "Asymmetrical activities allowing for nullification of opponent's advantage in

---

13 T.M. Huber, *Compound Warfare: A Conceptual Framework*, in: T.M. Huber (ed.), *Compound Warfare: That Fatal Knot*, U.S. Army Command and General Staff College Press, Fort Leavenworth 2002, p. 1, online access:http://carl.army.mil/download/csipubs/compound_warfare.pdf – downloaded in June 2015.

14 Author's translation – Ibidem, p. 1.

15 В. Герасимов, *Новые вызовы требуютпереосмысления форм и способов ведения боевых действий,* Военно-Промышленный Курьер No 8(476), 27 февраля –5 марта 2013 года. Main theses in the lecture on *Basic tendencies in developing forms and methods of the armed forces usage, current tasks of the military science in their improvement* – by the Russian Federation Chief of Staff, General Gierasimov – online access: http://vpk-news.ru/sites/default/files/pdf/VPK_08_476.pdf – downloaded in April 2015.

military combat leaped to prominence. These include using the special forces in operations[16] and internal opposition forces to establish a permanent front within the whole territory of a hostile country, as well as exercising informational influence, the forms and methods of which are constantly changing"[17]. Theses formulated in this way stem from the analyses of recent conflicts in the Middle East and experience of Russians drawn on guerrilla forces from the years of the Great Patriotic War and on fighting with irregular formations in Afghanistan and in the Northern Caucasus.

As the defence specialists noticed, *the hybrid conflict*, contrary to the classic one, does not undergo development over the course of time according to a determined dynamics and does not only occur within a limited combat area, but it is more extensive and multi-layered in scope, reaching cultural, socio-political, economic, or even psychological spheres, where a result of given confrontations affects what happens in the military activities. It was also stressed out in the lecture by general Gerasimov.

An analysis of the available hybrid war definitions indicates that they can be recognised as having a nature of hybridity, as the essential characteristics of this type of activities are present there. In its armed struggle for Islamic identity and values (the fight against globalisation and the Western lifestyle; the internal religious conflict between Sunnis and Shiites) ISIS combines the activities of conventional forces (organised militant troops fighting against the Syrian and Iraqi armies and coalition forces) with unconventional forces (all kinds of guerrilla and opposition groups operating in other countries, e.g. Libya, Mali), additionally supported by terrorist attacks (France, Belgium, etc.) and criminal activities (organised crime). All these activities are reinforced by exerting informational influence, appropriately prepared, primarily aimed at evoking and constantly raising awareness of threat among opponents, using modern forms and means of communication in all available media. Researchers of *hybrid wars* clearly point out that an essential element of strength held by a *hybrid enemy* is external support, i.e. the so-called state sponsor. With regard to the so-called Islamic State, there have been many sponsors at different times of its existence, the most important being the Sunni states, including Saudi Arabia and Qatar, and their financial contributions. Turkey, which allowed the recruitment of ISIS fighters on its territory and their transit across its borders, and bought oil from them, can also be called a sponsor. Israel was another country that supported the fighters by providing medical assistance to injured fighters on the Golan Heights.

---

[16] Significance of special forces in future conflicts was validated by 2013 establishment of the Special Operations Command, to which all the other sub-units of Spetsnaz were subordinated – note by the author.

[17] Translation: G. Kuczyński, *Strategia Rosji wobec Zachodu*, the quarterly of NSB *Bezpieczeństwo Narodowe* no. 9-10 (I-II/2009), p. 159 – online access:http://www.bbn.gov.pl/pl/prace-biura/publikacje/kwartalnik-bezpieczens/wydania-archiwalne/9-102009/1671,Irak-Piec-lat-i-co-dalej.html –downloaded in January 2015, p. 2.

A separate analysis should be made in the scope of support provided by the USA and other Western countries to Arab opposition groups before and during the so-called *Arab Spring*, which was later joined the ISIS ranks and had variable impact on the current situation in the Middle East and Europe. Each of the presented protectors had and still has a different purpose: Saudi Arabia – to weaken Iran's role in the Middle East through the fall of the Assad regime in Syria and the fight against Shiites, who Sunnis see as traitors of Islam, something worse than infidels – followers of other religions; Turkey –to find a solution to the Kurdish problem; Israel – to bring down the Assad regime and recover the Golan Hills from Syria.

Further exploration of the *hybridity of activities* deals directly with the already known *asymmetry* in the area of security, which consists in determining the disproportion between participants in the conflict by comparing the war potential of the opposing parties resulting from numerical combination of forces and means applied in combat. It should be stressed, however, that complexity of contemporary conflicts and the variety of ways and means of resolving them dictates that a visible difference between the parties does not necessarily mean strategic imbalance between the opponents. This can be seen very clearly from the comparison of the combat potential of ISIS fighters and coalition states – overwhelmingly in favour of the coalition, but as a result of the complexity of activities in the political and cultural areas in the Middle East and their direct impact on the area of military activities, as of 2016, the so-called Islamic State was not brought down yet. It validates the thesis voiced by many security experts that technological superiority, organisational excellence and psychological superiority are not the decisive factors for ultimate success today.

When analysing the asymmetry in ISIS activities in terms of threat to the southern flank of Europe, one should refer to the definition of asymmetry as formulated in the science of security, which the *Defence Lexicon* describes as: "(...) a different way of thinking, organising and acting, resulting from social, civilisational and military factors, pursuing victory by maximising one's own strengths and exploiting the weaknesses of an enemy".[18] The same source also points to forms of asymmetry resulting from the adoption of criteria for division, such as: disproportion, difference and incompatibility. Among the forms of asymmetry the following are distinguished: *classical asymmetry and non-classical asymmetry*. The latter is divided into: "(...) asymmetry of involvement, civilisational and cultural asymmetry, technological asymmetry and systemic asymmetry". For further consideration it is necessary to provide a definition of *asymmetry of engagement* which "includes involvement not only of the armed forces but also of society as a whole in the course of military activities. This is particularly important when one of the parties to a conflict treats the fundamental values of life and death differently.

[18] M. Huzarski, J. Wołejszo [ed.], *Leksykon obronności. Polska i Europa*, Wyd. Bellona, Warsaw 2014, p. 173.

The asymmetry of engagement also applies to a role, duration and extent of participation in the conflict. It is closely related to the factor of willingness to engage in a fight, but most often it occurs in conflicts entailing a great cultural difference between antagonists. It emerges when one of the opponents is mentally prepared for a long battle, while the other wants to finish it as soon as possible".[19] What is closely associated with this definition is the *civilisational and cultural asymmetry*, which refers primarily to perceiving war by hostile parties and is considered through the prism of civilisational achievements, such as: the way of exercising power, socio-political system, education of society, its religion and the standard of living.[20]

Interesting conclusions on *hybrid activities* were drawn from an analysis of Israel's actions in Lebanon against Hezbollah in 2006, and Hamas in 2009 – it was carried out on behalf of the US army's land forces.[21] The author of the analysis, David E. Johnson, showed that in the clash with Hezbollah (2006) the methods of fighting used in the conflict in Kosovo (1999), as well as in OEF operations in Afghanistan and OIF in Iraq in Iraq, in the form of the so-called "fire attack", using primarily airborne attacks on enemy targets without land operations, turned out completely ineffective. In addition, misconstrued conclusions drawn by the Israeli military personnel led to the training of ground military sub-units being focused solely on preparing them for Low-Intensity Conflict (LIC) and to counter-terrorism activities, thereby severely weakening their ability to carry out joint arms operations[22], including the removal of Joint Terminal Attack Controllers (JTACs) from the brigades.[23] In fact, the Israeli Defence Forces (IDF) were confronted with disciplined and well-trained small sub-units, equipped with modern weapons (anti-tank guided missiles, rockets, mortars, mines and IEDs, as well as man-portable air-defence systems), which additionally took advantage of the field conditions (hilly terrain). After suffering initial losses, the IDF modified its tactics and started to eliminate the enemy by isolating its position (using strikes – artillery and air attacks) and then dispatching ground sub-units supported by tanks.

---

19 Ibidem, p. 175.

20 Ibidem, p. 173.

21 D.E. Johnson, *Military Capabilities for Hybrid War. Insights from the Israel Defense Forces in Lebanon and Gaza,* RAND Corporation 2010, accessed online: http://www.rand.org/content/dam/rand/pubs/occasional_papers/2010/RAND_OP285.pdf – downloaded in July 2014.

22 It includes the fight conducted by formations including various types of armies and armed forces. The basic formation of the combined forces in a tactical unit (division, independent brigade), and in relation to the modern combat rules with the use of the so-called combat modules, one may speak of a brigade or a battalion combat group – note by the author.

23 Ibidem, p. 2.
Similar conditions occurred out of directing NATO to expedition missions, which, in given Member States, led to limitation of finances fed to the military, also resulting in army reductions, especially the heavy units – note by the author.

Israeli experience allowed to recognise the characteristics of a *hybrid* opponent, who is both trained at a medium level and disciplined. Structurally, its forces are organised to the level approximating a battalion. They are equipped, similarly to the irregular forces, in small, including RPGs, as well as mortars and short-range rockets, and have the capability to lay down indirect fire on targets with anti-tank guided missiles, MANPADS and mid-range missiles. An essential element of its strength is an external support, the so-called state sponsor, an example of which is Iran in relation to Hezbollah, or the USA in relation to the Mujahideens in the 1980s, during the USSR's activities in Afghanistan. The characteristics presented also apply to activities in eastern Ukraine, where separatists supported by Russia are equipped with armoured weapons, rocket artillery systems (GRAD, SMIERCZ, TORNADO-S) and anti-aircraft rocket systems (IGŁA, BUK).

As security experts point out, there is a very simple way to transform an irregular enemy with a multi-cellular structure (scattered groups of team count at maximum), low level of training and small arms, into effective, close-formation sub-units, if the so-called state sponsor emerges – the one able to provide armament and equipment, as well as ensure training. In today's conditions, Iran (Shia militia in the fight against the so-called Islamic State) and Russia (separatists in eastern Ukraine) are effectively doing this. On the other hand, the Americans experience problems with establishing Sunni Syrian guerrilla (among others, the organisation trained in Turkey, known as "*Division 30*"), supposed to be a force capable of fighting with the radicalism of the so-called Islamic State.

Experience gained from the wars in Iraq, Afghanistan or from the *Arab Spring* clearly shows that it is essential in modern wars to be able to combine military operations with civilian management, not only in crisis and post-conflict situations, but also in the course of a conflict. In the phase of military intervention, the asymmetric advantage of armed forces of a state or a coalition is sufficient to take control over a given area and create conditions for establishing local institutions of state authority. However, it turns out to be useless in the next phase of activities, i.e. stabilisation of the post-conflict situation, in which the *hybridity of activities* may be occur, changing the power relations of the parties to the conflict and forcing modifications, or even complete change of strategic objectives, operational and tactical tasks, as well as manners and methods of their implementation. All acts of terrorism are prominent in this phase and various forms of organised crime emerge. Herfried Münkler[24] analysed such situation and drew attention to the so-called pathologies accompanying modern wars, which are exploited differently by the parties to the conflict. These are: uncontrolled migrations (hard to control exodus of people from Africa and the Middle East to Europe – the so-called southern flank), trafficking in

[24] H. Münkler, *Wojny naszych czasów*, WAM, Cracow 2004, p. 97-128, [in:] A. Gruszczak, op. cit., p. 16.

human beings and sexual violence (e.g. the situation of Syrian women in refugee camps in Turkey), drug smuggling and trafficking, as well as overexploitation of raw materials and culture (e.g. trafficking in stolen cultural heritage by the so-called Islamic State). This would mean that the modern armed forces are required to combine their combat capabilities with those held by law enforcement and law enforcement authorities, such as police, border guards, customs service, etc.

It is precisely by drawing such conclusions and concentrating efforts on solving problems using light expeditionary forces far from their own borders the defence spendings have been reduced and regular forces have been cut short in most western countries, resulting in a drawback to NATO's combat capabilities and emergence of a dilemma as to the real possibility of fulfilling the allies' obligations under *Article 5 of the Washington Treaty*. The thesis put forward by Carl von Clausewitz was confirmed: "(...) war was created by politics. Politics is intelligence, and war is only an instrument, not the other way round. Thus, the only thing that remains is to make the military perspective subordinate to the political one"[25].

Below the author presents a hypothetical scenario of a hybrid conflict:

1. *Routine activity of Military Intelligence and Special Purpose Forces.*

Symptoms:
- permanent international cooperation (regional);
- exercising permanent international influence in the following areas: finance, economy, power industry, etc;
- conducting information campaigns within the society through the media (press, TV, Internet);
- purchases of equipment and organisational changes in accordance with the adopted plans;
- planned (cyclical) training courses for the Special Forces, Air Forces and Navy;
- reconnaissance and intelligence activities conducted at a constant level.

The main activities include e.g. the planned implementation of the *National Armament Programme for years 2011-2020* or ensuring compliance with international law and the *National Security Strategy of the State until 2030.*

2. *An increase in tension in bilateral relations.*

Symptoms:
- information activities at international and national level;
- the cooling of diplomatic relations;
- initiating actions: economic pressure (limiting the supply of power resources), introducing bans on importing specific products;

[25] C. v. Clausewitz, *O wojnie. Szkice do księgi VIII – Plan wojny*, Wyd. MIREKI, p. 456.

- policy changes and possible changes in war doctrines;
- Attempting to obtain information for the nomination of personal targets and critical state infrastructure;
- intensified reconnaissance activities (flights, cruises, satellite systems), increase in the number of WSP (Military Fire Brigade) exercises and specialist training courses, unplanned purchase of military equipment.

The main activities are the initiation of informational war, including the use of disinformation and propaganda elements, e.g. describing the government as "fascists", running a new historical policy, "monument wars", etc. In addition, direct use of owned media platforms, such as "Russia Today", radio "Sputnik", as well as social media (Facebook, Twitter, Instagram) and activities in cyberspace (cyber espionage, attacks on selected portals related to national security).

3. *Growing threat, increased activity of the Military Intelligence and the Special Purpose Forces*

Symptoms:

- attempts at stirring unrests between a state and its neighbours/NATO/EU (economic, ethnic, migration, export, currency, political and social pressure);
- attempts at buying out/buyout of strategically important treasury companies;
- discrediting the authorities at international and national level;
- creation of legal and administrative barriers at international hindering the functioning of armed forces at the international scene (conferences, transfers of troops and military equipment);
- influencing the staffing of key positions in a country by passive and/or controllable persons;
- influencing representatives of state and local authorities at lower levels;
- intensification of INFOOPS activities (disinformation, propaganda) effected on one's own society and on the international community and in the country concerned;
- using Polish minorities for provocation by the pro-Russian political forces for propaganda purposes on the territory of neighbouring countries;
- an increase in tension and insecurity (violations of air and sea space, military flights at low altitudes with transponders switched off);
- increase of intelligence activity (creation of new directions and structures);
- display of power through demonstrative manoeuvres of the Special Forces and the Airborne Forces.

Possible actions of the opponent include, predominantly, accelerating the implementation of e.g. "State Programme for the Modernisation of Armaments", violation of airspace, especially in the vicinity of borders, attacks in cyberspace on: communication systems, defence and security subsystems, subsystem of support

for the state economy, financial sector, power sector, transport, health service and intensification of cyber espionage, using the owned resources, as well as through sponsored groups. In addition, creating divisions in society can be pursued by using ethnic and national minorities to organise demonstrations, riots, unrest, and to trigger events, "accidental disasters", involving critical infrastructure, such as setting fire to bridges, damage to road junctions, etc.

4. *Emergency situation, creation of conditions for the implementation of operational and special activities*

Symptoms:
- increased border traffic (including from NATO and EU Member States);
- an increase in the number of tourists, in particular in the areas adjacent to the border area and in the regions where the sites of key importance for the state's security are located;
- an increase in the number of military exercises and manoeuvres in direct contact with the border area;
- an increase the number of diplomatic shipments and further intensification of intelligence activities within the national territory;
- intensified activities in collecting information to target individuals and critical state infrastructure;
- cooperation with pro-Russian political groups (including funding) and opinion-forming environments;
- international exploitation of the so-called useful idiots (actors, journalists, politicians);
- strengthening illegal links between criminal groups and business communities;
- exploitation of criminal groups;
- an increase in the number of troops in border areas;
- increasing the activity of the Border Guard Service of the neighbouring country;
- attempting to disintegrate the state security system by increasing cyber attacks.

The main activities of the opponent include influencing the economy/finance of a state by using the acquired companies/companies of strategic importance, violating the state border in order to check reactions and run a recon on border protection system, creating trafficking channels and "leakage" of the state border and provocations, intimidation of local government officials, the Border Guard, the Police. In addition, it is possible to trigger "Bomb Alerts", attacks on critical infrastructure for state security, such as triggering "Blackouts", identifying objects as targets for future attacks, the appearance of persons acting as advisors ("instructors"), especially among criminal groups and social dissatisfaction and groups formed on the basis

of national minorities, recruitment and training of persons to paramilitary groups, as well as provoking riots and public demonstrations and attempts to intimidate the population in the areas where national minorities exist.

5. *Direct threats and operational and special activities*

Symptoms:
- the concentration of troops in border regions;
- use (replacement) of the Border Guard by the army;
- armed, unmarked groups (including GRGs, criminal and paramilitary groups) occurring in border areas and key areas;
- increased border crossing attempts of persons whose passports contain modified spelling transcriptions of their personal data;
- increase in number of crossing the country borders from the territory of another EU country (intentional circumvention of Polish border control);
- obtaining visas and legal entry (false declarations of the "employer's" intention to give a job to a foreigner, "confirming" the booking of a hotel or a boarding house, participation in "religious pilgrimages", in "training courses and conferences");
- an increase in the number of illegal workers;
- mass irregular border crossings by individuals and groups.

Possible actions of an opponent at this stage include crossing borders and creating bases, hiding places for storage of explosives, weapons and ammunition, kidnappings, murders, assaults, roadblocks, crossings, communication facilities, elimination of individual targets, mass attacks in cyberspace, recon and disorganisation of the defence system. It is to be expected that the system of supplying military and material resources will be disrupted and destroyed, material and fuel stocks will be wiped out, local administration facilities and entire towns will be seized, the command and communication system of military units and state administration bodies will be disrupted, military traffic will be blocked, mobilisation process will be disturbed, riots will be provoked, Western countries will be deterred/intimidated by the demonstration of military force and that targets for long-range aviation and missile artillery strikes will be designated.

In conclusion, it is worth noting that the hybrid war is a fusion of classical military activities, both the regular and the irregular ones (guerrilla, sabotage, diversion, terrorist acts), combined with elements of informational warfare (propaganda, disinformation) and cyber-warfare, as well as activities carried out in the political, economic and cultural spheres. It is a non-declared war, and according to international law, it is formally not even a war. Taking into account the conclusions of the hybrid war analysis, it is possible to consider the occupation of the Crimea by Russia as a model example of conducting hybrid activities through a skilful combination of informational warfare, exercising political and economic influence,

supported by the activities of the army and irregular sub-units. An attempt to re-create this operation in the eastern Ukraine failed, which highlights the complexity of the modern security environment and confirms the rule stating that every war is different. Technological superiority, organisational excellence and psychological advantage are not the decisive factors guaranteeing victory in the combat of today. Modern armies should make use of more flexible methods of fighting and means to engage with both classic and new opponents with a different degree of organisation than a regular army (Al-Qaida, Hezbollah). The essence of this new opponent's activity is a wide use of unconventional methods, often going beyond the standards of international law (e.g. attacks on civilians), and avoiding the places and areas where opposing forces have a definite advantage.

BIBLIOGRAPHY

[1] Clausewitz C.V., *O wojnie*, Wyd. MIREKI, 2010.

[2] Evans M., *From Kadesh to Kandahar. Military theory and the future of war*, „Naval War College Review", 2003, no 3.

[3] Gierasimov V. (Валерий ГЕРАСИМОВ), *Новые вызовы требуютпереосмысления форм и способов ведения боевых действий,* Военно-Промышленный КурьерNo 8(476), 27 февраля – 5 марта 2013 года. Main theses in the lecture on *Basic tendencies in developing forms and methods of the armed forces usage, current tasks of the military science in their improvement* – by the Russian Federation Chief of Staff, General Gierasimov – online access: http://vpk-news.ru/sites/default/files/pdf/VPK_08_476.pdf – downloaded in April 2015.

[4] Gruszczak A., *Hybrydowość współczesnych wojen – analiza krytyczna*, [w:] *Asymetria i hybrydowość – stare armie wobec nowych konfliktów*, red. W. Sokała, B. Zapała, Warszawa 2011.

[5] Hoffman F., *Conflict in the 21st Century: The Rise of Hybrid Wars*, Potomac Institute for Policy Studies, Arlington 2007, online access: http://www.potomacinstitute.org- downloaded in November 2014.

[6] Huber T.M., *Compound Warfare: A Conceptual Framework*, in: T.M. Huber (ed.), *Compound Warfare: That Fatal Knot*, U.S. Army Command and General Staff College Press, Fort Leavenworth 2002 r., p.1, online access:http://carl.army.mil/download/csipubs/compound_warfare.pdf – downloaded in June 2015.

[7] Huzarski M., Wołejszo J. [ed.], *Leksykon obronności. Polska i Europa*, Wyd. Bellona, Warsaw 2014.

[8] Johnson D.E., *Military Capabilities for Hybrid War. Insights from the Israel Defense Forces in Lebanon and Gaza*, RAND Corporation 2010, accessed online: http://www.rand.org/content/dam/rand/pubs/occasional_papers/2010/RAND_OP285.pdf – downloaded in July 2014.

[9] Koziej S., *Bezpieczeństwo Polski w kontekście walki informacyjnej związanej z wydarzeniami na Ukrainie*, program publicystyczny *Racja Stanu* – TVP Polonia, date of publication 23.02.2015, available online: http://www.bbn.gov.pl/pl/wydarzenia/wypowiedzi-szefa-biura/6463,Szef-BBN-dla-TVP-Polonia-trzeba-wykorzystac-zainteresowanie-spoleczenstwa-sprawa.html?search=68766446 – downloaded in May 2015.

[10] Kuczyński G., *Strategia Rosji wobec Zachodu,* the quarterly of NSB *Bezpieczeństwo Narodowe* no. 9-10 (I-II/2009), p. 159 – online access:http://www.bbn.gov.pl/pl/prace-biura/publikacje/kwartalnik-bezpieczens/wydania-archiwalne/9-102009/1671,Irak-Piec-lat-i-co-dalej.html – downloaded in January 2015.

[11] Lasica D.T., *Strategic Implications of Hybrid War: A Theory of Victory*, School of Advanced Military Studies, United Army Command and General Staff College Press, Fort Leavenworth 2009.

[12] McCuen J. J., *Hybrid Wars*, „Military Review", 2008, no. 2.

[13] Münkler H., *Wojny naszych czasów*, WAM, Cracow 2004.

[14] Walker R.G., *SPEC FI: The United States Marine Corps and Special Operations*, Storming Media, Monterrey 1998.

HYBRYDOWOŚĆ – CECHA NOWYCH WOJEN

Abstrakt. Termin „hybrydowy" używany w odniesieniu do domeny wojskowej okazał się bardzo popularny na początku obecnego stulecia. Związane jest to z wykorzystaniem innych niż wojskowe narzędzi w połączeniu z wojskową presją, aby wpłynąć na sytuację bezpieczeństwa w innych narodach. Opiera się na prawidłowym założeniu, że nie jest konieczne wykorzystywanie siły bojowej w zglobalizowanym świecie do wpływania na wewnętrzną sytuację innych narodów, co może prowadzić do ich częściowego lub całkowitego podporządkowania.

Słowa kluczowe: hybryda, wojna hybrydowa, wyzwania hybrydowe, NATO, Rosja, asymetryczne działania, wojna na Ukrainie.