BUILDING UP STATE STRATEGIC RESISTANCE AGAINST HYBRID THREATS

Mirosław BANASIK

COL. ret., Associate Professor, Jan Kochanowski University, Kielce, Poland

Hybrid warfare, conducted in Ukraine since 2014, has become a new geopolitical phenomenon which threatens the Euro-Atlantic security that appeared after the collapse of the bipolar world. The paper discusses how the Russian Federation takes advantage of hybrid warfare to achieve its political objectives and to further its own interests. The paper also contains an assessment of the threat of hybrid warfare in Poland and determines what undertakings are necessary to effectively counter threats coming from Russia.

Key words: *hybrid war, hybrid threats, contemporary military conflicts, resilience*

1. INTRODUCTION

Russia twice surprised the West within the last two years. The first time Russia negated the West's wrongful conviction of Russia's Armed Forces' low effectiveness. As it turned out the international community was not able to reply in a coordinated maner to hybrid actions which led quickly to Russia's strategic advantage not only towards Ukraine but also the entire Western world. Hence, Ukraine as a state became incapable to lead its existence as an independent state. What is more, after two years we can still notice the helplessness of international organizations and separate states towards hybrid war. It turned out to be the second surprise when Russia used its armed forces in Syria for the first time from the end of the Cold War and outside the borders of the former Soviet Union. It is not yielding to the doubt that the European Union which has been adhering to the principle soft power solved neither the problems of Ukraine, nor its own problems with the immigration wave. In this situation the thesis right which states that Russia is the main beneficiary of the international policy seems to be. In experts' opinion Russia's success in foreign policy is owed to the military instrument. That has broken successfully the USA monopoly on

using armed forces in interventions with expeditionary character.

According to P. Goble the pace of preparing Russia for the global confrontation with West increased (Goble:2016). At the present we can observe that fundamental changes of the course in the Russian politics took place. Just the opposite, the fact supporting the above mentioned is the attempt to draw Belarus into the confrontation with the Western states. Analysts of the Belarusian Centre for Strategic and Foreign Policy Studies claim that Belarus while keeping the neutral position in the face of the crisis in Ukraine and the full control over its own territory performs a significant contribution into the stability of the region. However, recently one can see unprecedented military and political pressures to Belarus on the part of Russia which can allow Russia to create the gray zone (Banasik:2016 a) from which the Russian Federation (RF) will steer conflicts in the region and run the confrontation with the West (Białoruski:2016).

More and more in Moscow there are opinions emerging about the real war led up with the West and this is not just the propaganda of political leaders or media. These ideas have the dimension of real moves directed to the dominance of the armed forces of the Russian Federation and in consequence to achieving victory in the future hypothetical confrontation (Krutikov:[2016]). The success relatively easy reached in Georgia in 2008 and in Ukraine in 2014, as well as the effective projection of armed forces in Syria and grade-separated adaptation to the local conditions of military strategy made some top Russian commanders feel a probable victory against NATO in the future.

2. RUSSIAN PERCEPTION OF HYBRID WAR

In the geopolitical context hybrid war is a new concept. Russian strategists understand hybrid war as the concept applied mainly in the sphere of special operations connected with the actions of opposition forces, as well as exploiting experience of the fight against the national radicalism and non – state actors jeopardizing international security (Bartosh:2015, p.73). On the account of the nondirective influence on all possible spheres of state functioning and in all dimensions with military and non-military instruments of the influence, hybrid war is an excellent mechanism leading to the destabilization of the neighbor states of the Russian Federation. In the dynamic way it joins hard and soft power which includes entire societies (Palmer:2015, p.8) taking into consideration cultural and physical aspects. Hybrid war joins the final state of actions, capabilities, takes into account the risk, guarantees the achieving of the planned political aims. This perceived conceptualization of hybrid war can justify the argument

that it is a strategy in the hands of politicians and according to F. Hoffman's opinion allows for preventing the disadvantageous conduct of the potential opponent as well as the forming of its own conduct (Manea:2016).

V. A. Kiselev and I. N. Vorobiev point out the geopolitical dimension of hybrid war. They introduce the notion of hybrid war as the form of conducting the warfare (military actions). According to them the hybrid operations are conducted in order to tear the part of the territory of the state and incorporate it with another state. It is made with the help of comprehensive political and diplomatic, information and propaganda, financial and economic undertakings, and also those of military character. In addition, a military campaign in its meaning is not conducted stricto senso. The actions on the opponent territory can be backed up with special operations and armed structures which are organized and prepared earlier for acting on the territory being a subject to a detachment and their task is to neutralize the armed forces of the opponent (Kiselev:2015, p.1).

Making oneself aware of the essence of hybrid war it is important to understand what way the Russians perceive war in general. The Russian comprehension of war is settling *on the social and political phenomenon of radical changes to the relations between states and nations and moving the opponent from using non-military and forceless forms and methods of rivalry to the direct application of measures of the armed struggle for the achievement of the determined political and economic targets* (Rogozin). Other measures mentioned in the definition hint at hybrid as directed to the strong and weak points of the opponent. The war is hybrid by linking aspects of insurrectionary action treated as the element of the irregular war with the actions of the conventional armed forces. Threats are growing constantly. However, the level of aggression is always below the threshold of the open armed conflict. Such a situation causes growing pressure in the international relations. The dominance of hybrid actions causes the local escalation of conflict and reveals the next sensitivities. The threat of using regular armed forces creates also a strategic advantage of the Russian Federation in such places as Crimea or Syria and that causes the fear that in a direct confrontation there is a lack of a robust reply not only from the side of the opponent but also from the side of international organizations.

3.THE POLISH PERCEPTION OF HYBRID WAR

The National Security Bureau (NSB; Biuro Bezpieczeństwa Narodowego – BBN) undertook the definition of hybrid war. In the proposal of new definitions from the field of the security, hybrid war is understood as *the war combining different possible means and*

methods of violence simultaneously, including especially regular and irregular armed operations, operations in the cyberspace and economic, psychological actions and information campaigns (propaganda) etc. (Słownik). The notion of subliminal aggression supplements the above mentioned definition and allows for a better understanding of hybrid war. According to Professor S. Koziej, in its confrontation with NATO the Russian Federation can use the method of aggression below the threshold of open regular warfare, i.e. the so-called subliminal aggression as one of the element of hybrid war (Pach:2016). The subliminal aggression is understood *as the warfare where the swing and the scale are limited on purpose and kept by the aggressor on the level of the threshold below letting identify regular open war.*

*The aim of the subliminal aggression is achieving the proposed objectives and simultaneous causing troubles for international security organizations in agreeing upon the decision-making course of action (*Słownik). Hybrid war is understood by M. Fryc a bit differently in comparison with NSB. The author's of this article point of view is that hybrid war is directed at reaching strategic objectives. *A whole range of diverse both material and immaterial, military and non-military, legal and illegal, direct and indirect measures are used for it. In its essence it takes the total dimension. Next approximately it selects and links to the action so that they bring the intentional effects. All possible measures are used (political, diplomatic, military, information, economic and cultural) which concur together for the direct threat and indirect pressure with the limited actions using the armed forces* (Fryc:2015, p.65). Worth underlining is that in hybrid warfare the space of the influence is crucial. Unlike the traditional war, it does not limit itself to the physical dimension and it is current in other dimensions in which so far regular armed forces did not have influence. In hybrid war, the triggering of the planned and desired effects is synchronized, which according to M. Fryc is significant.

In this respect, A. Deep applies an innovative approach and claims that effects are achieved thanks to applying asymmetric techniques and tactics, which are next synchronized on the multidimensional battlefield (Deep:2915, p.1). F. Hofman indicates the synergetic effect in physical and psychological dimension of the conflict. He also claims that the above mentioned effect can be achieved through multidimensional activities carried out by separate entities (even just one subject), but in general they are directed operationally and tactically in the main space of the hybrid war (Hoffman:2007, p.8).

Taking into consideration all quoted arguments we should think that **hybrid war is a strategic**

category. We should understand hybrid war as the war directed at achieving political objectives thanks to triggering synchronized kinetic and behavioral effects, by multidimensional applying of the instruments of the influence and capabilities which are in the disposal of the attacking party.

4. THREATS OF HYBRID WAR IN POLAND

In the opinion of Polish political and military decision-makers or experts, open NATO border crossing by the Russian Federation and the aggression on a large scale are rather improbable. Triggering the war with NATO is an inconceivable decision but it is not possible to rule it out. The full-scale warfare and peculiarly with using the weapon of mass destruction would be, however, a suicide. The Russian strategic doctrine assumes after all attacking the enemy on the whole depth of its territory, in all possible dimensions of the influence. Consequences of such action would be dangerous for the Polish allies. It is estimated that not only due to the treaty obligations, but also in their immediate strategic interests, the allied states would be interested in stopping aggression as far as it possible from their territories. The rational strategic calculation would suggest them to dispatch troops to stop the aggressor in Poland, overthrow it up as soon as possible so that do not conduct any fights on their territories and avoid losses in a follow-up war (Pach:2016). In the Polish reality the threat of hybrid war is more probable combined with limited kinetic action.

The so-called grey situations are considered to be the biggest threat in Poland and in NATO as well. The Russian Federation on purpose keeps the level of aggression below the red line which determines the border of a conflict. Russia consciously avoids violating Article 5 because it is in Russia's interest to avoid direct confrontation with the opponent which has a global majority of conventional power. In circumstances of non-supporting political climate, a competent selection and application of instruments and methods of influence by the potential aggressor can lead the international community to ambiguous statements. It is estimated that in such situations we would react in a longer time and in some cases perhaps all the time, independently. This can be caused by an aggression limited temporarily, by space and by involved forces. Moreover, it can be applied hidden, irregular, sabotage, and asymmetrical activities combined with selective surgical strikes of „unknown authorship", terrorist attacks in combination with the application of non-military means of violence to which it is possible to enumerate information war, cyber-attacks, energy blackmailing etc., as well as possible local collaborators (Pach:2016). Considerable risks connected with hybrid war can constitute unidentified individuals

who appeared in Ukraine and were called *little green men*. This is the notion which is popularly applied *to identify soldiers without military insignias or other signs, which would let the identification of their nationality, who run the armed regular and irregular operations on the territory of the Eastern Ukraine measured up against its integrity and independence* (Słownik).

In Poland it is considered that it is not possible to ensure the matter of the state security exclusively by enlarging the military strength. It is necessary to look at it from the perspective of the functionality of the entire national mechanism, in particular these processes which protect us against the effects associated with the internal threat. These hybrid threats can take the format of offensive actions in cyberspace, multi-dimensional diplomatic actions and the threat of performing terrorist attacks and disinformation operations. Equally important threats are attempts of destabilizing the political and economic situation through the compilation of action aimed at strategic objectives of the state, political sabotage and activities of hostile centers of propaganda (Ścios:2015).

The activity of the Russian secret services clearly intensified in Poland. Espionage is one of very effective forms in the frames of hybrid war. According to S. Koziej, hybrid war lasts already nowadays in the essence of considerable political and strategic pressure. *We are all the time under this pressure, this information war, for instance, this frightening, blackmailing by flights, transferring rockets, this all takes place* (I kto tu:2015).

A spectacular example of hybrid war was conducting the attack using anti-Polish propaganda against the state's interests. The minister of national defense and his spouse were attacked with counterfeit and completely irrational indictments which generated an increased public interest and build an atmosphere of suspicion. The further step consisted on including into the political action the agents of influence and using the publication as a pretext for formulating the application of dismissing the Minister of National Defense. The correlation of specific stages of influence shows that we dealt with synchronized and completely deliberate action the culmination of which had to take place in the eve of the Warsaw NATO Summit. The objective of this operation was undermining trust to the minister and management of the MoD, redirecting the public attention, triggering chaos and information confusion, weakening the negotiation position of Poland during the summit and creating negative image of the Polish authorities in the eyes of the NATO partners (Ścios:2015).

The Report of the Computer Security Incident Response Team presenting the data for 2014 does not leave any doubts that Poland became the target of one the elements of

hybrid war - which is information warfare. It is evident the distinct growth in dynamics of persistent, long-term attacks based on advanced tools. It means that apart from quantitative progress, the significant qualitative progress is also observed in led attacks. Simplifying the above stated, it is not enough that there are more attacks but they are currently much more dangerous. The crucial factor here remains a participation of groups managed and sponsored by foreign states.

In this regards, there were noted the attacks conducted on the Polish President's website and stock exchange website, as well as on some websites of public administration institutions. The „Cyber Berkut" group claimed its responsibility for the mentioned attacks, giving alleged incorporation of Poland into the conflict situation in Ukraine (Raport:2014, p.38). Computer Security Incident Response Team underlines that the Internet and social media – on account of availability and the easiness of using them – became also the tool applied for assisting military and intelligence actions led by the states through the effective usage of the propaganda and disinformation actions. Analysis of Internet discussions in social media during last year indicated a precipitated, increased and unnatural usage of this subject in the activity of Internet users (the so-called trolls which give comments to the Russian Federation actions connected to the Crimea annexation and conflict in Ukraine). Comments of this type literally "flooded" Polish information portals in the initial phase of the Ukrainian conflict (Raport:2014, p.48).

5. WAYS OF OPPOSING HYBRID THREATS

Hybrid character of the armed activities, including the spectrum of measures applied in the Russian-Ukrainian conflict, constitutes today the main challenge for the state authorities, as well as the reactivation of defensive systems or decisiveness of international security organizations. The reply to such a threat must assume multidimensional and international character. It requires creative thinking and appropriately coordinated combined activities of different institutions, services as well as applying untypical tools and capabilities (Fryc:2015, p.66). In Poland it was paid attention to hybrid threats both in *the National Security Strategy of the Republic of Poland* and *in the White Book on National Security of the Republic of Poland.* In the *Strategy* attention is being paid to the fact that in adverse circumstances military threats to the security of Poland can appear and they can take the form *of armed conflicts of different scales - from the military action below the threshold of the classic war, to less probable conflict on a large scale* (Strategia:2014, p.20). In the *White Book* attention is turned to the fact that in the foreseeable perspective high probability of the out of the

territory conflict appears. This means such a form of threat in the frames of which the opponent is not aspiring for taking control over an attacked territory but uses the measures with consciously limited range, and unknown authorship which are calculated on „disarmament" of legal mechanisms of security and in such a way forcing the attacked party to lead independent military actions in conditions of the international isolation in the result the so-called hard agreement situations (Biała 2013, p.128).

In hybrid war context regulations of the Strategy are still valid and they concern the state created strategic resistance to aggression. Military and non-military actions are aimed at increasing the unavailability of the territory, universality of non-military structures defensive preparation, as well as weakening effectiveness of the armed forces support including the possibility of organized resistance on areas occupied by the aggressor (Koziej:2016, p.84). Under the strategic resistance of the state it is necessary to understand *capabilities of resistance and surviving aggression through: a) defensive preparation of the society (defensive and patriotic awareness of the nation, ability to behave properly in the face of armed aggression); b) increasing the operational inaccessibility of the territory (operational preparation of the territory, secure infrastructure); c) irregular and supporting activities of different state structures reinforcing regular actions of the operational armies* (Słownik).

Leading and organizing irregular actions on the territory occupied by the hybrid opponent should be performed above all by Special Forces. Nowadays there is no possibility to think about the above mentioned in categories of ancient, traditional guerrilla formations. Therefore one should consider directing the Special Forces to the national defense, increasing their number and organizing training with the other state structures on the territory of the state (Koziej:2016, p.87). Non-military security institutions should also ensure the security for the state structures, citizens and critical infrastructure against hybrid threats. This should be connected with the need of the definition of tasks and preparation of the police, secret services, self-government guards or security agencies and formations for property security (Koziej:2016, p.87). Generalizing it is possible to note that the idea of the system of resistance created in Poland is based on the coordination of various activities in many security sectors (legislative, operating, training, organizational, technical etc.) serving for the increased strategic resistance of the country to threats.

Poland takes into account that in situations of leading aggressive actions by the Russian Federation between binary borders of war and peace it would have to react independently, for a longer period

of time and in some cases all the time even. Therefore it is considered that it is necessary to prepare for hybrid threats, especially subliminal ones. The basis for the external state security assurance is proper deterrence policy which can have both offensive (retaliatory) as well as defensive (discouraging) dimensions. In offensive deterrence one should use the maximum range of the allied potential (nuclear and conventional) and build up own capabilities in a selective way (Koziej:2015, p.4). It seems that the best measure to stopping, inhibiting and deterring the potential opponent from using such a strategic method is deploying the allied NATO armies on territories of the border states (Pach:2016). However, taking into consideration the duration of reaction, permanently placed bases with equipment would be the most advantageous. In such a way the potential aggressor have to calculate into its plans that if he encroaches on the territory of the NATO state, he will enter into the conflict not only with the attacked country but also with the forces of its allied states. In the significant degree it should moderate its aggressive intentions (Pach:2016). However, conventional deterrence can turn out to be insufficient. Nuclear deterrence is more effective, especially in the situation when there is a lack of agreement of the Alliance on permanent stationing of the impressive forces on territories of the new Alliance members. It seems that in current political conditions the conventional deterrence combined with the nuclear will bring the best effects. A signal towards changes in the nuclear policy was made by the Polish F-16 aircrafts which took part for the first time in history, in the NATO nuclear exercise in 2014 and, by the informal offer of the vice-Minister of Defense Tomasz Szatkowski's from the end of the last year about stationing in Poland American nuclear tactical weapon (Sauer:2016, p.2). The best strategy for the blackmail with the nuclear weapon is creating the balance between potential incomes from the blackmailing and the scale of risk which is connected with it (Pach:2016).

The process of building capabilities for credible military deterrence in Poland was determined by „the Polish fangs" („Polskie kły"). The transformation and modernization efforts taken in the frames of the military potential lead to development of selected capabilities, which in the land, air, sea and cyber dimension will be able to deter the opponent effectively and dissuade him from the intention or attempts of conducting the armed operations against the Republic of Poland. In this case, the essence of classic dimension of deterrence is supposed to be the capabilities' achievement (by the Polish armed forces) for precise fire and counteraction for the wide spectrum of asymmetric threats (Fryc:2015, p. 69).

Apart from building up the system of the strategic resistance of the state to aggression and deterrence, it seems that in counteraction to comprehensive hybrid threats the most crucial is the use of the national power (Kitler:2010, p.118). It will be possible to perform this through integration of the national security system. It is intended to be created the Committee of the Council of Ministers on National Security and strenghten the Government Centre for Security as the Staff body of this Committee. Unfortunately the security of Poland is still being managed minister-centered. There are distinct systems of defensive and crisis reaction planning and management which reach the main office, through ministries, county offices, up to self-governments. The integrated and comprehensive approach is missed. It is necessary to integrate substantially the main strategic documents in the state concerning the security issue. The system of security management integration requires also the regulation of the law provisions, which is possible to be reached by preparing the act concerning the national security management (Koziej:2015, p.3).

Taking into consideration the biggest Polish vulnerability on hybrid threats, manifested in the form of political and military pressure mainly performed in information sphere and cyber sphere, it seems that the further priority is building up the effective information security system with a well-organized sector of cyber-security (Koziej:2015, p.4). The strategic target in the information security sphere is to insure the secure functioning of the Republic of Poland in the information space, taking into account information security of the state structures (especially public administration, security and public order services, secret services and armed forces), private sector and civil society (Projekt:2015, p.5). It is necessary to create and develop information security units (including cyber-security) in defense and protection (military and non-military) elements of the national security system. These should be the structures ready for tasks performing both in defensive and offensive character (Koziej:2015, p.5). The strategic objective in cyber-security sphere of the Republic of Poland (which is formulated in the *National Security Strategy*) is providing security for the functioning of the Republic of Poland in the cyberspace, including the appropriate level of security for the national information and communication technology systems (ICT) – in particular state ICT critical infrastructure – as well as for the key private economic entities: financial, energy, and health care (Doktryna:2015, p.9).

It is also particularly significant to ensure the sovereign operating and technical rule over highly advanced ICT systems of fight and support including management systems

(having at one's disposal source codes of their programming). Over-ministerial coordination of these issues is an important task as part of building up the integrated system of managing the national security (Koziej:2015, p.5). The above mentioned is based on the assumption that one of the hardest management aspects in crisis situations resulting from hybrid threats is the aspect of communication and working out common situational awareness, cyberspace and information sphere becoming the most prominent fields of conducting the fight and the forefront. The correct detection of the activity of the opponent and the correct functioning of the early warning system in the very two areas will decide about the capabilities for conducting of preventive operations in other dimensions concerning state security and its citizens (Liedel: 2015, p. 56).

6. CONCLUSION

In the situation of comprehensive influence of the entire Russian state against the West (which is being treated by Putin as threat), the need of having a strategy to counter hybrid threats becomes a priority. Achieving the agreement between NATO and UE and preparing the common strategy could be the representative solution. NATO should perform the leader's role in such areas as preparing the military reply, reconnaissance and scaring off and in case of a needed intervention. It seems that in peaceful times the best element of scaring off is permanent presence of the NATO armies on the territories of the most endangered countries. EU should be responsible for counteraction in the cyberspace, energy and migration policy, and counteractions for propaganda. The aspiration to achieving the synergy in all the instruments available of both above mentioned organizations should be intentional (Banasik:2016c, p.68).

East European countries facing hybrid threats, in spite of the fact that they are in the Alliance, must change their fundamental security strategies and defensive structures. Neither NATO nor EU will guarantee the absolute security of member states in the face of hybrid threats but will certainly help in building the resistance towards them. The identification of the capabilities which the state must possess (not only its armed forces) will be a big challenge for planners. As a result of that it will be necessary to change the entire process of defensive planning in such a way that to concern also non-military areas. Undoubtedly it will be necessary to increase defensive budgets, but it is not known whether the ambitious declarations taken at the Summit in Newport (concerning the allocating of 2 % of the GDP for defense) will be efficient in practice. Certainly it will be necessary do introduce changes in NATO and individual member states defensive planning. The need for creating legal and procedural mechanisms of fast using of armed forces and

synchronizing them with other non-military instruments became the priority. Centralized management on the governmental level will guarantee the integrity of all instruments and send coordinated counteraction to hybrid threats (Banasik:2016c, p. 69).

It is recommended to aspire to the integration in the frames of one security management organization of all the institutions (military and non-military, administration and media, military and uniformed forces, diplomacy, politics, NGOs, humanitarian, information etc.) with the aim of using the potential and gaining the synergy effect in the state security system. On the governmental level there is the intention to develop capabilities for the diagnosis and estimation of the threats in cooperation with NATO and winning the capabilities for the response to hybrid threats also through integrated conventional-nuclear scaring off. On the Ministry of National Defense level the change of previous law regulations is rather justified with the purpose of enabling the usage of the armed forces entire potential in peaceful times. The priority is to develop capabilities like unmanned systems of reconnaissance and classified communication to defensive and offensive activities in cyberspace and strategic communication. Goal-directed activities include also development of cooperation with paramilitary organizations and other civilian entities acting in the defense area in order to use their potential and capabilities for counteraction to hybrid threats (Banasik:2015a, p. 25).

REFERENCES

[1] Banasik M. (2016a), *Siły zbrojne we współczesnych uwarunkowaniach środowiska bezpieczeństwa*, [w:] M. Kopczewski, D. Sienkiewicz (red. nauk.), *Edukacja warunkiem bezpieczeństwa w XXI w. – instytucje publiczne w systemie bezpieczeństwa*.

[2] Banasik M. (2016b), *Unconventional war and warfare in the gray zone. The new spectrum of modern conflicts,* Journal of Defense Resources Management, Volume 7, Issue no. 1 (12), April 2016, Brasov Romania; http://journal.dresmara.ro/issues/volume7_issue1/00_jodrm_vol7_issue1.pdf; access: 31.10.2016.

[3] Banasik M. (2016c), *Wyzwania dla bezpieczeństwa wynikające z koncepcji prowadzenia wojny nowej generacji przez Federację Rosyjską* [w:] T. Szmidka, J. Kozioł (red. nauk.), *Zarządzanie Bezpieczeństwem Państwa – Wyzwania i Ryzyka*, Piotrków Trybunalski.

[4] Bartosh A.A. (2015), *Гибридные войны как проявление глобальной критичности современного мира,* Геополитика и безопасность, No 1 (29); http://www.paodkb.ru/upload/iblock/38e/2015_geopolitika-i-bezopasnost-_zhurnal_.pdf, access 15.02.2016.

[5] *Biała Księga Bezpieczeństwa Narodowego Rzeczypospolitej Polskiej* (2013), BBN Warszawa.

[6] *Białoruski raport o naciskach Rosji*, (2016), Portal Interia, 21.08.2016; http://fakty.interia.pl/swiat/news-bialoruski-raport-o-naciskach-rosji,nId,2255464, access: 21.08. 2016.

[7] Deep A. (2015), *Hybrid War: Old Concept, New Techniques*, Small Wars Journal; http://smallwarsjournal.com/jrnl/art/hybrid-war-old-concept-new-techniques, access: 28.10.2016.

[8] Diego A., Palmer R. (2015), *Back to the future? Russia's hybrid warfare, revolutions in military affairs, and Cold War comparisons*, Research Paper NATO Defense College, Rome – No. 120 – October 2015; https://www.files.ethz.ch/isn/194718/rp_120.pdf, access 20.08.2016.

[9] *Doktryny bezpieczeństwa informacyjnego RP* (2015), Warszawa; https://www.bbn.gov.pl/ftp/dok/01/Projekt_Doktryny_Bezpieczenstwa_Informacyjnego_RP.pdf, access: 01.11.2016.

[10] Doktryna cyberbezpieczeństwa RP (2015), Warszawa 2015; https://www.bbn.gov.pl/ftp/dok/01/DCB.pdf, access: 01.11.2016.

[11] Fryc M. (2015), *Polska strategia obronności wobec zagrożenia militarnego z elementami „wojny hybrydowej"*, Bezpieczeństwo Narodowe 2015/I, Warszawa; https://www.bbn.gov.pl/ftp/dok/03/FRYC_33-2015.pdf, access: 31.10.2016.

[12] Goble P. (2016), *Putin's Longstanding Plan for Long-Term Confrontation with the West Being Implemented Ever More Rapidly, Illarionov Says*, Window on Eurasia - *New Series*, Saturday, May 28, 2016, http://windowoneurasia2.blogspot.ca/2016/05/putins-longstanding-plan-for-long-term.html, access: 01.11.2016.

[13] Hoffman F. (2007), *Conflict in the 21st Century: The Rise of Hybrid Wars*, Arlington; http://www.potomacinstitute.org/images/stories/publications/potomac_hybridwar_0108.pdf, access: 30.10.2016.

[14] *I kto tu straszy Polaków? Gen. Koziej: wojna przeciwko Polsce trwa, zaś rosyjskiej inwazji wykluczyć nie można* (2015), Portal Polityka, 19.02.2015 ; http://wpolityce.pl/polityka/234372-i-kto-tu-straszy-polakow-gen-koziej-wojna-przeciwko-polsce-trwa-zas-rosyjskiej-inwazji-wykluczyc-nie-mozna, access: 31.10.2016.

[15] Kitler W. (2010), *Bezpieczeństwo narodowe. Podstawowe kategorie, dylematy pojęciowe i próba systematyzacji*, „Zeszyty Problemowe TWO" 2010, nr 1 (61).

[16] Koziej S. (2015), *Dekalog priorytetów strategicznych w dziedzinie bezpieczeństwa narodowego*, Warszawa; https://www.bbn.gov.pl/ftp/dok/01/Dekalog_priorytetow_w_dziedzinie_bezpieczenstwa_RP.pdf, access: 01.11.2016.

[17] Koziej S. (2016), *Strategiczna odporność kraju i rola*

w niej podmiotów niepaństwowych, „Krytyka Prawa", Vol. 8, No 1/2016; https://w%C4%87+kraju+i+rola+w+niej+podmiot%C3%B3w+niepa%C5%84stwowych, access: 31.10.2016.

[18] Kiselev V.A. and Vorobiev I.N. (2015), *Гибридные операции как новый вид военного противоборства*, Военная мысль № 5, Москва.

[19] Krutikov E. (2016), *Военная тактика России имеет преимущества перед тактикой США и НАТО*, 13 мая 2016; http://vz.ru/politics/2016/5/13/810243.html , access 20.08.2016.

[20] Liedel K. (2015), *Zagrożenia hybrydowe. Jak zmienia się środowisko bezpieczeństwa RP?,* Przegląd Bezpieczeństwa Wewnętrznego Wojna hybrydowa - Wydanie Specjalne, Warszawa 2015; http://www.abw.gov.pl/download/1/1924/Liedel.pdf, access 20.08.2016.

[21] Manea O. (2016), *The Strategy of Hybrid Warfare*, Small Wars Journal, 02.02.2016; http://smallwarsjournal.com/jrnl/art/the-strategy-of-hybrid-warfare, access: 10.08. 2016.

[22] Pach H.A. (2016), *Rozmowa z gen. Stanisławem Koziejem o wojnie i pokoju*, Portal Wiadomości24.pl; http://www.wiadomosci24.pl/artykul/z_gen_stanislawem_koziejem_o_wojnie_i_pokoju_332111.html, access: 31.10.2016.

[23] Rogozin D., *Военно-политический словарь*, Глава 1. Государство и безопасность, мир и война, 1.47. Война; http://www.voina-i-mir.ru/article/47, access: 20.08.2016.

[24] *Raport o stanie bezpieczeństwa cyberprzestrzeni RP w roku 2014*, CERT.GOV.PL, marzec 2015; http://www.cert.gov.pl/cer/publikacje/raporty-o-stanie-bezpi/738,Raport-o-stanie-bezpieczenstwa-cyberprzestrzeni-RP-w-2014-roku.html, access: 31.10.2016.

[25] Sauer T. (2016), *Just Leave It: NATO's Nuclear Weapons Policy at the Warsaw Summit*, Arms Control Today, Volume 46: June 2016; https://www.armscontrol.org/ACT/2016_06/Features/Just-Leave-It-NATOs-Nuclear-Weapons-Policy-at-the-Warsaw-Summit, access: 30.08.2016.

[26] *Słownik BBN: propozycje nowych terminów z dziedziny bezpieczeństwa*; http://www.bbn.gov.pl/pl/bezpieczenstwo-narodowe/minislownik-bbn-propozy/6035,MINISLOWNIK-BBN-Propozycje-nowych-terminow-z-dziedziny-bezpieczenstwa.html, access: 31.10.2016.

[27] *Strategia Bezpieczeństwa Narodowego Rzeczypospolitej Polskiej* (2014), BBN, Warszawa; https://www.bbn.gov.pl/ftp/SBN%20RP.pdf , access: 31.10.2016.

[28] Ścios A. (2015), *Bez dekretu: przegrana wojna – (1) Diagnoza*, portal internetowy, 06.07.2015; http://bezdekretu.blogspot.com/2016/07/przegrana-wojna-1-diagnoza.html, access: 31.10.2016.