TEME, г. XLII, бр. 4, октобар – децембар 2018, стр. 1359–1372

Прегледни рад DOI: 10.22190/TEME1804359M
Примљено: 23. 10. 2017. UDK 004.738.5
Ревидирана верзија: 3. 3. 2018.
Одобрено за штампу: 12. 6. 2018.

HYBRID GENESIS OF INFORMATION OPERATIONS IN CYBERSPACE [a]

Miroslav Mitrović[1*], Milan Miljković[2]

[1]University of Defence of Republic of Serbia, Startegic Researche Institute, Belgrade,Serbia
[2]Government of the Republic of Serbia, Office of the National Security Council and Classified Information Protection, Belgrade, Serbia
[*]*mitrovicmm@gmail.com*

Abstract

Contemporary global security environment could be labeled as complex, dynamic, multidimensional and ‘’beyond limits’’ of conventional understanding of Warfare. Diversity of threat forms and its interactions and non-conventionality contribute that most of the actual security crises and conflicts are marked as Hybrid security endangering, or Hybrid Warfare. Globalised tehnology introduce new ‘’battlefild’’ in global digital arena. Massive application of information and communication technology has brought about new risks and threats represented by physical and software related dangers to critical information infrastructure and cyberspace that are of relevance to the nation and its security. In same hand, wolnurability and inportance of Cyber space tends to provoke necessity for ultimate resilaince copabilities against ataks and informational warfare. Hybrid form and asimetrical nature of endangerment of Cyber space which is crutial for national defence copabilites, rised analiticial approach to the political, security and organizational forms as well as clasification of threats in cyber space which were elaborated in this paper. Authors’ contribute to the understunding of threats in Cyber secyrity arena, trough analyses of China PLA approach to the subject. In addition, unique contribution is given with analyses of Cyber-Information Warfare during 1999 NATO aggression to the Federal Republic of Yugoslavia.

Key words: hybrid warfare, cyber security, informational security, cyber-informational operation.

[a] Paper is a consisting part of the Project „Hybrid Warfare-experience and perspectives“, that is run by Strategic Research Institute, University of Defense of the Republic of Serbia.

ХИБРИДНА ГЕНЕЗА ИНФОРМАТИВНИХ ОПЕРАЦИЈА У САЈБЕР ПРОСТОРУ

Апстракт

Актуелна глобална безбедносна сцена може се описати као сложена, динамична, мултидимензионална и „ван граница" конвенционалног разумевања ратовања. Диверзитет форми угрожавања безбедности, њихова међусобна интеракција и неконвенционалност доприносе томе да највећи број актуелних безбедносних криза и конфликата могу бити означени као хибридно угрожавање безбедности или Хибридно ратовање. Глобализована технолошка сцена промовише нова „бојишта" у оквиру глобалне дигиталне арене. Масовна заступљеност и примена савремених информационих и комуникационих технологија успостављају нове ризике и претње које се очитавају у формама физичких и софтверских ризика према критичној информационој инфраструктури и сајбер-простору, који је од високог значаја за државу и њену безбедност. У исту руку, сајбер-простор исказује потребу за неопходним развојем одбрамбених способности према нападима и информатичком ратовању. Хибридне форме и асиметрична природа угрожавања сајбер-простора, који су од критичног значаја за националне одбрамбене способности, истичу потребу за аналитичким приступом политичких, безбедносних и организационих форми, као и класификацију претњи у сајбер-простору, што је постављени циљ овог рада. Аутори успостављају основу за аналитички засновану основу разумевања неких аспеката арена у којој се остварује сајбер-безбедност, синтетичким приступом сагледавању наведних изазова са становишта Кинеске НОА, као и анализе случаја сајбер-информационог ратовања током НАТО агресије на СРЈ у 1999. години.

Кључне речи: хибридно ратовање, сајбер-безбедност, безбедност информација, поверљиве информације, кризни менаџмент у сајбер-одбрани, сајбер-информациона операција.

INTRODUCTION

Contemporary security paradigm indicates globalization as the main driver for escalation of Hybrid and Asymetrix forms of world's security endangerment (Mitrović, 2017a). Namely, implementation of indirect and non-linear forms of warfare were known since ancient times (Watson, 2017), but by actual general list of conflict generations (Renz& Smith, 2016, p.5), modern hybrid concept of warfare could be recognized as a developed 4th, or even 5th generation (Mitrović, 2017a) of warfare. Since the noun Hybrid Warfare is not a new, and it was recognized in operations during Cold War period, as well as in conflicts in Yugoslavia during the last decade of 20th Century, actualization of the concept, especially by Western authors is raised since 2014, after the annexation of Crimea by the Russian Federation, where this action is identified with the postulates of ''hybrid warfare''. At the same time, the Russian authors in their works, sought to ''color revolution'' in connection with the hybrid warfare concept. Only those approaches of two great powers indicate that

current geopolitical scene represents a polygon of hybrid warfare, primarily due to the fact that there is an engaging non-military means, such as diplomacy, economy, energy, information and intensive use of media (Mitrović, 2017b). Considering contemporary analysis and critical observation, we could conclude that hybrid warfare is not de-facto conducted as war in conventional understandings, but mostly as a concept of actual, geopolitical clash of interests (McCulloh& Johnson, 2016).

According to theories (Hofman, 2007, p. 8), hybrid warfare personifies a whole range of various models of the conflicts, which are being carried out with conventional and unconventional tactics and engaged forces, including violence and civil unrest and criminal activity. Also, usage of information, psychology and dominance in communication controlling and commanding sphere are recognized as very powerful weapons since the middle of last century (Hart, 1954). In short, hybrid warfare is based on the discovery and articulation of hybrid risks thought threats, in order to accelerate weaknesses of targeting state, with purpose of achievement of their own interests, without (or with minimal) usage of direct military power.

Through the overview of the hybrid application forms, we could remark further pillows of hybrid concept of security violation: 1) *Special and psychological operations* - limited time performance, high intensity with very high direct effects. Recognized in the anti-rebel operations, information operations, counter terrorism, unconventional warfare, foreign internal defense (support of other countries in the aggression from outside), stability operations, security transition, and reconstruction, strategic communication, psychological warfare, information operations, civil-military operations, intelligence and counterintelligence operations (DOD, 2007, p.7); 2) *Economic, energy and political pressures*–actions of variable duration and intensity, depending on the interaction, relationship and buck effects which could be affected to the side who use pressure. The complexity of hybrid forms of endangering national security in the energy and economic field rise from the fact, that this area impose negative impacts to the entire state structure, compromising its functional capacity, encouraging the internal instability and public dissatisfaction, rise the sense of frustration among the population, etc. (Mitrović, 2017c); 3) *Information, media, Internet* and all its platforms-variable intensity activities, depending on the phase of others forms/fields implementation. The essence of achievement in this field is the penetration and changes of public opinion, as well as the introduction of doubt, uncertainty and fear; 4) *Public diplomacy*-low-intensity, very long-term-oriented activity, comprehensive hybrid operation tool, which makes activities in the sphere of social life more diverse (Mitrović, 2017d).

However, contemporary globalized security environment has hybrid and asymmetry characteristics. Also, developed technical, informational,

cyber solutions that are the base for implementation of channels for communication make actual societies dependable on informational and communicational technologies. Moreover, it could be concluded that actual civilization is existent linked with digitalized communication solutions, which makes all systems (especially defense and security) potentially fragile for all sorts of enlargement of communicational and informational systems, or vulnerable to the attacks in cyber space.

HYBRID SECURITY ENDANGERMENT IN CYBER SPACE

Massive application of information and communication technology has brought about new risks and threats presented by physical and software related dangers to critical information infrastructure and cyberspace that is relevant to the nation and its security. Cyberspace has become the determining feature of modern-day life and the key area of world economy. Every day, more or less tens of thousands hazardous attacks are registered in cyberspace. Leading countries in the world, as well as international organizations show growing awareness of the necessity for immediate action in purpose of raisin the security level in this domain. Many of them already have their own cyber security strategies and established cyber defense systems. Since the scholarly literature as well as expert studies dealing with this thematic area is scarce in the Serbian language, we need to try to define basic notions and classification of threats in cyberspace, and make a subsequent analysis and proposal for setting up a possible system for the protection of the Serbian critical infrastructure in cyberspace.

However, precise definitions of the cyber and cyber space terms have not been established yet. Various national cyber security strategies offer different definitions of "cyberspace". In some of them it is synonymous with the Internet whereas other strategies contain much broader definitions of that term. Thus the Cyber Security Strategy for Germany defines cyber as virtual space for all information and telecommunications (IT) systems connected at the level of databases on a global scale (FMI, 2011, p.14). This strategy points that the Internet is a core prerequisite for the existence of cyberspace, as a universal and publicly accessible network that could be further expanded and upgraded by adding networked databases. It also argues that IT systems in the isolated virtual space are not part of cyberspace. On the other hand, the UK Cyber Security Strategy (UK OCS, 2009) sets forward that cyberspace implies the internet, although it is not the basic condition for its existence. It states that cyberspace is an interactive domain composed of the digital network used for storage and modification, which means for work on data and information, as well as for communication. It includes the internet and other information systems supporting various business processes, infrastructure and services. In this context, the question that is arises why defining the basic terms relating to

cyberspace challenges is so complex and difficult. The experiences gained so far suggest that the core of this problem belongs to different angles of approaching to this problem, distinct political and legal attitudes to this problem by the world's leading countries. Namely, it is recognizable that global and even regional powers stem from their particular interests in connection with the use of cyberspace for achieving goals on the national and international level. It follows from understanding that every security problem has the following three dimensions: 1) Political and security (strategic); 2) Legal; 3) Technological.

The political and security aspect covers adoption of appropriate policies and laws on cyber defense, informational assurance, critical infrastructure and other rules necessary for legal regulation of deterrence, prevention and response in case of cyber defense on critical infrastructure. Listed documents generally set out the following main state mandates in area of defense and security: 1) Military activities; 2) Suppression of high-tech crime; 3) Intelligence and counterintelligence activities; 4) Critical infrastructure protection and crisis management; 5) Cyber diplomacy.

One of the important issues which should be defined within this aspect is the choice of responses to threats from cyberspace. From this perspective, operations in Cyber environment could be defined as offensive or defensive, with consequently same approach to cyber defense of critical infrastructure. The choice of political approach is characterized with following dilemmas:

In organizational terms, crisis management in cyber defense implies engagement of capacities of the Ministry of Justice and Public Administration, Ministry of Transport, Ministry of Defense, Ministry of Foreign Affairs, Ministry of Finance, Ministry of Internal Affairs and the security and intelligence community. Consequently, over the last two years the developed countries have made important steps to identify the existing civilian and military capacities and set up new ones to be responsible for cyber defense, as well as made efforts to define interdepartmental cooperation and roles of the private sector in this area. From point of view that surveillance of Internet communications, detection and protection from cyber-attacks necessary require advanced knowledge and state-of-the-art technology which are prevalent in the private sector, and that Internet communication runs through private providers, it is necessary to define obligations for the IT sector, as well as the concept of public- private partnership in the field of cyber defense. In organizational terms, it very important to identify a coordinating body, which is most often derived from the executive branch, to take over the role of coordinating and directing the overall policy in the area of critical infrastructure cyber defense in the public and private sector alike.

THREATS IN CYBER SPACE - CLASSIFICATION

For more than a decade, analysts have been speculating as to potential consequences of threats coming from cyberspace. The attacking scenarios have ranged from ''injecting'' computer viruses to destroy financial records and slow down the functioning of stock exchanges to posting fake messages (Hollis, 2007), till the entering in command chains with commands that make disturbing effect on the operation of nuclear reactors and flight control systems, as well as envisaging other events resulting in economic or physical damage (GAO, 1998). In the meantime, there is no generally accepted definition that identifies and classifies these and other cyber incidents. At this point there are two predominant but different pro-governmental concepts of understanding and defining a scale of threats from cyber-attacks. One has been declared by the US Government and the other one by the Shanghai Organization of Cooperation headed by Russia and China (Hathaway& Crootof, 2012, p.8). In this context, the difference in understanding this problem by the United States on the one side, and Russia and China on the other does not come as a surprise. On the other hand, analyzes of the solutions that were presented in the cyber strategies of the developed countries, generally cyber activities could be divided into four groups: 1) Cyber-crime; 2) Cyber terrorism; 3) Cyber espionage; 4) Cyber – information operations.

It should be emphasized that the physical forms of cyber terrorism, cyber warfare, cyber espionage and cyber crime often look alike or identical. Example for that could be illustrated in work of Lech J. Janczewski and Andrew M. Colarik, on the case of an individual breaking into the hospital databases to prescribe a medicine to a patient who is allergic to its ingredients. As a consequence of that, the patient dies. If the attacker's intention were to harm or kill the patient for some personal reasons, then this event would constitute a criminal offense committed by means of computer technology, i.e. an act of high-technology or cyber crime. In case the attacker made it known later on that he was ready to commit more offences along these line, in case his/her conditions had been fulfilled, than such conduct would be described as an act of cyber terrorism. Moreover, if the above offender was also an agent of the adversary structures and there also occurred a theft of classified information of relevance to the national security, that act would be qualified as cyber espionage. So, the attacker's intention is one of the factors that influence the classification of malicious activities in cyberspace into cyber terrorism, cyber espionage or cyber-crime (Janczewski&Colarik, 2008).

Malicious activities in cyberspace could be carried out by state or non-state actors, which mark them also as asymmetrical weapon; they involve active conduct of attackers and are aimed at jeopardizing the functioning of the victim's computer network with a view of accomplishing political or national security objectives. In this sense, in our attempt to give

an approximate definition of cyber war, we can say that this terms implies only cyber-attacks with state actors behind them whose impact is equivalent to a conventional "armed assault" or alternatively that it entails cyber-attacks that occur in the context of an armed conflict and develop into a cyber war (Hathaway&Crootof, 2012, p.17).

ESSENTIAL FEATURES OF CYBER - INFORMATION OPERATIONS

Information operations are in essence of military origin, and is logically that definitions of information operations are primarily found in security and military doctrinal documents of the Western countries and China whereas theoreticians in the Russian Federation use the term "information operations" or "information war" (*информационная война*).

Information operations are comprised of activities ranging from measures to prevent the adversary from exploiting information to those to ensure integrity, availability, and interoperability of friendly information resources. According to the objective of action information operations are divided into: 1) Offensive information operations, and 2) Defensive information operations (Arquilla&Ronfeldt, 1995, p.141-165).

Offensive information operations imply the use of different techniques with the support of intelligence factor with a view of disabling the adversary's leadership to make relevant decisions. The above-mentioned activities include the operational security, military deception, psychological operations, electronic war, physical attack (destruction), as well as attacks on the computer network (JCS, 1998). The ultimate targets of offensive information operations are the processes of human decision making.

In the Western doctrinal theory defensive information are defined as activities applied for the protection of they own information and information systems. Defensive information operations are used to ensure access to timely, accurate and relevant information.

When considering the division of information operations according to the means of execution, it is important to take into account the approach of Russian theoreticians who take the view that information operations are conducted in the military, political, economic and social spheres, and are applied through a whole set of activities of relevance to the national security (Sinkovski, 2005, p.49). Russians authors stand at the opinion that the security of information sphere is a complex and an essentially multi-layered problem. It is also the object of interdisciplinary technological and humanitarian scientific researches (Petrović, 2012, p.3). For that reason, Russian theoreticians argue that according to the resources used information operations can be divided into operations conducted by: 1) Information-technical means (assailing national critical infrastructure facilities with cyber-attacks), and 2) Information-perceptive means (propaganda, adversary's

perception management, disinformation, psychological operations and deception) (Thomas, 1996, p.25-35).

Cyber - Information Operations in the Modernization of the Chinese People's Liberation Army (PLA)

The book entitled "Unlimited warfare", which argues in favor of winning a victory over a potential adversary by attacking not only its armed forces but also all elements of its national power i.e. the adversary's political, economic and information infrastructure represents perhaps the best example of the Chinese thinking of cyber-information warfare (Liang&Xiaosui, 1999).

In the military sense, the Chinese understanding of asymmetry rise from thay standpoint, by which the fact that despite of its modernization over the last three decades, PLA is still incapable of winning a military victory in the event of a direct conventional warfare with China's main potential adversary - the U.S. Armed Forces. Upon that, instead of attempting to streamline all PLA branches, China has decided to combine modernization of particular branches of its military (thus giving priority to cyber operations units, air force and the navy, and putting the land force in the last place) with development of specific methods of action against a potentially superior adversary based on the exploitation of vulnerabilities and deficiencies of potential adversaries. In the meantime PLA had to identify the areas of developing its capabilities that could be relatively quickly streamlined without investing large resources, and by which massive losses will be inflicted to the superior adversary. Elaborated process presents the essence of developing PLA asymmetric warfare capabilities (Barić, 2010).

Some Chinese analysts hold the view that there is currently no need for developing a modern mechanized army capable of opposing the U.S. armed forces. Instead that, in PLA an information warfare concept is attached as ultimate increasing importance, which constitutes the core of the ongoing revolution in military affairs (RMA). The Chinese information warfare concept is based on four components: 1) Delivering precise blows - by using precisely guided weapon systems for attacking the adversary's command posts and communication hubs in order to paralyses its military forces on the battleground; 2) Electronic warfare; 3) Psychological warfare and deception - performing propaganda campaign with a view of undermining the adversary population's fighting spirit, attempts at influencing the adversary fighters' morale, and isolating a conflict (preventing the third party to engage in the conflict in question); 4) Attacks on computer networks - making direct assaults on the adversary's entire information structure that can be executed by asymmetric attacks and forces (Mulvenon&,1998, p.175-186).

The Chinese military doctrine emphasis the use of asymmetric warfare against a superior adversary, and the key method of waging war

is information (cyber) warfare, which represents a way to deliver a decisive blow to the adversary without taking risks related to the use of weapon systems, whose application will cause unacceptable collateral damage.

Information warfare should enable the Chinese military to apply tactics called "*sashoujian*" (assassin's mace) (Bruzdzinski, 2004, p.309-364) in the Chinese technical literature. This scenic term describes the application of weapon or tactics that deal a blow to the adversary by careful application of sudden calculated moves to bring about the change in the force ratio between the two adversaries. These strikes are based on ignoring customary rules of warfare in order to equalize the force ratio between the stronger and the weaker adversaries. Therefore the matter concerns asymmetric warfare methods by which the stronger adversary should be dealt a decisive blow with an incapacitating effect.

With no doubt, information (cyber) warfare is becoming a strategic alternative for China, taking into account its assessments that China will not prevail in a conventional military confrontation with the U.S. In this sense, China looks on cyber-attacks and cyber espionage as components of an integral strategy by which it is planning to win the technically superior adversary (Miljković, 2012, p. 81-97).

Cyber-Information Warfare during 1999 NATO Agresion against Federal Republic of Yugoslavia (FRY)

The Yugoslav Armed Forces action during the 1999 NATO aggression in Kosovo and Metohija can be quoted as an example of the information and asymmetric warfare. Due to the impossibility of responding to NATO airstrikes, the Yugoslav Armed Forces resorted to asymmetric means to oppose the Alliance. In the course of the aggression it put to good use its own media, foreign journalists, security services and the Internet to influence the general public across the world and achieve its political objective - maintaining the national sovereignty and territorial integrity. In addition to turning to the Internet for propaganda purposes, it also served for carrying out operations in cyberspace in the form of distributed denial of Service attacks (DDoS). At the beginning of the bombing more than 2.000 virus infected emails were sent to NATO addresses (Hubbard, 1999, p.11). The Alliance websites also suffered cyber-attacks during the second week of the war. In this way domestic hacktivists managed to temporarily incapacitate the above site by bombing it with ping attacks. Namely, a ping attack is commited by exposing a server to a large number of queries within a short period of time. As a result, the server gets overloaded with more queries than its envisaged capacity can handle, which causes a congestion outage of the computer system. Such attacks compelled NATO to provide extra material and human resources to improve the security of the computer

systems. Moreover these attacks forced the U.S. Department of Defense to enact a regulation prohibiting the access to Serbian websites in order to prevent the so-called "mapping" i.e. identifying U.S. official websites (Harmon, 1999, p.A14). After the aggression ended, NATO experts released detailed researches on the information aspect of that conflict, which suggest that the Yugoslav Armed Forces won the information war, given that they managed to achieve information superiority during the conflict (Larsen, 2000).

CONCLUSION

In modern conflicts, cyber asymmetric actions have reached the point where they are extensively used thus enabling cancellation of the adversary's advantage. Such actions include the application of special information operations forces and the internal opposition tasked with creating an operational front within the entire inland territory of the adversary's state (Larsen, 2000). The application of cyber-information warfare leads to the situation where modern militaries are forced to engage in conflicts without front lines for which many of them are unprepared, given that they have been primarily trained in conventional warfare (Zaitsev, 2014).

The use of information means for achieving political, defense and strategic aims of a conflict has been on the rise, and in many cases it has beaten out the military force in its effectiveness (Gerasimov, 2013).

Hybrid characteristics of information and cyber space enable extensive asymmetric possibilities for diminishing combat potentials against stronger and richer adversary (Gerasimov, 2013). The following cyberspace features are suitable for the application of information and cyber weapons in asymmetric attacks: 1) Possibility for remote access; 2) Difficulties in identifying an attacker, and attributing responsibility for an attack, and 3) Low prices of high-tech products that are freely available on the market.

"The soft dimension"of information operations i.e. its information-perceptive aspect (propaganda, deception and misinformation) demands much less financial resources, taking into account that lots of poor countries have a long tradition of studying the skills of management perception on the tactical and operational levels.

Information weapons can be exploited towards the adversary objective more rapidly in relation to other kinds of weapons with a capability of causing the required damage to the adversary within a definite period of time; it is inexpensive enough, simple for production and its mass production is possible in comparison with other kinds of weapons in the same class (Gerasimov, 2013, p.7-8). Its widespread use and availability are well suited for the application of the old "armed people" concept in the asymmetric warfare.

It should also be recalled that a victory is achieved not only by a nation's material means but also by its spiritual resources, unity and striving to stand up against an aggression with all its might. On the other hand, taking action against the adversary's population, as one of the most important objectives (given that population constitutes the center of gravity of the resistance and whose behavior crucially influences the course of events) is possible by using a great number of asymmetric operations on the information level.

Some scholars (Chekinov&Bogdanov, 2013) concluded that information warfare will play a crucial role in the present-day and future conflicts. The objectives of coming wars will not be achieved if information superiority over the opposing side has not been achieved. The framework for asymmetric and hybrid warfare and non-linear conflicts, as presented by the Russian military experts, Chekinov and Bogdanov, builds on an effective application of information operations at the start of a conflict to create favorable conditions for carrying out military operations. Here is one of their arguments: new generation of warfare's are predominantly information-based and psychological in nature because in this way information superiority and control over the adversary's units and weapon systems are attained, as well as the adversary's depressed psychological state and falling fighting spirit caused. The application of these operations reduces the need for a more considerable military engagement in attack operations (Chekinov&Bogdanov, 2013).

The highly efficient application of information operations in asymmetric conflicts have resulted in the decreased level of conventional forces engagement. Owing to that a significant number of nations are likely to incorporate asymmetric warfare in their military doctrines and operations. It can be expected that the major nations having resources for executing sustainable military operations (especially, against an equal adversary) will draw on principles and means of hybrid and asymmetric warfare to reach their strategic aims within a short period of time, and in such a way as to prevent the efficient response from the opposing side and international community. For that reason, it is of crucial importance that military strategy thinkers should improve their understanding of asymmetric cyber-information war, as well as develop and prepare a practical response to the adversary application of asymmetric warfare on the strategic, operational and tactical levels.

A nation's unpreparedness to defend itself from an asymmetric scenario poses a challenge to its security and defense nowadays. It is usually a result of a simplified defense strategy. However, the national security demands a multilevel approach. Nations should develop comprehensive, multilayered and asymmetric defense plans.

REFERENCES

Arquilla, J., Ronfeldt, D., (1995). *Networks and Netwars-Comparative Strategy*, Volume 12, Santa Monica, CA: Rand.

Barić S., (2010). „Vojne strategije i asimetrično ratovanje" [Military strategy and asimetric warfare], *National Security and the Future*, 4 (11), Zagreb.

Berzins, J., (October 11, 2016). *Russia's New Generation Warfare,* http//www.thepotomacfoundation.org/The New Generation of Russian WarfareThe Potomac Foundation.htm

Bruzdzinski, J., (2004). *Demystifying Shashoujian: China's "Assassin's Mace", Civil-Military Change in China-Elites, Institutes, and Ideas after the 16th Party Congress*, Strategic Studies Institute, U.S. Army War College.

Chekinov S.G., Bogdanov S.A., (2013). "The Nature and Content of a New-Generation War, *Voyennamysl, No.4, October 2013*. Retrieved from, http://www.eastviewpress. com/Files/MT_FROM%20THE%20CURRENT%20ISSUE_No. 4_2013.pdf

DOD- Department of Defense of US Government, (2007). *Irregular Warfare (IW)*- Joint Operating Concept (JOC), 2007, Washington, DC.

FMI- Federal Ministry of Interior (2011). *Cyber Security Strategy for Germany*. Retrieved from, http://www.cio.bund.de/.../css_engl_download.pdf?.

GAO-General Accounting Office (1998). *Air Traffic Control: Weak Computer Security Practices Jeopardize Flight Safety*. Retrieved from, *www.gao.gov/archive/ 1998/ai98155.pdf*.

Gerasimov, V., (2013). "The Value of Science in Foresight: New Challenges Require Rethinking on the Forms and Methods of Warfare," *Voroshilov General Staff Academy conference*, reprinted in Military Industrial Kurier, (27 Feb. 2013). Retrieved from, http://vpknews. ru/sites/default/files/pdf/VPK_08_476.pdf .

Harmon, A., (April 1, 1999) : "Serbs' Revenge: NATO Web Site Zapped", *New York Times*.

Hart, L., (1954). "The Strategy of Indirect Approach", *National War College Internet Archive*.

Hathaway A., Crootof, R., (2012). ''The law of cyber attack''. *California Law Review*, Retrieved from, http://www.californialawreview.org/assets/pdfs/100-4/02-Hathaway.pdf.

Hoffman, F., (2007). *Conflict in the 21st Century: The Rise of Hybrid Wars.* Institute for Policy Studies Arlington, VA: Potomac.

Hollis, D., (2007). ''Why States Need an International Law for Information Operations'', *11 Lewis & Clark L. Rev.* 1023-1042. Retrieved from, *http://www* law.lclark.edu/live/files/9551-lcb114art7hollispdf.

Hubbard, Z., (1999). "Information Warfare in Kosovo", *Journal of Electronic Defense*, November 1999, Vol. 22, No. 11.

Janczewski, L., Colarik, A., (2008). *Cyber Warfare and Cyber Terrorism*, Information Science Reference.

JCS-US Army Joint Chiefs of Staff (1998). *Joint Pub 3-13: Joint Doctrine for Information Operations.*

Larsen, A., (2000). *Serbian Information Operations During Operation Allied Force*, Air Command and Staff College, Air University, Maxwell Air Force Base, Alabama.

Liang, Q., Xiaosui, W., (1999). *Unlimited Warfare*. Bejing.

McCulloh, T., Johnson, R., (2016). *Hybrid Warfare*. JSOU, Tampa.

Miljković, M., (2012). „Ocene SAD o sposobnosti Narodno-oslobodilačke armije Kine (NOAK) za izvođenje sajber špijunaže" [US evaulation of capabilities of

Chinese People's Liberation Army (PLA) for implementation of Cyber espionage actions]. *Vojno delo*, Belgrad, Summer/2012.

Mitrović, M., (2017 a). "Hybrid warfare and asymmetric security threats".*Vojno delo No 5/2017*, Belgrade.

Mitrović, M., (2017 b). ''Hybrid Security Threats and Contemporary approach to National Security'', Thematic Conference Proceedings of International Significance, International Conference ''Archibald Reiss Days'', Academy of Criminal and Police Studies, Belgrade, Vol 1. p. 337-345.

Mitrović, M., (2017 c). ''Economic and energy aspects of a hybrid endangering of national security", *Vojno delo, No 6/2017*: Belgrade.

Mitrović, M., (2018d). ''Public Diplomacy in paradigm of Hybrid conflict concept'', *Vojno delo No 2/2018*.

Mulvenon, J., (1998). *The PLA and Information Warfare- Mulverton, The People's Liberation Army in the Information Age*, RAND, Santa Monica.

Petrović, L., (2012). „Informaciona bezbednost – pravni, ekonomski i tehnički aspekt" [Information security-law, economu and technical aspects], *Informaciona bezbednost 2012 – naučno-stručni skup*, Beograd.

Reisdorff, N., (2003). *Winning the hundred battles-China and asymmetric warfare.* US Army Command and General Staff College, Forth Leavenworth.

Renz, B., Smith, H., (2016). *Russia and Hybrid Warfare–Going beyond the Label*. Finnish Prime Minister's Office, Government's analysis. Retrieved from, https://helda.helsinki.fi/bitstream/handle/10138/175291/renz_smith_russia_and_hybrid_warfare.pdf?sequence=1&isAllowed=y

Sinkovski, S., (2005). „Informaciona bezbednost – komponenta nacionalne bezbednosti" [Information security-component of national security]. *Vojno delo*, 2/2005, Belgrad.

Thomas L.T., (1996). "Russian Views on Information-based Warfare", *Airpower Journal-Special Edition*.

UK OCS-UK Office of Cyber Security (2009). *Cyber Security Strategy of the United Kingdom*. Retrieved from, http://www.official-documents.gov.uk/document/cm76/7642/7642.pdf.

UKG-United Kingdom Govermant (November 2011). *Cyber Security Strategy, Protecting and promoting the UK in a digital world*. Retrieved from, https://www.gov.uk/government/.../uk-cyber-security-strategy-final.pdf.

Watson, J., (2017). "Sun Tzu's Art of War - Chapter 3: Attack by Stratagem". Retrieved from http://suntzusaid.com/book/3.

Zaitsev, A., (2014). *Partisan Warfare: The modern army should know how to fight without front lines,* MIC Media in English Translation, 3 September 2014. Retrieved from, http://www.vpk-news.ru/articles/21649.

ХИБРИДНА ГЕНЕЗА ИНФОРМАТИВНИХ ОПЕРАЦИЈА У САЈБЕР ПРОСТОРУ

Мирослав Митровић[1], Милан Миљковић[2]
[1]Универзитет одбране, Институт за стратегијска истраживања, Београд, Србија
[2]Канцеларија Савета за националну безбедност и заштиту тајних података Владе Републике Србије, Београд, Србија

Резиме

Поједини принципи „нове генерација ратовања", као што су 1) из сегментног ратовања до тоталног рата; 2) из рата у физичком окружењу до рата у људској свести и у сајбер-простору; 3) од симетричног до асиметричног рата – истовременом и усклађеном применом политичких, економских, информационих, технолошких и еколошких кампања – указују на актуелност хибридног ратовања, сајбер и информационих операција. Масовна примена савремене информационе технологије и феномен обиља информација довели су до интензивирања надметања информацијама, због чега информационе операције постају све важније за националну безбедност. Информационе операције воде се преко читавог скупа активности (цивилних и војних) од значаја за националну безбедност, због чега су погодне за хибридно ратовање.

О томе можда најбоље говори кинеско размишљање о асиметричном и хибридном ратовању, које је представљено у књизи „Неограничено ратовање", у којој се њени аутори залажу за победу над потенцијалним противником кроз напад на његове оружане снаге, али и на све елементе његове националне моћи – политичку и економску, а посебно информациону инфраструктуру противника. Кинески концепт употребе информационих операција и сајбер-простора за „надвладавање јачег од стране слабијег противника" делом је потврђен током 1999. године и бомбардовања СРЈ од стране НАТО, имајући у виду да је експертска оцена да је Војска Југославије успела да оствари информациону супериорност током конфликта.

Сајбер и информациони простор отвара широке могућности за вођење хибридног ратовања и смањење борбеног потенцијала јачег и богатијег непријатеља. Применом ових операција смањује се потреба за значајнијим ангажовањем војних снага у нападним операцијама, због чега теоретичари закључују да ће информационо ратовање имати кључну улогу у савременим и будућим конфликтима.