

**MINISTRY OF DEFENCE
OF THE REPUBLIC OF SERBIA**

UNIVERSITY OF DEFENCE
STRATEGIC RESEARCH INSTITUTE
&
NATIONAL DEFENCE SCHOOL

ASYMMETRY AND STRATEGY

THEMATIC COLLECTION OF ARTICLES

Belgrade 2018

Published by
STRATEGIC RESEARCH INSTITUTE
&
NATIONAL DEFENCE SCHOOL

For Publisher
Jovanka Šaranović, PhD
Miroslav Talijan, PhD

Editorial Board:

Editor-in-Chief
Stanislav Stojanović, PhD

George Popper, PhD (Hungary)
Aleksandar Fatić, PhD (Serbia)
Siniša Tatalović, PhD (Croatia)
Marios Efthymiopoulos, PhD (UAE)
Andrej Krzak, PhD (Poland)

Editorial Assistant
Hatidža Beriša, PhD
Miloš Milenković, PhD
Milinko Vračar, MA

Thematic Collection Reviewers
Božidar Forca, PhD (Serbia)
Zoran Kilibarda, PhD (Serbia)
Miloš Šolaja, PhD
(Bosnia and Herzegovina)
Marjan Gjurovski, PhD (Macedonia)

ISBN 978-86-81121-17-7
(STRATEGIC RESEARCH INSTITUTE)

Co-Publisher
MEDIA CENTER “ODBRANA”

Library „Vojna knjiga“
Book no. 2189

Director
Stevica S. Karapandžin

Editor-in-Chief
Dragana Marković

Graphic Editor
Goran Janjić, dipl. ing.

Cover Design
Nebojša Kujundžić

Printed in
300 copies

Print
Vojna štamparija Beograd

ISBN 978-86-335-0594-9
(MEDIA CENTER “ODBRANA”)

ASYMMETRY AND STRATEGY

~ THEMATIC COLLECTION OF ARTICLES ~

CONTENTS

INTRODUCTION

INTRODUCTION OF EDITOR	11
------------------------------	----

THE CONCEPT OF ASYMMETRIC THREATS

<i>Milica Ćurčić</i> ASYMMETRIC THREATS IN SECURITY STUDIES	17
<i>Zoran Jovanovski</i> A CONCEPT OF ASYMMETRIC THREATS	31
<i>Darko Trifunović</i> INTERNATIONAL SECURITY AND ASYMMETRIC THREATS.....	47
<i>Valentina Rapajić</i> DE-TERMINOLOGIZATION OF <i>ASYMMETRICAL WARFARE</i> : METALEXICOGRAPHIC ANALYSIS OF THE TERM IN LEARNER MONOLINGUAL DICTIONARIES OF ENGLISH.....	63
<i>Andrej Krzak</i> NEW TYPES OF WARS – HYBRID AND ASIMMETRIC WARFARE – LOOKING FOR MODERN CANON OF THE ART OF WARFARE	77
<i>Nebojša Vuković</i> HUMANS AS A WEAPON: ASYMMETRY AND DEMOGRAPHY.	93

<i>Dušan Proroković</i> GEOPOLITICAL DIMENSION OF ASYMETRIC THREATS TO THE NATIONAL SECURITY OF SERBIA.....	107
---	-----

<i>Marios Efthymiopoulos</i> HYBRID CHALLENGES IN THE BALKANS.....	127
---	-----

<i>Danuta Gibas-Krzak</i> INTRODUCTION TO THE METHODOLOGY OF RESEARCH ON ASIMMETRIC THREATS – BALKAN CONTEXT.....	143
---	-----

<i>Miroslav Mitrović</i> CRITICAL NATIONAL INFRASTRUCTURE IN THE SCOPE OF ASYMMETRIC SECURITY THREATS INVOLVED IN HYBRID WARFARE CONCEPT	157
---	-----

<i>Sladjan Milosavljević, Hatidža Beriša</i> SECURITY STRATEGY - AN ATTEMPT OF CONCEPTUAL DEFINITION AND DETERMINATION OF ASSYMETRIC AND TRANSNATIONAL FORMS OF THREATS CONCEPT	181
--	-----

STRATEGIC CONTEXT OF CONTEMPORARY ASYMMETRICAL THREATS

<i>Miroslav Talijan, Saša Antanasijević</i> ASYMMETRICAL WARFARE AND TERRORISM	207
---	-----

<i>Miloš Šolaja</i> SUB-STATEHOOD AND STRATEGIC RESPONSES ON ASIMMETRIC THREATS.....	233
--	-----

<i>Igor Novaković, Irina Rizmal</i> CYBER WARFARE: NEW TYPE OF WARFARE OR ADDITIONAL ELEMENT OF CONVETNTIONAL WARFARE.....	249
--	-----

<i>Duško Vejnović, Predrag Obrenović</i> ASYMMETRIC THREATS AND SECURITY OF THE WESTERN BALKANS WITH A SPECIAL REFERENCE TO BOSNIA AND HERZEGOVINA	263
---	-----

<i>Dragan Đukanović</i> CURRENT FOREIGN POLICY CHALLENGES OF SERBIA AND ASYMMETRIC SECURITY THREATS	277
<i>Milan Miljković</i> INFORMATION WAR AND ASYMMETRIC CONFLICTS.....	291
<i>Žarko Ćulibrk</i> TERRORISM AS ASYMMETRIC THREAT AND ASYMMETRIC COUNTERTERRORISM RESPONSES	305
<i>Branislav Milosavljević, Ljupka Petrevska</i> A STRATEGIC APPROACH IN PREVENTION ORGANIZED CRIME	321
<i>Vanda Božić, Željko Nikač</i> FIGHT AGAINST ORGANIZED CRIME IN THE STATES OF THE REGION AND EU MEMBERS STATES.....	339
<i>Ljubiša Despotović, Aleksandar Gajić</i> GEOPOLITICS OF MIGRANT CRISIS AND SECURITY RISKS AS THE FORMS OF OFFENSIVE ASSIMETRIC THREATS IN THE BALKAN	357
<i>Mitar Kovač, Brankica Potkonjak-Lukić</i> THE MIGRANT CRISIS IN EUROPE AS A SECURITY THREAT TO THE REPUBLIC OF SERBIA	371
<i>Dragan Knežević, Jovanka Šaranović</i> RECENT TENDENCIES IN INTERNATIONAL LAW REGARDING THE REGULATION OF MIGRATIONS INDUCED BY ARMED CONFLICTS.....	389
<i>Dalibor Kekić, Miloš Milenković</i> STRATEGIC AND LEGAL ASYMETRICITY OF MIGRATION AS A FORM OF EMERGENCY SITUATIONS	417
<i>Vanja Rokvić</i> UN PEACEKEEPING OPERATIONS IN CONTEMPORARY SECURITY ENVIRONMENT	431

<i>Duško Tomić, Proda Šećerov</i> ANALYSIS ASYMMETRIC THREATS ON CORRIDOR 10 AS ONE OF THE KEY SERBIAN CRITICAL INFRASTRUCTURE	447
--	-----

<i>Stephan U. Breu</i> FINANCING OF COMBATANTS IN ASYMMETRIC CONFLICTS...	475
--	-----

<i>Николай Бузин, Сергей Мусиенко</i> ИНФОРМАЦИОННО-ПСИХОЛОГИЧЕСКИЙ КОМПОНЕНТ «ГИБРИДНОЙ» ВОЙНЫ И КИБЕРПРОСТРАНСТВО	489
---	-----

RELEVANCE OF CLASSICAL STRATEGIC THOUGHT

<i>Božidar Forca</i> KLASIČNA STRATEGIJSKA MISAO I SAVREMENA MEĐUNARODNA BEZBEDNOST	507
---	-----

<i>Stjepan Domjančić</i> WHY STRATEGY HAS COME OUT FROM SECURITY AND DEFENCE AREA?	531
--	-----

<i>Владлена Тикхова, Милинко Врачар</i> АРМИЯ ЕВРОПЕЙСКОГО СОЮЗА – АДЕКВАТНЫЙ ОТВЕТ НА АСИММЕТРИЧНЫЕ УГРОЗЫ СОВРЕМЕННОСТИ?	547
--	-----

<i>Дарина Григорова</i> ЭЛЕКТРОННЫЙ СММ МЕЖДУ ТЕРРОРИЗМОМ И ИНФОРМАЦИОННОМ СУВЕРЕНИТЕТЕ	559
---	-----

<i>Zoran Jeftić, Ivica Dorđević</i> SIGNIFICANCE OF HUNTINGTON'S STRATEGIC THOUGHT ON DEVELOPMENT OF CIVIL-MILITARY RELATIONS	571
---	-----

<i>Orlando Mardner</i> ASEMMETRY AND STRATEGY	587
--	-----

<i>Andrej Kubiček</i> DISCOURSE AS A FIELD OF ASSYMMETRIC COMFLICTS	603
--	-----

<i>Zoran R. Vitorović</i> PREVENTIVE DIPLOMACY AS A KEY FOR CONFLICT REDUCTION AND REDUCING THE THREAT POSED BY RADICAL ISLAMISTS.....	617
<i>Veljko Blagojević, Milovan Subotić</i> DEFENCE DIPLOMACY IN STRATEGIC CONTEXT OF ASYMMETRIC THREAT TO NATIONAL SECURITY	635
<i>Ivan R. Dimitrijević, Nenad Stekić</i> INTELLIGENCE ANALYSIS MODELS FOR ASYMMETRIC THREATS.....	653
<i>Srđan Starčević, Goran Vukadinović</i> ASYMMETRY OF POSTAMERICAN WORLD AFTER 2025 ACCORDING TO ZBIGNIEW BRZEZINSKI	669
<i>Snežana Vasić, Goran R. Nenadović</i> COMPARATIVE ANALYSIS OF THE NATIONAL SECURITY SYSTEM OF THE COUNTRIES OF THE WESTERN BALKANS IN CONDITIONS OF ASYMMETRIC SECURITY THREATS.....	685
<i>Marjan Gjurovski</i> STRATEGY FOR DEFENSE DIPLOMACY OF THE REPUBLIC OF MACEDONIA	705

CRITICAL NATIONAL INFRASTRUCTURE IN THE SCOPE OF ASYMMETRIC SECURITY THREATS INVOLVED IN HYBRID WARFARE CONCEPT

Miroslav Mitrović*

Strategic Research Institute, University of Defence, Belgrade,
Republic of Serbia

Abstract: Contemporary geopolitical events indicate that modern conflicts are nonlinear, hybrid and asymmetric. Furthermore, this environment points to a tendency towards displacing the conflicts arena from the classic milieu of very conventional battlefields to the non – convectional arena. Also, critical national infrastructure became a likely primary operational goal of the unconventional opponents. Those characteristics further lead to the necessity of contemporary conceptual analysis of the acting indication of asymmetric security threats and hybrid warfare operations and their impact on national critical infrastructure. Namely, we bear witness that states and non-state actors mostly practice unconventional forms of conflict based on interest positioning. Common notion of contemporary security paradigm with general unconventional forms of threatening is defined as the hybrid security concept. In the scope of critical national infrastructure, hybrid security coercions are an acting form of asymmetric security threats. In the article, the author aims to contribute to answering the following questions: What is hybrid warfare and where is its link with asymmetric security threats? Which part of the Critical National Infrastructure is most vulnerable to asymmetric threats? How to develop the prevention and effective Hybrid anti - measures? The analysis which is offered in the paper is accomplished by using a broad base of scientific and expertise literature, as well as actual indicators related to the situation of the Republic of Serbia regarding Hybrid forms of endangering national critical infrastructure.

Key words: asymmetric security threats, hybrid warfare, national critical infrastructure.

* miroslav.mitrovic@mod.gov.rs

HYBRID SECURITY THREATS – WAR OR CONCEPT?

Hybrid warfare represents the actual expression of primeval aspirations of the strategic advantages of the achievements over the opponent, mainly by non-armed means.²⁴¹ The analysis of contemporary conflicts concludes that they have characteristics of emerged forms of the fourth²⁴² or even the fifth generation of wars²⁴³. In addition, some authors have developed a theory of the so called ‘‘Wars of 6th generation’’²⁴⁴, as well as Asymmetric warfare²⁴⁵.

However, it can be said that the hybrid conflict concept announced in 1989, when Lind predicted an increase in information warfare and psychological operations in future conflicts. Lind argues that ‘‘Psychological operations may become a dominant operational and strategic weapon in the forms of media / information intervention ... [and] the main target will be enemy population’s support of its government and the war. Television news may become a more powerful operational weapon than armored divisions’’.²⁴⁶ Furthermore, some authors²⁴⁷ consider that the last decade of the twentieth century commits to a new era of warfare, with no - limit in terms of assets (armed or unarmed), the consist form of the deployed forces (national, transnational, multinational, non-governmental), as well as with the ambient of appearance attacks (territory, waters, resources, trade, finance, information, media, beliefs, culture, technology, military, political system). According to some theories²⁴⁸, activities that lead to the destabilization of a country or the

²⁴¹ Tzu, S., (2000). *Art of War- Chapter 3: Attack by Stratagem*. Allandale, Leicester, pp. 9.

²⁴² Renz, B., Smith, H., (2016). *Russia And Hybrid Warfare –Going Beyond The Label*. Finnish Prime Minister’s Office, Government’s analysis.

²⁴³ Mitrović, M., (2017). ‘‘Hybrid warfare and asymmetric security threats’’. *Vojno delo*, Beograd, 5/2017.

²⁴⁴ Regarding Vladimir Slipchenko, Russian strategy scholar, US and NATO engagement in 1999 in aggression against FRJ, with predominant characteristics of technical and technology supremacy, is model of 6th Generation of Warfare. See more in: Слипченко, В. (1999). *Война будущего*. Москва: Московский Общественный Научный Фонд.

²⁴⁵ Asymmetric warfare, according to many authors, is not a new phenomenon. According to them, conceptual basis Asymmetric warfare can be observed through the Sun Tzu Wu writing. The basis of the concept of asymmetric warfare represents a model in which the technological and abundance inferior opponent inflicts losses to the opposite side, presenting the results in order to promote their views and objectives tending to evolve new, motivated minded.

²⁴⁶ Lind, W., Nightengale, K., Schmitt, J., Sutton, J., Wilson, G., (1989), ‘‘The Changing Face of War: Into the Fourth Generation’’, *Marine Corps Gazette*, Oct. 1989., pp. 26.

²⁴⁷ Qiao, L., Xiangsui, W., (1999). *Unrestricted Warfare*. PLA Literature and Arts Publishing House, Beijing.

²⁴⁸ Kofman, M., Rojansky, M. (2015). *A Closer look at Russia’s ‘‘Hybrid War’’*. Woodrow Wilson International Center for Scholars, Kennan Cable No. 7, April 2015, pp. 5

change of its government, with the aim of establishing the state of disturbing the balance in international relations and the realization of its own interests, predominantly by non-combat means, can be termed as a *hybrid*.

Hybrid security threats gather all phenomena which engage synergy implementation of conventional weapons, unconventional and irregular tactics, terrorist acts and criminal activities, simultaneously acting on one battlefield, with the goal of achieving political objectives.²⁴⁹ This concept of achieving national interests is called the unconventional, political (hybrid) warfare.²⁵⁰ Hybrid security threats are generated to establish the conditions which disrupt the balance of power in international relations and the realization of its own interests, predominantly by non-combat means.²⁵¹

US military doctrinal documents²⁵² recognized that the actual conflicts could not be solved only by military means, and in order to achieve the success, it is necessary to engage all national capacities: diplomatic, informational, military and economic.

Also, according to the Russian military doctrine²⁵³, modern warfare is described as an integrated engagement of military forces and resources which have no military character, with an emphasis on the application of rate information warfare with the goal of achieving political objectives without the direct involvement of military forces, with the aim of shaping the desired response of world public opinion. Furthermore, the Russian doctrine predicts the specific form of modern conflicts in which they will apply an integrated operation of military and political, economic, informational and other non-military activities.²⁵⁴

Taking into account the characteristics and manifestation forms of hybrid forms of endangering national security²⁵⁵, in summary, it could express the main pillars of hybrid operations expressions:²⁵⁶

²⁴⁹ Hofman, F., G., (2007). *Conflict in the 21st Century-The Rise of Hybrid Wars*. Potomac Institute for Policy Studies.

²⁵⁰ Hoffman, F., G., (2016). *On Not-So-New Warfare: Political Warfare vs. Hybrid Threats*. Retrieved from: <http://warontherocks.com/2014/07/on-not-so-new-warfare-political-warfare-vs-hybridthreats/>; 12/05/2017.

²⁵¹ Kofman, M., Rojansky, M., (2015), pp. 3.

²⁵² Department of the Army (2008). *Field Manual No. 3-0: Operations*. Washington, DC.

²⁵³ Президент России, Москва, (2010). *Военная доктрина Российской Федерации*. Retrieved from: <http://kremlin.ru/supplement/461>.

²⁵⁴ Президент России, Москва, (2014). *Военная доктрина Российской Федерации*. Retrieved from: http://www.consultant.ru/document/cons_doc_LAW_172989/.

²⁵⁵ Mitrović, M. (2017). "Hybrid asymmetric warfare and security threats", *Vojno delo*, Belgrade, 5/2017.

²⁵⁶ Mitrovic, M. (2017). "The economic and energy aspects of a hybrid threat to national security". *Vojno delo*, Belgrade, 6/2017.

- Special and psychological operations which represent the armed, conventional-unconventional forms of the engagement of forces and resources.
- Economic, energy and political pressures. Beside the fact that the economy has intensified as a reflection of the state power, not explicitly by military forces, but thus it becomes a key subject of military operations planning, with the overall military strategy relying on the engagement of various economic instruments, while the classic application of the armed forces is projected only when it is absolutely necessary.²⁵⁷
- Information campaigns - media and the Internet (ab)use. The essential aim of this pillow is to make an impact on retained public opinion, deviation of altitudes, changing the existence or adoption of new attitudes, as well as the introduction of doubt, uncertainty and fear. Campaigns are being carried out by the usage of all propaganda instruments, launching half-truths, unchecked sensations, media manipulation, cyberspace attacks, and others. These strong performances of creating public opinion contribute significantly to resultant effects of foreign policy which aims to achieve the strategic dominance in a particular region.²⁵⁸
- Public diplomacy is an activity of low intensity, long-term oriented, directly related to the concept of soft power, in which it is based on intangible and indirect influences, such as culture, social values and ideology.²⁵⁹ Also it is the instrument of communication between professional services, such as diplomats and foreign correspondents, and it is the process of intercultural communication.²⁶⁰ Public diplomacy is an activity which deals with the influence of the foreign public attitude in order to formulate and realize applicants of foreign policy, including international relations beyond traditional diplomacy.²⁶¹

²⁵⁷ Taillard, M. (2012). *Economics and modern warfare*. Palgrave MacMillan.

²⁵⁸ Mitrović, M., (2017). "The potential influence of interest groups on the US Foreign Policy – Case of 'Kosovo' ". *Zbornik Matice srpske za društvene nauke*, No.162 - 163.

²⁵⁹ Nye, J., (1990). "The misleading metaphor of decline". *The Atlantic Monthly*, March 1990.

²⁶⁰ Cull, N. (2006). *Public Diplomacy Before Gullion: The Evolution of a Phrase*. Retrieved from <https://uscpublicdiplomacy.org/blog/public-diplomacy-gullion-evolution-phrase>.

²⁶¹ Mitrović, M., (2017). „Public Diplomacy in Hybrid Warfare paradigm“, *Vojno delo*, Belgrade, 7/2017.

All listed forms of activities have the purpose of destabilizing the country or changing political and government power in it, organized and carried out with the purpose of achieving the strategic interests of outer power centers, in order to establish the state of disruption of balance in international relations, and the realization of their own interests, mostly by non-combat means. On the basis of these theories, it could be concluded that hybrid warfare does not present warfare *per se*, but a form of a conflict concept in which a wide range of military and non-conventional activities are applied, with a purpose of achieving the strategic advantages for applying the entity. Furthermore, raised dilemma point in correlation of hybrid conflict concept and phenomena of asymmetric security threats.

ASYMMETRIC SECURITY THREATS AND THE HYBRID CONCEPT OF CONFLICTS

Regarding some theories, asymmetry principles in warfare are old as the war itself and belong to the mankind warfare history.²⁶² In some scholar's thoughts, the asymmetric warfare concept is recognized as a possibility of technically and by men power weaker opponent to achieve significant losses than other, stronger side, with simultaneous promotion of results in order to mobilize new members.²⁶³ Asymmetry in contemporary security environment could be recognized through disproportionality in technical development of conflicted parties, imbalance in moral power and psychological readiness of units as well as of wider population. Also, an organizational technological asymmetry could be recognized in war perseverance and others which mostly depends on social-psychological characteristics of conflicted parties.²⁶⁴

Some authors, in summarizing the form of a description of asymmetric security threats, indicate its determinants as:²⁶⁵

- New, unorthodox, unusual, surprised and unexpected threats;
- Presence of ultimately new and flexibly developed tactics and capabilities, as well as unconventional technical goods and arms.

²⁶² Metz, S., and Johnson, D., (2001). *Asymmetry And U.S. Military Strategy : Definition, Background, And Strategic Concepts*, Strategic Studies Institute, US.

²⁶³ Renz, B., Smith, H., (2016), pp.5.

²⁶⁴ Metz, S., and Johnson, D., V, (2001), pp. 10.

²⁶⁵ Lambakis, S., Kiras, J., and Kolet, K., (2002). *Understanding "Asymmetric" Threats to the United States*. National Institute for Public Policy, Fairfax.

- Ambient globalizes the security environment with the state and understate security subjects and stake holders;
- Positions and altitudes of security subjects and stake holders regarding global international relations and security issues;
- Classical, convectional approach to the state and under state security and defense issues are relatively obsolete, out-of-date, and do not have appropriate organizational capabilities in defense of asymmetric threats.
- State system of defense shows latent institutional weaknesses, especially in the area of prevention and protection development.

Hybrid warfare and asymmetric security threats, conditionally called asymmetric warfare, are terms which are very close. The main reason for that is in acting forms, targets, nonlinear approach of exposing, unconventional means, distinguishing classical, so called Clausewitz's "shape" of war, as well as often absence (or at least, no clear presence) of state subjects in conflicts. But, regarding some scholars analysis, it is obvious that hybrid and asymmetric warfare have some significant applications especially in contribution to some theories of conflict, subjects, stake holders, aims and goals. The common point of analysis could be established in Hart's view in the best strategic way of winning strategy. Namely, Hart thought that significantly longest and unproductive way is the direct clash of armed capacities, and that the most fecund is strategically indirect approach with different forms of unarmed means, which effectively demolishes psychological and psychical balance of opponent, and leads to his defeat.²⁶⁶ Basically, the logic of hybrid and asymmetric warfare could be recognized through the Chaos and Network centric theories of conflict management. Chaos theory correlates with hybrid and asymmetric warfare basically upon common multivariable process, which at first sight, are not tuned to the same aim. Upon some theories²⁶⁷ which analyses Man's Chaos theory, constructive sub-chaos could be controlled as sub-strategy contests of hybrid warfare.²⁶⁸ The origin of this consideration contributed to the understanding of some contemporary conflicts in the papers

²⁶⁶ Hart, L., (1954). "The Strategy of Indirect Approach". *Internet Archive*, National War College.

²⁶⁷ Korybko, A., (2015). Hybrid Wars: the indirect adaptive approach to regime change, Moscow, Peoples' Friendship University of Russia, pp 23.

²⁶⁸ Mann, S., (1992). "Chaos Theory and Strategic Thought", *Parameters*, Autumn 1992.

of Darius²⁶⁹ and Shahskov²⁷⁰. On the other hand, in support of ‘‘chaos’’ rout of asymmetric warfare, we could say that even the origin of asymmetry is connected with the creation of chaos and demolishing the capabilities of states, by acting with the unconventional means directly to the weaken point in national infrastructure. Some analytical works recognized asymmetry as a part or ‘‘small’’ hybrid war. Furthermore, hybrid warfare could be recognized as a chain of different activities, in which asymmetric acts are sublimated among them.²⁷¹

Network-centric warfare theory is also in correlation with hybrid and asymmetric endangerment of security. According to some theories²⁷², network-centric warfare is a conflict basically different from a classical war, in which actors use network forms of organizations, doctrines and strategies, based on modern technologies and cyber space networks. Actors mostly represented by small groups, or even solo players, who coordinate, communicate, and synchronize actions, usually without solid centered core or base. At the same time, the concept is strongly supported with a frequent usage of *soft power* mechanisms, especially in informational campaigns of perception management, public odium shaping and branding the organization, movement or acts.²⁷³ Additionally, asymmetry could be recognized even in a network-based organization, which is acting predominantly as a nonlinear actor, such is Al Qaida. At the same time, this organization is network based asymmetrically organized, communicated, resources, means and support delivered, as well as media and message broadcasting supported.

Through the analysis of subjects, determinants, as well as the aims of acting, it could be concluded that hybrid and asymmetric warfare closely correlate in areas of: conceptual approach of conflict management, acting subjects (which predominantly aren't state centralized), flexibility, adaptability, unconventionality, means and methods, way of acting, choosing targets, communication strategy, mobilization of supporters and new members. At the same time, the hybrid concept of conflict has a wider meaning and inner compositions than the asymmetric way of security endangerment, which

²⁶⁹ Darius, M., (2014). "Iraq and Syria are Burning, "Constructive Chaos" and America's Broader Strategy to Conquer Eurasia." *GlobalResearch.ca*, June 2014.

²⁷⁰ Shahskov, S., (2011). "The theory of 'manageable chaos' put into practice." *Strategic Culture Foundation*, 1 Mar. 2011.

²⁷¹ Mitrović, M. (2017). "Hybrid asymmetric warfare and security threats", *Vojno delo*, Belgrade, 5/2017.

²⁷² Arquilla, J., and Ronfeldt, D., (2001). "The Advent of Netwar (Revisited)." *Networks and Netwars: The Future of Terror, Crime, and Militancy*. Santa Monica, CA: Rand.

²⁷³ Cebrowski, A., and Garstka J., (1998). *Network - Centric Warfare: Its Origin and Future*. U.S. Naval Institute.

indicates a frequent usage of ‘war’ idiom in a hybrid conflict connotation. Also, hybrid as well as asymmetric security endangerment imposes acts mostly on the most vulnerable, critical society components, resources or infrastructures. We consider both wider socio-psychological, economical, and political components, or more concrete acts against elements of infrastructure, personal safety and daily life activities, with postponed psychological effects.²⁷⁴

CRITICAL NATIONAL INFRASTRUCTURE IN THE CONTEMPORARY SECURITY PARADIGM

Critical national infrastructure (CNI) could be understood as basic facilities, services, and installations needed for the functioning of a community or society²⁷⁵, or organizational and physical structures and facilities of such vital importance to a nation's society and economy that their failure or degradation would result in sustained supply shortages, significant disruption of public safety and security, or other dramatic consequences.²⁷⁶ A contemporary approach to the concept of CNI evolves from simplified identification with the general public infrastructure, which becomes, due to the technological development, more sophisticated, and sensitive, for the national high priority core value, which is primarily, a potential aim of hybrid and asymmetric security threats. Thus, during the eighties, CNI was mostly seen through the Public Infrastructures as „a wide array of public facilities and equipment required to provide social services and support private sector economic activity“.²⁷⁷

However, the complexity of geopolitical relations and the disappearance of global military polarization involve the growing threat of hybrid and asymmetric forms which compromise critical infrastructures, particularly with terrorist threats. This development of relations at the global

²⁷⁴ Mitrović, M. (2017). "Hybrid asymmetric warfare and security threats", *Vojno delo*, Belgrade, 5/2017.

²⁷⁵ Editors of the American Heritage Dictionaries, *The American Heritage Dictionary of the English Language*, 3rd Ed. Houghton Mifflin Harcourt, 2000.

²⁷⁶ Federal Ministry of the Interior, (2009). *National Strategy for Critical Infrastructure Protection (CIP Strategy)*. Federal Republic of Germany, pp 2-7.

²⁷⁷ Namely, in this period the critical infrastructures corpus included roads, bridges, water and sewer systems, airports, ports, and public buildings, and might also include schools, health facilities, jails, recreation facilities, electric power production, fire safety, waste disposal, and communications services. See more: Vaughan, R., and Pollard, R., (1984). *Rebuilding America, Vol. I, Planning and Managing Public Works in the 1980s*. Washington, DC: Council of State Planning Agencies, pp.2.

security stage leads to the present necessity for redefining the understanding of CNI in mid-nineties of the last century, when CNI was viewed through „framework of interdependent networks and systems comprising identifiable industries, institutions (including people and procedures), and distribution capabilities that provide a reliable flow of products and services essential to the defense and economic security of the state“.²⁷⁸ The terrorist attack on the United States on 11 September 2001 contributed significantly to the general approach and attitude to critical national infrastructures. In particular, after taking the attack effect into consideration, it was concluded that all U.S. national security stakeholders, institutions and organizations should devote to prevention and a system for monitoring and maintaining capacities to save CNI from potential new asymmetric, terrorist attacks with hybrid consequences regarding national security and defense capabilities. Elements of CNI officially include all systems in the national infrastructure which are involved in the areas of vital importance to the nation: Agriculture, Food, Water, Public Health, Emergency Services, Government, Defense Industrial Base, Information and Telecommunications, Energy, Transportation, Banking and Finance, Chemical Industry, Postal and Shipping.²⁷⁹

The European Union as a specific form of Interesting associated states, whose existence is based on a broad platform of common economic, political, social, market and the human rights and freedom values, certainly recognizes the vulnerability of CNI. Whether we are talking about general, common or special, national capacities, critical infrastructure, from the EU point of view, institutions are noticed as general resources of all EU citizens. Endangering one component of CNI of any EU member causes consequences for the whole community. That's a reason why the EU has approaches to the regulation of access to CNI which is under the authority of the EU Member States, but also, it is recognized as collective resource.²⁸⁰ In this context, the EU defines critical infrastructure as a European infrastructure that consists of physical resources, services, devices, information technology, security, and network infrastructure, security, economic or social well-being: a) two or more Member States, b) three or more Member States.²⁸¹

²⁷⁸ US Federal government, (1996). *Executive Order 13010—Critical Infrastructure Protection*. Federal Register, Vol. 61, No. 138, pp 37347-37350.

²⁷⁹ Office of Homeland Security, (2002). *The National Strategy for Homeland Security*. Washington D.C.

²⁸⁰ Commission Of The European Communities, (12.12.2006), European Programme for Critical Infrastructure Protection, COM (2006) 786 final Brussels, EU.

²⁸¹ EU Council directive 2008/114/EC of 8 December 2008 on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection.

Results of the research which was made about CNI vulnerability based on strategy documents of several developed countries (Canada, UK, US, Germany, Norway and Switzerland), indicate that most of them, as most vulnerable parts of CNI recognized elements in the following fields: *energy* (electric, nuclear, gas, oil as well as their installations and transportation facilities), *communication* (telecommunication, informational broadcasting facilities, IT infrastructure) and *public services* (financial, food, water and medical supplying, public information), *transport, security* (nuclear, emergency and rescue services), *government* (institutions, buildings, basic defense industry, defense, police and customs system, public safety). Also, it indicated the existence of variability of priorities, which could be recognized as differences in specification of each country national economy, political and institutional strengths.²⁸²

The Republic of Serbia has a long and demanding path in regulation of CNI, especially in the perspective of ongoing EU integration process. Namely, Serbia, in accordance with the Law on emergency situations since 2009 has made the frame of regulations regarding the vulnerability assessments, sources of potential threat, the possible consequences, needs and possibilities for the implementation of measures and tasks of protection and rescue, which is delegated to the Ministry of Interior of the Republic of Serbia.²⁸³ In the same Law, Serbia recognizes CNI, but still without a clear definition of which elements or areas of infrastructure it is all about. In the process of EU integration, the Republic of Serbia should provide in the very near future: identifying National and European critical infrastructure; To perform risk analysis and assessment of the effects of threat; To establish a system of cross-sector criteria, as well as a set of general criteria / rules for assessing the risk of separate part of systems and networks of critical infrastructure; To set up a system of specific criteria / rules and to assess the risk to CNI based on them; To define the criteria and procedures for classified information relating to the National and European critical infrastructure which is conducted in accordance with the EU legislative; To designate a focal point, which is the central body of the state administration conducted communication and coordination with the competent bodies of the EU and other countries; To realize the Plan for

²⁸² Škero, M., and Ateljević, V., (2015). „Zaštita Kritične Infrastrukture i osnovni elementi usklađivanja sa direktivom Saveta Evrope 2008/114/ES“. *Vojno Delo*, 3/2015, Beograd, 192 - 207.

²⁸³ Government of Republic of Serbia, (2009). *Zakon o vanrednim situacijama*. Retrieved from: www.paragraf.rs/propisi/zakon_o_vanrednim_situacijama.html.

operational approach to protecting CNI; To establish control and penalties measures related to jeopardizing the CNI.²⁸⁴

POSSIBLE FORMS OF ENDANGERMENT OF CNI

Considering the contemporary events which affected the security and defense capabilities of the country, and which do not directly involve armed forces in conventional means of war, but primarily non-classical armed conflict forms and endangerment of national security (such as conflicts in Ukraine, Syria, situation in Iraq, Afghanistan, Libya, migration crisis, energy crisis, frequently terrorist acts all around the world, etc.), it is possible to develop two main approaches to the assessment of endangerment of CNI as a part of crucial national legitimacy:

- Hybrid operations as a part of Hybrid Warfare. It could be recognized in the field of energy, military technology dependence, IT, media, and economy. Main characteristics are hard clarification, acting forms which correlate with high political actions and influence, as well as diplomatic relation and deep impact on public diplomacy. Furthermore, it can be concluded that domination in this area has states which are recognized as global and regional powers, concerning the small and less developed countries. Critical national infrastructure is the aim of Hybrid warfare, mainly targeted by hybrid operations and asymmetric threats. Prevention of damage, destabilization of functions, partially or even completely losing control or possessing NCI could be recognized in strategically and rationally orientated national policy planning. Namely, small countries with limited resources, and small international influence are just part of the biggest game of influence. By the Hybrid warfare point of view, they are objects and polygon of interests clash in strategic geopolitical arena. Understanding this rational position could help responsible and future orientated nations to prevent endangering, demolition or losing National Critical Infrastructure or a part of it.

- Asymmetric threats, as specific form of nonlinear acting of groups, with a variety of motives and organizational aspects. Mostly recognized forms of acting are different forms of terrorist activities against the CNI, with the purpose to achieve damage, losses of functionality of CNI, impairment of human health and life, security, trust in Government and the introduction of massive panic and fear. By the analysis of parameters of endogenous aspects of CNI, possible vulnerable points, and introducing precaution measures, it is

²⁸⁴ Škero, M., and Ateljević, V., (2015), pp. 206.

possible to conduct effective, but not absolutely exact miserable, predicted, pre effected action against terrorist threat. There are many different definitions concerning asymmetric threats, but it is necessary to find one which can describe²⁸⁵:

- New, unorthodox, surprising, urgent, and unfamiliar threats;
- The historically unique security circumstances facing the institution of security governance;
- Organization vulnerabilities, or lack of defense;
- Institutional weaknesses in executing responses to threats; and,
- New tactics and operations available to potential enemies.

New, asymmetric security issues could be confined to the area related to three dominant security threats, which are not directly connected with the traditional military structures: terrorism, organized crime, and ethnic unrest or conflict.

The priorities of EU security policy towards the region of the Western Balkans (WB), including the application of European conditionality, the pace of the integration of the region, and the European posture towards the resolution of the territorial disputes in the region should all be lined up with a sober and constructive estimate of the nature and volume of the security threat arising from the region. Some research²⁸⁶, that has been done, provides a conclusion that all countries in the Western Balkan region have different methodology in the approach to asymmetric threats analysis in the region. If we recognize the asymmetric threat as the main security threat regarding CNI, we must notice that the main challenge for all countries in the WB is to establish gathering through asymmetric approach. Yet, we still have a potential collision in understanding, because some of the countries do not recognize terrorism as potential risk, threats or crisis generator. That could be the path to potential misunderstanding of terms and a possible different approach. So, the conclusion would be that it is necessary to learn and find common approach to define asymmetric threats, if we want to preserve our regional, Western Balkan CNI. If we look at the possible asymmetric threats from the joint

²⁸⁵ Lambakis, S., Kiras, J., Kolet, K., (2002), *Understanding "Asymmetric" Threats to the United States*, VA: National Institute for Public Policy, Fairfax.

²⁸⁶ Štrbac, K., Mitrović, M., (2011). "Asymmetric Threats-Common Response In Western Balkans". *The Review of International Affairs*, vol. LXII, No 1143, pp. 89-105, Belgrade.

standpoint, we might develop an effective crisis management approach, free of political influence.

Regarding the WB, it's very important to stress regional approach to the aim of EU integration process as the tool against asymmetric threats pointed regding NCI. The research²⁸⁷ indicates that for Balkan countries it is necessary to have a joint approach to integrations as balanced toll for safety of CNI.

In conclusion of the analysis of CNI endangering forms, it could be sublimated that physical endangerment and availability factor have dominant role. Namely, CNI could be endangered, ruined, destroyed or abused by physical means, by terrorist's acts or diversion, which are predominantly asymmetric forms of security threats, or even the part of wider hybrid operations. The availability is related to the ownership under CNI structures and possibilities of a country to gain full control of the content (gas, oil, coil, mineral, water, etc.) as well as physical part of CNI (pipe lines, delivering routes, reservoirs, mines, etc.). Namely, a country, which does not have a complete legitimate control over vital CNI, is potentially in a very high CNI risk position.

If we elaborate upon the previous hypothesis, the actual position of the Republic of Serbia will be analyzed in the frame of the Western Balkan and Europe. Namely, if we consider that role of CNI, it is not just infrastructure (objects and facilities) by itself, but potentials and resources which are in correlation with it, we could notice that hybrid and asymmetric activities against a state could be noticed in two main pillows:

Economy acts; Economic warfare is not a new idea, and it could be said that it has existed since the war itself. Contemporary economic warfare has forms of sanctions, embargo end other macroeconomic political acts, which have the purpose of conflict management tool, without the usage of armed forces.²⁸⁸ Thus economic means have the purpose to endanger:

- Supplying, by endangerment of availability of common and special resources;
- Trade, by limitation of the exchange which could supply necessary resources;

²⁸⁷ Mišćević, T., Mitrović, M., (2011). "Evolving Asymmetric Threats in the Balkans". *NATO Science for Peace and Security Series, E: Human and Security Dynamics*-Vol. 85, Publisher: IOS Press BV, Amsterdam.

²⁸⁸ Taillard, M.,(2012). *Economics and modern warfare*. Palgrave MacMillan.

- Market, by needs - offer manipulations with the purpose of influence on strategic interest.

Listed measures are directed according to general capabilities of the country to react against outer or inner generated forms of security threats. Economic pressures or economical straggle presents the engagement of economy, economical means and science in achieving the advantage in strategic areas of society, and thus in security and defense sectors of the state. Namely, they are involved in achieving inner – state effects, change of state policy, political system, general weaknesses, even defense capabilities, as well as foreign policy effects.²⁸⁹ In the scope of previous listed CNI areas which are recognized in developed countries (energy, communication, public services, government, transport and security) it could be concluded that any economical, hybrid attack could make an impact on the defense and security capabilities of a country. Also, asymmetric threats, for example terrorist attacks, could seriously endanger economy system of a country, and not just psychical damaging of parts of CNI, which is a direct impact. Furthermore, asymmetric threats could seriously damage economy system of a country, by non-direct influence, such are, insecurity regarding direct terrorist threats (an impact in tourism, small business and supported services), bio and animal health attacks (meat and other food production), diseases and contagions (transport), etc. Also, asymmetric threats and attacks could be recognized as a symbiotic part of some hybrid operations. For example it could be the usage analysis of terrorist attacks on so called KLA, during 1998-1999 against and in the vicinity of economy important centers in Kosovo and Metohija, as a part of wider, hybrid operation against Yugoslavia.²⁹⁰

Shortly, hybrid economic acts reflecting a possible negative influence on the whole country, and asymmetric attacks could consider a contribution to the total states CNI capabilities. In this term, asymmetric security threats could be understudied as a part of a hybrid concept of endangerment of states capabilities, which directly correlates with national security and defense.

Energy acts; Energy safety is a relatively new term, which considers different connotations, respectfully from the stand point of suppliers, consumers or transit countries. Oil, gas and electric power are recognized as main factors for energy safety analysis. Energy safety is directly related to geopolitical position of a country and it represents available energy resources, economic growth and political power and influence. Hybrid aspects of

²⁸⁹ Taillard, M.,(2012), pp. 15.

²⁹⁰ Мијалковски, М., (2002), *Тероризам албанских екстремиста*, Београд: Војска.

influence are especially indicated with correlation between energy and defense system of a country. Namely, a military factor is the last attribute which a country could use, after diplomacy, politics and economy efforts fail, in order to achieve energy resources. Also, the armed forces and police are guardians of energy corridors, transportation infrastructure and storages. So, we consider energy safety a part of national security cortex, which indicates that beside asymmetrical, for example terrorist acts, availability of energy resources are dominantly important for the CNI issue. From this point of view, Serbia is energy dependable country. Less of the energy sovereignty has more aspects: Serbia doesn't have national oil or gas companies. Russian „Gasprom“ bought „Naftna industrija Srbije“ in 2008 for 400 million euros, and made a new company „Srbiagas“ in which Russians have 51% of the ownership. Beside production and storage capacities, Russians controls even the land of tubes corridors. As far as oil is concerned, situation is similar. The Serbian oil company „Beopetrol“ was bought in 2003, by Russians „Lukoil“, for 117 million euros, and was overtaken with complete infrastructure and reproduction facilities. Those acts are also recognized as a part of „Russian Energy Offensive“ to South East Europe²⁹¹. Coal as energy resource also has tendency to be in deficit. Namely, more than 60% of Serbia coal reserves are on the territory which is unilaterally, by force taken, and named „The Republic of Kosovo“. More analyses²⁹² show that a secessionist movement of Albanians is supported by some interest groups in US, which had more than clear financial motivation to approach the Serbian coal reserves on Kosovo and Metohija²⁹³. Hybrid forms are recognized in a conceptual way of overall endangered national security, and asymmetry is conducted through stake - holders of endangering, whether we are looking at the paramilitary and terrorist organizations which are proxy used, or on scene where there are corporations and multinational companies, which took possession under national vital CNI structures. In summary, Serbia is energy insecure country from fossil fuels point of view. Moreover, Serbia doesn't have sovereignty

²⁹¹ Strategic Research Institute, Strategic – Security trends in South East Europe till 2020, Belgrade, 2015, p -101 – 109.

²⁹² For example: Flounders, Sara (2000). NATO troops seize mining complex, *Workers World Newspaper*, August 24, 2000; http://iacenter.org/folder04/kosovo_mines2.htm.;28/12/2016; then: Lydall Harold (1989), *Yugoslavia in Crisis*. Oxford: Oxford University Press; and: Hedges, Chris (1998). Kosovo War's Glittering Prize Rests Underground. *New York Times*, <https://groups.google.com/forum/#!msg/soc.culture.bosna-herzegovina/28/12/2016>.

²⁹³ Original name of Autonomous province, whose second part „Metohija“ originally means "Country under the administration of the monastery". The reason for that name is in the fact that the west part of Serbian south Autonomous province, since 12 century till communist regime 1945, belonged to ancient orthodox monasteries in Pec, Djakovica and Prizren.

under the oil, gas and main coil infrastructure, which makes a country deeply vulnerable.

CONCLUSION

CNI is a vulnerable point of national security and defense system. At the same time, hybrid and asymmetric way of endangerment is highly present during the peaceful time. Hybrid is mostly dangerous for the long distance point of view, because of a deep impact, correlation with related buildings, mass psychology shaping and so on. Asymmetric security threats are clear and present danger, with most devastating and psychologically expounding effects, which have a direct influence on the life of population. Both of them are hardly predicted, well camouflaged, long and secretly planned, etc. All above listed lead to the conclusion that CNI is permanent and high priority target of hybrid and asymmetric security threats. From this point of view, it has raised an ultimate necessity for comprehensive approach to the protection of CNI. Asymmetric security threats are in a wide role of national hybrid security endangerment, so it has a great potential influence on the CNI.

Specification of the WB and Serbia as its part, in prevention against hybrid and asymmetric security threats to CNI, correlate with complex history, present and future perspective of all countries in this region. Namely, the Balkan region is viewed as a common market by the investors, common infrastructure has some denominators (Corridor 7, 8 and 10), human resources are important from the standpoint of a unified approach and are counted only at the regional level, the transition problems and the industrial development have a relatively consistent level in all countries in the Balkans. All these reasons indicate the necessity for a common approach to dealing with potential hybrid and asymmetric threats, particularly in the field of solving unemployment and economic development. Specifically, future investments are viewed from the standpoint of the rate for capital risk investment, which is still relatively high in this region. If we take into account that there will no be possibilities for job creation and an increase in employment without investment, it is clear that precondition for the overall stability of the region are achieving a balanced approach to the asymmetric threats and a common response to the challenges. On the other hand, more standardized economic development means that CNI is more protected, because during the integration, we have to obey the rules of EU institutions regarding the protection of CNI, as a vital, essential, part of national and EU community.

The meaning of Comprehensive Approach is to bring all governmental and supranational stakeholders to prevention and crisis management regarding protection of CNI. Supporting tools for this purpose could be: 1) promotion of

shared values as well the understanding of the situation and common aims regarding the preservation of CNI on all levels; 2) development of the structures and planning the processes which can provide support and help in planning and implementation of appropriate reactions in situation when CNI are endangered; 3) establishing relationships and multilateral understanding, through common education, value building, training, exercising, analysis and planning a responding scenario in potential CNI endangered situation.²⁹⁴

We can say that comprehensive and strategically are the synonyms for the approach to the analysis of asymmetric endogenous of CNI in the hybrid concept of conflict. The reasons for that we can see in the various aspects of nature of CNI, stakeholder of safety and preventive role, to the wide range of security risks and threats, as well as risk and threats holders. So, we can conclude that comprehensive should be an organization and action planning of stakeholders of security measures regarding CNI, analyzing types and sources of endangering of CNI (man caused or natural disasters), and, of course, analyze the risk holders (organizations, states and non-states, proxy, natural disasters, environment degradation, pollution, etc).

Having in mind asymmetrical nature of risks and threats for CNI, we can conclude that comprehensive security measures for CNI have the following purposes:

- Development of capabilities for physical protection and legitimated ownership under CNI;
- Low regulation and it's incorporated in standardization forms of controlling and protection of CNI.
- Building the partnerships among the stakeholders of CNI security roles at national as well as regional and international level;
- Implementation of an all-hazards risk management approach through daily based stakeholders communication;
- Advance the timely sharing and protection of information among partners on all levels of CNI security management system.

Comprehensive approach involves strategic based planning process with a purpose to achieve a reliable and appropriate combination of security measures. Aims of those measures are: 1) to address intentional and accidental incidents, 2) to develop business continuity practices which can deal with

²⁹⁴ Mitrovic, Miroslav, Comprehensive Approach to the Asymmetric Endangerment of National Critical Infrastructure (July 10, 2013). Retrived from SSRN: <http://dx.doi.org/10.2139/ssrn.2942036>.

disruptions and ensure the continuation of essential services, and 3) emergency management planning with the aim to ensure adequate response procedures that should be in place to deal with unforeseen disruptions and natural disasters.

Regarding those aims, comprehensive approach has the purpose to provide a framework for the functions of the multi-level (sector, nation, regional, international) of CNI protection networks, regarding Canadian²⁹⁵ model could include:

- Enabling in-time data availability for all stakeholders;
- Identification of national, regional or sector risks holders and threats by NCI;
- Development time and expert made studies of real danger to CNI; and
- Creating Procedures and practices for the purpose of strengthening the resilience of CNI and their readiness for prevention, mitigation, response and recovery

From the German²⁹⁶ point of view, comprehensive approach can be divided by the nature of causes on: 1) natural events, 2) errors (technical failure or human error), and 3) organized violence activities (terrorism, crime, war). Taking into account the complexity and comprehensiveness, it can be said that the comprehensive strategic approach is necessary because of the need for:

- Open risk communication among the state, companies, citizens and the general public, taking into account the sensitivity of certain information;
- Co-operation among all stakeholders in preventing and managing incidents;
- Greater self-commitment by operators regarding incident prevention and management;
- A greater and self-reliant, self-protection and self-help capability of individuals or institutions affected by the disruption or compromise of critical infrastructure services.

²⁹⁵ Canadian government, (2009). *National Strategy for Critical Infrastructure*, Her Majesty the Queen in Right of Canada.

²⁹⁶ Federal Republic of Germany, Federal Ministry of the Interior, (2009), *National Strategy for Critical Infrastructure Protection* (CIP Strategy), pp 2-7.

At the end, all stakeholders in crisis management process (planning, analyzing, educating, training, lessons-learning, equipping, etc.) in order to provide security and severity of CNI, should work together. Finally, due to the fact that the hybrid warfare concept, as well as asymmetric security threats aim to the perceived vulnerable components and CNI of nation, the most effective defense regarding them, is prevention. Namely, hybrid warfare, as well as asymmetric threats, have the aim to plan, organize and conduct operations which are significantly different from the opponent's ones, with the purpose to maximize own advantage, using the opponent's weaknesses, take the initiative, and the achievement of greater freedom to create activities with the ultimate aim of achieving strategic goals. Based on the above mentioned, the prevention of a state which would proactively commence with the creation of defensive attitude towards hybrid and asymmetrical threats includes a preventive planned operation. Such an approach would imply strategically conceptualized attitude towards the key structures of a state and society, the development of legitimacy and legality of state institutions, strengthening the economy, the establishment and enforcement of legislation, raising the level of general culture and education of the population, media and information environment, verification and highlighting positive moral and ethical values at the level of national social consciousness, etc. Applied in practice, preventive response to hybrid and asymmetric threats, regarding the key national resources, including CNI, involves the development of all the elements of a state and society, such as military capacities and capabilities, the economical, diplomatic information and communications, intelligence and security, legislative and judicial, scientific, educational and administrative resources of the state²⁹⁷.

LITERATURE

1. Arquilla, J., and Ronfeldt, D., (2001). "The Advent of Netwar (Revisited)." *Networks and Netwars: The Future of Terror, Crime, and Militancy*. Santa Monica, CA: Rand.
2. Canadian government, (2009). *National Strategy for Critical Infrastructure*, Her Majesty the Queen in Right of Canada.
3. Cebrowski, A., and Garstka J., (1998). *Network - Centric Warfare: Its Origin and Future*. U.S. Naval Institute.

²⁹⁷ See more: *Dealing With Today's Asymmetric Threat to U.S. and Global Security*, An Executive Summary of the May 8th 2008 Symposium, 2008 CACI International Inc.

4. Commission Of The European Communities, (12.12.2006), European Programme for Critical Infrastructure Protection, COM (2006) 786 final Brussels, EU.
5. Cull, N. (2006). Public Diplomacy Before Gullion: The Evolution of a Phrase. Retrieved from <https://uscpublicdiplomacy.org/blog/public-diplomacy-gullion-evolution-phrase>.
6. Darius, M., (2014). "Iraq and Syria are Burning, "Constructive Chaos" and America's Broader Strategy to Conquer Eurasia." GlobalResearch.ca, June 2014.
7. Dealing With Today's Asymmetric Threat to U.S. and Global Security, An Executive Summary of the May 8th 2008 Symposium, 2008 CACI International Inc.
8. Department of the Army (2008). Field Manual No. 3-0: Operations. Washington, DC.
9. Editors of the American Heritage Dictionaries (2000), The American Heritage Dictionary of the English Language, 3rd Ed. Houghton Mifflin Harcourt.
10. EU Council directive 2008/114/EC of 8 December 2008.
11. Federal Republic of Germany, Federal Ministry of the Interior, (2009), National Strategy for Critical Infrastructure Protection (CIP Strategy).
12. Flounders, Sara (2000). NATO troops seize mining complex, Workers World Newspaper, August 24, 2000; http://iacenter.org/folder04/kosovo_mines2.htm./;28/12/2016;
13. Government of Republic of Serbia, (2009). Zakon o vanrednim situacijama. Retrieved from:
14. Hart, L., (1954). "The Strategy of Indirect Approach". Internet Archive, National War College.
15. Hedges, Chris (1998). Kosovo War's Glittering Prize Rests Underground. New York Times, <https://groups.google.com/forum/#!msg/soc.culture.bosna-herzgvna/>;28/12/2016.
16. Hofman., F.,G., (2007). Conflict in the 21st Century-The Rise of Hybrid Wars. Potomac Institute for Policy Studies. Hoffman., F., G., (2016). On Not-So-New Warfare: Political Warfare vs. Hybrid Threats. Retrieved from: <http://warontherocks.com/2014/07/on-not-so-new-warfare-political-warfare-vs-hybridthreats/>; 12/05/2017.
17. Kofman, M., Rojansky, M., (2015). „A Closer look at Russia's „Hybrid War“. Woodrow Wilson International Center for Scholars, Kennan Cable No. 7, April 2015.
18. Korybko, A., (2015). Hybrid Wars: the indirect adaptive approach to regime change, Moscow, Peoples' Friendship University of Russia.

19. Lambakis, S., Kiras, J., and Kolet, K., (2002). Understanding "Asymmetric" Threats to the United States. National Institute for Public Policy, Fairfax.
20. Lind, W., Nightengale, K., Schmitt, J., Sutton, J., Wilson, G., (1989), „The Changing Face of War: Into the Fourth Generation“, Marine Corps Gazette, Oct. 1989.
21. Lydall Harold (1989), Yugoslavia in Crisis. Oxford: Oxford University Press.
22. Mann, S., (1992). "Chaos Theory and Strategic Thought", Parameters, Autumn 1992.
23. Metz, S., and Johnson, D., (2001). Asymmetry And U.S. Military Strategy: Definition, Background, And Strategic Concepts, Strategic Studies Institute, US.
24. Mišćević, T., Mitrović, M., (2011). "Evolving Asymmetric Threats in the Balkans". NATO Science for Peace and Security Series, E: Human and Security Dynamics-Vol. 85, Publisher: IOS Press BV, Amsterdam.
25. Mitrović, M. (2017). "The economic and energy aspects of a hybrid threat to national security". Vojno delo, Belgrade, 6/2017.
26. Mitrović, M., (2017). "The potential influence of interest groups on the US Foreign Policy – Case of 'Kosovo'". Zbornik Matice srpske za društvene nauke, No.162 - 163.
27. Mitrović, M., (2017). „Hybrid warfare and asymmetric security threats“. Vojno delo, Beograd, 5/2017.
28. Mitrović, M., (2017). „Public Diplomacy in Hybrid Warfare paradigm“, Vojno delo, Belgrade, 7/2017.
29. Mitrovic, Miroslav, Comprehensive Approach to the Asymmetric Endangerment of National Critical Infrastructure (July 10, 2013). Retrived from SSRN: <http://dx.doi.org/10.2139/ssrn.2942036>.
30. Nye, J., (1990). "The misleading metaphor of decline". The Atlantic Monthly, March 1990.
31. Office of Homeland Security, (2002). The National Strategy for Homeland Security. Washington D.C.
32. Qiao, L., Xiangsui, W., (1999). Unrestricted Warfare. PLA Literature and Arts Publishing House, Beijing.
33. Renz, B., Smith, H., (2016). Russia And Hybrid Warfare –Going Beyond The Label. Finnish Prime Minister's Office, Government's analysis.
34. Shahskov, S., (2011). "The theory of 'manageable chaos' put into practice." Strategic Culture Foundation, 1 Mar. 2011.
35. Škero, M., and Ateljević, V., (2015). „Zaštita Kritične Infrastrukture i osnovni elementi usklađivanja sa direktivom Saveta Evrope 2008/114/ES“. Vojno Delo, 3/2015, Boegrad.

36. Strategic Research Institute, Strategic – Security trends in South East Europe till 2020, Belgrade, 2015.
37. Štrbac, K., Mitrović, M., (2011). "Asymmetric Threats-Common Response In Western Balkans". The Review of International Affairs, vol. LXII, No 1143, pp. 89-105, Belgrade.
38. Taillard, M.,(2012). Economics and modern warfare. Palgrave MacMillan.
39. Tzu, S., (2000). Art of War- Chapter 3: Attack by Stratagem. Allandale, Leicester.
40. US Federal government, (1996). Executive Order 13010—Critical Infrastructure Protection. Federal Register, Vol. 61, No. 138.
41. Vaughan, R., and Pollard, R., (1984). Rebuilding America, Vol. I, Planning and Managing Public Works in the 1980s. Washington, DC: Council of State Planning Agencies.
42. www.paragraf.rs/propisi/zakon_o_vanrednim_situacijama.html
43. Мијалковски, М., (2002), Тероризам албанских екстремиста, Београд: Војска.
44. Президент России, Москва, (2010). Военная доктрина Российской Федерации. Retrieved from <http://kremlin.ru/supplement/461>.
45. Президент России, Москва, (2014). Военная доктрина Российской Федерации. Retrieved from, http://www.consultant.ru/document/cons_doc_LAW_172989/.
46. Слипченко, В. (1999). Война будущего. Москва: Московский Общественный Научный Фонд.

KRITIČNA NACIONALNA INFRASTRUKTURA SA STANOVIŠTA ASIMETRIČNIH BEZBEDNOSNIH PRETNJI U OKVIRU KONCEPTA HIBRIDNOG RATOVANJA

Miroslav Mitrović*

Institut za strategijska istraživanja, Univerzitet odbrane, Beograd,
Republika Srbija

Apstrakt: Savremeni geopolitički događaji ukazuju da su aktuelni sukobi po prirodi nelinearni, hibridni i asimetrični. Osim toga, ova nekonvencionalna sredina razvoja sukoba upućuje na fenomen da se aktuelni

* miroslav.mitrovic@mod.gov.rs

sukobi sve više udaljavaju od klasične, konvencionalne teorije ratovanja i da kreiraju ambijent nekonvencionalne paradigme konflikata. Sa tim u vezi, kritična nacionalna infrastruktura, pored ostalih nastavlja da bude sve više jedan od prioritarnih operativnih ciljeva novih, nekonvencionalnih napada protivnika. Specifičnosti ranjivosti i važnosti kritične nacionalne infrastrukture, naročito doprinose karakteristike i priroda savremenih hibridnih koncepata sukoba i posebno asimetričnih formi ugrožavanja nacionalne bezbednosti, i njihovi potencijalni efekti na elemente kritične infrastrukture, a time i opšte odbrambene sposobnosti nacije. U aktuelnom trenutku, svedoci smo da državni i nedržavni akteri dominantno i preovlađujuće koriste nekonvencionalne forme konflikata radi ostvarivanja svojih interesa. Ova nekonvencionalnost predstavlja zajednički imenitelj koji obuhvata hibridnost i asimetričnost konflikata. Može se reći da je kritična nacionalna infrastruktura cilj delovanja asimetričnih formi ugrožavanja bezbednosti kao deo hibridnog koncepta sukoba. U radu su iznesena razmatranja koja imaju za cilj da doprinesu iznalaženju dela odgovora na pitanja: Šta je hibrid rat i gde je njena veza sa asimetričnim pretnjama bezbednosti? Koji deo kritične nacionalne infrastrukture je najugroženiji od strane asimetričnih bezbednosnih pretnji? Kako razviti prevenciju u zaštiti kritične nacionalne infrastrukture? Analiza je zasnovana na širokoj bazi naučne, stručne i normativno-pravne literature, kao i analizi aktuelnog stanja u Republici Srbiji u vezi sa navedenom temom.

Ključne reči: asimetrične bezbednosne pretnje, hibridno ratovanje, kritična nacionalna infrastruktura.