AARMS Vol. 17, No. 3 (2018) 71–82. **10.32565/aarms.2018.3.5**

Comprehending Gerasimov's Perception of a Contemporary Conflict – The Way to Prevent Cyber Conflicts

Robert JANCZEWSKI,[1] Grzegorz PILARSKI[2]

Alongside with the appearance of the so far unknown reality called cyberspace, the new conditions of the course of conflicts emerged, consequently both the scientists as well as practitioners started to use the term cyber conflict. Unfortunately, presently there is no consistent, common view concerning a cyber conflict.

The article presents a theoretical basis of cyber conflicts based on the research carried out by the authors. The article itself is an added value since it provides the suggestion and explanation of the perspective for the understanding of cyber conflicts through the prism of Gerasimov's perception of a contemporary conflict. Moreover, it presents a new definition of a cyber conflict as the process being the system of activities. The authors also present the stages of a conflict according to Gerasimov, as well as the structure of a cyber conflict. Additionally, the article envisages the aspects of Russian attitude to conflict solving which are worth paying attention to. The presented article offers the perspective of the Russian understanding of the resolution of conflicts, it bridges the gap in research on cyber conflicts as well as assures a strong theoretical basis for the understanding of a Russian point of view on the solution of contemporary conflicts, which might be useful for counteracting cyber conflicts. The authors hold the view that the article is the incentive for further research on cyber conflicts during competition.

Keywords: *component, cybernetic environment, information processes, Signals Intelligence, information processing*

Introduction

In a changing world the state, non-state, military and non-military entities still cooperate with one another both in the national and international dimension. Alongside with the positive cooperation, the interactant states run campaigns for the development and protection of their own national interests, which can often lead to conflicts. Still, whenever people cooperate, competition and conflict are natural and inevitable phenomena.

The civilization development of societies has contributed to the creation of the so far unknown sphere which has been named cyberspace. Cyberspace creates possibilities for countries, their allies and partner countries to obtain and keep constant benefits, as well as to assure the safety of their countries. Cyberspace in its range is not limited by the geographical

[1] War Studies University, Section of Cyber Security, Warsaw; e-mail: r.janczewski@akademia.mil.pl
[2] War Studies University, Section of Cyber Security, Warsaw; e-mail: g.pilarski@akademia.mil.pl

and geopolitical borders. The access to the Internet and other spheres of cyberspace provides the users with a worldwide range, creates chances for fast development, but at the same time it creates proper conditions for cyber threats e.g. the possibility of infringing the integrity of critical infrastructure in a direct and indirect way without physical presence.

The latest experience indicates that activities performed against countries are transferred from physical dimension i.e. land, sea and air space into cyberspace. Scientists have been expressing their points of view on the new areas of combat for many years. In 2009, Colin S. Gray wrote that it has been rare in history for a new geography to be added to the elite short list of environments for warfare. Now there are two such new geographies, space and cyberspace, and we are becoming ever more dependent upon them both. Thus far, at least, we have not taken space or cyber system vulnerability as seriously as we shall have to. It is a law of war: The greater the dependency on a capability, the higher the payoff to an enemy who can lessen its utility, in effect turning our strength into a weakness. [1] This remark clearly depicts the meaning of cyberspace for competition and conflict.

It seems to be a cliché the statement that there are still more advanced technological and technical solutions and the theatre of operations is still changing. However, in the context of conflicts, the issue is not as trivial as it seems to be. The emergence of the new space where societies function resulted in the fact that we live in the era of cyber conflicts. Thus, the question emerges whether the phenomenon is understood and whether it is possible to counteract it.

In order to understand the meaning of the new, so far unknown piece of reality – cyberspace for security, it must be realized that the constant, dynamic development of methods, techniques and measures of combat contributes to the multi-dimensional character of the area of conflicts and new technologies, technical solutions, methods or methodology of operations determine the reasons and course of conflicts.

The main methodological assumption of the article is a deep belief of the authors that the acquaintance and comprehension of the character of the contemporary understanding of conflicts in general, the characteristics of cyberspace as well as the essence of operations run in this domain as well as making use of it by the potential adversaries allow to know the nature of cyber conflicts and most of all how to counteract them. Thus, the main goal of deliberations presented in the article will be the quest to find the answer to the question: whether the comprehension of the views of Gerasimov on the contemporary conflict shall allow to counteract cyber conflicts?

This paper makes the following novel contributions:

- cyber conflict as the process being the system of operations;
- the structure of a cyber conflict;
- the factors and elements of a cyber conflict;
- the identification of a cyber conflict as the element of a conflict in the general meaning;
- the decomposition of a cyber conflict into stages.

According to the authors the primary stakeholders of interest for the outcome of this analysis should be the military, non-military, state and non-state actors.

Cyber Conflict – Whether We Realy Understand It

The connotation of the concept of a cyber conflict seems to be fairly simple and clear-cut. Unfortunately, a deeper analysis of the concept leads to a conclusion that it is not like this. As M. Afzalur Rahim [2: 17] noticed, the term "conflict" has no single clear meaning. Much of the confusion has been created by scholars in different disciplines who are interested in studying a conflict. It is exactly the same with the concept of cyberspace.

Thus, there is a question if it is possible to expressly indicate the referents of a cyber conflict if it is impossible to indicate the referents of a conflict and cyberspace. The scope of a cyber conflict is unfortunately not examined enough and because of that, it is misunderstood by the scientists and practitioners. Thus, it is not clear, in what way the conventional mechanisms of security such as deterrence or collective defence refer to the new phenomenon.

The subject literature presents the view that a conflict is an improved relative position, without concern for absolute welfare consequences ("zero-sum" orientation – the sum of winnings equals the sum of losses). This reflects a classic game-theory outcome with non-cooperative players and often occurring in real conflicts. The authors of the article hold the view that if you ask the wrong question, you probably will get a wrong answer. And cyber—and what to do about cyber conflict—is an arena where there is generally no agreement on what is the question, certainly no agreement on what is the answer, and evolving so fast that questions are transmuted and affect and change the validity of answers that have been given. [3]

A prove for the rank of the issue is the bilateral cooperation signed in 2011 between the East West Institute and the Information Security Institute of Moscow State University aiming at a terminological convention in the scope of cyber. As a result, 20 terms were established through the initial bilateral negotiations and publication in April 2011. Building on the then-established collaborative relationship, the joint team reinitiated the discussion in 2013, to further define critical terms.

Moreover, the vitality of the problem issue is proved by the fact that in June 2013 presidents Vladimir Putin and Barack Obama signed an agreement on the commencement of cooperation in the scope of cyber security. The common understanding and the definitions of the key terminology concerning a cyber conflict elaborated by the above mentioned institutions were of significant importance for the agreement.

Lexically, a cyber conflict is determined very laconically. According to the Macmillan Dictionary a cyber conflict is a conflict in cyberspace and at the same time a cyber conflict is a cyber warfare. [4]

The above mentioned Report Critical Terminology Foundations 2 defined a cyber conflict (Russian: Киберконфликт) as a state that is on a continuum with war, but falls short of a critical threshold, is a tense situation between or among nation-states or organized groups where unwelcome cyber-attacks result in retaliation. At the same time the report defines a cyber conflict as a tension between states and/or organized political groups where the hostile (unwanted) cyber-attacks provoke (lead to) retaliation. The phenomenon of a cyber conflict is also of significance for the definition of a cyber war. Cyber war, according to the Report, is an escalated state of a cyber conflict (Russian: высшая степень киберконфликта) between or among states in which cyber-attacks are carried out by state actors against cyber

infrastructure as part of a military campaign. Cyber conflict can be also a precursor to an escalated situation. [5]

The subject literature indicates objectives in preventing and managing a cyber conflict. L. Kello claims that to prevent or minimize activities that threaten the functioning of the global Information Communication Technology (ICT) system and the global political economy, states and relevant private actors should be expected to undertake a range of policies and activities to fulfil the following functions:

Military cybernetics distinguishes three basic directions:

- enhance the capacity to detect and attribute cyber exploitations and attacks and to distinguish their purposes;
- augment various forms of defence against such activities, both to protect assets and raise the costs to potential perpetrators;
- increase the resilience of key cyber dependent systems;
- while more difficult, pursue political and technical analogues to arms control agreements, or understanding that could inspire confidence that malware and other "weapons" will be sparingly used and will not have unintended consequences, including proliferation;
- assert state control over actors that use their territories to conduct unlawful cyber activities and over their citizens who do so abroad;
- upgrade capabilities to signal, threaten and initiate cyber and other actions to inflict sufficient "pain" on adversaries to motivate them to eschew or desist from hostile activities; and
- develop, over time, norms to restrain the most potentially destabilizing sorts of cyber activities.

These steps would contribute to the prevention and mitigation of actions that could threaten the dynamic stability of the domain and of the international political economy. [6]

The subject literature presents the view that the term "cyber conflict" denotes an offensive cyber-attack for political or strategic purposes as well as responses to such an attack. [7]

A cyber conflict is also the use of computational means, via microprocessors and other associated technologies, in cyberspace for malevolent and/or destructive purposes in order to affect, change or modify diplomatic and military interactions between entities. [8]

At the same time, according to the subject literature, a cyber conflict might not have any political basis. [9]

The results of the research carried out by the authors allow to formulate a conclusion that a cyber conflict is a process that is a system of activities. Details will be described later in this article.

Cyber Activities – Russian's Point of View

The analysis of subject literature revealed that the Russians also started to use the concept of cyberspace and to develop abilities to run operations in the cyberspace or with its use. It is significant in the context of the role of cyberspace in the course of a conflict.

On the 21st of March 2012 during a meeting with military scientists, the vice Prime Minister of the Russian Federation being responsible for the defence industry, Dmitrij Rogozin announced that the Russian authorities are taking into consideration the idea to form forces proper for operations in cyberspace within the structure of their own Armed Forces. He said that at that time they were deliberating on the creation of a cyber command. It stemmed from the need to assure the safety of information both of the armed forces, as well as of the state infrastructure as a whole. [10] Rogozin assured at the same time that all documents had been already prepared and he expressed hope that the technical predator, as he dubbed it, would appear soon. According to him, the main tasks that forces need to tackle include the monitoring and processing of information coming from the outside, as well to combat cyber threats, as he said "in other words it would be something similar to American cyber army. The officers who had been trained to serve in those forces would have to go through a language training, namely learn a foreign language, first of all English language". As we learnt from the press, in order to attain a maximum control of the cyberspace, general Siergiej Szojgu announced the beginning of "a great hunt" for computer programmers. This is enforced by the multitude of computer software which is needed by the Army within the next five years. [11]

At the beginning of July 2013 also the Ministry of Defence of the Russian Federation announced publicly that Russia will have forces responsible for combating cyber threats and for fighting cyber-attacks. [12] The head of the Russian Foundation for Advanced Research Projects, Anderei Grigoriev, also confirmed that in the Russian armed forces a new type of forces specializing in the fight against cyber threats was being created. In the radio station Echo of Moscow, A. Grigoriev announced: "cyberspace—now the task has been formulated, a decision has been made to create cyber command within the Ministry of Defence as well as to create a new type of forces. We have already contacted the potential people who will work there and now we are preparing a common programme which will have to be constantly developed."

In 2014 a Concept of the Russian Federation of cyber security strategy was created. [13] In this document the Russians noticed that Information and Communications Technology (ICT) was developing very fast exerting still bigger influence on all key spheres of citizens', organizations', and state's activities in the Russian Federation. The Internet and other elements of cyberspace have become a systemic factor of Russian economic development and modernization. The implementation of ICT into the management processes is the basis to create an effective and socially responsible democratic state of the 21st century.

According to the concept, cyberspace is the sphere of activities in information space, created by a set of Internet communication channels and other ICT networks, technological infrastructure assuring their functioning, as well as any forms of human activity (of private people, organizations, the state) realized through their usage. Such understanding of cyberspace differs from the one presented in the above-mentioned Report, where cyberspace is understood as an electronic medium through which information is created, transmitted, received, stored, processed and deleted. In fact, such understanding of cyberspace is limited to only a medium of information processes.

In the concept, it has been noticed that the cross-border character of cyberspace, its dependency on advanced information communication technology create not only new possibilities but also new threats in the sphere of the rights, interests and the functioning

of people, organizations, or state bodies. Cyber-attacks carried out by cyber criminals and cyber terrorists pose a threat to the secured information resources. It is possible to use cyber weapons in special operations and cyber war, as well as during traditional war operations. The last sentence is clearly incorporated in the philosophy of a hybrid conflict.

The importance of cyberspace is emphasised by the Russians also in the report of the Centre for Strategic Research of the Russian Federation of 22nd of December 2017 entitled *The future of information security: global changes and scenarios for Russia.* [14]

In the Centre's report the authors notice that in the context of Information Communication Technology as the means of running military operations as well as cyberspace as a synthetic concept used to indicated a new technological environment for operations, it is not obvious that it is possible to use the existing set of international norms of humanitarian law and the law of a military conflict. The literal application of the existing basic norms (The Geneva Convention of 1949 and others) is impossible due to the technological specificity of cyberspace, and effective adjustment of such norms, taking into consideration the technical twists and turns, has not been prepared yet. A separate problem is the lack of universal definitions and the classification of the objects and assets (critical information infrastructure/ critical objects) which must be protected.

In the context of a cyber conflict, according to the Centre's report, the key problem is the lack of trust to the system of international relations which enables the creation of common security mechanisms. It is also well-based to set the boundaries of operations which, if crossed, could result in military reaction. Thus, Russia should prepare and introduce into international discussion its own stance towards this issue.

The Centre's report recommends that till the year 2020 the Russian Federation should prepare and publish a separate strategy for the operations of the armed forces in the information realm (similar to the Pentagon's cyber security strategy). Russia reserves the right to limitless use of its military capacity as a response to operations with the use of ICT, the use of force in accordance with Moscow's standards.

According to the Centre's report there is a necessity to carry out work, in the framework of closed consultations and briefings, between the Russian Federation and the United States, NATO, EU, Great Britain, China, Israel as well as other states and organizations in the scope of the interpretations of certain international norms of humanitarian law with reference to cyberspace (including the definition of the threshold of force used in cyberspace), the common management of the escalation of conflicts in cyberspace in order to assure a minimum acceptable level of strategic stability in cyberspace.

The above analysis revealed that the Russian Federation builds military capability to run operations in cyberspace. It is of great importance in the context of the course of conflicts in cyberspace.

Gerasimov's Perspective of Conflict

In February 2013 general Valery Gerasimov, the head of the General Staff of the Armed Forces of the Russian Federation published an article in a weekly magazine *The Military-Industrial Courier* under the title *The Value of Science in Prediction.* [15] The starting point of the article was an opinion that the new challenges require deliberation on new forms and

methods for running military operations. In the article, the general presented his own view on the forms and methods of running military operations in the contemporary conditioning, as well as the role of non-military methods in solving conflicts between countries.

W. Gerasimov has distinguished six stages of conflict development:

1. Concealed primary operations.
2. Intensification.
3. Commencement of conflict operations.
4. Crisis.
5. Settlement of a conflict.
6. Re-establishment of peace (following a conflict).

The analysis of the article revealed that the head of the General Staff of the Armed Forces of the Russian Federation noticed that in the settlement of conflicts between countries, a bigger role is presently played by non-military measures. The latter one include:

In stages 1, 2 and 3:
- Settlement of coalitions and alliances.

In stages 1 and 2:
- Creating political opposition.

In stages 2 and 3:
- Economic sanctions.
- Severance of diplomatic relations.

In stages 2, 3, 4 and 5:
- Political and diplomatic pressure.

In stages 3 and 4:
- Activities of opposition forces.

In stage 4:
- Economic blockade.

In stage 5:
- Rearrangement of the economy into the state of war.
- Change of military-political command.

In stages 5 and 6:
- Seeking for ways of settling the conflict.

In stage 6:
- Running comprehensive activities aiming at the decrease of tensions in relations.

The military measures include:

In stages 1, 2, 3 and 4:
- Military measures of strategic deterrence.

In stages 3 and 4:
- Strategic expansion.

In stages 4 and 5:
- Running military operations.

In stages 4 and 5:
- Peace operations.

While informational confrontation present in every stage of a conflict is, according to the general, both a non-military and military activity.

W. Gerasimov highlighted that presently the achievement of political goals is realized through the use of political, diplomatic, economic and other non-military measures linked with the use of military power, and not only through armed combat. Such points of view create ideal conditions to run activities both in cyberspace, as well as with its use to attain the set goals.

The view that new challenges require re-thinking of the forms and methods of settling conflicts is depicted by Gerasimov on Figure 1.

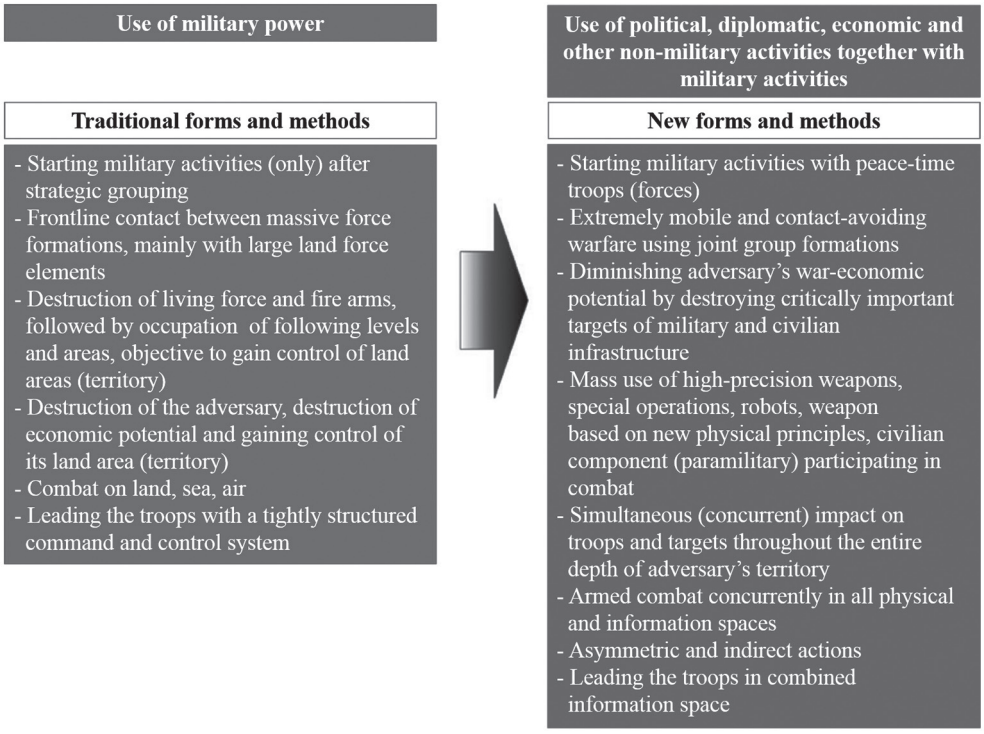

Figure 1. *The evlolution of political goals achievement according to Gerasimov.* [15]

The analysis of new forms and methods presented above in the evolution of the character of combat fight in the process of attaining political goals clearly shows the meaning of cyberspace in the course of a conflict. A cyber conflict can be commenced in cyberspace or with its use by specialized forces (army) proper for the time of peace prepared to act in cyberspace. Moreover, cyberspace creates perfect conditions to support task-oriented groups in conducting highly manoeuvrable, non-contact military operations. It is hard to appreciate enough the role of cyberspace in diminishing the military and economic potential of a country by neutralizing in short time critical objects of military and civilian infrastructure. ICT networks and systems facilitate running special operations and the use of precision-guided munitions, robotic platforms, and of weapons based on the state-of-the-art solutions, civilian forces (paramilitary ones) on a large scale. The characteristics

of cyberspace significantly facilitate simultaneous impact of military forces and civilian objects of the enemy on the whole territory. Cyberspace can be effectively used to run military activities at the same time on all physical areas and in information space, as well as asymmetric and indirect activities. The new operational domain enables the organization of a single information space, which is of great importance for the management of forces and resources at the time of a conflict, and consequently of a cyber conflict.

Presently, next to traditional techniques, non-standard ones are introduced. The role of single, mobile task-oriented groups is increasing due to the use of new possibilities that are offered by the command and support systems. Military operations are becoming more and more dynamic, active and effective. Tactical and operational gaps, which might be used by the enemy, are disappearing. The new Information Communication Technology made conditions for shortening the time, reducing the space and the information gap between the fighting groups and the command and control bodies. Front clashes between big military groups (forces) on a strategic and operational level are going down in history. The development of ICT is one of the reasons for the disappearing difference between operations on strategic, operational, or tactical level. Precision-guided weapons used in combat is based on advanced robotic systems. The use of cyberspace in asymmetric operations allows to balance the predominance of the enemy in armed combat. Owing to that, it is possible to carry out operations on the whole territory of the enemy as well as to exert influence on information and at the same time to constantly improve the forms and methods of activity. The changes which are taking place are reflected in the doctrines of the leading world powers and are being constantly tested.

The considerable meaning of cyberspace is proved by the fact that the Federal Security Service (FSB; Russian: Федеральная служба безопасности Российской Федерации [ФСБ]) of the Russian Federation has formed the Centre for Electronic Communications Surveillance responsible for intercepting, de-coding, and processing of the data and information sent via electronic communication. The Centre is also known as number 16 and for protective aims FSB unit 71,330.

The analysis of internet sources proved that the Military Unit 71,330 called for a tender to assure access to information from the world and regional IT and ICT networks (including the Internet) that was to begin on the 15th of January 2015. The cost was covered from the federal budget. The contract price totalled 557,500,000,014 RUB. The tender was won by the Limited Liability Company NEO PRINT, located in Mytiszczi – a city in the Moscow district, located 19 km from Moscow. [16]

Cyber Conflict – A Process

L. R. Pondy has argued that "organizational conflict can be best understood as a dynamic process underlying organizational behaviour. This is a very broad definition that excludes very little of anything transpiring in a group or individual". [17]

The authors' research proved that a cyber conflict is a process. The process is based on the elaborated methodology and a system of activities realized with certain resources. It has its beginning and the end, it also lasts continuously in time. The structure of a cyber conflict is formed by sub-processes which include stages, phases, and activities. The primary

and secondary factors qualify the structure and the course of a cyber conflict. A cyber conflict can be disturbed by organizational, procedural, and technical barriers. They exert a negative influence on the course of a cyber conflict.

The threshold of a cyber conflict is of great importance. This is the point which if crossed can trigger a cyber conflict. The threshold of a cyber conflict indicates that disagreements, incompatibilities or differences between subjects are so serious that the parties move on to the state of a conflict. However, some quality of a cyber conflict is worth paying attention to. It does not take place only because of disagreements, incompatibilities or differences between the potential parties of a conflict. In order for the cyber conflict to take place, each party must be convinced that the threshold of a cyber conflict has been crossed. The difficulty is based on the fact that the subjects might have (and usually have) different vulnerabilities and tolerance, if they are exceeded, it marks the beginning of a conflict. It means that in the same conditions some subjects might engage in a cyber conflict earlier than others, and some of them might even not notice the conflict aspects.

A cyber conflict as a process has a structure dependant on the adopted criterion, i.e. a spatial, informational, organizational, procedural and technical one.

Spatial structure – it means that particular elements of a conflict can be identified in a given location, in places which have been purposefully chosen and properly prepared to realize activities in the framework of a cyber conflict.

Informational structure – the structure refers to the data and information resources. It is strictly connected with information processes at a time of a conflict. The informational process gathers information for further proceeding which means that the information is obtained in different language or sign systems (e.g. Morse code). Information resources are obtained by different functional teams and analysed in different analytical teams. The informational structure concerns both data as well as information which are a material in the information process.

Procedural structure – the structure entails the procedures of conduct during a conflict.

Organizational structure – the structure entails the parties of a cyber conflict divided functionally and organizationally. There are official and functional relations both between the personnel, as well as between the teams taking part in a conflict.

Technical structure – technical resources e.g. technical (ICT) devices, information carriers, transmission media, software or data bases. A cyber conflict as a process in intangible, i.e. it does not include material resources and consequently it uses technical resources of information systems used in a cyber conflict. The transfer of intelligence data and information between the technical resources creates specific technical relations.

A cyber conflict is determined by twofold factors: primary and secondary. A primary factor is the goal. The goal's realization is the reason for the appearance of a cyber conflict. The secondary factors of a cyber conflict include the resources of the information system used in a cyber conflict. At the same time, a cyber conflict determines the resources of information systems and it depends on them. The goal of the information process exerts influence on the choice of proper sources of information at the time of a conflict. Running a conflict in such a way that it would be beneficial requires proper technical devices, specialized personnel, as well as proper organizational structures and procedures that would assure the effective realization of tasks. Each of the elements has a secondary influence on a cyber conflict. Each factor has impact on a cyber conflict individually and

in connection with others. Synergy effect is observed here. The factors also exert influence on one another. Different factors exert influence on different parameters of a cyber conflict to different extents.

The factors of a cyber conflict are:

- Primary: The goal of a cyber conflict.
- Secondary:
  - the sources of data and information;
  - data and information;
  - the resources of an information system:
    - technical;
    - organizational;
    - procedural.

Conclusion

Taking into consideration the fact that international alliances, coalitions and any multilateral agreements create peculiar organizations, a cyber conflict has a distinctive feature. On the one hand, it is an internal conflict since it takes place inside an alliance or a coalition. On the other hand, from the point of view of the member state, it is an external conflict since it takes place between subjects who care about their own interests.

Cyberspace, in spite of its short history, has already been used to run cyber conflicts, which is vital for the national security. Cyberspace is changing gradually, such progressive change is also observed in the way of perceiving and settling conflicts. Thus, the understanding of the perception of a cyber conflict, the evolution of the way of settling it by a potential adversary or the real enemy is the main manner of counteracting cyber conflicts. Making use of the experiences gained from the course of conflicts in the latest history depicts the implications of the development of the new cognition of the course of a cyber conflict. A cyber conflict might be as destructive as the conflict run with the use of conventional measures and methods.

The article presents theoretical aspects of a cyber conflict. The presented results shall be helpful in counteracting cyber conflicts. The presented analysis showed that knowledge concerning the phases, stages and factors, as well as the structure of a cyber conflict as a process is indispensable and necessary to prevent cyber conflicts. The depicted knowledge will help to understand the way of thinking of the Russian army about the course of a cyber conflict. Due to the lack of scientific grounds for the research problem, the article complements the gap in the field of science concerning the prevention of cyber conflicts, it provides a theoretical basis and inspires for further research on the understanding of the course of cyber conflicts and the way to prevent them.

References

[1] GRAY, C. S.: *The 21st Century Security Environment and the Future of War.* www.hsdl.org/?abstract&did%2520=38291 (Downloaded: 21.11.2017)

[2] AFZALUR RAHIM, M.: *Managing Conflict in Organizations.* Piscataway: Transaction Publishers, 2012.

[3] REVERON, D. S. (ed.): *Cyberspace and National Security: Threats, Opportunities, and Power in a Virtual World.* Washington D.C.: Georgetown University Press, 2012.

[4] *Cyber conflict.* [Online]. www.macmillandictionary.com/dictionary/british/cyber-conflict (Downloaded: 12.06.2018)

[5] GODWIN III, J. B., KULPIN, A., RAUSCHER K. F., YASCHENKO, V.: The Russia–U.S. Bilateral on Cybersecurity. *Critical Terminology Foundations,* 2, (2014). (Policy report.)

[6] KELLO, L.: The Meaning of the Cyber Revolution: Perils to Theory and Statecraft. *International Security,* 38 2 (2013), 7–40. DOI: https://doi.org/10.1162/ISEC_a_00138

[7] PERKOVICH, G., LEVITE, A. E.: *Understanding Cyber Conflict: Fourteen Analogies.* Washington D.C.: Georgetown University Press, 2017.

[8] VALERIANO, B., MANESS, R. C.: The 10 things you need to know about cyberconflict. *The Washington Post* (online), September 11, 2015. www.washingtonpost.com/news/monkey-cage/wp/2015/09/11/the-10-things-you-need-to-know-about-cyberconflict/?nore-direct=on&utm_term=.4421a9d469b5 (Downloaded: 17.03.2017)

[9] Kaukasus-Konflikt tobt auch im Cyberspace. *Vorwärts* (online), 12.08.2008. www.vorwaerts.ch/tag/cyberkonflikt/ (Downloaded: 07.06.2018)

[10] В российской армии может появиться киберкомандование, заявил Рогозин. *Риа Новости* (online), 21.03.2012. https://ria.ru/defense_safety/20120321/601798789.html (Downloaded: 12.02.2018)

[11] Минобороны может создать отдельный род войск по борьбе с киберугрозами, (online) Available: https://ria.ru/defense_safety/20130705/947802340.html

[12] Источник: в России появятся войска для борьбы с киберугрозами, *Риа Новости* (online), 19.08.2013. https://ria.ru/defense_safety/20130819/957318341.html (Downloaded: 03.03.2018)

[13] *Концепция стратегии кибербезопасности российской федерации – проект.* (online) http://council.gov.ru/media/files/41d4b3dfbdb25cea8a73.pdf (Downloaded: 28.03.2018)

[14] *Будущее информационной безопасности: глобальные трансформации и сценарии для России.* Москва: Центр Стратегических Разработок, s.d. (online) www.csr.ru/?s=информ ационной+безопасности (Downloaded: 16.04.2018)

[15] ГЕРАСИМОВ, В.: Новые вызовы требуют переосмысления форм и способов ведения боевых действий. *Военно-Промышленный Курьер,* 8 476 (2013).

[16] *Информация о заключенном контракте.* (online) http://zakupki.gov.ru/epz/contract/printForm/view.html?contractInfoId=19087186 (Downloaded: 16.04.2018)

[17] PONDY, L. R.: Organizational conflict: Concepts and models. *Administrative Science Quarterly,* 12 2 (1967), 296–320. DOI: https://doi.org/10.2307/2391553