International Journal of Engineering & Technology, 7 (4.8) (2018) 741-744

International Journal of Engineering & Technology

Website:www.sciencepubco.com/index.php/IJET

Research paper

Information Wars Concepts in Present Social and Communication Technologies Realities

Ruslan Hula[1], Iryna Perederii[2], Olena Vinrynska[3]*

[1]Kharkiv National Ivan Kozhedub University of Air Force, Ukraine
[2]Poltava National Technical Yri Kondratyuk University, Ukraine
[3]Poltava National Technical Yri Kondratyuk University, Ukraine
**Corresponding author E-mail: vitrynska@gmail.com*

Abstract

Present information wars concepts evolution tendencies in the global information space in the conditions of informational confrontation are revealed. Social and communication technologies functioning peculiarities in the information wars are considered. Information war transformation concepts modern tendencies in military theory are analyzed. Military-applied and psychological approaches interrelation with social and communicational technologies usage is analyzed.

Keywords: *information confrontation, information war, social and communication technology.*

1. Introduction

In XXI century Humanity has finally transformed into a new era characterized by an increase in the volume of information, telecommunication development, information technology improvement, free access to information resources, globalization, modernization and whole society informatization.
Modern civilization processes development takes place within the framework of a fundamentally new philosophical and political postmodern era paradigm. Scientific discourse new objects are code and matrix social phenomena. The information confrontation is radically reoriented. Its task and purpose is to change the nation mentality and national memory patterns deformation, which is determined by information warfare purpose. Based on the theory of "controlled chaos", the latest developments in postmodern military concepts network centric, hybrid, conspiracy, preemptive, network wars, as well as the "strategic communications «concept are grounded. Therefore, information wars evolution study, the process of their origin and development, the forms of manifestation and implementing over-complex socio-political phenomenon methods is extremely relevant.
The article purpose is to reveal information wars modern concepts the essence with the help of the most widespread approaches complex theoretical analysis.
Scientific works in the field of philosophy, political science, state and law general theory, managemen theory, information law and security science V. Horbulina, O. Daniljana, O. Lipkana, Yu. Maksimenko, V. Manilova, O. Manila, N. Nyzhnyk, D. Ovsyannik, V. Ostroukhova, I. Panarina, V. Petryka, G. Pocheptsova, V. Prokofiev, G. Sitnik, O. Skakun, Yu. Starylova, V. Tikhonova, L. Kharchenko, A. Fisuna, D. Frolova, Yu. Shemchuchenka, V.Tsimbalyuk, O. Judin and others became the scientific basis for in-depth study the problems of disclosing informational confrontation and information wars content and essence.
It is also worthwhile to highlight a number of special monographic works of Russian, European and American authors on the issues of information wars, propaganda and special information operations S. Zueva, G. Yemelianova, A. Levakova, S. Rastorgueva, J. Arcville, D. Cul, R. Molander, J. Naya and others.
The article source was also the works of foreign scientists who considered some aspects of the "risk society"idea, W. Beck, K. Dike, M. Douglas, A. Giddens, S. Kirsch, F. Knight, N. Luhmann .
Information war transformation features in the concept of "network-centric", "hybrid", "conspiracy" and "preemptive" wars are disclosed in the works of J. Garstock, D. Alberts, Fr. Stein, A. Sebrovsky, F. Hoffman, Yu. Gromyko, Yu. Krupnov, N. Komlevoy, V. Makarov. National security theory was developed by T. Scheling and G. Kan (theory of international conflicts); R. Liska and G. Snyder (theory of blocks and coalitions); K. Norm (state potential theory); Zb Brzezinski (geostrategic models); E. Lyttwak and M. Porter (international economic competition) and others.
Scientific researches and scientists publications analysis by O. Morozov, V. Lipkan, O. Teterich, N. Kostrich and others indicate robust analytical conclusions regarding information threats content and protection construction system and counteraction to information influence.

2. Problem Search

Conceptual changes in the military doctrines of martial arts different spheres have emerged as a result of two trends domination that emerged in the late 1990s.
The first tendency is related to the growth of the "informational component" of armament and military equipment in the detection, combat management, communications, and intelligence, computer and space systems. It has led to an increase in nuclear and conventional weapons and military equipment efficiency by increasing accuracy, reducing flying time to the target, and improving identifying and tracking goals quality [1].
The second trend emphasizes information and communication systems vulnerability to external, hostile effects, software errors, technical failures, and suggests the importance and significance of

Copyright © 2016 Authors. This is an open access article distributed under the Creative Commons Attribution License, which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

the "human factor" in conducting military operations against hostile information systems.

It should be noted that there is a number of approaches to the wars interpretation new concepts essence. Leading among them is the military-applied and psychological.

2.1. The Military-Applied Institute counts the informational aggression to the sphere of military confrontation and considers it as an integrated information forces and means usage and armed struggle. Information Component is an essential component in the organization and conduct of military operations. First of all, it is the concept of "network-centric", "informational-centered", "knowledge centric", "hybrid" and "pre-emptive" wars.

At present military theorists determine the "network-centric warfare" as the principle of combating the application of the complex-interconnected and interacting platforms (subsystems) used to create a new effective model for managing the processes of collecting, processing and using all kinds of information in the cyberspace to achieve the goals and objectives of a military campaign in the form of a weaponized, but ideally unarmed conflict [2, p. 102].

With concept development, the concept of "network" has become in-tagged systemic and is currently defined as a collection of a single computers set in the space of informational and technical networks and social networks that ensure the functionalization of a military organism in the system of organized contacts and connections between different categories of military servicemen: the military-political decision-makers, chiefs and subordinates, combat units and providing sub-sections, soldiers on the battlefield, taking into account interspecies, institutional and international (coalition) military nature of these "social" networks [3].

The model of "network centric war" is a system consisting of information, sensory and combat platforms (subsystems). Moreover, the information platform (subsystem) is the leading one.

It should be emphasized that the network-centric war is not a new war type, but only proclaims modern principles and approaches to the organization and conduct of hostilities, where the "network" concept as a global information platform (subsystem) becomes the main object of attention. GIG is an interconnected set of information that can be accumulated, stored, distributed and managed to meet the needs of military, economic and political entities [4].

Elements of the sensory platform (subsystem) are «sensory» intelligence, and battle platform components (sub-system) perform destroying the enemy functions by defeat mean. The platforms (subsystems) are united by a single management body. The system of relations between them is complex and multi-variant, but it provides a real opportunity for the effective use of the combat subsystem when receiving information immediately from "sensors", command orders and independently [5, 5].

Characteristic condition for the effective usage and network-centric war basic principles practical implementation is developed democratic society and mechanisms existence citizen participation in political decision-making processes. According to the English expert on information S. Slade, "the possibility of exchanging information, transmitting data and providing free unrestricted flow of information through the network gives people the opportunity to get a tactical picture." As an example of ignoring the principles in the practice of military use, S. Slade uses the experience of Operation Desert Storm (1990-1991): "Countries where frozen flows of information, ideas and data will not be able to use these systems ... The Iraqi system is tree-like, and at the root of it is Saddam Hussein. The rupture of the system in any chain will lead to a catastrophe, especially if the division commander, who is cut off from the root, knows that the reward for his initiative will be a bullet in his head "[6, p. 207-262, 219.].

«Information Centric War» is the principle of conducting hostilities in order to achieve information superiority over the enemy based on set of high-tech information systems for the collection, processing, modeling, visualization of data and support decision-making in real-time [2, p. 109].

The next logical step in information wars theory development was the concept of "knowledge center war", which is now actively developing in the scientific and military-scientific environment. The brilliant scientific prediction of E. Toffler and H. Toffler about the latest military knowledge strategy, the definition of the necessary components of the "knowledge war", the study of a complex system of their interactions and the construction of a "model of knowledge" expands the strategic capabilities of using this perspective direction martial art development [7, with. 207-262].

"Knowledge centric warfare" is the principle of conducting military operations, which, based on a complex information, uses innovative methods of forecasting the development of the military-political situation and the nature of combat operations with the help of "artificial intelligence" and the latest technologies of obtaining knowledge.

The main functional task of "knowledge centric war" is not the transfer of information, but the transfer of knowledge. The essence of this concept is that the complex of operational data, which was previously only available to the command, will be passed on to every soldier of the future in order to ensure the implementation of the principle of decentralization management forces and means. It should be noted that this step, albeit logical, is not obligatory at all. Given the dynamic development of information and communication technologies, the main task of the future «knowledge centric war» wills no longer transfer knowledge to their troops, and the destruction and deformation of the enemy's knowledge system, or the combined implementation of these two tasks [8]. As the scientists rightly point out "it is possible to distribute false information, disinformation, the truth (when it is useful), propaganda and knowledge together with anti-knowledge" [7, p. 221.].

The forms of attempts manifestation to destroy the competitors and opponents knowledge system at the present stage should be considered "brain drain" from the target countries and state intellectual potential destruction and the method used to prevent this situation the creation of conditions that complicate such "m-grace of knowledge".

Table 1: Warfare modern concepts evolutionary development

№	Concepts	Aim	Technologies
1	Network centric war	Creating a new effective management model for the collection, processing and all types information usage in cyberspace	1. Technologies for the management of troops and weapons. 2. Network technologies. 3. Technologies of systems and means of communication.
2	Information and centric war	Informational superiority advantage over the opponent	1. Information technology. 2. Technologies for decision-making. 3. Techniques for modeling and simulation
3.	Knowledge centric warfare	Knowledge transfer, forecasting the development of the military-political situation and conduct hostilities peculiarities	1. Methods of forecasting the combat situation. 2. Technologies of artificial intelligence. 3. The latest technology of knowledge acquisition

Military-applied approach should include the concept of "hybrid war". A hybrid war is a form of armed conflict, which involves traditional means usage of armed struggle, mixed forms of regular and irregular military formations tactical usage under conditions of undeclared military (emergency) status on a limited territory, fighting against the background of the intensification of the information warfare in the global informational space, the economic warfare in the system of world economic and trade integration, the diplomatic war as a means of pressure on the enemy through global international relations institutions to the conflict and "state sponsor" or coalitions of states with geopolitical interests in the region of conflict [9].

It should be noted that "hybrid war" concept development was the result of military theory study and practice that was used during the wars of the past (partisan movement, diplomatic struggle, informational factor, economic blockade, etc.). A unique feature that makes it possible to distinguish this concept in the theory of martial art is the unique coordination and interconnection of all components of the military-state mechanism, dynamics and flexibility in determining the priority forms of influence and pressure, as well as the growth of the significance informational factor that becomes independent. A component that, by the level of destructive potentials on the consciousness of the population and servicemen of the opponent armed force, is no less important than a military factor.

The military factor in the "hybrid war" can be realized by the armed forces within the so-called concept of "three quarters". This type of war, which is typical of modern postmodern, can be defined as "non-trinitarian "; it denies the classical model of fighting: "government – army – population". The founder of this concept should be considered an Israeli polemologist M. Van Krevelda, who in 1991 in the book "Transfiguration of the war. The most radical interpretation of the armed conflict since the time of Clausewitz "revealed its essence through the complex meaning of «modern soldier» functions. This functionary in one quarter must conduct a joint battle, in the second one to perform police tasks, in the third to be the carrier of humanitarian missions. That is, the combat use of regular armed units can be directed at the implementation of aggressive tasks in a complex using the "cover" of a quasi-humanitarian mission (for example, "protecting citizens or people", preventing humanitarian catastrophe, etc.), while simultaneously fulfilling police-specific functions of blocking the political opponents protest. A characteristic feature of this type war is the active use of non-military tactics of illegal armed units criminal and semi-criminal contingent. According to M. Van Krevelda, "in the future of the war will be conducted not by the army, but by the groups whose members we call today terrorists, partisans, bandits," and "the main motivation is not professionalism, but a fanatical, based on ideology and loyalty "[10].

The concept of "preemptive war" is at the crossroads of military-applied and psychological approaches, but the significance of the armed component in the conduct of hostilities makes it possible to enlist it first and foremost in the epidemiological and applied approach. It is also worth emphasizing its steady logical and dialectical connection with the concepts of "network centric" and "hybrid" wars. The concept of the imperial war is an organic synthesized form of fighting modernity based on "network centric" concept development, "conscientious" and "hybrid" wars. The victorious war is a complex form of armed conflict, the components of which are targeted information warfare, the network-centered principle of warfare, the "hybrid" nature of regular and irregular formations usage in order to achieve political goals and the trans-humanitarian transformation of individual and social consciousness, transcoding of national mental traits (national identity) of the defeated people.

The imperial warfare mechanism usage algorithm disclosed in Table 2.

Table 2: Preemptive War Concept

Stages	Aims	Methods	Means
Preparative	Aggression victim choiceї	Creating the image of "paria", "terrorist" state, "fascist" ("nazi") regime	Massive informational impact through mass media and MMC
1	Creation in the society the state-object of the oppositional stratum	Peaceful "democratic" protest actions	Provoking aggravation of national, religious and social contradictions in the world by the world's mass media and MMC
2	The escalation of armed violence, tension and turmoil in the country. Creation of a temporary (opposition) government Створення тимчасового (опозиційного) уряду	Peaceful demonstrations take on the form of an armed clash of the opposition with the authorities. There is a seizure of weapons stockpiles, the neutralization of military and law enforcement units, inter-national conflict-provocations, and illegal armed formations employment (NFF) across the state border	The capture of the national segment mass media and the MMC (or on a limited territory), the establishment of censorial restrictions in favor " people power
3	IAF maximum activation	Combat clashes intensification with regular troops, the destruction of local residents which disloyal to the "rebels", criminalization and marginalization of public life	A large-scale information campaign by the state-aggressor in order to form the world public opinion on the need to change the non democratic" regime
Final	Legitimate government change to "democratic" ("legitimate", "anti-fascist", "public trust")	Direct armed aggression or the "peacekeeping" contingent send-in (in case of failure to reach the final stage goal)	International organizations, world political, spiritual leaders authority usage

2.2. The psychological approach

The psychological approach determines information war essence as psychological influence ways and means system on the individual and mass consciousness in order to direct it in a direction favorable for the subject of influence. The approach includes the concepts of "conspiratorial" war and "strategic communications".

Conspiracy war concept is based on the principles of building a networked society and logically linked to the principles of network-centric and preemptive wars and the theory of "collision of civilizations" by S. Huntington. The essence of the end-point is revealed through the concept content definition of "self-identification of the individual" as the conspiracy war impact main object, that is, through the active information-psychological pressure of the information and communication networks, the given ethno-religious identity of the individual, value orientations, life style , cultural preferences [11]. Consciousness certain types «are displaced" beyond the limits of civil-law norms [12].

In the opinion of the Belarusian researcher V. Makarov, "under the consciental war, in the meanings sphere, one should understand the psychological warfare in a form, a civilized in content and informational means, where the influence object is the demolition or destruction of the intellectual resource of the nation and population universal guidelines destruction[13]. Thus, considering the close connection between human values and culture, one can consider the main object of the culture, history, mentality and identity war destruction as a kind in conscience war. The main purpose of the conspiratorial war is the nation's diaspora, the fragmentation of regional and social-strata communities due to the crisis of existing identities through special mechanisms of influence (Table 3).

Table 2: Individual and collective consciousness "blurring" main ways

№	Aim	Influence mechanisms	Consequences
1.	Neuro cerebral defeat substrate	Chemicals, air pollution, radioactive influence effects	Brain function effectiveness reducing
2.	Information and communication environment organization reducing	Information and communication environment disbalance, disintegration, primitivization	Consciousness disorientation
3.	Desired forms of thinking intrusion	Influence through the practice of occultism	consciousness Neutralization (paralysis)
4.	Attacks Intensification on consciousness	Necessary images and texts communication channels special dissemination	Consciousness destruction
5.	Identity forms destruction relative to fixed communities	All forms and mechanisms influence complex effect	Self-determination and depersonalization changing forms

During wars of the XXI century NATO armed forces, especially the United States, are paying a lot of attention to the role of "non-lethal weapons" and related technologies, primarily information weapons and psycho-propaganda operations that significantly change the nature of the land, air and navy forces in battle ground military operations and the geopolitical and civilizational confrontation of the multi polar world main centers. In September 2006, US Secretary of Defense D. Rumsfeld launched the Strategic Communications (SC) concept, which supplemented the preliminary concept of information warfare as "informational operations of indirect action" concept.

Information warfare in the form of "strategic communications" is a set of purposeful influence measures on military-political leadership, social and political movements and forces, international organizations (so-called target audience), government organizations through information campaigns, economic and humanitarian aid to create an ideal image of the United States in order to persuade or coerce the target audience to adopt decisions and actions that ensure the national interests of the United States.

Basic concepts implementation principles are:

- professional centralized management is the existence of a unified system for managing forces and means of "strategic communications" based on goals, specifics and tasks clear understanding;
- purposefulness is subordination of military operation goals and objectives;
- coordination is strategic definition of all components of civil and military information-communication structures concrete actions in the operation;
- efficiency is information warfare forces and means ability to high activity and rapid response to events, the right choice of target audience, time and place of shares, using the given amount and information direction in due time;
- continuity is constant systematic impact on the target audience;
- authenticity is declarative statement of "right-divination" of information in the interests of target audience gaining trust;
- persuasion is persuasion and suggestion all forms and methods complex application;
- efficiency is complex traditional methods of influence with target audience, operational situational correction of actions with maximum coverage [14, p. 26].

3. Conclusions

The concepts peculiarities analysis present information wars gives grounds to acknowledge that their trans humanitarian character is common in all approaches of interpretation. The ultimate goal of information wars all types is the radical change in the mental code of man, society, nation, the deprivation of its traditional ideological constants, the deformation of ethical and cultural foundations, the leveling of national identity in order to inculcate a colonial, adaptive ideology.

States struggle in the information space is carried out for many centuries by the zones of political and economic influence, sources of resources, markets and territories both in the international arena and within each state, first of all for power, property and political influence, for the opportunity to manipulate mind attitude and behavior of large population masses. And the highest form of this confrontation is the information warfare, which at the present stage is dynamically transformed into qualitatively new forms of complex psychological knowledge, innovative technologies and ideological changes effective application.

References

[1] Kharchenko V., Ponochovnyi Y., Abdulmunem AS.M.Q., Andrashov A. (2018) Availability Models and Maintenance Strategies for Smart Building Automation Systems Considering Attacks on Component Vulnerabilities. In: Zamojski W., Mazurkiewicz J., Sugier J., Walkowiak T., Kacprzyk J. (eds) Advances in Dependability Engineering of Complex Systems. DepCoS-RELCOMEX 2017. *Advances in Intelligent Systems and Computing*, vol 582. Springer, Cham. https://doi.org/10.1007/978-3-319-59415-6_18

[2] Tkachuk P.P., Gula R.V., Sivak O.I., Shurko O.M., Shemchuk V.V., "*Informacijna vijna i nacionalna bezpeka*", Lviv, ASV, 2015, pp. 265.

[3] Hutchins S.G., Kleinman D.L., Hocevar S.P., Kemple W.G. and Porter G.R., "Enablers of Self-synchronization for Network-Centric Operations: Designof a Complex Command and Control Experiment", *Proceedings of the 6 the international command and control research and technology symposium*, 2001, available online: http://www.dtic.mil/cgi-bin/ GetTRDoc?AD, last visit:28.09.2018.

[4] Alberts D.S., Garstka J.J., Stein F.P., *Network Centric Warfare: Developing and Leveraging Information Superiority*, CCRP Publication Series, 2000, 334 p.

[5] Garstka J., "Network-centric warfare offers warfighting advantage: Datalinks are the new weapon of the information age". *Signal*, pp.57–60, May 2003.

[6] Popov I., "Setecentricheskaya vojna. Gotova li k nej Rossiya?" *Krasnaya zvezda*, 2012, available online: http://archive.redstar.ru/index.php/2011-07-25-15-56-32/item/4659-setetsentricheskaya-voyna, last visit:13.09.2018.

[7] Toffler E., *Vojna i antivojna. Chto takoe vojna i kak s nej borotsya. Kak vyzhit na rassvete XXI veka*, Moscow, Ast: Tranzitkniga, 2005, 412 p.

[8] Burenok V.M., Kurs – na setecentricheskuyu sistemu vooruzheniya, *Krasnaya Svesda*, No. 5(48), 2009, pp. 6-13,2009.

[9] Kharchenko V., Ponochovnyi Y., Boyarchuk A., Gorbenko A. (2015) Secure Hybrid Clouds: Analysis of Configurations Energy Efficiency. In: Zamojski W., Mazurkiewicz J., Sugier J., Walkowiak T., Kacprzyk J. (eds) Theory and Engineering of Complex Systems and Dependability. DepCoS-RELCOMEX 2015. *Advances in Intelligent Systems and Computing*, vol 365. Springer, Cham https://doi.org/10.1007/978-3-319-19216-1_19

[10] Van Creveld M., *The Transformation of War: The Most Radical Reinterpretation of Armed Conflict Since Clausewitz*, NY, Free Press, 1991, 272 p.

[11] Gromyko Yu. Konscyentalnoe oruzhye i konscyentanye vojny, available online:https://gtmarket.ru/library/articles/782, last visit:13.09.2018.

[12] Gromyko Yu. (1997), Oruzhie, porazhayushee soznanie, – chto eto takoe? *Komu budet prinadlezhat konscientalnoe oruzhie v XXI veke?* Moscow, Rossiya 2010, pp. 7-8.

[13] Makarov V. (2011), Vojna v sfere smyslov, *Referativnyj zhurnal sociokulturnogo i politicheskogo analiza*, Vol. 1, pp.40-46. 2011.

[14] Olevskij V., «Koncepciya «strategicheskoj propagandy» NATO», *Zarubezhnoe voennoe obozrenie*, No 10, 2014, pp. 19–28.