HYBRID WAR SPHERES AND TECHNOLOGIES

Giorgi Kokhreidze
LEPL David Agmashenebeli National Defence Academy of Georgia, Georgian Technical University

ჰიბრიდული ომების ტექნოლოგიები და სფეროები

გიორგი კოხრეიძე
ეროვნული თავდაცვის აკადემიის უფროსი მასწავლებელი

რეზიუმე

სტატიაში განხილულია ჰიბრიდული ომების ტექნოლოგიები, მისი შემადგენელი კომპონენტების თავისებურებანი და მათგან მომდინარე საშიშროებების საწინააღმდეგო ქმედებები. სტატია შედგება: შესავლისაგან, ხუთი თავისაგან და დასკვნისაგან. შესავალში განხილულლია თანამედროვეობის და მომავლის საბრძოლო ხელოვნებისა და საომარი მოქმედებების განვითარების მთავარი მიმართულებები. წარმოდგენილია ჰიბრიდული კონფლიქტების თანამედროვე მაღალტექნოლოგიური საშუალებენი. თანამედროვე სტრატეგიების და საბრძოლო ხელოვნების გათვალისწინებით გაანალიზებულია ჰიბრიდული ომის თავისებურებები. განხილულია თანამედროვე ჰიბრიდული ომების შემადგენელი მაღალტექნოლოგიური ელემენტები, ჰიბრიდული კონფლიქტების ინფორმაციულ-ფსიქოლოგიური და კიბერნეტიკული ასპექტები.

სტატიაში წარმოდგენილია კრიზისული სიტუაციების წარმოშობის, მათი პირვანდელი სიმპტომების არმოჩენის და სპეციალური ძალების მიერ მათი აღკვეთის თავისებურებანი. გაანალიზებულია ჰიბრიდული ომების მიმართულების სფეროები. განხილულია სახელმწიფოს მიერ ჰიბრიდული საფრთხეების პრევენციისთვის გასატარებელი სამუშაოები.

საძიებო სიტყვები: ჰიბრიდული ომი, ინფორმაციული და კიებერ უსაფრთხოება, მაღალტექნოლიგიური.

RESUME

The article analyses hybrid war components, technologies and countermeasures to hybrid threats. The article consists of introduction, five chapters and conclusions. The main tendencies of present and future military art and combat actions development are discussed in the introduction. Modern highly technological means (measures) of hybrid conflicts are represented in the article. It is conducted the analysis of main hybrid war peculiarities in the framework of new strategies and concepts of military art. Highly technological hybrid war components, information, psychological and cyber aspects of hybrid conflicts are considered. The article displays crisis situation formation, detection of its consequences by Special Operations. It is conducted the analysis of hybrid war spheres. State training peculiarities to hybrid threat countermeasures are represented in the article.

Key words: Hybrid War, Information and Cyber Security, high technologies.

* * * *

ABSTRACT

Geopolitical and geostrategic analysis identifies new tendencies in the world. The tools for their formation were not phenomena in the art and philosophy of war. The basis for phenomena birth became achievements of high technologies, modified, transformed existing and totally new methods, forms, and measures of conflict objectives achievement.

INTRODUCTION

The analysis of the ways of ensuring the state national security in conditions of hybrid threats reflected the use of two main components by the majority of countries with the purpose of timely response to present and future hybrid challenges and threats and their prevention, deterrence, neutralization. The main components are

Deterrence potential, which consists of traditional branches of armed forces (ground forces, air forces and navy);

Conducting new type wars potential (new type army components), the basis of which are Special Operations forces and measures, Information Psychological Operation and Electronic Warfare, and also Cyber Forces (Cyber Intelligence, Security, Countermeasures), branches of Intelligence (Technical Intelligence, Military and Special Intelligence, OSINT), Operation Control of communication, units, which are equipped with robotic (unmanned) complexes, countermeasures and other highly technological forces and measures [3].

Technological progress has always been a driving force for war art development. It led nowadays to transformation from war philosophy notions to more pragmatic categories, which helps to identify new tendencies of such complex phenomena evolution as armed combat actions. That`s why leading experts and researches reflecting the essence of present and future combat actions talk discuss Highly Technological Wars, Military Conflicts and Combat Actions. [4].

Actually, it is a regular transformation of basic principle of objective achievement. It turns into the principle of political, information-economic-force countermeasures.

The new thing is Highly Technological War Generation, which is connected with design and mass use of highly technological measures, systems and complexes, which are designed by the most developed countries. The achievements give them military technical and strategic advantages during combat actions without use of significant force groupings [4].

INNOVATIVE TECHNOLOGIES IN HYBRID WARS AND COMBAT ACTIONS

Samples of weapons and military equipment gained new opportunities with the help of innovative technologies. It led to development, implementation and practical use in leading countries of the world of new strategic concepts of combat actions ("Global Combat Action", "Global Presence", "Global Coverage", "Network Wars", "Hybrid Wars", "Strategic Paralysis", "Parallel Wars", "Controlled Wars" etc.).

All the concepts consider combat influence on possible enemies in a distance with the use of covering information intelligence software, information and highly technological weapons, robotic (unmanned aircraft complexes, unmanned ground and navy complexes).

Innovative technologies of combat actions control consider that attacks usually are done mainly on principal objects with the support of maximum achievable speed and accuracy of actions on critical components, mainly on all the territory of the state (region). The approaches realization provides effective objective achievement. It is supported by analysis of National Security Support Systems of leading states of the world. The analysis reflected the weakest points (subsystems, components, objects), which were named "weak points", "sensible spots", "critical points". Influence on them may destroy the system or in an unauthorized way change its characteristics and algorithms of functioning. Disorder in functioning or any other destructive influence on them deprives the state, which did not take security measures, the opportunity to conduct combat actions further [4].

Practically, support of defense capacity of a state demands in conditions of hybrid wars balanced national security and defense sector. Its key components are modern, resisting to present and future challenges and threats, armed forces, equipped with highly technological samples of weapons and military equipment. Also there is a necessity in relevant specialist services, staffed with trained personnel. The personnel should be able to conduct powerful information and special operations with the purpose of influence on economy, politics, energetic infocommunications, control, native and enemy population.

HYBRID WARS MILITARY COMPONENT

The peculiarities of the military components of highly technological (hybrid) wars are

• transfer from weapon and forces control to armed combat actions control, the basis of it is constant realization in near real time and stealing a march of processes: intelligence, decision making and realization, influence (defeat) [5];

• transfer from the basic load of actions (armed combat actions) into information cyber space and airspace;

• robotization of armed combat actions measures, withdrawal of a person from combat field, conducting combat actions in a distance;

• formation and use of reconnaissance/strike system and complexes;

• mass use of effective non-lethal weapon;

• increase of irregular troop formations quantity and its influence on the results of combat actions;

• increase of asymmetry in the character of combat actions;

• increased role and developed use of Special Forces;

• early and constant information psychological influence and constant maintenance of information and cyber actions;

• transfer to adaptive forms and methods of actions on the enemy in all spheres [9].

Mainly influences on critical objects and processes in a state are conducted in a distance with the asymmetry in actions, used forces and measures, scope of consequences and results. In hybrid conflicts the objective achievement starts with (and further followed by) soft power: economic, political, diplomatic, information (information psychological, information, cyber), demonstrative measures of military deterrence etc. However, in hybrid conflict of any kind of intensity combat actions are component of mutually correlated in common plan and thought of other (soft) actions, which prevail on all their stages (early, acute phase and solution). It creates destabilizing internal and external processes, which are the object of aggression (destabilization of economy, formation of fears and frustration among population, exacerbation of the conflict-protest potential in society or its separate groups, creating conditions for controlled migration processes, public protests etc.). Later power methods of conducting combat actions are used with involvement of intelligence forces and measures, Special Operation Forces, Operational Control of forces and measures, traditional and innovative measures of conducting war, state armed formations and also conflict participants, who represent non-governmental sector (terrorists, criminals, radical armed groups, private military campaigns, resistance movements, contractors, gorillas) etc.

Hybrid wars differ from classical wars in early stages, way of conducting, involved forces, measures and forms of actions. It is necessary to mention that irregular formations play the main role in hybrid wars, especially on early stages,. The protest potential of separate layers of native population is widely used. Regular armed forces participation in a conflict has mainly hidden nature. It is conducted mainly by Special Operation Forces, sabotage-reconnais-

sance groups, units of different branches of intelligence [11], widely using non-governmental military formations.

MODERN HIGHLY TECHNOLOGICAL HYBRID CONFLICTS MEASURES

In modern war success is defined by availability and effective use of innovative designs of weapons and military equipment, highly technological samples:

- Electronic Warfare systems ad complexes and other technical types of intelligence;
- Modern Information Communication Systems;
- Innovative Control Complexes of forces and means (measures), Automatic Weapon Control Systems;
- Innovative, including Automatic Program Complexes for conducting information, information and cyber actions and actions in cyber space;
- Integrated reconnaissance-strike complexes;
- Life Support Systems in space;
- Robotic systems of all types (mainly unmanned aviation complexes) and their countermeasures. (Figure.1) [18]

Electronic Warfare
- automated intelligence systems "Armada", *"Areal", Automated Control Complex (ACC)-ПОМ1 (eng.POM1), Automated Control Complex -Д13Р(eng.D13R);* *-stationary moniring АРК-ССИ (eng. automated control complex), АРК-ССИНМ,* АРК-СП, «Аргамак-ЦС»(eng."Argamak CS"), 5В65-VSAT *-mobile electronic warfare means* "Oasis-T", "Mercury-S", "Torn-MV", "Grebeshok-M1", "Argus-M2", "Dozor", АСС-ПОМ2 (eng.POM2), "Argument-E", "Argument-P" , "Articul-M";
Electronic Warfare Countermeasures
Ground-Based *-Electronic Warfare Complexes* "Borisoglebsk-2", "Diabazol"; - Automated complexes and automated control points "Moscow-1", Automated Control Complex-1, Р-330К, Р-330КМА, Р-330КМБ); *-jamming stations, airborn stations* 1РЛ296/РБ-261А "Krasuha-2", 1РЛ257/РБ-271А "Krasuha-4С, "Topol-M", СПН-40М2, СПН-30, СПН-2, СПН-4, СПН-4.02; *-jamming stations (short-wave communication, ultra-short-wave communication)* Р-378А, Р-378Б, Р-325У, Р-330Б, Р-330Т, Р-934Б, Р-934УМ, Р-330Ж, Р-330БМВ, Р-325УМВ, РБ-531Б "Infauna", МКТК-1А "Judoist", "Leer-2", РП-377УВМ1Л "Lesochek", РП-377УВМ2, РП-377Л, РП-377ЛА "Lorandit-M"; *Air-Based* *-Electronic Warfare complexes and stations* (electronic countermeasures, aviation individual and group protection): Л175В, "Kedr", "Omul", "Gardenia 1FUE", "Vitebsk", "Porubshik", "Hibiny", "Himalayas", "President-C", Л005-С; *- jamming helicopters* Ми-8 (Ми-17); *-Drone Jammers* "Stroy-PM", "Moshkarec" and "Moshkara"; *-Small Jamming Station* МСП-418К; *-electro-optical warfare system* "Zashita-EK" (eng. Protection-EK), «АДРОС-КТ-01АВЕ» (eng. "ADROS-KT-01AVE"); *Sea-Based* -Complexes and systems of electronic warfare, signal environments, setting deceptive targets, jamming ТК-25Е, МП-401С, МС, МП-405, РЕП МП-407, ПК-2, ПК-10, ПК-1, "Podzagolovok -23" (eng. subheading); - self-contained, drifting and hauled devices of sonar countermeasures МГ-74МЕ, "Berilliy-E", "Tunec" (eng.tuna), "Sprut", "Zmey" (eng.snake)
Technical Means of Information and Psychological Operation Forces
Technical Means of Oral Speech *-powerful audio-lingual station МЗС-83 "Grom" (eng.thunderstorm);* *-medium-powered audio-lingual stations ЗС-82 "Decorator";* *- medium-powered audio-lingual stations ЗС-96.03;* *- lightweight audio-lingual stations ОЗС-78 "Komar";* *- audio-lingual stations ВЗС-85 "Mnogoslozhnost";* Systems of information automation, reception and processing *-portable reception point* И2-80; *-portable complex* ПСК-84; *polygraphic means, technical means of radio and TV-propaganda.*
Means of Space and Missile Defense Forces
Space Apparatus - electro-optical intelligence "Persona-2"(eng. person), radio-locating «Kondor», radio-electronic «Lotos-C», «Celina»; *- communication* «Meridian», «Raduga-1M», «Raduga 2»; *- navigation* «Glonas-M», «Glonas-K»; - double designation «Resource-P1», «Resource -П2», «Kanopus-B», « Resource DK-1»; *Missile Carriers* *- light* «Start-1», «Cosmos-3M», «Cyclon-2», «Cyclon-3»; *- middle* «Soyuz-B», «Zenit».

Robotic (Unmanned Aircraft) Vehicles
Umanned Aircraft Vehicles «Orlan» «Forpost», «Tahion», «Tipchak», «Aleron», «ZALA», «Irkut», «Dozor», «Granat», «Zastava» [18-21]

Operational control complexes and automated control systems of weapon are becoming system-forming in modern combat actions. During Anti-Terrorist Operation (ATO) in Ukraine Armed Forces of the country came across with militias, which quickly adapt to changes and dynamics of modern combat and widely used conventional and asymmetric tactics. It turned out, ATO authorities were not sufficiently prepared to the actions at that moment. It resulted in absence of reliable control over the situation, and it decreased efficiency of troops command and control. Mainly insufficient response coordination of military groups and groups of National Guard of Ukraine, State Border Guard Service of Ukraine and Security Service of Ukraine led to significant loss of human and territorial resources [6].

Experience of the latest military conflicts confirms that it is not enough to have troops automated control system. There should be common automated control system of troops, which provides cooperation of integrated task forces. It should also provide operational command and control of module structures of two and more branches of armed forces. Due to the necessity of control over the formations from one command post and integration of corresponding, cooperating subsystems in unique system there is a demand in common information processing and use in conditions of combat actions. It means following the same rules of information transfer, its processing, storing and visualization in single information space (SIS). [17].

The mentioned conditions confirm the necessity of new method design for automated control from small in quantity mobile units in multi-service forces, well-armed and prepared to execute different tasks separately from main forces (force groupings).

It is a reason for constant work over design and development of the complexes and systems by leading countries of the world. The most significate design of automated control system is USA strategic concept– C4I «Command, Control, Communications, Computers and Intelligence». The automated control system is represented by troops of operational strategic level, Global Command and Control System (GCCS). The basis of C4I information infrastructure is an information system unity of operational strategic, operational tactic and tactic levels of control, which are interconnected vertically and horizontally [9].

From technical point of view C4I is a global, territory distributed, integrated tele-

communication system of information computer centers and automated working stations, placed at command points of headquarters and armed forces operation control points, functioning according to single information space concept.

Russian Federation follows the same trend. In Russian 2025 Year Development System Concept of Armed Forces Control one of the main goals is guaranteed forces control in SIS. According to the concept there is a number of planned national arrangements: conceptual basis design with armed forces application and use of SIS; design of integrated transport net, united with computer automated communication system of armed forces; information telecommunication system of armed forces, information protection system; integration of all information resources in single information infrastructure of armed forces; creation of perspective research center in the sphere of information technologies and their use for development and design of means for combat actions. All aspects are represented in ASUP 2.0 (АСУП 2.0) project.

It is necessary to underline achievements of Poland in this sphere. Poland designed its own automated control system JASMINE. JASMINE system is universal information telecommunication platform based on component (module) construction according to the concept of NATO Network Enabled Capabilities (NNEC). Elements of JASMINE system can be used at any military level from strategic to tactic.

The conducted analysis shows the achievements of leading countries of the world in troops automated control system design. It promotes the efficiency and quality control, significant decrease of time necessary for decision making and creation of conditions for efficient use of combat capabilities, success achievement in combat actions including decrease of forces and facilities [2]. Table 1 represent main troops automated control systems of leading countries of the world. According to Table 1 the main focus is on the design of automated control systems for troops of strategic and operational levels of military authorities.

Nowadays in Ukraine Armed Forces there are automated control systems of troops of tactical level ("Combat", "Krapiva", "Vual-15" and others).

INFORMATION, PSYCHOLOGICAL AND CYBER ASPECTS OF HYBRID CONFLICTS

One of the distinctive features of the "hybrid war" in Ukraine is how much it has occupied all aspects of social life, how wide-ranging, multidimensional and employment of multifactorial information focused on both psychological and cyber sources.

Destructive information and psychological effect on the population of the country and its authorities (discrediting government authorities, Ukrainian Armed Forces authorities, and encouraging an increase in crime and separatism activities) at the beginning of the conflict fostered socio-political destabilization in the country and continues to negatively affect the country. Successfully planned and conducted according common idea with the use of innovative technologies of action led to Crimea annexation and drawing Ukraine into long military conflict. Along with there is a formation process of conditions in the country for instability zones, maximum exhaustion of country resources, destruction of economy and society.

Comprehensive analysis, researches, analyzed combat experience, methods, forms of today and future countermeasures predicted hybrid effects and threats, showed sig-

Table 1

Troops Automated Control Systems of World Leading Countries

Country	Control Levels			
	Soldier, section	"Platoon-Company-Batallion"	"Brigade-Devision"	Automated Complexes, branch of forces
Germany	Idz-Es "Gladius" ("Warrior-21.)	FAUST, IFIS, ADLER-II, SAFES, FUWES	Fulnfosys H, HEROS-2/1, FAUST, IFIS, ADLER-II, Hflaafusys, SAFES	Finfosyssk, Fulnfosys, HEROS-3, HEROS-2/1, ADLER-II, DIFA Hflaafusys, SPIA, IRIS, HERGIS,Syseloka H, Opinfo, RAFES, SAFES
Russian Federation	Sozvezdiye 2M Andromeda-Д ASUV 2.0 (АСУВ 2.0)	Poliot-K Sozvezdiye 2M Andromeda-Д ASUV 2.0 (АСУВ 2.0)	Poliot-K Sozvezdiye 2M Andromeda-Д ASUV 2.0 (АСУВ 2.0)	Andromeda-Д ASUV 2.0 (АСУВ 2.0)
USA	FBCB2	FBCB2 ABCSS, ATCCS, MCS	FBCB2 ABCSS, ATCCS, MCS	GCCS, DISN, ATCCS, ABCSS, AGCCS, ATCCS, MCS

nificant and intense role of information and cyber activities. Along with there is separate specific sphere (environment, through which information effect is realized) cyber space.

The effect through cyber space gives an opportunity along with the realization of already existing threats to create new diverse crisis situations. Mainly it is connected with realization of terrorist threats, destructive effects on critical objects of infrastructure, society, state authority, armed forces personnel, on individuals.

Practice proved that in modern hybrid actions information and cyber effects are dominant, and at the same time can be independent and followed by other soft and force methods of enemy goal achievement. Mainly information effect is realized through cyber space. It combines information, psychological and cyber components with the effect of their mutual synergy. Information (information, psychological and cyber) effect is followed by intensification of use, rapid self-development, modernization, transformation and adaptation of forms, methods and means of their realization.

Besides crisis situations, which appear as a result of information and cyber actions in conditions of hybrid conflicts. It means unity of conditions and matters, created by realization of information, psychological and cyber threats of terroristic, economic, military, diplomatic, ideological nature. Crisis situations are directed on critical infrastructure of a state, society, its authorities, security sector, technical and ergatic components of control systems (of a state, critical objects, troops, and weapons). Control systems lead to significant decrease of all indicators of mentioned objects and subjects functioning separately and as a unity till final rejection of work.

CRISIS SITUATIONS COUNTERMEASURES

Effective countermeasures to crisis situations in cyber space according to ATO (Ukrainian occupied areas) experience can be realized in

Systematic development of forms, methods and means of operational detecting, protection and active countermeasures to information threats in cyber space;

Scientific research and development of specialized software and hardware capability for information activity in cyber space;

Professional military education and training and combat experience in this sphere;

Conducting applied national and international training, war-gaming and consultations;

Improving training and education of military and civil specialists in the sphere of information and cyber security;

Operational implementation of learned material in national and international security systems.

Experience demonstrates that modern methods of hybrid effects realization are followed by significant flow of changing crisis situations. They are characterized by priori uncertainty according to the goal, subject and object of effect, content, essence and method of realization.

Technological design of well-known countermeasure systems for mentioned crisis situations, forms, methods and use of the systems must be oriented toward the formation of static excessive structure of a target system. Distribution of tasks among all components of cyber attacks on the system are often conducted evenly with a choice of components only according to their purpose. The increase of quantity and density of crisis situations` flow leads to ascend of structural complexity of systems designed to respond to them. It provides information redundancy of data and complication in its transfer and processing. The same principles are the basis for design of software means aimed at realization of operational detecting processes, protection and active countermeasures to information threats in cyber space. The mentioned approaches are not efficient in real conditions of the situation during enemy`s use of predominant or equal in content and level of information effects development and conducting massive information and cyber attacks, which are followed by other soft and force methods of conflict objectives achievement. This is peculiar for present hybrid wars.

Principles of situational control implementation give opportunities for rational distribution and redistribution of personal resources. The focus is on on critical (for providing security) directions of enemy`s actions. Methods of fractal analysis, self-organization and bifurcated models give an opportunity to detect threats and critical situations in time, predict their direction development and real objectives. Practically, this approach increases the effectiveness of information warfare countermeasures as a result of advance warning systems, the completeness and accuracy of information, and timeliness of reactions.

HYBRID WAR SPHERES

It is necessary to consider the impacts of an aggressor desiring to increase internal instability in multiple spheres of activity (Fig. 2). Intended impacts can include increasing distrust of institutions and shared values, increase of crime, erosion of economic activity and trust, and a confusion of objectivity, expertise, ideology, and other sources of social cohesion, destruction of national security and defense [1, 7, 12].

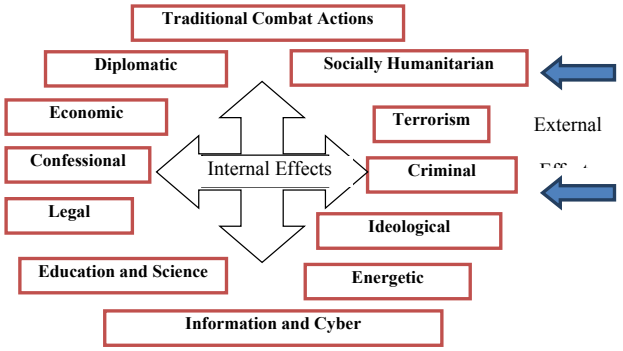

Figure. 2 Hybrid War Spheres

THE HIGHLY TECHNOLOGICAL DEFENSE CLUSTER

The mentioned above spheres providing defense capacity of a state support technical component of military security of a state. But effective use of highly technological samples of weaponry without well-trained personnel is next to impossible. Exploitation of expensive highly technological complexes of weapons and military equipment by personnel, which does not have special training, exclude the possibility of its effective use (fully use its capacity). Moreover, due to unprofessional use the complexes very often are out of order. It means that tasks are not executed and the state suffers damages. That`s why the important role in providing military state security plays personnel training.

Due to this fact Highly Technological Cluster design demands great attention as single integrated, training, research structure in highly technological, priori for providing necessary level of state defense capacity.

The Highly Technological Defense Cluster should include:

- A robust system of military research with proper scientific organizational structure;
- Academic orientation toward highly technological expertise;
- Scientifically-based manufacturing complex, with stationary and mobile samples of weaponry and military equipment, command posts and laboratories;
- Technologically advanced experimental combat and combat units, developed according to academic/scientific research of the cluster (Figure 3).

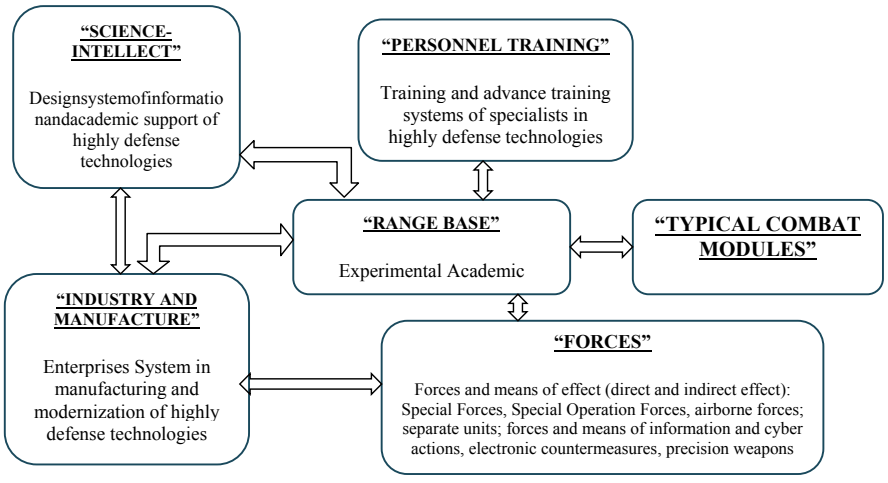

Figure. 3 The Highly Technological Defense Cluster

Practical military personnel training, testing and implementation of new technological systems of weaponry and military equipment, and the formation of new units must be based on developments of the Highly Technological Defense Cluster and active military units.

Cooperation in training, research and innovations issues is conducted with scientific establishments of the state and of other world leading countries, with companies and firms of different types of subordination and ownership.

It is crucially important to create a Military Scientific Technical Expert Center in highly technological spheres with a purpose of

avoiding of different organizations` double functioning;

efforts concentration on one place in researches, design, creation, testing and use of highly technological systems;

personnel training in highly technological directions for all branches of Armed Forces and for other ministries and establishments of National Security and Defense Sector of the state;

use of the military component, industrious and manufacturing base of the region;

avoiding additional financial and temporary expenses.

Practicability of the center can be substantiated and supported by relying on experience of leading countries of the world gathered in the search of innovative ideas and their implementation in the military sphere (e.g. DARPA – Defense Advanced Research Projects Agency (USA)).

Rational elaboration of all practical issues in the Highly Technological Defense Cluster must be conducted in close coordination with central military command and control organizations. It should work directly with forces cooperating with central control authorities. Central control authorities correspond with military units, and subdivisions with their range base and interacting organizations (structures).

CONCLUSIONS

In modern hybrid conflicts the goals of aggression are achieved by complex realization of special operations, coordinated economic, political, diplomatic, information, psychological, cyber and directly military actions with comprehensive use of highly technological forms, methods and means of their conduct.

State policy, providing highly technological, information and cyber security, becomes one of the main components of state security policy in military sphere, which obtains more and more independent status.

Modern high technologies are changing processes of effect on the enemy, organizations of soft power effect and military actions, methods of their control. And that`s why they demand specific personnel training.

World experience proves that to provide necessary level of state defense and security capacity in conditions of world economic crisis and significant decrease of expanses

on armed forces is possible on the basis of complex use and new highly technological and already existing traditional facilities.

Military conflicts of last decades prove that in modern war wins the one, who faster comprehend new technologies and contributes them to life, takes on new military doctrines and concepts, which are relevant. And finally, whose commanders not only use new technologies and ideas themselves, but also know which of them, when and how enemy can use.

The use of highly technological systems gives the opportunity with minimal expanses not less than at third to increase efficiency use of already existing state military potential. That`s why corresponding to demands of providing state security in military sphere in modern conditions, guided by items of national security strategies and national military strategies, authorities of the most developed countries order science and industry high-tech weapons of war, implement and use innovative control technologies, which provide fast, convincing victory in the present and future military conflicts.

LITERATURE:

1. Герасимов В. Ценность науки в предвидении / В. Герасимов // Военно-промышленный курьер. - 2013. - 27 февраля - 5 марта (№8(476)). - С. 1-3.

2. Даник Ю. Г. Военные аспекты классификации высокотехнологических систем / Ю. Г. Даник, Д. А. Іщенко, О. В. Манько // Проблемы создания, испытание, применение и эксплуатации информационных систем : зб. наук. работ. - Житомир : ЖВІ НАУ, 2013. - Вип. 8. - С. 5-13.

3. Даник Ю. Г. Особенности обеспечения национальной безопасности в высокотехнологическом обществе / Ю. Г. Даник, О. О. Труш // Государственное строительство. – 2010. – № 1. – Режим доступа : http://nbuv.gov.ua/UJRN/DeBu_2010_1_42.

4. Донбасс и Крым : цена возвращения : монография / за заг. ред. В. П. Горбулина, О. С. Власюка, Э. М. Лібанової, О. М. Ляшенко. - К. : НІСД, 2015. - 474 с.

5. Джозеф Н. Мягкая сила. Составу успеха в мировой политике / Пусть Джозеф С. // − Нью-Йорк: Паблік афферз, 2004, 192 с.

6. Руснак І. С. Воєнна безпека України у світлі реформування сектора безпеки і оборони / І. С. Руснак // Наука і оборона. – 2015. – № 2. – С. 9–14.].

7. Телелим В. М. Планирование сил для выполнения боевых задач в «гибридной войне» / В. М. Телелим, Д. П. Музиченко, Ю. В. Пунда // Наука и оборона. - 2014. - №3. - С. 30-35.

8. Телелим В. М. Военное образование в системе обороноспособности государства: проблемы, мировые и национальные тенденции развития / В. М. Телелим, Ю. И. Приходько // Військова освіта. – 2013. – № 2. – С. 3-19.

9. Crocker C. A. Leashing the dogs of war: Conflict Management in a Divided World / C. A. Crocker, F. O. Hampson, P .R. Aall // – US Institute of Peace Press, 2007. –726 p.

10. Nossel S. Smart Power / S. Nossel // Foreign Affairs. - 2004. - 83 (2). - Г. 131 - 142.

Указ Президента Украины № 287/2015 «О решении Рады национальной безопасности и обороны Украины от 6 мая 2015 года “О Стратегии национальной безопасности Украины”» [Электронный ресурс]. – Режим доступа: http://zakon5.rada.gov.ua/laws/show/287/2015.

Kofman M. Russian hybrid warfare and other dark arts [Электронный ресурс] / M. Kofman. - Режим доступа http: // warontherocks.com/2016/03/russian-hybrid-warfare-and-other-dark-arts/.

Miller G. CIA plans major reorganization and a focus on digital espionage [Электронный ресурс] / G. Miller – Режим доступа: //https://www.washingtonpost.com/world/national-security/cia-plans-major- reorganization-and-a-focus-on-digital-espionage/2015/03/06/87e-94a1e-c2aa-11e4-9ec2-b418f57a4a99_story.html

Густерин П. Где готовят американских разведчиков [Электронный ресурс] / П. Густерин. – Режим доступа : http://topwar.ru/57485-gde-gotovyat-amerikanskih-razvedchikov.html.

Тинченко Я. Где взять новых командиров [Электронный ресурс] / Я. Тинченко. – Режим доступа : http://tyzhden.ua/Society/155279.

11. Сайт Российской военной техники [Электронный ресурс]. – Режим доступа : http://www.rusarmy.com.

12. Информационное агентство «Оружие России» [Электронный ресурс]. – Режим доступа : http://www.arms-expo.ru.

13. Сайт «Информационное сопротивление» [Электронный ресурс]. – Режим доступа: http://sprotyv.info/ru/news/kiev/rossiyskie-sredstva-reb-v-nachalnoy-faze-agressii-protiv-ukrainy-analitika

14. Сайт «ИНОtv» [Электронный ресурс]. – Режим доступа: https://russian.rt.com/inotv/2016-10-03/DO-Gospodstvo-Rossii-v-vozduhe

15. Сайт «IPNEWS», “National Interest: Оружие, с помощью которого РФ надеется подчинить Украину” [Электронный ресурс]. – Режим доступа: http://www.ipnews.in.ua/news/world/112840-national-interest-oruzhie-s-pomoshchyu-kotorogo-rf-nadeetsya-podchinit-ukrainu

16. Сайт «Україна» [Электронный ресурс]. – Режим доступа: http://ukrainian.voanews.com/a/bezpilontnyky-ato-ukraina-ameryka-rosiya/3457268.html