# SPECIAL OPERATIONS FOR DISRUPTION OF STATE AND MILITARY CONTROL SYSTEM

Prof. Yuriy DANYK, PhD
PhD Serhii HUDZ\*
Korolyov Zhytomyr Military Institute, Ukraine

#### Abstract

The article deals with the essence of special operations for implementation of destructive actions aimed at disruption of state and military control. Basic forms and methods of influence are described. The main ways of detection and response are proposed.

**Key words**: information security, cyber security, information and psychological influence.

#### Introduction

Ensuring the effective functioning of the state (military) control system, committed to the adoption and implementation of political, administrative, economic and other solutions is an extremely important task for any country that cares about protecting its national interests and maintaining the required level of national security and defence. Radical changes in society, achievements in the development and implementation of various strategies of destructive influence

<sup>\*</sup> Yuriy Danyk, doctor of Engineering, professor, The Head of the S. Korolyov Zhytomyr Military Institute (Ukraine). Serhii Hudz, PhD, researcher, University teacher S. Korolyov Zhytomyr Military Institute (Ukraine).

on the management systems leads to the need for its comprehensive analysis and developing appropriate strategies for protection.

Intensive destruction of the global order, established in recent decades, has inevitably led to changes in the classical paradigm of international and national security<sup>1</sup>. Today we are witnessing the transformation of the main efforts in confrontations and conflicts into information and cyberspace

In accordance with the experience of leading countries, in modern hybrid wars most efficient and effective operations of Special Forces include influences aimed at the destruction of governance and its defence and security sector. Those operations are focused on discrediting the military and political leadership of the state in the perception of the armed forces, public and international community by various information and cyber actions<sup>2</sup>.

Analysis of the destructive actions which are conducted using special technologies in information and cyberspace revealed an agreed on purpose, concept, place and time and cyber impacts on all layers of the population, social and demographic groups, the leadership of the country, Ukraine's Ministry of Defence o and commanders of the Ukraine Armed Forces.

To achieve this goal, television, linternet resources (information sites, social networks and specialised forums, etc.) are used.

Out of these destructive psychological, informational and cyber actions, the most effective are those that are directed against the leadership of the states and armed forces.

Research showed that, as a rule, such actions are complex and include elements of "indirect influence", reputation manipulation and suggestive influence. Within these system-wide actions are determined leaders, those persons whose influence provides the best achieving of the objective. They further choose methods and forms of influence and conduct information operations.

<sup>1</sup> Welt C. (2010) After the Color Revolutions: Political Change and Democracy Promotion in Eurasia [Electronic resource] / [By ed. C. Welt, A. Schmemann]. – Available from: https://www.gwu.edu/~ieresgwu/assets/docs/PONARS Eurasia After the Color Revolutions.pdf.

**<sup>2</sup>** Danyk Y.G. (2011) The main aspects of cyber security paradigm. – Available from: http://jrnl.nau.edu.ua/index.php/IMV/article/view/3171.

The decisive fact is that it is enough to launch information and, then, given the peculiarities of society, it will produce gossip, conjecture and disseminate information

Thus, special content in the cyber field has been already created, whose activation may, at some point, block the action of any manager and thereby block the actions of the structure led by him, or make its functioning ineffective, or coerce him to work as somebody who conducts the information operations desired. Moreover, such actions are the prerequisites for creating panic, disobedience disorientation, desertion  $etc^3$ .

This article explores the ways some of these special operations aimed at the disruption of the system of state and military control are conducted. Using this information, ways in which to counter it are proposed.

## The concept of "soft power"

One of the most effective strategies to influence the state and military control strategy is the so-called "non-forcible action", "indirect influence" and "soft power", etc., widespread as a strategy of attack, and a defence strategy as well<sup>4</sup>.

The effectiveness of those actions is caused by the fact that, in artificial systems (state or society), weak or mostly subtle effects on some vulnerable "critical" point of these systems over time may lead to mistakes in its operation. This fact could ultimately lead to a crisis or allow external control, resulting in harmful effects for state institutions to which such impacts are implemented.

The results of such crises in politics and the economy occurred in many countries over the past decades and can be considered as evidence of the introduction

<sup>3</sup> Hovorukha V.V., Danyk Y.G. (2008). The impact factors of motivating and demotivating the efficiency of public administration in national security and defence. State building, (2).

<sup>4</sup> Nye J. (2003). The Power of Persuasion: Dual components of US leadership. The conversation with J. Nye. – Harvard International Review, Winter.

and development of new forms of implementation of these strategies, as well as whether they were effective or not<sup>5</sup>.

It should be noted that this approach is not only officially accepted but, as a rule, is regulatory and defined in many countries of the world. The main areas of influence are: organisational principles of the country, its resources and logistical capabilities.

It should be noted that the provisions that form the theoretical basis for "non-force actions" strategies, which have become a worldwide practice nowadays, were known in the ancient world. As early as the 5th century BC, the famous Chinese philosopher Sun Tzu, in his treatise "On the art of war", wrote<sup>6</sup>: "The art of war is to destroy the enemy within. Anyone who wages war skilfully shall conquer an alien army without fighting, capture an alien fortress without siege, and destroy another state without protracted campaigns. A hundred battles and victories are not the best of the best. The best of the best is to conquer a foreign army without battle".

Even in ancient times, experienced government and military leaders sought to achieve victory over the opponent state by disorganising the management of its army during peacetime, and through it trying to get victory before the decisive battle.

In modern terms, this principle has become common and widespread in all areas of human activity. Many authors agree at this point. British scientist, J. Sherr, said: "Accents began - and should - shift from the identification of threats to identification of vulnerabilities that can be used to undermine the state from within, destroy connections between the authorities, and damage relations between state and society".

It is exactly the search for vulnerable objects in the information infrastructure on which the doctrine of "soft power" is built. At the same time, rapid development of technology is transforming the basis of the "soft power" doctrine into a conception

<sup>5</sup> Danyk Y.G., Katkov Y.I., Pichuhin M.F. (2006) National security: prevention of critical situations. -388 p.

<sup>6</sup> Sun Tzu. The Art of strategy. 2006.- 528 p.

<sup>7</sup> Sherr, J. (2013). Hard diplomacy and soft coercion: Russia's influence abroad. Royal Institute of International Affairs.

of modern wars and wars of the future, where the information battle issues are focused on four areas: moral, psychological, electronic, and cyber.

It should be noted that a large number of countries devotes considerable attention to this direction, including China<sup>8</sup> and Russia<sup>9</sup>.

Thus, non-forcible methods of foreign policy in the leading countries are the main paradigm of national security, and are focused primarily on manipulation of the individual, society and individual countries and also their informational and cyber resources.

Guarantees of security for a person, social groups, communities and nations as a whole are possible only on the basis of systematic preventive activities of state and military control on forecasting possible threats, their timely detection and neutralisation.

The technology for affecting states of interest by "indirect action" and "soft power" strategies is based on the following basic ideas and approaches:

- open and hidden forms and methods of influence to destroy an enemy in the absence of open confrontation or direct force collision;
- domination over the target country is conducted using deprivation of economic and resource sustainability, eliminating its ability to sustain development.

This is accomplished by creating a framework of state and military control of the country, offering the special institutional mechanism, "external control," which allows hidden and indirect control over life processes to be achieved.

In general, there are two possible options for the "indirect action" strategy development: aggressive and non-forcible.

A specific feature of the non-forcible option is to promote the desired changes in the geopolitical power of the state at the expense of "natural" degradation of the victim's country. This allows the state-aggressor to wait for his opponent to

**<sup>8</sup>** Huang, Y., & Ding, S. (2006). Dragon's underbelly: An analysis of China's soft power. East Asia, 23(4), 22-44.

**<sup>9</sup>** Concept of the Foreign Policy of the Russian Federation, adopted on 12 February 2013; an unofficial English translation is available at www.mid.ru/bdomp/ns-osndoc.nsf/1e5f0de28fe77fdcc32575d900298676/869c9d2b87ad8014c32575d9002b1c38!OpenDocument.

be weakened to the required level and the emergence of the conditions where no power is needed for capturing the territory. In this case, the role of the armed forces will be reduced to the means of consolidating the current economic and demographic situation in a particular region.

Implementation of the aggressive strategy of "indirect action" can be illustrated by the events that took place in the former Soviet Union and the Middle East. It is considered that these events occurred as a result of the application of the theory of "controlled chaos", authored by J. Sharp¹⁰ and St. Mann¹¹, based on which the technology for implementing the strategy of "soft power" was developed. The above-mentioned strategy proposes the following principles:

- the unification of all political forces that oppose the current legitimate government;
- undermining confidence in its leadership abilities for stabilising the situation inside the country and the loyalty of power structures;
- destabilising the country by initiating dissent that is cultivated in various sectors
  of society to undermine the legitimacy of the existing political regime;
- initiating regime change by challenging the election results and acts of civil disobedience.

In almost all countries caught up in riots related to these strategies, "spontaneous" gathering of crowds was organised by sending messages about planned actions and protests through social networks and email, as well as mobile phones.

Moulded by political technologists, the rise of protests is generated in social networks on the following levels:

- at the informational level, people's opinion is focused on existing problems. This forces a sharp reaction to populist proposals for solving them;
- at the mental level, the firm conviction that "it is much worse now, life has become unbearable" and "we cannot live like this any longer";
- at the social level, ethnic, social, religious and regional groups are stimulated to use radical methods to solve existing problems in society.

<sup>10</sup> Sharp, G. (2012). From dictatorship to democracy: A conceptual framework for liberation. The New Press.

<sup>11~</sup> Mann, S.R. (1992). Chaos theory and strategic thought. ARMY WAR COLL CARLISLE BARRACKS PA.

Therefore, these events should be categorised not as a revolution but as a nation's speeches disguised as natural in order to change undesirable, for appropriate forces, political regimes.

The application of a "soft power" strategy is usually implemented in the following sequence:

- in the first stage, destabilisation of the socio-political and economic systems of a country by creating a large-scale systemic crisis and dipping it in a state of "controlled chaos" that makes the political regime of the country vulnerable to external influence;
- in the second stage, in "controlled chaos" conditions, a socio-political structure
  of influence is formed to capture power in the country by changing the political
  regime;
- in the third stage, the process of forming new institutions of public administration and the security forces under the guidance of international organisations begins.

Thus, the strategy of "soft power" is an important potential political tool, which should take into account the modern conditions of the formation of a new world order.

### **Reputation manipulations**

The strategy of "soft power" cannot be provided in conditions where there is adequate response from the state and military control system. Such counteraction operates if key figures (leaders) are in their own places and operate effectively. Therefore, one of the main elements of the strategy of "soft power" is the blocking of the respective leaders by influencing them. One way to implement this is the manipulation of reputations.

The effectiveness of public administration in such a complex and dynamic system, which is a system of state and military control, depends on many factors<sup>12</sup>, primarily the following:

- correct determination of true national values, national interests and national objectives;
- early detection of threats to the vital interests of individuals, society and the state:
- elaborating the legislation; ability to reduce the opportunities for altering state and military control;
- real powers of each branch of government, respective leaders in the field of national security and defence;
- security coordination positions of key participants engaged in the formation and implementation of state policy in the sphere of national security and defence;
- availability of strategic thinking in the state leadership and political will on its practical implementation;
- matching the composition, structure, tasks and functions of the National Security and its individual components and their relationships to existing and potential threats;
- information-analytical, scientific, methodical, organistional and technical, resource and regulatory support activities of national security and defence;
- availability of trained state and military control specialists, as well as effective training system;
- · rational staff selection and placement;
- motivation of civil servants to perform their duties effectively.

These factors are very closely interrelated with each other. Generally, the integrated efficiency of the system of state and military administration is based on professionalism and rational distribution of hierarchical authority and motivation, and also depends on the reputation of subjects.

Therefore, in determining ways to implement the strategies being considered, special attention should be paid to the possible impact on the human resources

<sup>12</sup> Hovorukha V.V., Danyk Y.G., Klevec V.V. (2009). Areas of improvement of mechanisms of functioning of the administration in terms of transformation technologies external information and psychological impact on them. Actual problems of governance, (1), 9-16.

system, given its features that are able to detect and use the most vulnerable elements

It is well known that management, as a form of social activity, suggests a system of coordinated actions by the subject to the object to achieve specific organisational goals. Therefore, "non-forcible action", aimed at reducing management efficiency, achieves this goal by certain effects on the same subjects. The choice of specific methodologies, techniques and methods of implementation of these strategies arisies from their specific activity.

The most frequently used method of implementing strategies is a special operation to remove qualified personnel from key leadership positions. The main objective in this case is substitution of professionals, or creating conditions to force them to leave their position or failing to conduct qualified performance of duties.

Blocking of work can be done by different methods and at different levels: at the level creation of appropriate regulations, instructions, orders, etc., usage of moral and psychological pressure, demotivation and discrediting of persons.

The successful violation of the entire state and military control system can be achieved by controlling laws in the field of defence and security and their contents.

One of the options to paralyse a country in these ways in the conditions of modern warfare is the impact of the adoption of such laws, each of which are right and necessary, but collectively block the adoption of any effective solutions. Thus, a system is created where laws are in conflict with each other. This greatly complements the arsenal of reputation manipulation because every leader somehow gets into a situation where a solution is correct according to one law, but is criminal according to another.

There are several general levels of manipulative influence on persons holding managerial positions.

1. To persuade. The first step, implemented to influence the leader, is keying his life experiences, attitudes, preferences and beliefs. A person can be loyal to the influence and be ready to change his employees in accordance to his personal beliefs. An example of this influence can be the transition of government agencies managers and officials of the Armed Forces of Ukraine in Crimea,

which occurred in March 2014, to the governance of the Russian Federation<sup>13</sup>. Some personnel deliberately intended to make such a step under the influence of a long-term information campaign against the Ukrainian people. Some people did not want to change their place of residence and accepted the aggressor's terms.

- 2. To buy. If the manager (commander, chief) cannot be persuaded, the next way to force him to perform the necessary steps for the other side is bribery. A frequent phenomenon is that with the beginning of hostilities, most of the commanders left their units, resulting in a loss of control and subsequent defeat of troops in the military.
- 3. Manipulation of reputation. A common way to "destroy" the leader is to manipulate his reputation. In this scenario, i the formation and distribution of false information that discredits leader occurs. Another way is to create the idea that he may generate danger for the organisation, or is incompetent.

The simplest way to distribute such information is by means of the Internet. The uncontrolled spread of almost false information and one that is difficult to verify through social networks, forums, blogs is used to create a negative image of the leader.

An example of this phenomenon is the opening of websites, forums, social network groups and notes in blogs with the beginning of Russian aggression in Ukraine. This was designed to accommodate information about president, government, parliament, Ukrainian defence and security agencies executives' specifying alleged betrayal and offences against the Ukrainian state and people of Ukraine. Information actively replicated and distributed in order to establish an appropriate resonance influenced public opinion.

4. Physical destruction. An extreme measure, used in some cases if the corresponding leader is in a key post, is professional and substantially prevents enemy plans, and other ways to remove him from his duties were unsuccessful.

In the described context, one of the most important and effective means of influencing the leader is suggestion<sup>14</sup> as a process of influence on the human

<sup>13</sup> http://www.ccu.gov.ua/doccatalog/document?id=242321.

<sup>14</sup> Rizun, V. V. (2008). Mass Communication Theory: textbook. for the students in the sphere of "journalism and information" K.: Publishing House "Prosvita" 55.

psyche associated with decreased consciousness and the perception of criticality inspired content that does not require full-scale personal analysis or evaluation of the inducement to certain actions. The essence of the suggestion is the impact on human feelings and, through them, on his will and mind.

As the main consciousness manipulation method, suggestion became an integral part of special operations aimed at violation of the state and military control.

The following objectives may be achieved by using suggestion:

- In peacetime: preparation of a socio-political situation around the designated officials:
- In wartime: providing reputation manipulation of managers of the defence and security sector using all active destructive forms, methods and ways of suggestion;
- In the postwar period, ensuring creation of a positive image of the new government system.

The analysis showed the use of such methods of suggestion: misinformation, propaganda, diversification of public opinion and psychological pressure, spreading rumours, beliefs.

In known works, there are a few suggestive approaches in the implementation of psychological influence to manipulate consciousness, thoughts, beliefs and actions of people<sup>15</sup>:

- 1. Psychoanalytically oriented approach, using the "subconscious" for manipulation purposes.
- 2. Hypnotic approach, which uses trance.
- 3. Introductory hypnosis approach, which involves the use of language strategies to neutralise resistance to suggestion.
- 4. Neurolinguistics programming approach, which is provided by a specially designed neuro-semantic hypertext, containing the most important words and phrases for the person or group of persons under suggestion.

Suggestive technologies are especially effective on the Internet. This is caused by a number of reasons:

<sup>15</sup> Petryk V. M., Prycyazhniyk M. M., Kompanceva L. F., Skulish E. L. (2011) Suggestive technologies of manipulative influence -248 p.

- credibility of the informal network resources, which still remains high;
- audience can be involved in the information by hoping to solve any problems;
- formation of network communities based on empathy (compassion).

Thus, reputation manipulation is another effective type of destructive action aimed at disruption of the state and military control system, and in some cases the most effective.

## **Synergetic effect**

It can be concluded from the practice of non-forcible confrontation between countries in tinformation- and cyber- space that all mentioned technologies and ways of providing destructive actions, directed at the disruption of the state and military control system are applied comprehensively within single information and psychological operations (see. fig. 1)<sup>16</sup>, which can be illustrated by the example of Russian aggression against Ukraine.

Recently, the media, both Russian and domestic (especially television), has resorted to dangerous public methods of information and psychological influence.

For example, the analysis of news releases from the Russian channel, Russia 24, conducted within two months, showed the following ways that information was often manipulated:

Half or selective truth;
Citing anonymous source or authority;
Multiple repetition of non-reliable information;
Shift of accents;
Hyperbolising of details;
Labelling (punitive, junta).

<sup>16</sup> Hryshchuk, R. V., Kankin I. O., & Ohrimchuk, V. V. (2015). Technological aspects of today information confrontation. Information security, (17,№ 1), 80-86.

Thus, the amount of negative (destructive) information is insignificant and is filed carefully and hidden. There are no scenes of frank violence, murders are retouched and are accompanied by correct comments.

The emotional form of information presentation is widely used, where the speaker demonstrates excessive sarcasm and deliberate articulation of speech.

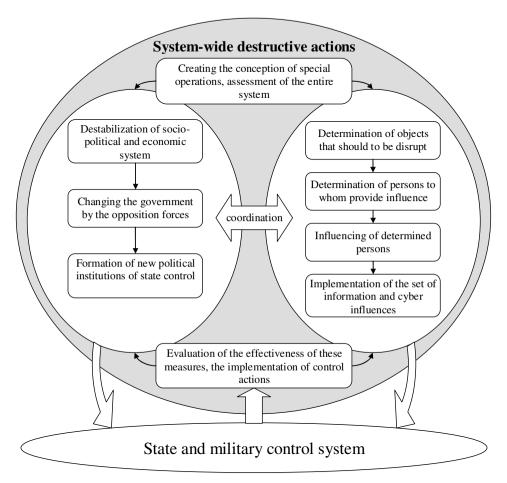


Fig. 1 System-wide destructive actions directed on disruption of state and military control system

There are also interesting facts about the frequency certain events are mentioned in the media. It has been noted that such high-profile events in the Donbass fighting such as Ilovaysk and Debaltseve preceded a significant surge of activity in the information field. Information with negative content actively spread to key

leaders of the Armed Forces of Ukraine and public figures. For example, content analysis conducted and modelled in the "InfoStream"<sup>17</sup> about the events in Debaltseve on February 2015 shows the fluctuation of the quantity of distributed messages of that kind (see. Fig. 2). Analysis of the given relationship indicates that the information operation for injection of a situation and creating panic in Ukrainian society began long before the military operation and peaked directly with the course of fighting.

Media analysis shows that the trend for using negative socio-political information became widespread. It leads to the following consequences:

- 1. Increased flow of negative information, resulting in gain from deviant behaviour, not only of individuals, but also of entire social communities.
- 2. Strengthening the potential of social media to effectively influence, without exception, social groups or negative egoistic purposes.
- 3. The ability of social media to influence not only on people's minds, but also on the subconscious sphere, resulting in zombification of the individual.
- 4. The emergence of a real opportunity for information to actively intervene in the processes of conflict management, and transformation of information into means of psychological warfare.
- 5. Creation of information weapons and the possibility of information warfare being waged as the main means for state policy continuation.

To hide the fact of information-psychological influence, wide ranges of manipulative techniques are used.

Here are just a few of such approaches: anonymous authority, everyday story, half-truth or selective repetition, information overload, use shortcuts, comments, joining the audience, the substitution of facts, substitution or rewriting history, a shift of emphasis, the combination of facts, false prototype, use of 25<sup>th</sup> frame technology.

Unfortunately, the actions of the national media resources that, intentionally or not, support the action initiated by the RF information to create cheap "sensationalism", significantly worsen the situation. Classically, unreliable and non-authoritative sources are widely used. Negative messages far exceed the

positive ones. Constant pressure, sarcasm, ridicule over the actions of security forces senior commanders is stimulated, which creates a backlash and pessimism in units of force against terrorism, the security and defence sector.

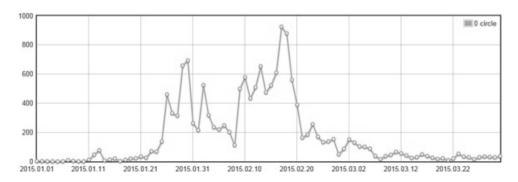


Fig. 2 The frequency of messages in the electronic media of destructive content before and during the operation at Debaltseve<sup>18</sup>

The consequence of the abovementioned actions are the discrediting of the Armed Forces of Ukraine and their leaders, undermining the Commanders' authority, inciting discontent with the actions of the senior military and political leadership of the state, implementation of doubts in the necessity of struggle, undermining the moral and psychological stability of the military, encouraging them to desert. In the absence of an effective response to the proposed information-cybernetic action, it became possible to predict the inevitable consequences of undermining the defence capacity of the state sector and the Armed Forces of Ukraine.

#### Ways of counteraction

To counteract the negative information and psychological influence, it is necessary to ensure the protection of personal data and to launch the practice of responsibility for defamation. World experience shows that the person is guilty of committing a crime only from a court decision. Thus, negative information about leaders of state and

<sup>18</sup> Shnurko-Tabakova E. (2015) Defamation of Ukrainian generals: shown in statistics. – Available from: http://hi-tech.ua/article/diskreditatsiya-ukrainskih-generalov-govorit-i-pokazyivaet-statistika.

defence structures, distributed in the information (cyber) space, should be thoroughly reviewed and persons who are guilty in distributing it should be brought to justice. This decision should be based on the fact that in war conditions they become accomplices in large-scale information operations of the aggressor's country.

#### Therefore, it is necessary:

- to ensure state control over the distribution of unconfirmed information;
- to create responsible departments in defence structures to prevent the dissemination of information in the information (cyber) space and to provide timely response;
- to ensure responsibility of persons who spread and store the information of destructive influence, in accordance with international and Ukrainian legislation;
- to conduct organisational activities with owners of webservers, networks and related facilities used for criminal purposes.

The analysis of the application of "indirect action" and "soft power" strategies allows possible ways of response to be formulated.

- 1. A strategy of vigilance and alertness towards hidden potential external and internal threats by introducing contemporary political and psychological technologies of state and cultural identity of the nation destruction to wide masses of people.
- 2. A strategy to ensure the stability of the state and social institutions. Public awareness of attempts by external and internal forces to deform and transform the socio-political system of the country.
- 3. A strategy for counteracting the information technologies designed for destruction of statehood, implemented through wide and prompt dissemination of reliable information about the situation in the country and the ability to defend one's own interpretation of events within the global information field. Basic strategies for protection against suggestive manipulation are so-called protective systems: withdrawal, expulsion, blocking, fading and neglecting.
- 4. A strategy to support the required level of social optimism index in the population, the state apparatus and security forces on the basis of the formation of the national idea, national ideology, success in protecting state and national interests.

The course of recent events, the undeclared war against Ukraine, current and projected threats and challenges clearly and convincingly show that to save the

life of personnel, to win and to ensure the necessary level of defence capability in the future, our country needs a modern, powerful, high-tech army.

In the majority of countries, in order to timely respond to the challenges and threats of today and tomorrow, to prevent unwanted actions, the state defence and security sector includes two main components:

- deterrent potential, consisting of traditional types of armed forces;
- potential for waging wars of a new type, which is based on means of special operations (SO), information and psychological operations (I&PsyOps) and electronic warfare (EW) and cyber-troops (cyber intelligence, security and effects), technical and OSINT intelligence bodies, operational management of forces and means units that are equipped with robotic complexes and so on.

In accordance with the experience of leading countries, these elements are combined into high-tech force with a high degree of readiness for use.

Rapid and efficient development of priority directions of the state's defence capability, quality of training for military personnel and carrying out appropriate research, and, most importantly, sustainable use of resources is essential. That is why immediate concentration of all available military-technological and human resources for these areas in a single national educational and scientific testing and implementing complex should be created as soon as possible. The best location for this is in the centre of the state, away from prying eyes, big cities and metropolitan highways, close to landfills and troops.

Forming the foundations for creating a new type of army should be attributed to the priorities of the state defence and security sector.

#### **Conclusions**

In conditions of hybrid warfare's destructive impact on the system and authorities, state and military control is an integral part of the overall system of the enemy actions. In these conditions, elements of the known (discussed) strategies with their transformation according to situations are widely used.

It is suggested the method of action to counteract specified impacts includes:

- identification of preparation for action in the information and cyberspace (based on information from electronic mass media, activity in social networks);
- analysis and modelling of the development of a situation, evaluation of threats, warning objects which are projected for impact by the enemy;
- preparation of proposals for counteracting, localising, identifying and isolating the sources of threats:
- taking measures to protect one's own resources;
- creating the conditions in which the actions of the enemy would be ineffective, or in which the enemy will be forced to abandon the destructive actions.

Ensuring effective state and military control in the conditions listed above should be achieved by conducting preventive actions. These actions should preclude or impede practical implementation of harmful strategies, taking into account the specificity of possible scenarios and their implementation.

It is necessary to control all the factors mentioned above and to weaken and limit all factors controlled by a third party and to strengthen the state's own resources and initiate damage to the attacker's resources.

We should convert determined factors to random and uncertain ones, limit access to the party with influence, and show only information that should be given to alleviate its impact and the violation of its plans to reduce the efficiency of public administration. Opponents should be misled about the situation and trends of development.

Solving this problem is also directly related to the need for the proper regulation of activities in this field, with sufficient motivation and labour management system, with the improvement of training, retraining and maintaining a high level of knowledge of the specified component of their activities. We should provide and coordinate integrating action on several fronts:

- conduct permanent monitoring of the activities in this field in Ukraine and the leading countries of the world;
- comprehensive generalisation and consideration of achievements and experience;
- direct combination of knowledge and timely consideration of trends and changes taking place in the area in question in the leadership training.