Scientific and Practical Cyber Security Journal (SPCSJ) 5(3): 11-24 ISSN 2587-4667 Scientific Cyber Security Association (SCSA)

INFORMATION WAR IN MODERN CONDITIONS PART 2

Volodymyr Khoroshko, National Aviation University, Doctor in Technical Sciences, Professor, Kyiv, Ukraine,
Volodymyr Artemov, National Aviation University, Doctor of pedagogical sciences, Professor, Kiev, Ukraine,
Lytvynenko Oleksandr, Taras Shevchenko National University of Kyiv, Doctor in Technical Sciences, Professor, Kyiv, Ukraine
Mykola Brailovskyi, Taras Shevchenko National University of Kyiv, PhD in Engineering Science, Associate Professor, Kyiv, Ukraine,

ABSTRACT: The article is based on the model of information warfare and the methods of psychological influence on the consciousness of people and society are considered. The influence of Russia's aggression on Ukraine through the three-level network concept, which combines all permissible types of influence on the enemy and represents a comprehensive strategy of influence, is proved. The concept of informational and psychological confrontation of society is developed, attention should be paid to the manipulation of information in a society, which aims to change the behavior of the object in the right direction for the subject as well as influence of information and psychological action of mass media on young people, expressed in violence, unmotivated aggression, hostility, cynicism.

KEYWORDS*: information warfare, information influence, aggression, information attack*

Introduction

At all stages of the historical development of human civilization, information has been both the most important object and a means of struggle between peoples, nations, states, military-political blocs and alliances. Some facts of informational influence on a wide audience can be found throughout human history. It is clear that in different periods the intensity of the application of certain methods of influence, as well as the perfection of its organization, differed greatly.

As a result, information and information technology in general have become extremely important for national security and particularly for military security. A number of countries, most notably Russia, have been intensifying the study and resolution of information and information warfare since the 1990s. Thus, the information war has turned from a futurological ghost into a real military discipline, which is being under development and study [1,2,3].

Thus, the geopolitical authority of the state in the international arena and its ability to influence world events today depends not only on economic and military power. Informational factors rather than the power ones are becoming increasingly important, i.e. the ability to effectively influence the intellectual potential of other countries, to disseminate and implement in the public consciousness the relevant spiritual and ideological values, to transform and undermine the traditional foundations of nations and peoples. A new stage is coming in military affairs, which is the transition from a strategy of nuclear deterrence to high-precision counter-force information weapons [4,5].

The role of information struggle are constantly growing in the system of national security of the states. The leading countries of the world, first of all Russia, the USA, France, Germany, Great Britain, Japan, that possess powerful information potential, are constantly increasing it on a scientific basis and at high culture of management.

In these and other countries, the scientific basis for the creation and application of means of information confrontation is the achievement of two main branches of science: cybernetics and computer science, which have been able to integrate many provisions of not only natural but also humanities.

Information is a terrible thing. Now it is indeed the fourth element of state power, which very often comes to the fore in the 21st century. It is enough to take a look at the influence of information on the electorate of such countries as France, Germany, and the United States. And Russia uses it very

well: it creates an artificial world, and if the real world brings it up all the time, it's very soon that the real world begins to believe in the unreal one.

Therefore, information confrontation is the rivalry of social systems (nations, blocs of countries) in the information sphere over the impact on certain areas of social relations and the establishment of control over the sources of strategic resources, as a result of which one group of rivals gets the benefits they need for further development.

According to the intensity, scale and means used, the following stages of information confrontation are distinguished: information expansion, information aggression and information war [6,7].

Information expansion i.e. the activities to achieve national interests by the method of conflict-free penetration into the information sphere in order to:

- carry out gradual and planned change in the system of social relations on the model of the source of expansion invisible to the society;
- displace the provisions of national ideology and national value system and replace them with their own values and ideological attitudes;
- increase the degree of its influence and presence, establish the control over strategic resources, information and telecommunication structure and national mass media (mass media);
- increase the presence of their own media in the information sphere of the object (system), penetration, etc.

Information aggression can be defined as illegal actions of one of the parties in the information sphere, aimed at inflicting specific, tangible damage to the enemy in certain areas of its activities through limited and local use of force.

Information warfare is the highest degree of information confrontation aimed at resolving socio-political, ideological, as well as national, territorial and other conflicts between states, peoples, nations, classes and social groups through the large-scale implementation of means and methods of information violence. (information weapons) [4,5].

Information aggression in the information sphere is assumed to escalate into war if one of the parties to the conflict begins to use information weapons widely against its opponents. This criterion makes it possible to distinguish from all the variety of processes and phenomena occurring in the information society those that pose a danger to its normal (peaceful) development.

In addition, it should be noted that currently there are no international and national legal norms that allow in peacetime (in the absence of an official declaration of war by the aggressor) to legally qualify hostile actions of a foreign state in the information sphere, accompanied by damage to information or other security such, as actions of information aggression or information war of material, moral, other damage. This allows to actively use the most dangerous and aggressive arsenal of forces and means of information warfare as the main means of achieving a political goal in peacetime.

Main part

In information warfare, information weapons are widely used, which represent devices and means designed to inflict maximum damage on the opposing side during the information struggle (through dangerous information influences) [4,5]. For the widespread use of information weapons (as well as any other) it is necessary that it:

- as quickly as possible in comparison with other types of weapons could be applied to the object of influence;
- caused the object of influence the necessary damage in a given time interval;
- was quite simple and cheap to manufacture compared to other weapons of the same class of influence.

At the turn of the XX-XXI centuries. there were conditions that allowed us to speak of information weapons as the most important weapons of the modern era. These include:

- a sharp decline in the cost of data production due to the advent of computer technology. And the production of information is put on the assembly line;
- creation of automated tools for obtaining knowledge from data;
- a sharp reduction in the cost and reduction of time for delivery of messages to almost anywhere in the world due to the development of telecommunications and the Internet;

- a sharp increase in the effectiveness of information impact, due to the emergence of advanced theories in the field of reprogramming of self-learning information systems: the theory of programming for computers and NLP;

- programming for social systems, including a large number of methods and techniques of information and psychological influence.

Objects of influence of information weapons can be:

- information and technical systems;
- information and analytical systems;
- information and technical systems, including service personnel (operator);
- information-analytical systems that include people;
- information resources;
- systems of formation of public consciousness and opinion based on mass media and propaganda;
- human psyche.

In cases where information weapons are not directly or indirectly used against the human psyche (or social group), it is practically possible to name only three objects of influence, each of which belongs to a certain type of information confrontation (in its pure form). These are information-technical and information-analytical systems (which do not include a person) - information-technical confrontation.

Sources of information hazards can be natural (objective) and intentional.

Considering the theory of information confrontation in the political sphere, it should be borne in mind that it occurs at the strategic, operational and tactical levels [1,2].

Basically, the higher political elite should operate at the strategic level, and the information unit of the political clan should operate at the operational and tactical levels.

According to experts, information warfare consists of actions taken to achieve informational advantage in ensuring national, military strategy by influencing the information and information systems of the enemy while strengthening and protecting their own information and information systems and infrastructure.

Information advantage is defined as the ability to collect, process and distribute a continuous flow of information about a situation, preventing the enemy from doing the same. It can also be defined as the ability to assign and maintain a pace of operations that exceeds any possible pace of the enemy, throughout its conduct, while remaining unpredictable, ahead of the enemy in its respective actions.

The information advantage allows you to have a real idea of the combat situation and gives an interactive and highly accurate picture of the actions of the enemy and their troops in real time. The information advantage is a tool that allows the command in critical operations to apply a wide range of different forces, to ensure the protection of troops and the introduction into battle of groups whose composition best meets the task, as well as to provide flexible and targeted logistics.

Previously, information weapons in terms of efficiency / cost were significantly inferior to any other weapon. The value of this parameter (efficiency / cost) in turn depended on the climatic conditions, the development of science, industrial production, the level of relevant technologies.

Currently, a classification is proposed, which has two subgroups of information weapons, the first subgroup includes: mass media; psychotropic generators; psychotropic drugs.

Information weapons of this subgroup are designed to have a negative impact on people. In particular, this influence can be exercised through various media. According to the Law of Ukraine "On Mass Media", these media mean periodicals, radio, television, video programs, newsreels, and other forms of periodic distribution of mass information.

Mass media means printed, audio, audiovisual and other messages and materials intended for an unlimited number of persons. The chronology of many military conflicts in recent years has included, as a rule, at the beginning of their development the stage of psychological treatment of the world community through the media [2, 9].

Psychotropic generators are devices that affect a person by transmitting information through unconscious perception. It has long been established that various human organs have their own resonant frequencies, using which you can influence the mental and physiological state of an

individual or group of people, causing them fear or other feelings. These and other features of the human body are used in the construction and selection of parameters (frequency range, radiation power, duration, etc.) of psychotropic generators.

Psychotropic drugs are drugs that can cause a state of dependence, have a stimulating or depressant effect on the central nervous system, causing hallucinations or impaired motor function of the body, under the influence of which there is a violation of thinking, mood swings, behavior.

The second group includes [7]:

- means of electronic warfare;
- complexes of special software and hardware influence.

Electronic warfare (EW) means systems for detecting and electronically suppressing enemy command and control systems and electronic weapons of the enemy, its reconnaissance and navigation systems, as well as systems for ensuring the stable operation of their systems.

Complexes of special software and hardware (CPT) - software, hardware or software and hardware, which can be used to make unauthorized copying, distortion, destruction of information, its transmission outside the controlled area or blocking access to it.

Currently, in addition to land, sea, air and space, the information sphere has been added to the number of areas of hostilities. According to military experts, the main objects of defeat in the new wars will be the information infrastructure and psychology of the enemy (there was even the term "human network").

The main objects of influence in the information war are [10]:

- communication networks and information and computer networks used by state organizations in performing their management functions;
- military information infrastructure, the crucial task of which is the management of troops;
- information and management structures of banks, transport and industrial enterprises;
- Mass media (primarily electronic).

There are now many definitions of information warfare. Let's focus on one of them. In August 1995, the US National Defense Institute published Martin Libiki's work "What is Information Warfare?" In it, the author identified 7 types of information warfare: command and control, intelligence, psychological, hacking, economic, electronic and cyber warfare. [11].

Command-and-control war as the main object of influence considers the channels of communication between command and executors. By cutting the "neck" (communication channels), the attacker isolates the "head" from the "body". It is said that this is better than just killing the "head". It is believed that the Internet was born as a defensive version of this war ("scattered neck").

Reconnaissance war aims to gather militarily important information and protect one's own.

Electronic warfare is affected by electronic communications networks - radio, radar, computer networks. Its important component is cryptography, which allows you to close and open electronic information.

Psychological warfare is carried out through propaganda, "brainwashing" and other methods of information processing of the population.

M. Libiki identifies 4 components of psychological warfare: undermining the civic spirit; demoralization of the armed forces; disorientation of command; war of cultures.

The purpose of the hacker war is total paralysis of networks, interruptions of communication, introduction of errors in data transmission, theft of information, theft of services due to unauthorized connections to networks, their secret monitoring, unauthorized access to closed data. To achieve these goals, various software tools are used: viruses, "Trojan horses", "logic bombs" sniffers.

Economic information war. Martin Libiki distinguishes two forms of it - information blockade (directed against the United States) and information imperialism (the method of the United States itself).

The world is changing rapidly and raises many new questions for humanity. The capital that plays a major role in the "digital revolution" is intellectual capital, especially in the field of information technology.

Finally, the main product of this sector - information - has unique properties that are not unique to other sectors of the economy. Information, unlike all other resources, is reusable and for

many users, and the more it is used, the more valuable it becomes. The same can be said about networks that connect different sources of information.

This is one of the approaches to determining the nature and content of information warfare. Among the first official documents on this issue is the US Department of Defense Directive T3600.1 of 21.12.1992 entitled "Information Warfare". In 1993, a directive of the Committee of Chiefs of Staff № 30 already set out the basic principles of information warfare. Finally, in 1997, the following definitions of information warfare were given: "Actions taken to achieve information advantage in the national interests of the country and carried out by influencing the information of enemy information systems while protecting their own information and their own information systems."

Since 1994, the United States has held official scientific conferences on "information warfare" with the participation of prominent representatives of the country's military and political leadership [12]. To this end, the Center for Information Strategy and Policy was established in the United States, the task of which is to study the possibilities of using information technology in military conflicts of the XXI century.

In all conflicts involving the United States ("Desert Storm", the operation in Haiti, Panama, against Yugoslavia and others), various types of information weapons were tested. To date, information warfare officer positions have been introduced in the U.S. Army, Navy, and Air Force. One can trace the evolution of the views of the top US leadership on the formation of the concept of "information operations". There are two periods of their origin, formation and development [11,12].

The first period (1950 - 1985) In this period there are two stages: at the first stage (1947 - 1973) the basic approaches to future information operations have arisen. The content of the second stage (1974 - 1985) was a comprehensive study of the experience of information components of hostilities during local wars and armed conflicts.

The second period consists of four stages.

The first stage 1985 - December - 1992 - the use of the latest information technology, psychological operations, electronic warfare at the strategic, operational and tactical levels.

The second stage of December 1992 - February - 1996 - is characterized by active theoretical development (with a great variety of approaches) of a single concept of information warfare on the scale of the armed forces, as well as the corresponding types of their contacts in the land forces, navy and air force.

The third stage, February 1996 - October - 1992 - completion of the development of the theoretical foundations of information warfare, preparation and conduct of information operations. These years clearly showed the limitations of the forms and methods of information warfare used, which prompted the further development of its theory, including in peacetime, as well as in the whole range of hostilities and in so-called military operations other than war.

The fourth stage, October 1998 - to date - the adoption of the view of the information struggle as a strategic means of achieving the goal of the national military strategy and the strategy of national security of the United States through information operations.

Many definitions of information warfare are associated, apparently, with the complexity and versatility of such a phenomenon as information warfare, the difficulty of drawing analogies with traditional wars.

If we try to transform the definition of war into the concept of "information warfare", it is unlikely to be constructive. This is due to a number of features of information warfare. For war in its usual sense, the subjects (different sides) are clearly defined, there are notions of the beginning and end of the war, the front line. Different sides are usually described by the same models. The outcome of the war is largely determined by the ratio of military capabilities of the parties.

For information warfare, defense is usually clearly defined, the concepts of beginning and end can be applied only to individual operations of information warfare, the front line is not defined, defense and offensive are described by different models. The success of the information operations is not directly related to the ratio of military capabilities of the parties. Ensuring information security in the field of state and municipal government (SMU) is based on a detailed analysis of the structure and content of the SMU, as well as information processes and technologies used in management. In this case, the determining factors in the development of information weapons are the individual

characteristics of the elements. It is clear. In order to model the behavior of the basic elements, it is necessary to know the individual characteristics and preferences.

The time interval at which systems try to win the information war, in this case can be compared with the lifetime of the elements (their time in the control system), which means that we are talking about insignificant in terms of generational changes in the time interval. Therefore, for a specific situation for a while it becomes permissible to talk about the victory of a particular algorithm. However, it should be remembered that the lifetime of the system and the training time are constantly changing. New learning technologies appear and the characteristics of the information environment change. This means that comparing the lifetime of the elements with the time interval of active information warfare is not entirely correct. Here it is necessary, first of all, to note the following: the intensity of modification of the surrounding world often does not leave the information system the opportunity to get out of the proposed scenarios of behavior [11]. It should also be noted that in modern models and methods of protection of man and social group from influences are used, as a rule, only the personal characteristics of a particular person, which distinguish him from others. Moreover, it is promising to create such a set of information and psychological characteristics of man, which would be characteristic of a broad and correct definition of the circle of persons. Moreover, it is desirable that such characteristics be objective in nature, that is, describe the real nature of man, rather than his subjective representation.

Based on what is stated about the simulated basic elements, we can formulate a statement: the greater the power of the set of basic elements and their relationships, the more resistant the system to targeted information.

In conditions when the time of information counteraction between the systems is small (for example, does not exceed the average lifetime of the system element) and the enemy system has simulated basic elements, we can offer the following algorithm, which should "always win":

- definition of basic elements of the information space of the enemy system;
- study of individual features and potential capabilities of basic elements;
- modeling of different variants of behavior of basic elements at different input influences;
- selection of the best scenario of basic elements;
- preparation of the environment in which the basic elements (public opinion) function, and themselves;
- implementation.

Given the above, the general scheme of information warfare can look like in Fig.1.

The given scheme, certainly, does not reflect all possible approaches and receptions to the organization and carrying out of operations on information influence. The human mind is more refined than any possible projection of the thoughts generated by it into the plane of practical algorithms.

The typical strategy includes only what is obtained from previously proven theorems, statements and consequences. From here we have: if the information system has influence against itself a complex of receptions of the scheme of fig. 1, it may mean that this information system is in a state of information warfare.

Many methods and techniques have changed, they have received a scientific basis. There are whole scientific disciplines on how to manage human behavior, team, society. These include: sociology, psychoanalysis, advertising theory, suggestology, NLP programming, dianetics, etc.

Hypnosis has been substantiated, attempts have been made to transfer the methods of hypnotic influence from the individual to groups and to entire human societies. Production and dissemination of information is put on the assembly line. All this was not even in the last century - there were not enough effective media, there were no scientifically sound algorithms for managing society, and these algorithms could arise only with the advent of programming theory for today's computer technology. Because to carry out an information operation means to select the input data for the system in order to activate certain algorithms in it, and in their absence to activate the algorithms for generating the necessary algorithms. The current theory of algorithms allows us to explain how automatic writing of programs can be carried out for certain subject areas, which is very important for the management of the individual, group and society as a whole.

In the conditions of information war a special place is occupied by information and psychological influence. It is a type of psychological influence, which is defined as a way to influence

people (individuals and groups), carried out to change ideological and psychological structures, their consciousness and subconscious, emotional transformation, stimulation of certain types of behavior using different ways of explicit and implicit psychological coercion.

Currently, which is characterized by intensive use of various methods of information, psychological pressure, which is especially associated with the development of modern technologies that can affect the consciousness, the psyche of many people simultaneously without influence and direct contact with them. The problem of psychological influence on people's consciousness becomes relevant, especially in the conditions of information warfare in various spheres of society.

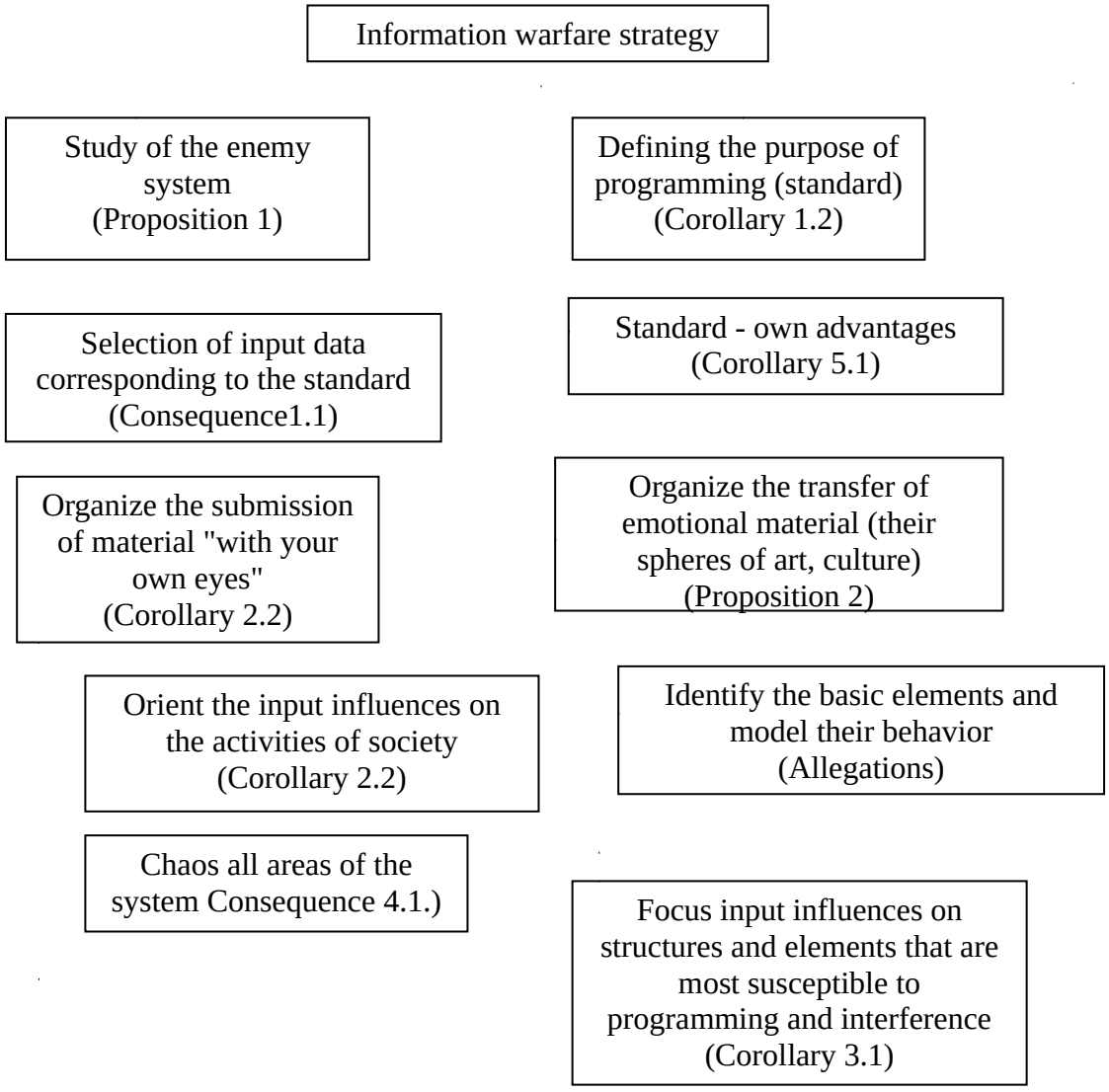

Fig. 1. A typical information warfare strategy

Of particular concern is the impact of information and psychological action of the media on young people, which is expressed in violence, unmotivated aggression, hostility, cynicism, legal negativity, rejection of traditional social values, etc. Information and psychological influence affects the following areas of the psyche of an individual, social group of people and society as a whole [10, 11, 12]: consumer-motivational sphere (values, desires, desires, beliefs, knowledge); intellectual and cognitive sphere (feeling, imagination, thinking and memory); emotional and volitional sphere (moods, emotions, feelings, will); communicative-behavioral sphere (nature and specifics of interpersonal perception and interaction).

Thus, only taking into account the features inherent in these areas of functioning of individual, group and social consciousness, information and psychological influence gives the most real effect.

It should be noted that any influence that aims to change the behavior of the object in the right direction for the subject, even if this influence is carried out for the benefit of the object, but without his consent, is considered a manipulative effect.

Regarding the consequences of information and psychological impact on objects, there are two types of information and psychological impact: positive and negative. In information warfare or confrontation, negative informational and psychological influence is of paramount importance. Experts distinguish a significant number of types of negative impact: [8,10] falsification (fraud) and misinformation; zombification or targeted programming to perform certain actions, including negative ones; introduction to a hypnotic state; harm to life and health; astro-terfing, which is defined as a deliberate centralized manipulation of public opinion on the Internet for the purpose of misinformation, distortion of statistical information, their use by public opinion; trolling - posting informational messages in order to persuade users to discuss a certain direction or create a conflict situation, etc.

Among the facts that determine the tendency to negative information and psychological influence are psychological factors, which include situational and non-situational [11,12].

Situational factors are due to a specific information and communication situation (psychological state, various stressors, extreme conditions, etc.). Non-situational factors include a person who is exposed to negative information and psychological influence, which affects his propensity to psychological manipulation, etc.

The information environment, acquiring the character of the second, subjective reality, in the part that contains information that adequately reflects the world around us, and its characteristics and processes that complicate or hinder the adequacy of perception and understanding of the world and himself, despite his illusory, becomes a significant external source of threats to information and psychological security of the individual.

The process of bringing a hypnotic state to a particular society in the context of information warfare can, for example, look like this [11]:

1) to relax society - to instill through the media that there are no enemies, while discussing individual historical periods and the interests of individual peoples (the body as a whole must disappear as an object of consciousness);

2) to force society to listen only to the enemy, not paying attention to any other thoughts or feelings, for example, to focus the media exclusively on any one paradigm of social development (eg, Western), excluding any other experience: China, Japan, the Muslim world (goal - the process of loading the public consciousness and the action of the forming forces are weakened);

3) to force the society not to think about what the opponent is saying, for this purpose to exclude from the mass media serious analytical studies of problems (the goal is to help slow down the continuous flow of opinions);

4) to focus society's attention on something other than the incoming information flow, such as internal cataclysms, wars, acts of terror (the goal - the protection subsystem responsible for processing incoming information, is unable to perform its function and as if disconnected);

5) constantly inspire that society itself and everything around it is getting better and better (the goal - such a suggestion weakens the historical memory and sense of self-identification, which characterizes the normal state of society);

6) the media at the same time must convince members of society that caused the state - this is not exactly what it should be (the goal - to create a passive state of consciousness, which retains the possibility of dependence on the informational influence of the enemy).

Today, the number of channels of information influence on people and society is growing. And mostly the number of those channels and factors that affect not only the rational but also the emotional perception of reality by man.

Thus, people and social groups are under increasing informational and psychological influence.

The above algorithm generally reflects the work of the media in Russia from 1990 to 1997. In addition, it should be noted that this algorithm is used in the Ukraine-Russia confrontation.

Management of human behavior is one of the primary tasks of the state. It must be understood that the state is created by its citizens in order to reconcile their own interests, but state or political power finds its own interests and its primary task is to manage those who have chosen and maintained the goal of trivial self-preservation.

If citizens begin to express dissatisfaction with the current policy pursued in the narrow corporate interests of the ruling elite and its proxies, then to avoid violence against the people, this can be countered only through the use of tools used by the media.

Noam Chomsky, a professor at the University of Massachusetts Institute of Technology, identified 10 ways to control the masses in his book, Silent Weapons for a Peaceful War.

Method № 1. Distraction.

The main element of public administration is to distract people from important problems and decisions made by political and economic circles of the country, by constantly saturating the information space with insignificant messages. The method of distraction is very important in order not to give the citizens of the country the opportunity to receive important data and knowledge in the field of modern philosophical currents, advanced science, economics, psychology, neurobiology and cybernetics. Instead, the information space is filled with sports news, show business, mysticism, and other informational components based on relict human instincts from eroticism to brutal pornography or from household soap operas to dubious ways to make easy and quick money.

Method № 2. Create problems and then suggest ways to solve them.

This method is also called "problem-response-solution". A problem is created, a kind of "situation" designed to provoke a certain reaction among the population so that it itself would demand the necessary measures to be taken by the ruling circles. That is, to cause some kind of economic, man-made and terrorist crisis in order to force people in their minds to take measures to eliminate its consequences, even in violation of their social rights, as a "necessary evil." But it is necessary to understand that crises are not born by themselves.

Method № 3. Method of gradual application.

To achieve any unpopular event, it is enough to implement it gradually, day after day, month after month, year after year. This is how fundamentally new socio-economic conditions (neoliberalism) are globally imposed. Minimization of state functions, privatization, uncertainty, instability, mass unemployment, wages that no longer provide a decent standard of living. If all this happened at the same time, it would probably lead to a revolution.

Method № 4. Delay execution.

Another way to push through an unpopular solution is to present it as "painful and necessary" and to obtain at the moment the consent of citizens to implement it in the future. It is much easier to accept any sacrifices in the future than at present.

First, because it will not happen immediately. Secondly, because the people in their mass are always inclined to cultivate naive hopes that "tomorrow everything will change for the better", that the sacrifices demanded of them will be avoided. This gives citizens more time to get used to the idea of change and humbly accept it when the time comes.

Method № 5. Address the people as small children.

Most propaganda speeches intended for the general public use arguments, characters, words and intonations, as if they were school-age children with developmental delays or mentally handicapped individuals. With this link, someone is trying to mislead the listeners, that is, to a greater extent he is trying to use infantile language expressions. If a propagandist addresses a person as if he or she were 12 or younger, then due to the suggestion, response, or reaction of that person, there is also a certain degree of probability that there will be no critical appraisal, which is typical for children 12 years or younger. Pre-naive reasoning and capitalized truths embedded in political speeches designed to be perceived by a wide audience, which are already used in the described methods of manipulating consciousness.

Method № 6. Works that focus on emotions to a much greater extent than on reflection.

Influence on emotions is a classic technique of neurolinguistic programming, aimed at blocking the ability of people to rational analysis, and ultimately to the ability to critically comprehend what is happening. On the other hand, the use of the emotional factor allows you to open the door to the subconscious state in order to root there thoughts, desires, fears, fears, coercion or stable patterns

of behavior. Spells are not as brutal a terrorism as an unjust government, as the hungry and humiliated suffer, who bring to the fore, while ignoring the true causes of what is happening. Emotions are the enemy of logic.

Method № 7. Keep people in ignorance by cultivating mediocrity.

To make people unable to understand the techniques and methods used to control and subordinate them to their will. The amount of education provided to the lower social classes should be as meager and mediocre as possible so that the ignorance that separates the lower social classes from the higher ones remains at a level that the lower classes cannot overcome. This includes the promotion of so-called "modern art", which is the arrogance of mediocrity, claiming popularity, which is unable to reflect reality through those works of art that do not require detailed explanation and agitation for their "genius". Those who do not recognize innovation - are declared backward and stupid and their opinion is not widely publicized.

Method №8. Encourage citizens to admire mediocrity.

Introduce into the population the idea that it is fashionable to be stupid, vulgar, and rude.

This method intersects with the №7 method, because everything mediocre in the modern world appears in large numbers in all social spheres - from religion and science to art and politics. Scandals, yellow pages, witchcraft and magic, dubious humor and populist actions - all good to achieve one goal - to prevent people from being able to expand their consciousness to the vast expanses of the real world.

Method № 9. Strengthen guilt.

To make a person believe that he alone is to blame for his own misfortunes, which occur beyond his mental capabilities, abilities or efforts. As a result, instead of rebelling against the economic system, man begins to engage in self-destruction, blaming himself for everything that causes depression, which leads, among other things, to inaction. And without action there can be no talk of any revolution! Both politicians and scientists (especially psychotherapists) and religious figures use fairly effective doctrines to achieve the effect of self-flagellation of patients and "flocks" to manage their life-affirming interests, directing their actions in the right direction.

Method № 10. Find out more about people than they know about themselves.

Over the past 50 years, advances in the development of science have led to the formation of a growing gap between the knowledge of ordinary people and the information possessed and used by the ruling classes.

Thanks to biology, neurobiology and applied psychology, the "system" has received advanced knowledge about man, both in physiology and psychology. The system has managed to learn more about the average person than it knows about itself. This means that in most cases, the system has more power and controls people more than they control themselves and their actions and deeds.

It should be noted that currently there is a strong negative information and psychological influence from Russia. At the same time, the terms "Russian-speaking population", "Russian world" and others are actively used by Russia in order to exert a negative information and psychological impact on people and social groups of Ukraine. These terms are not clearly defined - they are used solely as metaphors or analogues. The purpose of such use is to make a person or social group feel their "unity" with others. Psychologically, it is possible to reject the individual and come into conflict with himself, which dramatically reduces the threshold of suggestiveness and practical perception of information about the surrounding events [13]. It should be noted that the hybrid war was invented by Eugene Messner - a White Guard colonel who was chief of staff of the Kornilov division. He developed the theory of the rebellion of the war in 1967 in Argentina published a book "Theory of the Third World". However, elements of the "hybrid war" were already used during the First World War.

Realizing that fighting on two fronts was extremely exhausting and dangerous, Germany in 1914 turned its back on subversive activities in France, Britain and Russia, funding the so-called fifth column, ie various organizations, political forces and newspapers, campaigning for the defeat of its governments in war. That is, the "hybrid war" that the Kremlin is waging against Ukraine today is far from new. Its elements were used by the German General Staff in the fight against Russia and its allies 100 years ago.

By the way, the German and Austro-Hungarian governments provided material assistance in organizing Ukrainian political emigrants - the Union for the Liberation of Ukraine, whose members

conducted propaganda and agitation in the camps among fellow prisoners of war and tried unsuccessfully to organize resistance to the tsarist army in Galicia. This fact led to the spread of the myth that Germany allegedly financed the Ukrainian People's Republic - to split Russia. The General Staff of the Soviet Union began to develop and implement this concept in the early 1980s. Russia has adopted this concept and is now using it.

This concept is to create three levels of the network [13]. First, the territory of the enemy is covered with a very dense network of Russian broadcasting, the necessary history is introduced (it does not matter whether it is true or false). Then cultural societies and circles are created that support politics and ties with Russia. Organizational moments are superimposed on the cultural basis, ie pro-Russian parties are created.

Building a level 2 matrix are people who sympathize with Russia without recruiting. There are those who studied in Russia. The apologists of the Russian world, those who have come to this themselves and say: "They have a layer of culture more interesting than ours" - they become information nodes. Without realizing it, such a person is already conducting information intelligence. Moreover, all this is open, everything is legal [13].

Then, the so-called combat platform is inserted into this territory - from one person to a division. You are told to create a fighting cell of people who will be ready to side with Russia in case of force majeure. At the same time, they ask to create a combat group that will protect against the fascist coup or Bandera. This is what happened in Ukraine in Donbass. Donbass "feeds all Ukraine and Ukraine lives at its expense".

Any system responsible for processing the input data must be "fed", ie must consume energy in order to activate the algorithms embedded in the processing of input data and generate new ones. The basic elements of each system have a certain physical nature, which largely determines the reaction time, and hence the choice of a particular algorithm for solving a particular problem [8, 11, 14].

When considered as information self-learning systems of the states under "other kinds of influence" in the light of the above it is necessary to understand first of all economic war. But in a narrow sense, related exclusively to economic sanctions such as "it is impossible and it is impossible", and in a broader sense, which includes "economic interventions" in the form of goods and products at dumped prices.

The time of information and economic wars has come also because today's world is no longer characterized by a shortage of information and industrial goods, on the contrary, it is distinguished by their excess. This means that as in the case of information warfare, when the system must think more not about the protection of information, but about protection from information and the promotion of its vision of the world, and in economic warfare should be about protection from other people's goods and news. their own.

Competent combination of all permissible types of influence on the enemy is a comprehensive strategy of influence.

Permissible types of influence here are those actions that "grossly" do not violate the currently accepted norms and rules of conduct in society.

Adherence to the principle of complexity in the formation of a common security strategy to influence the enemy can enhance the effect of the use of information weapons and thus may be another sign of information warfare.

In recent years, the information war has increasingly turned into a geopolitical information confrontation. This is well illustrated by the example of Russia, which is conducting active advocacy activities in the global information space.

Not only ordinary people in Russia and the world are exposed to these propaganda influences, but also many of those who define, create and influence public opinion. Moreover, Russia has in its arsenal many different developments aimed at propaganda and manipulation of public opinion and consciousness.

It should be borne in mind that the purpose of geopolitical information confrontation is to violate the information security of the enemy state, in certain cases - the integrity (stability) of public and military government, effective informational influence on their leadership, political, public

opinion and decision-making, and also providing information security for gaining (providing) information superiority in the world information space

There are two types of information confrontation (struggle): information-technical and information-psychological [15].

In information and technical confrontation, the main objects of influence and protection are information and technical systems (communication systems, telecommunications systems, data transmission systems, electronic means, information protection systems, etc.).

In information and psychological confrontation, the main object of influence and protection are the psyche of the political elite and the population of the opposing parties, the system of formation of public opinion and consciousness, decision-making.

The confrontation includes the following stages:

- forecasting and planning;
- organization and incentives;
- feedback;
- regulation;
- performance control,

as well as the stages of testing decisions during the information confrontation:

1) assessment of the situation:
   - determining the composition of indicators and criteria;
   - assessment of the reliability of data receipt;
   - analysis of the state of the control object;
   - analysis of the state of the subject of management;
   - analysis of deviations.
2) goal setting;
3) definition of the plan and decision;
4) the formation of solutions (there must be at least three).

Information confrontation (especially in the political sphere) has three components:

- strategic political analysis;
- informational influence;
- information counteraction.

Strategic political analysis is a set of measures to obtain information about the enemy in the conditions of information confrontation; gathering information about their political allies; processing information and exchanging it between members of their political clan in order to organize and conduct information confrontation. The information must be reliable, accurate and complete, and the information must be selective and timely. It is logical to call the solution of the listed tasks information maintenance of management of material and financial resources.

Information impact includes measures to block, retrieve, process and exchange information, and introduce misinformation.

Information counteraction (protection) includes the action of blocking the information needed to solve problems of political process management, and blocking misinformation disseminated and introduced into the system of formation of world public opinion by political competitors (opponents).

Levels of information confrontation are divided into: strategic, operational and tactical.

Basically, at the strategic level of information geopolitical counteraction, the highest state authorities of the country should act, and special services and large capital - at the operational and tactical levels.

The world's leading countries (primarily the United States, Russia, China, Britain, France, Germany, Israel) currently have a powerful information potential that can ensure them achieve political goals, especially since international legal norms of information warfare as such are absent.

Conclusions

At all stages of the historical development of human civilization, information has been both the most important object and the means of confrontation between peoples, nations, states, military-political blocs and alliances. Some facts of information and psychological influence on a wide

audience can be found throughout the history of society. It is clear that in different periods the intensity of the application of certain methods and methods of influence, as well as the perfection of their organization, differed greatly.

At the present stage, science has such theoretical constructions, on the basis of which the technology of information confrontation, ie the relevant governmental and non-governmental structures involved in such activities, develop and test new information technologies, techniques, methods of implementation, information and psychological impact, technical means necessary for such activities. Such changes could not but affect the growth of the effectiveness of information technology, which can lead to radical changes in society, economic, political and other areas of a country, or globally.

The uncontrolled spread of the use of information space, along with the significant benefits of their use, has led to the emergence of fundamentally new, related problems. The main one was the sharp intensification of international competition for ownership of information markets. At the same time, in order to ensure information confrontations and conduct certain operations during local hostilities and armed conflicts - the so-called information confrontation, the countries of the world began to actively use the information space (Internet), a vivid example of this was the events in Iraq, Yugoslavia, Libya. Chechnya, Georgia, Ukraine, etc. This state of affairs, as a consequence, in turn led to the strengthening of integration processes in the infosphere, gave rise to information confrontation, ie information wars.

In today's world, interstate conflicts are fraught with excessive losses for each of the warring parties. Therefore, the technique used is only half-truths, half-cooperation, mutual competition in development, in the pursuit of moral leadership. Activities in information confrontation and information-psychological influence give opportunities for the use of this approach.

It is proved that information war is an element of information confrontation, a political conflict in which political struggle in the form of information-psychological operations with the use of information weapons.

BIBLIOGRAPHY

1. Litvinenko O.V. Information influences and operations. Theoretical and analytical essays / Litvinenko O. V. – Kyiv: National Institute for Strategic Studies, 2003.-240 p.
2. Pirtskhalava L.G. Information confrontation in modern conditions / Pirtskhalava L.G., Khoroshko V.A., Khokhlacheva Y.E., Shelest M.E. - Kyiv: CP "Kompint", 2019.-226 p.
3. Rastorguev S.P. Philosophy of information war / Rastorguev S.P. - Moscow: Moscow Psychological and Social University, 2003. – 496 p.
4. Litvinenko O.V. Special information operations and propaganda companies / Litvinenko O.V. - Kyiv: Satsanga, 2000. - 242 p.
5. Grishchuk R.V. Cyber weapons: classification, basic principles of construction, methods and means of application and protection against it / Grishchuk R.V., Khoroshko V.O. // Modern special equipment, No. 4. 2016. - pp. 30-37.
6. World hybrid war: the Ukrainian front / Edited by V.P. Gorbulina – Kyiv: National Institute for Strategic Studies, 2007.- 496 p.
7. Eremenko V.T. Actual problems of information confrontation in sociotechnical systems / Eremenko V.T., Pershukov V.M., Pikalov B.V., Tretyakov O.V. - Orel: Publishing House “Gosuniversitet” - Prioksky State University, 2015. – 291 p.
8. Prokofiev M.I. The concept of application of information influences and counteraction of information weapons / Prokofiev M.I., Khoroshko V.O., Khokhlacheva Y.E. // Legal, regulatory and logistical support of information security systems in Ukraine, Vol. 1 (31), 2016. – pp. 9-14.
9. Khoroshko V.O. Information war. Mass media as a tool of informational influence on society. Part 1. / Khoroshko V.O., Khokhlacheva Y.E. // Information Security, Volume 22, №3, 2016. - pp. 283-289.
10. Dereko V.N. - Theoretical and methodological principles of classification of threats to the object of information security / Dereko V.N. // Information security of man, society, state, No. 2918), 2015. – pp. 16-23.

11. Khoroshko V.A. Information and analytical security / Khoroshko V.A., Shelest M.E. - Kyiv: Private printing establishment “Zadruha”, 2016. - 183 p.
12. Ostapenko G.A. Information operations and attacks of socio-technical systems / Ostapenko G.A. - Moscow: Hotline - Telecom, 2007. -134 p.
13. Messer E.E. If you want peace, win the interwar / Messer E.E. - Moscow: Published by “Russkii Put’ ” 2005. – 485 p.
14. Artemov V., Khoroshko V., Ivanchenko I., Brailovskyi N. Geopolitics and Information Warfare // SPCSJ, vol. 4, No.1, 2020.- pp. 61-64
15. Prokofiev M.I. Problems of information protection in Ukraine / Prokofiev M.I., Khoroshko V.O. // Legal, regulatory and logistical support of information protection systems in Ukraine, Vol. 2 (30), 2015. - pp. 9-14