INFORMATION WARFARE AND INFORMATION SECURITY IN THE 21ST CENTURY

Atabayeva D.T., Mussayeva E.A.
Karaganda Economic University, Temirtau, e-mail: elvira.musaeva.75@mail.ru

The present paper is dedicated to studying theoretical and practical aspects of information warfare and information security maintenance. The authors analyzed and integrated different approaches to definition of "information warfare" and "information confrontation". The article contains data related to the typology of information warfare and its structural elements. The authors underscore the relevance and role of the information security both for states and individuals. The work contains information on the main aspects and issues related to information security, it resumes common principles and techniques of information-psychological warfare. The authors made an attempt to analyze and evaluate main issues that Kazakhstan faces providing information security.

Keywords: information warfare, information

With the development of new information technologies and global informatization, modern society has become an "informational", creating worldwide information space. It is becoming increasingly evident that social progress, as well as every person are largely determined by the development of their information sphere, that contributes to the formation of new national interests and brings up new controversial issues. Many of these problems relate to the pursuit of dominance in the global information space. The information space has become another field of confrontation between international actors, it implies such issues as formation of the concept of information warfare by a number of states, violation of the normal functioning of information and telecommunications systems, security of the information resources, as well as unauthorized access to them.

Information is reasonably considered as a strategic national resource. The political weight of the country, its ability to influence world events depend not only on real-power factors, but increasingly on information factors. It involves an ability to exploit the intellectual potential of other countries, spread and impose their values, and also impede spiritual and cultural expansion of other nations, transform and even undermine their spiritual and moral foundations.

There is an urgent need for a definition of such important notion as "information confrontation" and "information warfare". Thus, I.N. Panarin defines information confrontation as a form of struggle of the parties with the use of special (political, economic, diplomatic, military, etc.) methods and means of influencing the information sphere of the opposing side, as well as for self-defense [1, p.245].

An "information warfare" is a term that was introduced in the USA in 1967, but attracted the experts attention in 1991 during the Gulf War. The phenomenon of information warfare originated in the West during the Cold War. The term was firstly used by Allen Dulles, the main organizer of the information war against the Soviet Union, in his book "The Secret Capitulation" [2]. It introduced as a special intelligence operation. Given the militaristic origin of this concept, the American definition was oriented towards military objectives and the emphasis on the need to influence the enemy in a threatened period. "Information warfare" is a term of publicists, it is not used in a professional environment, where it was substituted by information or psychological operations. One of the reasons is that a war can not be waged in a peace period, but operations can.

S.N. Grinyaev, a Russian researcher, proposed the shortest and most adequate definition of information warfare that is a use of means of information influence on the enemy in the interests of achieving the objectives of the influencing party [3, p.98].

The majority of Russian researchers distinguish two main directions of the information warfare (confrontation): information and technical (systems communications and management, computer and telecommunication systems, radio electronic means, etc., as the objects of influence), information and psychological (public consciousness as the object of influence).

The detailed list of information warfare dimensions, according to the American sources, includes Electronic Warfare (EW), Psychological Operations (PSYOP), Computer Network Operations (CNO), Military Deception (MILDEC), Operations Security (OPSEC) [4].

There are following important subjects of information (psychological) warfare:

– national military units of psychological operations;

– state foreign policy;

– special state services;
– bodies of military and political propaganda of international organizations;
– international non-governmental organizations;
– national and international research and educational institutions;
– international religious extremist organizations;
– the media;
– individual network activists and their associations.

A.V. Bedritsky, referring to the authoritative American expert M. Libicki, singles out four categories of information-psychological operations conducted within the framework of the psychological struggle: operations against the structures of public administration, operations against military command structures, operations to demoralize the armed forces, the war of cultures ("kulturkampf") [5, p.97]. The first three areas perfectly fit into the basic concept, but the latter one is very specific. It is addressed to society as a whole and associated with the influence on the culture of the country or its individual elements. The war of cultures is a specific spiritual action directed against the public consciousness with the aim of changing the attitudes and orientations.

The existence of the cultural-ideological direction of the psychological warfare is also recognized at the highest political level. It was very clearly described by Vladimir Putin in 2012. As the historical experience shows, cultural identity, spiritual and moral values, value codes are a sphere of fierce competition, sometimes the object of open information confrontation is for sure, and certainly well-directed propaganda attack. And these are not phobias, it is real. This is at least one of the forms of competition. Attempts to influence the world view of whole nations, the desire to subordinate them to own will, to impose own system of values and concepts are an absolute reality, just as the struggle for mineral resources, which is faced by many countries, including Russia [6].

There are several common principles and techniques of information-psychological warfare.

1. The main and most effective method of information and psychological warfare is the systematic imposition of one's own point of view, one's own picture of the world, one's view of things. It is effective no matter whether the opponent is trying to consciously resist. If a person does not 100% realize that the opponent's imposed ideas are wrong, he can begin to give in and perceive things from the position of the enemy. At the same time, the opponent can impose a correct point of view, as well as partially correct and false ones.

2. There is a hidden imposition in addition to explicit imposition. The influence is carried out in such manner that the person does not realize this, therefore it is very effective. This method is very convenient, because nothing needs to be proved. The effective reception of the hidden imposition of representations is to present them through some information that looks neutral, formulate certain ideas, and look at things as something natural, non-alternative, self-evident.

3 The firmness and consistency in defending own position, confident behavior as a keystone.

4 Counter-propaganda in order to dissuade, make doubt, purposefully influence the key moments in the enemy's views on which he bases his behavior. When choosing an object, we must choose, first, the weakest points in terms of their reliability, correctness and persuasiveness, and secondly, those points that are the most sensitive.

5. Any information-psychological impact is useless, if it is not supported by real intentions, actions and willingness to commit them. Dissonance between what a person says and what he does, ruins the effectiveness of any propaganda.

The traditional rational direct method of influencing consciousness is based on persuading people to change their minds with the use of rational arguments and logic. Along with rational ways of influencing consciousness, there are ways that can be called irrational. They can have a destructive influence, suppress the rational principle and force people to serve their goals. It implies appealing to irrational arguments, lies, intimidation, suppression, disorientation, shocking and zombieing.

One of the most important problems associated with information warfare is the society's misunderstanding of the fact that a threat can be born by modern communicative processes. Also society is not ready to oppose attempts to manipulate public consciousness.

Information security in today's information warfare is relevant for Kazakhstan. There are no information wars against Kazakhstan, we are not the object of an information war, but our deep immersion in the foreign information space determines our involvement in the information confrontation. Therefore, the problem of information security is very urgent for the Republic of Kazakhstan.

The dynamics of the development of information technologies that reflect on socio-economic and cultural development stress the need of regulation of information security issues.

In accordance with the openness of national information space and popularity of foreign media, television and Internet resources, there is a real threat of information impact on public consciousness. Information impact can be expressed both in the form of direct imposition of the ideas that contradict national interests and creating a certain information background artificially maintained by information manipulation. To counteract this manipulation of public consciousness, it is required to seriously improve the effectiveness of the state information policy, increase the openness of the state bodies, and increase security of citizens' right to information.

Another serious problem is a non-competitiveness of the domestic content that forms national information space. Its quality remains insufficient for full-fledged competition with a foreign information and entertainment product. In conditions of the national information space openness it leads to unpopularity of the local information product. Consequently, low popularity does not allow to attract significant investments that causes scarcity of the domestic content.

A lack of the appropriate domestic information technologies for the state, business and society leads to the forced use of foreign equipment and information systems. As a result, it increases a probability of an unauthorized access to databases and data banks, as well as country's dependence on foreign manufacturers of computer and telecommunications equipment and software.

A specific threat is a low level of people's general legal and information competence including skills of the safe use of cyberspace.

A legal support of the information sphere is significantly insufficient for the current needs. Legal mechanisms regulating production, transmission, dissemination of information, information resources, information products and information services need to be constantly improved and updated.

Thus, the current state of information security is characterized by such threats as an underdeveloped information security system and disruption of the functioning of the important information objects; the low level of production and application of the relevant information and communication technologies that do not meet the objective needs of society; dependence on the import of information technology and information protection facilities, the use of which can damage national interests; the information warfare between confronting great powers; development of information manipulation technologies; a possibility of the destructive information impact on the public consciousness and state institutions damaging the national interests of any country; a misinformation or purposely distorted information capable of causing damage to the national interests of the Republic of Kazakhstan; the insufficient effectiveness of information support for public policy; weak security and low competitiveness of the national information space; a low quality of the national content that do not meet the objective needs of society; the growth of crimes, including transnational, extremist and terrorist activities that make use of the information and communication technologies; the insufficient development of the system of legal regulation of the information sphere; illegal actions of state structures resulting in violation of rights and interests of individuals and entities.

An effectiveness of the state policy related to ensuring information security depends on the national concept. Often, such concepts are not fully developed and do not meet the ever-changing global challenges and threats. For example, the Concept of information security of the Republic of Kazakhstan was adopted by the Decree of the President of the Republic of Kazakhstan on November 14, 2011 and was implemented during the next five years [7]. The purpose of the concept of information security is to create a national information security system that guarantees protection of the national interests of the Republic of Kazakhstan in information sphere. To achieve this goal, it is necessary to complete the following set of tasks:

1) to develop an information security management system that allows to ensure the security of the country's national information infrastructure and a single national information space;

2) to develop and implement a unified technical state policy in order to ensure information security, including development and strengthening of the national information protection system;

3) to protect the rights of the individuals and the interests of society;

4) to develop the national information space;

5) to improve legislation that regulates the information sphere;

6) to provide state's active participation in the processes of creating and applying global information networks and systems.

Despite of all, Kazakhstan's information security system is characterized by the low effectiveness of information management of the state policy, due to the shortage of the qualified personnel, lack of a system for the formation and implementation of the state information policy, insufficient coordination of the governmental bodies' activities. The situation is also aggravated by the fact that sometimes the official media is unable to fulfill its main function of conducting the state information and ideological policy because of unpopularity and low level of population's trust.

The information transfer has an extremely high speed, therefore it is practically impossible to completely restrict the dissemination of any information, except for private situations, so information is the most important social resource of the information society. As a consequence, control over information flows provides an opportunity for significant influence on various spheres of society, social institutions and the entire system.

Another important point relating to information is an information security of the person. Given the fact that in addition to the physical and mental characteristics peculiar to any individual, the latter gets a virtual dimension, representing a diverse array of information about the person, handling of the personal information becomes socially important requirement for participants of the information society.

If information security on a global scale and at the level of individual states is the subject of professional work of specialized departments, personal information security is an another growing issue.

In modern society information security is an essential component of national security. The level of economic, defense, social, political and other types of security largely depends on it.

Thus, information security creates conditions for the mental health of the individual and population in general, proper functioning of the state and public institutions, as well as formation of the individual and mass consciousness aimed at the progressive and sustainable development of societies and states.

References

1. Panarin I.N. Information Warfare and Geopolitics. – Moscow: Pokolenie, 2006. – 560 p.

2. Dulles A.V. The Secret Surrender. – New York: Harper & Row, 1966. – 268 p.

3. Grinyaev S.N. The Battlefield is a Cyberspace: Theory, Methods, Means and Systems of Information Warfare. – Minsk: Harvest, 2004. – 448 p.

4. Wilson C. Information Operations and Cyberwar: Capabilities and Related Policy Issues. CRS Report for Congress, 2006. // URL: https://fas.org/irp/crs/RL31787.pdf (reference date 07.02.2018).

5. Bedritsky A.V. Information War: Concepts and Their Implementation in the US. – Moscow: RISI, 2008. – 187 p.

6. A Shorthand Report on the Meeting of the President of the Russian Federation with Members of the Public on Issues of Patriotic Education of Youth. // URL: http://kremlin.ru/events/president/news/16470] (reference date 05.02.2018).

7. The Decree of the President of the Republic of Kazakhstan dated November 14, 2011 No.174 "On the Concept of Information Security of the Republic of Kazakhstan until 2016". // URL: http://adilet.zan.kz/rus/docs/U1100000174 (reference date 04.02.2018).