ABSTRACT

Mladonova A. D. Information warfare and security policy: information-legal dimension. Qualification scholarly paper: a manuscript.

Thesis submitted for obtaining the Doctor of Philosophy degree in Social and Behavioral Sciences, Speciality 052 – Political science. – V. N. Karazin Kharkiv National University, Minisry of Education and Science, Kharkiv, 2021.

The scientific novelty of our research topic is a comprehensive and systematic study of information warfare and information security means from the up-to-date theoretical and conceptual developments. Besides a significant array of scientific and information sources was introduced into scientific turnover, thus revealing the nature and peculiarities of the information warfare to the fullest extent. At present, the problems of the occurrence and development of information warfare and the development of effective mechanisms by states to prevent the harmful effects on the mass consciousness and mental state of citizens are insufficiently developed in present-day political science.

At present, the widespread use of the information warfare term is the absolute proof that humanity is entering a new "information" era. The main feature of this era is that information is gaining more and more material form, and its possession becomes the most crucial factor in making effective and efficient decisions both in public policy and in the private life of citizens. Under such conditions, the issue of information security becomes almost the most important problem from the point of view of state and human security.

The highlighted issues are also important for contemporary Ukraine. In our opinion, the most important issue is firstly related to the poor readiness of modern Ukrainian society to defend itself and be able to counteract any attempts to manipulate its consciousness; secondly, the lack of an effective system of state counteraction to the above manipulations.

In view of this, the development and improvement of the basics of information security is one of the most important tasks of the Ukrainian state.

Upon the research performed by the dissertator it was found that in modern society the term "information warfare" has gradually moved from the position of a sign-symbolic unit of publicist and political vocabulary to an independent category of scientific discourse. Since information warfare is a diversified and complex phenomenon of the today's world, this concept has many approaches thereto. Main approaches include as follows: socio-communicative, psychological and geopolitical. We believe that the psychological approach, grounded upon the information-psychological technologies of manipulating the consciousness of the masses, to be the basic and most fundamental one.

As for the means of information warfare, two groups are available. The first group is related to the conscientious nature of information warfare and has a direct impact on both the public opinion development and decision-making. Information warfare also contribute to the process of "reprogramming" of consciousness of the military and the civilians. The second group is focused on leveling the impact of information and information management systems of the enemy.

As for the types of information warfare, we should identify the following: psychological warfare; network warfare; cyber warfare; ideological sabotage; and electronic warfare.

In turn, the information warfare technologies can be divided into: software and computer, thus including technical means, as well as technologies and algorithms, aimed at striking computer systems of military and state control of the enemy. Such technologies include as follows: radio interception; linguistic means and methods of information impact; psychotropic means; rumors and gossip; proverbs, folk sayings and anecdotes; propaganda; censorship, etc.

As for the definition of the "information security" term, it provides primarily for the protection of the constitutional order, sovereignty and territorial integrity of the state via information means. According to the processed materials analysis, each country considers its specific national history and traditions, peculiarities of the management system, as well as its technical, scientific and economic potential, when forming its own system of information security. As for the context of information security systems classification, they can be divided into four types in our work: European; American; Russian; Chinese.

The main feature of the European information security system is that it is not effective at the legislative level due to the fact that Europeans are more concerned about the level of freedom of speech than the information security that ultimately complicates the construction of the efficient security system.

As for the American system of information security, unlike the European one, it is more advanced in terms of organization, legislation and technology. This is also facilitated by the fact that American society has a more restrained approach to freedom of speech and does not make it an absolute priority, as we see in Europe.

The peculiarities of the Russian information security system are, first of all, the priority of information security over freedom of speech; developed organizational structure, including several federal services and specialized departments of numerous ministries, etc. In terms of technical equipment, the Russian information security system is about the same level as the American system.

The main feature of the Chinese information security system is its unique technical support, based on the "Golden Shield" security system. This system effectively blocks any unwanted content on the Internet for the Chinese authorities.

The evolution of the Ukrainian information security system for over thirty years of our independence we have chronologically divided into three stages. The first stage is Domaidannyi (before the Maidan), covering the time interval from 1991 to 2004; the second stage is the period between the two Maidans - from 2004 to 2013; the third stage - the up-to-date one - lasts from 2013 to the present. As for the main types of information threats to the present-day Ukraine, they are divided into three main types: information warfare; cyber attacks aimed at damaging the information and material infrastructure of the opponent; cyber espionage to steal information that is not available to the public. As for the sources of information threats, they can be roughly classified as external, or created by external agents, and internal, created by internal agents.

When analyzing regulatory documents related to the legal regulation of information security policy in Ukraine, the researcher came to the conclusion that during the independence period a significant work related to information legislation development had been carried out. Thus, among the laws aimed at regulating the information sphere are the following: "On Information", "On Access to Public Information", "On the Fundamentals of Information Society Development in Ukraine during 2007-2015", "On the State Service of Special Communication and Information Protection of Ukraine", "On the National Information Program", "On the Concept of National Program of IT Development", "On Information Agencies", "On Information Protection in Information and Telecommunication Systems", "On Scientific and Technical Information", etc.

This paper also notes that the adoption of the Law of Ukraine "On the Fundamentals of Cyber Security of Ukraine" was a strong driver for the implementation of such modern European practices as information security management and auditing, application of industry standardized requirements for cyber protection of critical infrastructure.

Also, a basic conceptual and basic vocabulary of cyber security, namely the definition of critical infrastructure and its communication/technology systems: cyber attacks, cyber threats, cyber defense, cyber terrorism, cyber security was defined by the Law and introduced into the legal framework of Ukraine for the first time. In addition, over the past two years, a number of practical solutions have been implemented in terms of an effective organizational and technical model of cyber security development, in particular, the state cyber protection boundary has been established, the National Telecommunications Network is actively developing, and the Cyber Threat Response Center has been launched.

Along with the unequivocal positive aspects of domestic legislation on information security, the number of deficiencies and problematic issues that require urgent solutions are highlighted in this dissertation. They include, first of all, the spread of the process of regulatory and legal control of information security in numerous regulatory and legal acts of various legal powers. Another problem is the incompliance of regulatory legal acts with each other, as well as with the current Constitution of Ukraine. In this regard, the feasibility and timeliness of information legislation adjustment, its systematization, in particular through the adoption of the Information Code is justified in the present study.

Further ways of improving the legal regulation of information security of modern Ukraine are also considered: in identification or clarification of tasks, functions and powers of the information policy support entities; ensuring information sovereignty of Ukraine to eliminate and avoid information dependence and information expansion by other states and international structures; activation of international cooperation to use the other states experience related to the legal regulation improvement of information policy of our country.

In our opinion, an important trigger for the legislative system improvement of the Ukrainian state information security could be the development, adoption and implementation of:

a) the law on foreign agents and strict control of foreign agents by law enforcement agencies;

b) the defamation law, preventing the information field from false and fake information;

c) the legislative ban on media activities by any authorities, except judicial authorities;

d) the law on moratorium related to the media forced closure, etc.

The dissertator believes, the information warfare should be won not by bans (ineffective nowadays), but by the information content field.

Keywords: information warfare, information security, cybersecurity, state, regulatory act, computer system, freedom of speech, media.