INFORMATION INTERVENTIONS AS A NEW DIMENSION OF UKRAINE'S CYBER-VULNERABILITY

Ihor V. Diorditsa[1]
Armenui A. Telestakova[2]
Olga M. Koval[3]
Olha A. Nazarenko[4]
Andrii A. Nastiuk[5]

Abstract: In the article, the author analyzes information interventions as threats to the cybernetic security of Ukraine. The relevance of this study is due to the fact that large number of socially dangerous acts aimed at harming state interests can now be used both in the information space and in purely cyberspace. Since such actions are performed using computer systems and performed in cyberspace, we propose to define this type of intervention as "cybernetic intervention", describing it as a separate group of socially dangerous acts aimed at damaging the information infrastructure of States, vital areas of society's existence. The main aim of this study is to analyze information intervention as a threat to cyber security of Ukraine. The interpretation of terms that make up the conceptual and categorical apparatus of the subject of research is carried out. A narrow definition of the concept of "information intervention" is proposed as the violent intervention of one or more subjects of information relations in the activities of another or others, and a broad definition – a certain set of aggressive actions that are aimed at influencing public opinion and decision-making within one or another country and achieving clearly defined results. Negative consequences for the state caused by information interventions are defined. Attention is focused on the relationship between the

[1] Kyiv National University of Technologies and Design, Nemirovich-Danchenko Street, 2, Kyiv, 01011, Ukraine. E-mail: diorditsa-4@ust-hk.com.cn
[2] Kyiv National University of Technologies and Design, Nemirovich-Danchenko Street, 2, Kyiv, 01011, Ukraine
[3] Kyiv National University of Technologies and Design, Nemirovich-Danchenko Street, 2, Kyiv, 201011, Ukraine
[4] National Academy of Internal Affairs, Solomianska Square, 1, Kyiv, 03035, Ukraine.
[5] Academy of Labour, Social Relations and Tourism, Kiltseva doroha Street, 3-A, Kyiv, 03187, Ukraine.

concepts of “cyberwar” and “information intervention”.

Keywords: cyber security, hybrid warfare, cyberspace, information society of Ukraine, cyberwar.

Introduction

The formation and effective implementation of the state policy in the field of cybersecurity, in which is developed a complex of measures on legal and institutional framework – it is a necessary condition for the effective development of the cyber community in Ukraine. This complex of measures includes ensuring:

– the protection of vital interests of man and citizen, society and state,

– Ukraine's national interests in cyberspace,

– the formation and definition of the basic goals, directions and principles of this policy,

– the definition of the powers of state bodies, enterprises, institutions, organizations, entities and citizens in this sphere,

– the principles of state-private interaction and coordination of their activities on cyber security.

In the context of globalization of information processes and their integration into various spheres of public life, the leadership of the leading countries of the world is paying more and more attention to the creation and improvement of effective systems for both cyber defense and cybersecurity of critical infrastructure objects against external and internal threats of a cybernetic nature. Ukraine is entering a new era of information society – the era of information wars. Implementation of national interests to ensure national security is one of the most important directions of this transformation. So, in the text of the “Doctrine of information security of Ukraine”, which was adopted on 28 April 2014, but for unknown reasons cancelled in 2015, it was said that in the conditions of formation and development of information society in Ukraine and global information space, wide use of information and communication technologies in all spheres of life is of special importance to the problem of information (cyber) security.

A large number of socially dangerous acts aimed at harming state interests can now be used both in the

information space and in purely cyberspace. With the development of the information society, a certain direction of criminal intent to harm distant objects and encroach on objects that were previously virtually unattainable for such a large number of people has emerged. Committing attacks on state political and economic interests by interfering with the functioning of their participants and the institutions within which they operate, containing signs of intervention: violent interference in the interests of States and state authorities by other entities. Since such actions are performed using computer systems and performed in cyberspace, we propose to define this type of intervention as «cybernetic intervention», describing it as a separate group of socially dangerous acts aimed at damaging the information infrastructure of States, vital areas of society's existence. These and other factors determine the relevance of this study.

Certain aspects of the problem of information society formation have been studied in one way or another in the scientific works of local scientists, namely, the scientific school A. Lipkan (Lipkan and Cherepovsky, 2014; Lipkan, 2007; Baskakov, 2011; Zaliznyak, 2010; Loginov, 2005; Cherepovsky, 2013; Lipkan et al., 2006; Lipkan, 2010; Rudnik, 2015), in the works of I.V. Aristova (Aristova, 2000; Aristova 2002), V.S. Tsimbalyuk (Tsimbalyuk, 2004; Tsimbalyuk, 2010; Tsimbalyuk, 2011a; Tsimbalyuk, 2011b), I.V. Sopilko (Sopilko and Gurenko-Weitzman, 2011; Sopilko and Ponomarenko, 2013a; Sopilko and Ponomarenko, 2013b; Sopilko, 2013a; Sopilko, 2013b; Sopilko, 2015; Sopilko and Chuprina, 2013; Sopilko and Tunik, 2014) and others, however, despite the fact that the theory of the information society is in a certain way quite developed and presented with a variety of concepts, the issues of information intervention as a threat to cybernetic security is absolutely new, which causes the need for its detailed study. Special attention should be paid to the threats that exist in connection with the development of the information society in Ukraine. I will note separately the use of the works of political scientists, namely: G.G. Pocheptsov (Pocheptsov, 2013a; Pocheptsov, 2013b; Pocheptsov, 2014) and Ivanovsky (2008).

The purpose of this study is to analyze information intervention as a threat to cyber security. To achieve this

goal, the author formulated the tasks to carry out etymological analysis of the concepts that form the basis of the categorical series of this study, namely: information, intervention, threat, cybernetic and security, and then, by combining them, to realize the goal of the scientific groundwork.

Materials and Methods

The methodological basis of this study is a set of philosophical, general scientific, and special scientific methods that have their direct application in legal research. Among the general scientific methods that were used, the main one is the dialectical method of scientific knowledge, the use of which allowed us to study the continuous development, qualitative changes and the relationship between information interventions and state cybersecurity. Methods of legal linguistics, legal hermeneutics and logical-semantic analysis are used to clarify the content or formulation of the basic concepts of this study: “information”, “intervention”, “information intervention”, “information war”, “cyberwar”. The use of the system analysis method allowed us to establish the role of the information legislation of Ukraine as the legal basis of the state cyber policy in countering information interventions. The method of grouping and system-structural approach is used for classification distribution, clarification of the internal structure and analysis of the relationships of elements of information intervention, and methods of modeling, analysis and synthesis are used to develop proposals for countering information interventions.

The author's vision and solid scientific position is on the basis that science and its value lies in the prediction and formation of predictive models and scenarios for the development of various events with appropriate mechanisms of state response. With this approach, we do not lag behind, we do not respond, but we act proactively. Therefore, attempting to regulate existing cyber relations in the direction of protection against information interventions is always a fact finding of the past. Today, cyberspace is ahead of reality in its development, so the state's attempt to regulate these processes in some way should be based on predictive models and scenario approach, and not describe new phenomena with the help of only outdated matrices such as subject-object relations. That is why this research is

performed within the framework of administrative and information law, which are the most dynamic branches of law, reflecting the mobility of social relations inherent in the rapid development of society.

Important for this study is the comparative method, which was used to compare the principles, rules, techniques, methods and means of cognition of information interventions in the system of cybernetic relations, systemic properties of the cyber security system and the system of its legal regulation and the formation of theoretical scientific knowledge about them. The importance of this method is also confirmed by the study of cyber security practices from threats from information interventions at the international level, the study of the experience of developing national and international cybersecurity systems and the implementation of cybersecurity policy in the field of protection against information interventions in the context of civil society development and formation some tendencies towards deglobalization.

Results and Discussion

Information Intervention: Characteristics and Methods of Counteraction

Solving tasks, presented in this study, we analyzed the conceptual and categorical apparatus. First of all, let's define the concept of “information”. Using the explanatory dictionary of the Ukrainian language, we note that “information” means someone who is related to information containing information; who processes and issues information; refers to information as a newspaper and magazine genre that contains information, information about something; concerns information as a set of information or signals contained somewhere or transmitted from one object to another (Eroshenko, 2012). In my research, I will use the definition “informational” as something that concerns information. I also note that according to Ukrainian legislation, various actions can be performed with information: creation, collection, receipt, storage, use, distribution, protection and protection.

The next category is “intervention” – violent armed intervention of one or more states in the internal affairs of another state, aggression (Eroshenko, 2012).

Regarding the doctrinal interpretation of this term, I would like to note that intervention refers to the violent interference of one or more states in the internal affairs of another state, directed against its territorial integrity or political independence. In our time, such goals mean incompatibility with the purposes and principles of the UN Charter (The Charter of the United Nations…, 2005). In another source, we find a different interpretation: intervention (lat. interventio-interference) – interference of one or more states in the Affairs of another state or in its relations with third States (Tantsiura, 2008). Having analyzed, consolidated, and adapted these definitions prior to this study, I will define intervention as the violent intervention of one relationship subject in the activities (or Affairs) of another.

Also, in accordance with this and the previous term, the author's understanding of the term information intervention has been narrowed and simplified – the violent intervention of one or more subjects of information relations (since all actions take place when using information) in the activities of another or other subjects. Now the category of information intervention is studied and used by political scientists and politicians when writing various blogs, but it remains outside the legal regulation both at the national and international level. Therefore, this issue is relevant for the implementation of a comprehensive study in law and the promotion of reasonable proposals, primarily of a legal nature. There is a lot of discussion about what information intervention is and how to counteract it. To formulate a more comprehensive definition of "information intervention", we will analyze the scientific intelligence in which this category was of key interest.

Information intervention is defined as:

1) a set of purposeful, time-coordinated measures that ensure the presentation of mass tendentious information by distribution and telecommunications channels in a predetermined mode or its interpretation in the desired perspective in order to influence public opinion and decision-making in another state. As well as information technologies and information technology and equipment of foreign production, consumers of which are residents of the country-the object of information intervention (Ivanovsky, 2008);

2) biased information when subjective facts and subjective information that influence public opinion and decision-making in another state are distributed through communication systems. Within the framework of information intervention, information is manipulated to achieve a certain goal (Brahmann, 2012). It is difficult to agree with this definition, since, as mentioned above, intervention is an intervention, that is, certain active actions that are illegal, but not the object;

3) cybernetic intervention (as a specific concept to a generic one – information intervention) should be understood as a set of aggressive actions in cyberspace aimed at interfering through the use of information and computer technologies in the internal and external affairs of states in order to harm their sovereignty or the proper functioning of their governing bodies, or the main spheres of life, and, consequently, similar actions with respect to the orderly activities of interstate associations and their governing bodies (Savinova, 2012). In my opinion, this interpretation is very reasonable.

Thus, after conducting a content analysis of these and other definitions, we note that "information intervention" in a broad sense should be understood as a certain set of actions of an aggressive nature (aggression is outside the law), which are aimed at influencing public opinion and decision-making within one or another country and achieving clearly defined results. I also note that this phenomenon always has a negative manifestation.

Having analyzed and synthesized the situation in the information space of Ukraine, it is possible to divide information intervention into:

– spiritual (a set of purposeful, time-coordinated measures that ensure the presentation of mass tendentious information by distribution and telecommunications channels in a predetermined mode or its interpretation in the desired perspective in order to influence public opinion and decision-making in another state);

– material (information technologies and information technology and equipment of foreign production, which consumers are residents of the country-object of information intervention) (Ivanovsky, 2008).

Until 2016, there was no mechanism to counter this phenomenon, so as a result, the Ukrainian information space remained open and defenseless, which other countries took advantage of, using it in their own interests. As an example, we can recall the presence of Russian TV channels such as “Russia Today”, “Dozhd”, “Sputnik”. The presence of foreign broadcasters in the radio space of Ukraine is also significant. Russian radio and Mayak (Russia), Voice of America and Svoboda (USA), air force (UK), and others are known to Ukrainian listeners (The world of radio, 2016).

Both TV and radio stations often broadcast Ukrainian and foreign news (information), but with a certain “distortion” and, as a result, its erroneous use or forgery, distortions and distortions lead to large losses. This is facilitated by the absence of an Information code that would systematize the totality of legal norms that regulate the entire range of public information relations. Taking into account that each TV channel, publishing house and other media outlets belong to a certain person, there is absolutely no possibility of objective and comprehensive coverage of events in this case.

Today, in addition to the above examples, we can also talk about the «spiral of silence», when the mass media can manipulate public opinion by giving the floor to minority representatives and silencing the majority opinions, as well as by analyzing the processes of formation and functioning of public opinion. It is at the intersection of the influence of mass communication and the feedback of individuals that interaction is born, which changes public opinion. Since the delivery of information to consumers through the media is metered and with a clearly defined purpose, not for the purpose of familiarization, but with already formed and imposed conclusions, then, in this case, there is a certain manipulation of public opinion and the formation of prerequisites for preventing the development of an independent vision and the formation of their own opinion about certain events. This situation is favorable for mass intimidation or the allocation of “negative” and “superfluous” characters both in politics and in other spheres of public life (Rudnik, 2015).

An example of internal, even Soviet interventions should be considered TV shows Kashpirovsky and

Chumak, which "disconnected" the population from the problems of our time. Internal information intervention is also the "View" program of the perestroika period. That is, first the program "Vzgliad" was created for some purposes, and then began to function for others. But at that time it was already promoted as an interesting information product (Pocheptsov, 2014). Today, such information interventions often accompany election campaigns, trying to fundamentally change their course by reinterpreting the actions of their opponent (Pocheptsov, 2013a). It is worth noting that the presence of foreign media, especially electronic media, in the information space of Ukraine is quite high. On the one hand, this helps to diversify sources of information, develop a competitive environment in the media market, improve the quality of TV and radio programs, and on the other – creates opportunities for forming public opinion in Ukraine in the interests of foreign countries and "blind" adherence to imposed ideals and absolute unwillingness or inability to analyze.

It should be noted that if criminal intervention can take place only if an encroachment crosses physical state borders, then information intervention – an intervention in an information space that does not have physical borders that separate States from each other, can be either external (from the territory of another state or an interstate Association) or internal (from the territory of one's own state or an interstate Association). If information intervention is carried out with the participation of different States, it should be characterized as mixed. I would also like to emphasize that information intervention can be defined as the beginning of an information war. As you know, information wars are actions initiated to achieve information advantage by damaging information and processes based on information and information systems of the enemy while protecting their own information and processes based on information and information systems (Sopilko, 2015).

Ukrainian experts list such information wars that Ukraine has recently come under fire for:

– promoting the idea of racism in Ukraine before the start of the Euro 2012 football championship;

– glorifying Russian President Vladimir Putin in Ukraine;

– discrediting the European choice by focusing on issues of homosexuality;
– intimidating scenarios of war with Russia; maintaining an anti-Ukrainian thesis about the collapse of the Ukrainian state, spreading the concept of failed state in Ukraine;
– information counteraction to Russia in the field of arms trade.

We can also add the promotion of the idea of anti-Semitism in Ukraine in connection with the speeches of representatives of the political party "Svoboda", which for some reason were always accompanied by the presence of Russian media, which immediately replicated information about anti-Semitism in Ukraine (Pocheptsov, 2013b). My analysis of statistical data provides an opportunity to state that at present the greatest attention of criminals is focused on attempts to disrupt the operation or unauthorized use of the information systems of the state, credit-banking, utilities, defense, and manufacturing sectors. Information with limited access, which circulates in national information resources, is a stable object of interest from other states, organizations and individuals. In addition, politically motivated activities in cyberspace of groups of activists (hacktivists) that attack government and private sites, which leads to violations of information resources, as well as reputational and material losses, are becoming more widespread.

Taking into account the wide informatization of the security sphere, in particular the creation of a Unified automated control system for the armed forces of Ukraine, the defense potential of our state is becoming more sensitive to cyber threats. The introduction of modern cyber weapons by leading countries turns cyberspace into a separate sphere of warfare, along with the traditional "Land", "Air", "Sea", and "Space". In the near future, the level of the country's defense capability will be determined, including the presence of effective units for conducting combat operations in cyberspace and the ability to resist cyber threats in the field of defense. Therefore, the problem of creating Information troops in Ukraine is urgent.

Threats of Informational Enterference in Ensuring State Cybersecurity

In a global open society, what is the information society, cybernetic

(information – Auth.) intervention can have not only global consequences, which will directly consist in actions, but also be characterized by global features: the possibility of joint participation in the intervention of an unlimited number of subjects that are significantly removed from each other in relation to a certain object, or in relation to an unlimited number of objects at the same time. Similarly, it is possible to simultaneously commit cybercrimes with the aim of intervening up to a large number of objects or one extremely important, including a strategic object. Given the ability to do this outside borders at any distance, so the increased threat to cyber security becomes indisputable. Unfortunately, there is direct evidence of existing facts of cybernetic intervention, allowing us to establish the existence of such an intervention.

The simplest example of a cyber intervention is a three-day continuous cyber attack on the website of the President of Ukraine. A. Yushchenko, which began on October 30, 2007 and consisted of about 18 thousand targeted attacks that were made from the territory of the Russian Federation, Kazakhstan, Ukraine, the United States, Israel and the United Kingdom. However, such actions do not cause much surprise for the security services, because the websites of presidents of different countries of the world are constantly exposed to such hacker attacks. Hackers from "ESM" claim that after Yushchenko's site, they will "lay" the SSU's site (ESM hackers say…, 2007).

The threat to cyber security in the form of information intervention may not only be external. Ukrainian hackers also participate in cyber wars. So, after the events surrounding the act of vandalism on Hoverla (Eurasian Youth Union destroyed…, 2007), the sites of the Eurasian youth Union, which took responsibility for their conduct, were attacked from Ukraine. In response, the websites of the President of Ukraine and the SBU were attacked. A more modern example is the hacker activity of 2014-2019:

– the website of the Ministry of regional development was hacked by hackers – the press service of the Department on 27.12.2014 (The site of the Minregion…, 2014);

– hackers hacked the Twitter of the presidential Administration of Ukraine

on 14.07.2015 (Hackers have cracked…, 2015);

– the website of the President of Ukraine suspended work and issues errors on 20.07.2015 (The site of the President…, 2015);

– on December 6, a hacker attack on the internal telecommunication networks of the Ministry of Finance, the State Treasury, the Pension Fund, which disrupted a number of computers and destroyed critical databases, resulted in the delay of budget payments by hundreds of millions of hryvnia on 06.12.2016 (The biggest cyber-attacks…, 2017);

– computer virus ransomware Petya. A., similar to Wanna Cry attacked Ukrainian banks, public and private companies, called it the National Bank of Ukraine's largest “hacker” attack on 27.06.2017 (Korinovskaya, 2017);

– According to Cisco, a new virus VPNFilter has appeared in the world and this time the main purpose of cyberattacks was the routers of Ukrainian users on 29.05.2018 (Pashinska, 2018);

– for 2019 CERT-UA registered 330 cyber-incidents related to cyber-attacks on the websites of public authorities of Ukraine (Carter, 2020), etc.

Cyber-attacks on official websites of top government agencies are not limited to examples of attacks on websites of presidents and high-level government agencies. Computer systems of all branches of government around the world are attacked: attacks are carried out to obstruct the activities of the Prosecutor's office; to falsify voter lists and falsify the counting of votes in elections, respectively, encroaching on the functions of the public prosecution or the will of the people, which is an integral part of the state's sovereignty. It is impossible not to pay special attention to the possibility of directing cybernetic intervention into the militaristic sphere. Modern militaristic war is impossible without the use of information and computer technologies-ICT.

It should be emphasized that in the case of targeted cyber intervention to seize control of such an Arsenal, and this is not excluded in the context of the dynamics of ICT and it development, such an attack or certain elements of it can be used by criminals for their will against the internal and external interests of the state or cyber security, in

particular, or an interstate Association at the discretion of criminals. Individual crimes may be committed as part of an information intervention, and may result, at a minimum, in the loss of orientation of high-precision weapons or loss of communication with control points. The possibility of information intervention is determined by the state of development of ICT and their implementation in all spheres of life of modern society.

Information intervention is primarily directed at information computer technologies that ensure the proper functioning of society's life support systems, and this, structurally, is a defining feature of information intervention as a specific group of crimes that pose threats to the development of the information society. Social risks that can create an objective threat to the national security of so-called donor countries, i.e. countries that are subject to information intervention, are particularly dangerous. In the context of the spread of global globalization processes, the cybernetic spaces of different States interact, penetrating one into one, and mutually converge. The downside of this is the dangers associated with the complexity of state control and ordering of these self – organizing processes, which are most affected by the so-called weak States-the States of the information periphery.

First, these States have significantly less technical and technological capabilities and resources than well-developed ones. The information center is gradually moving away to such a distance that in fact the competition of information technologies may already become an unattainable goal, Competition will no longer occur at the level of States, but at the level of transnational corporations. Thus, the development of cyberspace in general threatens the existence of such an institution as the state.

Secondly, the state information policy of the information countries of the periphery is imperfect, properly unformulated, and under the slogans of democracy and free access of citizens to public information lies the inability of public authorities to ensure the implementation of cybernetic and information rights of their own citizens.

Third, the level of general information culture, including media and information culture, not only of the population of the respective countries, but also of the society as a whole is too low.

Therefore, the information space of these countries is almost not protected from information intervention, the spread of unauthorized, foreign media products produced by technologically more powerful aggressor States, and they themselves and their populations are excessively vulnerable to media consumption, especially in the cybernetic space.

Information intervention entails extremely dangerous consequences:

– it restricts the state sovereignty of countries;

– their dependence on the world, international situation, that is, formats the development of the country under a pre-developed foreign algorithm, which partly does not correspond to the national interests of this country;

– unifies their culture, that is, brings it under the standards imposed by manipulators: violation of traditions leads to loss of self-identification;

– turns them into hostages of world political, economic, financial events and crises (energy prices and fuel, environmental problems, etc.);

– compels unprofitable international cooperation;

– imposes low-quality, foreign media products (foreign ideas, standards, norms of life, media violence, pornography, etc.).

As a result, the national information space is replaced by its own, national that strengthens the nation, guarantees its identity (Petrunko, 2013). The emergence of new media has facilitated the process of international information interventions, because they create an information and communication space in which all exchange processes are accelerated. The state apparatus is not able to react and predict the possible consequences of such interventions. And almost at every step he loses (Pocheptsov, 2014).

Both open and closed systems may be subject to information interventions. Closed systems are more afraid of them, because interventions block alternative meanings, so when they fall into their information field, closed systems cannot withstand the impact. After all, it is the meanings to which this system is most sensitive that are blocked. This is how the Soviet Union «fell» when it was bombed with harmful meanings. But perestroika was also different in that this semantic bombardment was done by the government itself, only partly it was

about external information interventions. Information interventions in a closed system, as demonstrated by Perestroika, try to combine with those subjects and objects that were prohibited in this system. This creates mechanisms for self-expanding such information after it has been introduced from the outside (Pocheptsov, 2013b).

As a result of improper legal regulation in the national information space of Ukraine, there are a number of negative phenomena that create real and potential threats to cyber security. In 2014, on the territory of the Autonomous Republic of Crimea and in the South-Eastern regions of Ukraine, information and psychological pressure was exerted on the population of Ukraine by the mass media of the Russian Federation, and information expansion (or intervention) was observed. – Auth.) in the national information space of Ukraine, strategic objects of the Ukrainian telecommunications infrastructure were attracted.

Shared scientific position that to prevent abuse of information and the protection of information rights the modern state of national and cyber security of Ukraine requires:

– the development of evidence-based public policy and strategy in this area;

– the definition of the system of national values, vital interests of personality, society and state;

– the definition of external and internal threats to these interests;

– the search for effective measures to ensure safety in all areas;

– protection against information threats;

– the realization of the right to receive reliable information.

In parallel, all of the above indicates the need to adopt legal acts that would provide a mechanism for protecting information rights from illegal actions of third parties in relation to information (Sopilko, 2015). At the same time, in a broad sense, the ideology of cybernetic intervention in the information society is characterized by a different idea, separated from the idea of ordinary cybercrime, which is aimed, as well as criminal criminality, primarily at obtaining a certain material benefit. It is obvious that in the context of the development of the information society, the issues of criminalization of information intervention should be

violated at the international level on the initiative of individual States. However, the initiative to introduce appropriate criminal law policy measures should be mainly international in nature: at the level of model conventions, and, obviously, common strategies between countries of cooperative associations (NATO, EU) (Savinova, 2012).

Cyberspace has become an arena of struggle between the subjects of international relations. In these conditions, in addition to information intervention, the term “cyberwar” has become more widespread and widespread. However, this term is not well-established. Researchers and experts offer a wide range of definitions of cyberwar, in particular:

– cyberwar is a well-coordinated digital attack by one state aimed at infiltrating the computers and networks of another state in order to cause harm or destruction;

– cyberwar – a conflict involving the use of hostile, illegal attacks on computers and networks in order to destroy communications and other infrastructure elements as a mechanism for causing economic damage or undermining the country's defense system;

– cyberwar is the use of computer technologies and the Internet by one state, or with its direct support, against another state, directed against its security and defense, which is so intense and serious that it poses a real threat to the security and sovereignty of this other state (Zaporozhets, 2014).

Despite the fact that the content of these phenomena was analyzed above in the work, the author only indicated the existence of this period. I do not exclude that in the framework of subsequent security and information and legal studies, this term will acquire its corresponding scientific reflection, including in view of the lack of conceptualization of the concept of «hybrid war». After all, its wide application in normative acts and also in standard-design documents, speeches of state officials require the presence of a legal content for this concept. Therefore, this is also, the author is convinced, a separate and interesting, very necessary layer of scientific research (Tolubko, 2015; Cyber security strategy of Ukraine, 2016). There were no comprehensive statistical studies in this regard. But back in 1984, Fred Cohen (1984) in the work “Computer Viruses:

theory and experiments", devoted to the mathematical foundations of virus technology, proved that the set of all possible malignant codes is infinite, it follows that the set of attacks themselves is infinite.

Conclusion

The military sphere is undergoing almost the most dramatic changes due to the development of global cyberspace and the information landscape in general. Most of the world's countries are actively transforming their defense capabilities in the direction of enhancing cyber capabilities for combat operations and protection from similar actions by the enemy, as new types of threats become more and more relevant. Taking into account the wide Informatization of the security and defense sector, in particular, the creation of a Unified automated control system for the armed forces of Ukraine, the defense potential of our state is becoming more sensitive to cyber threats. The introduction of modern cyber weapons by leading countries turns cyberspace into a separate sphere of warfare, along with the traditional "Land", "Air", "Sea", and "Space". In the near future, the level of the country's defense capability will be determined, including the presence of effective units for conducting combat operations in cyberspace and the ability to resist cyber threats not only in the sphere of defense, but in all spheres of life.

In a narrow and simplified sense, information intervention is the violent intervention of one or more subjects of information relations in the activities of another or others, and in a broad sense-a certain set of aggressive actions that are aimed at influencing public opinion and decision-making within one or another country and achieving clearly defined results. This phenomenon always has a negative manifestation. Information interventions constitute a significant threat to cyber security, since the latter is part of national security and can harm both the state as a whole and individual individuals. Creating an effective system for ensuring cyber security requires Ukrainian state authorities to clearly define the legal basis of state policy in this area and to respond promptly to the dynamic changes taking place in the world in the field of cyber security with the possibility of applying international experience.

The choice of specific means and methods of ensuring cyber security of Ukraine is caused by the need for timely action, appropriate to the nature and scale of real and potential cyber threats to the vital interests of man and citizen, society and state. I note that there is still no general quantitative assessment of the types of cyber attacks and methods of their use.

References

Aristova IV. (2000). State information policy: organizational and legal aspects. Kharkiv: Univ. Affairs.

Aristova IV. (2002). State information policy and its implementation in the activity of law-enforcement bodies of Ukraine: organizational and legal bases. Kharkiv: National University of Internal Affairs.

Baskakov V. (2011). Restricted information: concepts and features. Kyiv: FOP Lipkan OS.

Brahmann Z. (2012). Information wars: theory, PR, public relations, diplomacy. https://politiko.ua/blogpost82707.

Carter S. (2020). In 2019, more than 300 cyber-incidents have been registered in connection with attacks on Ukrainian authorities. UNN. https://www.unn.com.ua/uk/exclusive/1848123-u-2019-rotsi-zareyestrovano-bilshe-300-kiberintsidentiv-povyazanikh-z-atakami-na-sayti-organiv-vladi-ukrayini .

Cherepovsky KP. (2013). Incorporation of information legislation of Ukraine. Zaporizhzhya: Zaporizhzhya National University.

Cyber security strategy of Ukraine (2016). https://zakon.rada.gov.ua/laws/show/96/2016.

Eroshenko O. (2012). The great interpretive dictionary of modern Ukrainian. Donetsk: Gloria Trade.

ESM hackers say they will "lay down" the SBU site following Yushchenko's website. (2007). Unian. http://www.unian.ua/politics/73946-hakeri-z-esm-zayavlyayut-scho-slidom-za-saytom-yuschenka-polojat-sayt-sbu.html.

Eurasian Youth Union destroyed the Coat of Arms of Ukraine on the top of Goverla. (2007). http://korrespondent.net/ukraine/events/212658-evrazijskij-soyuz-molodezhi-unichtozhil-gerb-ukrainy-na-vershine-goverly.

Hackers have cracked Twitter Administration of the President of Ukraine. (2015). TSN. http://ru.tsn.ua/ukrayina/hakery-vzlomali-

twitter-administracii-prezidenta-ukrainy-451401.html.

Ivanovsky VV. (2008). Structure of information intervention in Ukrainian society. Bulletin of Zhytomyr State University, 40, 37-40.

Korinovskaya NV. (2017). Dozens of companies and institutions have been attacked by a computer virus in Ukraine. Hromadske. https://hromadske.ua/posts/ukrposhtu-ukrenerho-ta-banky-atakuvav-podibnyi-do-wannacry-virus.

Lipkan VA. (2010). White paper theoretical concept. Entrepreneurship, Economy and Law, 9, 80-83.

Lipkan VA. (Ed.). (2007). Management theory in law enforcement. Kyiv: CST.

Lipkan VA, Cherepovsky KP. (2014). Incorporation of the information legislation of Ukraine. Kyiv: O.S. Lipkan.

Lipkan VA, Maksimenko YuE, Zhelikhovsky VM. (2006). Information security of Ukraine in the context of European integration. Kyiv: CST.

Loginov OV. (2005). Administrative and legal support of information security of executive authorities. Kyiv: National Academy of Internal Affairs of Ukraine.

Pashinska A. (2018). New cyberattack in Ukraine: what is a VPNFilter virus and how to fight it. Espresso. https://espreso.tv/article/2018/05/29/nova_kiberataka_na_ukrayinu_scho_take_virus_vpnfilter_i_yak_z_nym_borotysya.

Petrunko OV. (2013). Socialization resources and risks of an aggressive media environment. http://elibrary.kubg.edu.ua/id/eprint/2638/.

Pocheptsov G. (2013a). Internal information interventions. http://osvita.mediasapiens.ua/ethics/manipulation/vnutrishni_informatsiyni_interventsii/.

Pocheptsov G. (2013b). Information wars in closed and open systems. https://ms.detector.media/manipulyatsii/post/3642/2013-06-30-informatsiini-viini-v-zakritikh-i-vidkritikh-sistemakh/.

Pocheptsov G. (2014). New media as a means of international information interventions. https://ms.detector.media/manipulyatsii/post/5214/2013-01-06-novi-media-yak-zasib-mizhnarodnikh-informatsiinikh-interventsii/.

Rudnik LI. (2015). Right to access information. Kyiv: National University of

Life and Environmental Sciences of Ukraine.

Savinova N. (2012). Cybernetic intervention: on issues of origin and need of criminalization in the conditions of formation and development of information society. In E Sadowska (Ed.), Innovation, law and political science in warping (pp. 61-70). Czestochowa: Wyzsza Linguistic Szcoly.

Sopilko IM. (2013a). Methodological aspects of cybersecurity policy. Imperatives of Civilization Development, 1, 63-65.

Sopilko IM. (2013b). Scientific bases of cybersecurity policy of Ukraine. Lex Russica (Russian Law), 5(78), 521-527.

Sopilko IM. (2015). Information threats and security of modern Ukrainian society. Legal Bulletin, 1(34), 75-80.

Sopilko IM, Chuprina OV. (2013). Administrative responsibility for violation of the right to information. Kyiv: Computer Press.

Sopilko IM, Gurenko-Weitzman MM. (2011). Legal regulation of relations regarding the receipt of information by public authorities. Simferopol: Krymnavchpeddervizd.

Sopilko IM, Ponomarenko OV. (2013a). Copyright protection on the Internet: problems of theory and practice. Kyiv: Lesya.

Sopilko IM, Ponomarenko, OV. (2013b). Copyright protection on the Internet. Kyiv: Computer Press.

Sopilko IM, Tunik AW. (2014). Legal regulation of personal data protection in Ukraine: a comparative legal study. Kyiv: Lesya.

Tantsiura VI. (Ed.). (2008). Political history of Ukraine. Kyiv: Academic.

The biggest cyber-attacks against Ukraine since 2014. Infographics. (2017). NV. https://nv.ua/ukr/ukraine/events/najbilshi-kiberataki-proti-ukrajini-z-2014-roku-infografika-1438924.html.

The Charter of the United Nations and the Statute of the Tribunal. (2005). http://zakon4.rada.gov.ua/laws/show/995_010.

The site of the Minregion was hacked – the press service of the department. (2014). http://korrespondent.net/ukraine/3461338-sait-mynrehyona-byl-vzloman-khakeramy-press-sluzhba-vedomstva.

The site of the President of Ukraine has stopped working and gives an error. (2015). http://rian.com.ua/politics/20150720/370831489.html.

The world of radio. (2016). http://www.proradio.org.ua/wire/.

Tolubko VB. (2015). Information and cyber security: the social aspect. Kyiv: DUT.

Tsimbalyuk VS. (2010). Information law (fundamentals of theory and practice). Kyiv: Education of Ukraine.

Tsimbalyuk VS. (2011a). Information law: conceptual provisions for the codification of information law. Kyiv: Education of Ukraine.

Tsimbalyuk VS. (2011b). The concept of codification of the legislation of Ukraine on information. Kyiv: FOP Lipkan O.S.

Tsimbalyuk VS. (Ed.). (2004). Fundamentals of information law of Ukraine. Kyiv: Znannya.

Zaliznyak VA. (2010). Legal regulation of the right to information. Entrepreneurship, Economy and Law, 8, 69-72.

Zaporozhets O. (2014). Cyberwar: conceptual dimension. Actual Problems of International Relations, 121(1), 80-86.

Cohen F. (1984). Computer Viruses: theory and experiments. EECS at Michigan. https://web.eecs.umich.edu/~aprakash/eecs588/handouts/cohen-viruses.html