Lex Humana, v. 16, n.1, 2024, ISSN 2175-0947

INFORMATION SECURITY OF THE STATE: MOTIVES, NECESSITY, AND SUFFICIENCY CRITERIA

SEGURANÇA DA INFORMAÇÃO DO ESTADO: MOTIVOS, NECESSIDADE E CRITÉRIOS DE SUFICIÊNCIA

OLENA BORTNIKOVA
Diplomatic Academy of Ukraine named after Hennadii Udovenko, Kyiv, Ukraine
bortnikovalena11@gmail.com

DARIA KASHPERSKA
Taras Shevchenko National University of Kyiv, Kyiv, Ukraine
dkashperska@gmail.com

OLEKSANDR LEONOV
Kyiv National Economic University named after Vadym Hetman, Kyiv, Ukraine
578original@gmail.com

KARINA RUBEL
Military Academy named after Yevheniy Bereznyak, Kyiv, Ukraine
karinaroobel@gmail.com

OLEKSANDR CHUMAK
National Technical University of Ukraine "Igor Sikorsky Kyiv Polytechnic Institute", Kyiv, Ukraine
a_ch_i@ukr.net

Received: 08 Aug 2023

Accepted: 15 Nov 2023

Published: 10 Dec 2023

Corresponding author:
bortnikovalena11@gmail.com

Abstract: The scientific study of the motives, the degree of necessity, and the criteria of sufficiency of state information security included several research areas. First of all, the authors established that state information security is a component of the national security of any country. This part of the work of state bodies has a regulatory and normative basis, a developed professional apparatus, and institutions that collect and disseminate information. Since the beginning of the development of digital technologies in the late XX - early XXI century, the world has experienced an information revolution. This revolution was made possible by the invention of the Internet and the expansion of the sphere of influence of actors on society and its interests, as well as on the perception of reality. The study establishes the chronology of the formation of information threats to the country and society by creating a model of growing danger and, accordingly, the reaction of the state and law enforcement agencies to increasing problems in an information space. The article identifies the motives for the formation of events defined in space and time due to information noise, information chaos, information fake, information warfare, and information terrorism. The authors outline the criteria for responding to each level of information threat with appropriate actions. In addition, they identify the requirements for the sufficiency of the state's response to information threats of various kinds, taking into account the following principles: legality, the primacy of international law over national legislation, property rights in the process of ensuring information security, economic feasibility of database protection, impartiality, and continuity. The level, scope, and extent of the state's defense of its population and society is still controversial. This can violate the rights and freedoms of people and citizens established by the state. The study was conducted using general and special methods. The general methods used include the dialectical method, which is based on fairness, comprehensive research, and the use of the systematic nature of scientific knowledge; the logical method in presenting materials; the functional method in

combining parts of the study with its main topic; the systemic and structural method in forming integral parts of hypothesis proof. Special methods of scientific knowledge include: historical method when studying the sequential development of information threats; the method of system analysis when comparing information threats and the state response to their elimination; generalization of regulatory and practical materials when conducting research.

Keywords: Information security. Information threat. Motives for information protection. Criteria for data protection. Information warfare. Information terrorism.

Resumo: O estudo científico dos motivos, do grau de necessidade e dos critérios de suficiência da segurança da informação estatal incluiu diversas áreas de pesquisa. Em primeiro lugar, os autores estabeleceram que a segurança da informação estatal é um componente da segurança nacional de qualquer país. Esta parte do trabalho dos órgãos estatais tem base regulatória e normativa, um aparato profissional desenvolvido e instituições que coletam e divulgam informações. Desde o início do desenvolvimento das tecnologias digitais no final do século XX - início do século XXI, o mundo passou por uma revolução da informação. Esta revolução foi possível graças à invenção da Internet e à ampliação da esfera de influência dos atores na sociedade e nos seus interesses, bem como na percepção da realidade. O estudo estabelece a cronologia da formação de ameaças informacionais ao país e à sociedade, criando um modelo de perigo crescente e, consequentemente, a reação do Estado e das agências de aplicação da lei aos problemas crescentes no espaço de informação. O artigo identifica os motivos para a formação de eventos definidos no espaço e no tempo devido ao ruído informacional, ao caos informacional, à falsificação de informações, à guerra de informação e ao terrorismo informacional. Os autores descrevem os critérios para responder a cada nível de ameaça à informação com ações apropriadas. Além disso, identificam os requisitos para a suficiência da resposta do Estado às ameaças de informação de vários tipos, tendo em conta os seguintes princípios: legalidade, primazia do direito internacional sobre a legislação nacional, direitos de propriedade no processo de garantia da segurança da informação, economia viabilidade da proteção, imparcialidade e continuidade do banco de dados. O nível, o âmbito e a extensão da defesa do Estado da sua população e da sociedade ainda são controversos. Isto pode violar os direitos e liberdades das pessoas e dos cidadãos estabelecidos pelo Estado. O estudo foi conduzido utilizando métodos gerais e especiais. Os métodos gerais utilizados incluem o método dialético, que se baseia na justiça, na pesquisa abrangente e no uso da natureza sistemática do conhecimento científico; o método lógico na apresentação dos materiais; o método funcional na combinação de partes do estudo com seu tema principal; o método sistêmico e estrutural na formação de partes integrantes da prova de hipóteses. Os métodos especiais de conhecimento científico incluem: método histórico no estudo do desenvolvimento sequencial de ameaças à informação; o método de análise do sistema ao comparar ameaças à informação e a resposta do Estado à sua eliminação; generalização de materiais normativos e práticos na realização de pesquisas.

Palavras-chave: Segurança da informação. Ameaça de informação. Motivos para proteção da informação. Critérios para proteção de dados. Guerra de informação. Terrorismo da informação.

1. Introduction

Since 1991, the information warfare problem has been frequently raised in both publicistic and scientific literature. O. Krynina points to this, emphasizing especially their ideological and psychological components (Krynina, 2009, p. 69). In our opinion, the methods of such wars were actualized in the late XX - early XXI century for three main reasons:

1) the build-up of nuclear potential by some countries and the direct threat of its use against other territories carries the danger of destruction of all life on the planet. So far, such threats have been voiced only in the informational space;

2) increasing digitalization and computerization of society, widespread Internet use, which has become a revolutionary breakthrough in access to various information for users, including classified information;

3) a comparative cheapness of information warfare compared to real positional military operations and their higher efficiency of destruction (once again, we return to access to classified information and the use of public (social) space to introduce disinformation narratives).

These three aspects are incentives for spreading and continuously improving information aggression technologies. As a result, the state has an increasing need to ensure its information security and formulate appropriate policies both in the national and foreign space.

2. Literature review

The informational development of society, which began in the 1970s and was shaped by new technological revolutionary breakthroughs, attracted researchers in many fields, both directly and indirectly related to the information space. The direct studies that have become the basis for our research include the studies by Yu. Bondar, K. Vetrov, V. Voznyuk, E. Voznyuk, E. Kobko, V. Kolyadenko, O. Krynina, V. Lukyanova, A. Lautar, L. Lyubokhinets, O. Oliinyk, O. Poplavskaia, H. Pocheptsova, and S. Chukuta. The research by V. Bakumenko, E. Voznyuk, V. Knyazeva, V. Kolesnyk, A. Moskalenko, and N. Nychiporchuk became helpful in the field of information policy and state security. Although we recognize the scientific achievements of these scientists, we should take a deeper look at the motives and criteria for the sufficiency of the state information security system.

3. Aims

This research aims to examine several aspects and draw some general conclusions. First, it is necessary to study the essence of the information dangers and threats posed by the XXI century to the state and society's general existence. Then, it is essential to determine the motivations and the need to protect information borders and resources that affect the state's rating and security in the international space. Furthermore, it is crucial to outline the criteria for the sufficiency of state measures to ensure information security.

4. Methods

The methodological basis of the paper is a set of cognitive methods applied to the state information security system. The study was conducted using general and special methods. The general methods used include the following:

– the dialectical method is based on fairness, comprehensive study, and the use of the systematic nature of scientific knowledge.

– the logical method in presenting materials.

– the functional method combines parts of the study with its main topic.

– systematic and structural methods in forming integral parts of the hypothesis proof.

– the special methods of scientific cognition include:

– the historical method when studying the sequential development of information threats.

– the method of system analysis when comparing information threats and the state's response to their elimination.

– generalization of regulatory and practical materials when conducting research.

5. Results

In practically all civilized countries, national security has become a mandatory component, a specific imperative of foreign and national policy and military affairs. However, the concept of national security remains a term with many meanings. In American political science, national security is defined as the long-term preservation of values or systems and the absence of threats. It can be defined as a policy that provides social groups with autonomy, a certain level of political status, and a certain minimum expected level of good existence rather than just the physical survival

of people within national borders. At the same time, national security is traditionally considered a system of optimized relationships between possible societal threats and available resources to counter these threats, mediated by an information component. Societal threats always exist, and the level of protection against them never reaches sufficiency. Thus, national security is a mechanism for achieving and maintaining a balance between specific and concealed threats on the one hand and the subject's ability to counteract them on the other. V. Kolesnyk emphasizes that the threats to the current national security of Ukraine are a combination of conditions and factors that pose a danger to the vital interests of individuals, society, and the state (i.e., harm, destruction, or change them). According to the author, real and potential threats to the objects of national security in Ukraine come from internal and external sources. Therefore, they determine the course of the state's actions in terms of methods of influencing internal and external security (Kolesnyk, 2015, p. 169). Regarding its content, national security is a complex multi-aspect concept and includes the following types of security (Figure 1).

Among national security principles, the state's information security has been gaining increasing importance in recent times. All countries are transitioning from agrarian to industrial and then to information societies. Each stage's levers of influence (production forces and key components) are fundamentally different elements. The first one is land, the second is automobiles, and the third is information. In modern society, many entities are involved in processing and transforming data. Today, humanity has entered the information civilization. Therefore, countries like Japan, for example, can afford to replenish their budget and shape their GDP through the production and sale of information exclusively.

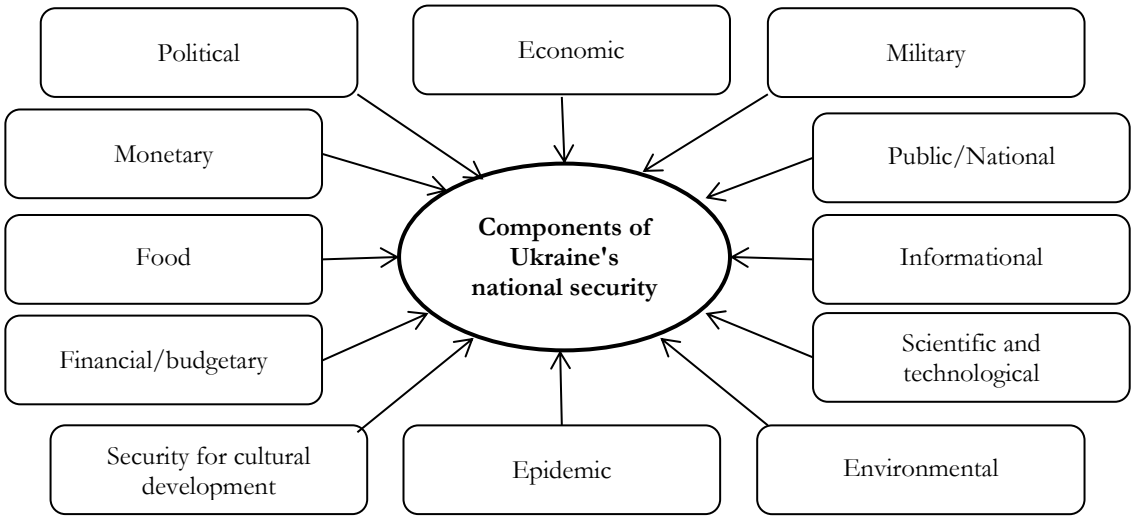

Figure 1. Components of Ukraine's national security
Source: compiled by the author.

Speaking about the information field of a particular country (which every country has), its borders are most often identified with its frontiers. They cover the state's territory, water area, airspace, and economy. The media operate in these spheres and inform, i.e., report, present, and create an idea of something. However, in general, the concept of the state information space is not limited to the territory of the country itself. This concept includes its subjects, the entire material and technical environment, and all intellectual and information property of these subjects. This is a rather large and complicated complex.

By the way, military theorists classify types of possible wars based on these elements. The war of an agrarian society was fought for land, and the industrial war was fought for machines. The war of an information society was fought for information. Military experts see the future war from a new perspective. It will no longer be just an information war. The war of 2025 is considered a war of knowledge. Just as knowledge leads to decision-making, insufficient knowledge will lead to wrong decisions. An adversary will always make bad decisions if they rely on incorrect knowledge. One subfield of this direction is called "perception management": we do not change objects because, in many cases, it is impossible, but we change how they are perceived. In our daily lives, for example, a channel like television also constantly changes our perception of events and people. A. Moskalenko lists the subjects of the national information space (Moskalenko, 1998, p. 45-46).

Information policy defines the main aspects of the formation and functioning of the information sphere. G. Pocheptsov and S. Chukut emphasize that when the system of social networks works effectively, it allows for the rapid cultivation of a new elite and active discussion of new projects. It promotes government transparency, bringing its activities closer to society. The rule of interaction between the government and society is the normal functioning of their communication. Not only should the population listen to the government, but the government should also listen to the thoughts and words of its people (Pocheptsov, Chukut, 2002, p. 9).

G. Pocheptsov separately emphasizes that information security involves analyzing threats that may arise in the information field and creating conditions to prevent them. This applies primarily to various technical aspects of information transmission and processing. Currently, in Ukraine, the concept of state information policy and the concept of information security are being developed. In the European Union, many regulatory documents have been and are being adopted, defining the transition to an information society (Pocheptsov, 2001, p. 25).

E. Vozniuk, in turn, believes that protecting information includes a system of measures to prevent unauthorized criminal access to information, its unauthorized alteration, loss, destruction,

violation of integrity, and so on (Vozniuk, 2021, p. 117). V. Vetrov, supporting E. Vozniuk, also emphasizes that the main goal of this sphere is to balance the protection of confidentiality, integrity, and availability of data, also known as the CIA triad, while focusing on effective policy implementation without causing significant performance disruptions to the organization (Vetrov & Voznyuk, 2019, p. 35).

Recently, a clear dependence has been found between the processes of stabilization/destabilization of modern countries and one or another process of activity of their information infrastructures. It means that today, a new type of toolkit has emerged, to which countries whose technological level was slightly or significantly lower than the level of developed democratic countries are not ready. On the contrary, the United States now believes that it should only be afraid of asymmetric information threats, especially from China, and is investing significant funds in ensuring its stability against such threats. The United States does not enter into any contractual relations related to information warfare and is ready to cooperate only in the fight against information terrorism.

Adequate information infrastructure determines the level of development of any country, as it:

– allows radically reducing the time for presenting and discussing new ideas, projects, and people;

– enables the development of the most efficient sector of the economy - the information economy, the economy of producing new knowledge;

– enables development inherent in human development a priori.

It should be emphasized that adequate information infrastructure can help the state solve numerous political, economic, diplomatic, and military tasks, which is a cheaper option for its implementation. Fundamental changes make it impossible to use modern and old models of information space management. In this case, the state's task is not to disseminate the same information throughout the country but to ensure the dissemination of other information and alternative opinions, thus representing the state's firm opinion. The State Committee of Ukraine for Communication and Informatization lists the following among the most important characteristics (Figure 2).

Why is the information space so highly valued today? At present, humanity has developed new technological capabilities to address its old problems. The information space is used as a tool for solving social, political, economic, and military tasks. It should be recognized immediately that it has attracted significant attention from politicians and military leaders throughout the existence

of states and their borders. However, in the past, the world has transitioned from sporadic use of this toolkit to its systematic use today.

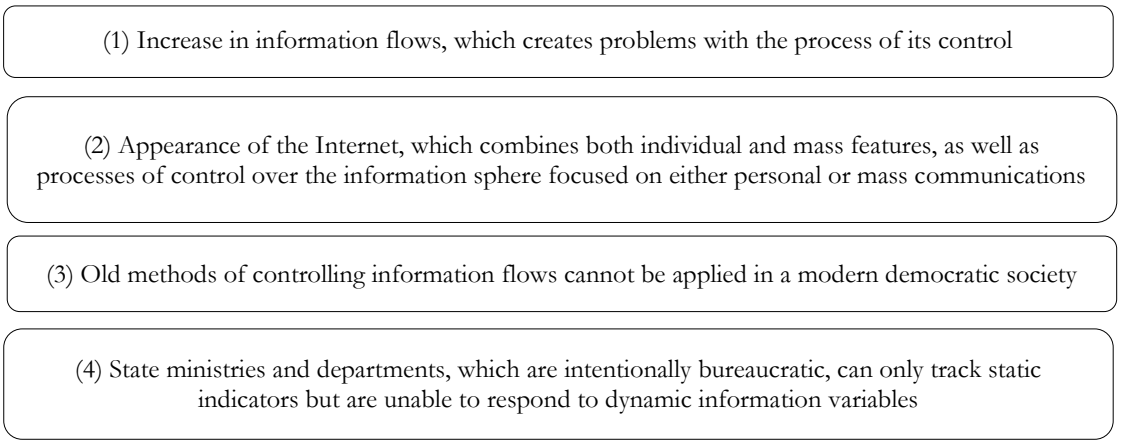

Figure 2. Reasons for changing the models of state information space management
Source: compiled by the author based on (State Committee for Communications and Informatization of Ukraine).

Furthermore, globalization has created a crucial role for information flows. Modern economics, politics, tourism, and trade fields depend entirely on external factors. A country's information status and representation in the global information space are part of its political or economic weight globally. There are no states whose status in the information realm significantly differs from those in other spheres. However, this is not a random process, as a strong state manages its image processes on par with others.

Information relations are classified as the fourth dimension of societal development by both theorists and practitioners of economic growth, confirming its equality with well-known levels such as diplomatic, economic, and military. It is not just an information civilization that includes developed countries but also a post-information society. Global events related to terrorism and its scale vividly demonstrate the importance of such an element as an information state. In the case of armed conflicts, there is a need to legitimize the use of force and change the approach to the values and assessments of one culture toward another. Terrorism as a phenomenon is usually closely associated with state and private media use. The latter gave birth to the definition of the XXI century, such as "hybrid warfare." This, by its nature, is based on the use of network technologies and mass media with beneficial or criminal intentions to destabilize the internal situation of a country.

The beginning of terrorist wars and information vulnerability was laid on September 11, 2001, with the bombing of two skyscrapers in the USA by hijacked planes in the airspace. It marked the beginning of the US defeat in this battle and, at the same time, the beginning of a new stage in

the relationship with the country's information space and control over it, as well as a new type of war. Here, the new network ideology clashed with the old hierarchical system when a network spread across different countries could resist state authority. This changed the type of war and information work, especially the Pentagon analysts.

At the beginning of the XXI century, television became the most powerful communication channel with the potential to influence mass consciousness. In the last decades of the XX century, radio played this role. In the quarter of the XXI century, the Internet has become the most crucial channel. Thus, the dominant channel in society is constantly changing. The Internet gradually created more opportunities for demystifying social messages (according to E. Toffler) since everyone controls what they want to read there, unlike traditional mass media. With the emergence of such political tasks, processes of intensive creation of a negative image of the country from the outside also occur. We remember the perestroika when a systemic approach initiated from the outside led to a change in the social order. Having such processes in the arsenal of capabilities today, they can be significantly facilitated by the existence of the Internet. It is also worth finding countermeasures, as no effective technology ever "retires" as long as it remains effective. On the contrary, technologies of this type become more advanced with each passing year, especially in the conditions of modern "hybrid warfare."

The development of the information sphere opens up new opportunities for Ukraine in economy, politics, and international relations. This is something that all countries have been doing for a long time, to varying extents and with different intensities. One American president once said that "a dollar invested in propaganda yields more than ten dollars invested in armaments because it acts immediately and realistically, whereas those ten will wait" (Pocheptsov, 1999, p. 6-10). According to leading political scientists and state leaders, it is necessary to constantly address the informational aspect of every action, which will be effective only if informative coverage is ensured but also active information preparation before the act itself and information support in the form of monitoring after its completion.

In the Sustainable Development Strategy "Ukraine - 2020," adopted on January 12, 2015, the threats in the information sphere of the state were defined as follows:

– firstly, limitations on freedom of speech and citizens' access to information.

– secondly, the spread of a culture of violence, cruelty, and pornography through mass media.

– thirdly, cybercrime and cyberterrorism.

– fourthly, the disclosure of information that constitutes state or other legally protected secrets, as well as confidential information that constitutes state property or is aimed at meeting the state's and society's common needs and interests.

– fifthly, attempts to manipulate public consciousness, including disseminating unreliable, incomplete, or biased information (On the Sustainable Development Strategy "Ukraine - 2020," 2015).

On February 25, 2017, the President of Ukraine signed the Decree on the Doctrine of Information Security of Ukraine (Doctrine of Information Security of Ukraine, 2017). This document established mechanisms for organizing information security within the specific geographical boundaries of Ukraine. It addressed protecting information security for Ukrainian diasporas abroad but did not define "national information security."

The Law of Ukraine on the Basic Principles of Ensuring Cybersecurity of Ukraine is also worth mentioning. It sets out "legal and organizational aspects of ensuring the protection of the vital interests of people and citizens, society, and the state, national interests of Ukraine in cyberspace, as well as the basic goals, directions, and principles of state policy in the field of cybersecurity, the powers of state bodies, enterprises, institutions, organizations, people, and citizens in this regard, and the basic principles of coordination of their activities in ensuring cybersecurity" (On the Fundamental Principles..., 2017). On May 14, 2021, by the Decree of the President of Ukraine, the Strategy for Cybersecurity of Ukraine was updated (On the Strategy for Cybersecurity, 2021), with the previous version dating back to 2016.

The Economic Security Strategy of Ukraine for the period up to 2025, adopted on August 11, 2021, categorizes the following factors as informational threats:

– "Incompatibility of the national economy structure with modern technological development, insufficient integration of Ukraine into global production chains" (About the Strategy... until 2025, 2021);

– "Low adoption rate of advanced production technologies" (About the Strategy... until 2025, 2021);

– "Unsatisfactory technical condition and level of protection of critical infrastructure objects, insufficient investments in their renovation and development, potential threats of unauthorized physical and cyber interventions in their functioning" (About the Strategy... until 2025, 2021).

On March 18, 2022, the National Security and Defense Council decided to implement a unified information policy during a state of war. The Council clearly stated that the realization of

a unified information policy is a national security priority under wartime conditions (Regarding the Implementation, 2022). Currently, Ukraine has the Center for Countering Disinformation under the National Security and Defense Council of Ukraine, where it is possible to find up-to-date information and events related to this field.

With the onset of Russia's full-scale invasion of Ukraine, along with warfare and the destruction of civilian infrastructure, and the expansion of means and methods of conducting a "hybrid war" through network platforms and internet-based systems, the country faced an increased threat to its information security. In general, we can trace the state's response model to information threats through the example of their emergence in Ukraine (Figure 3).

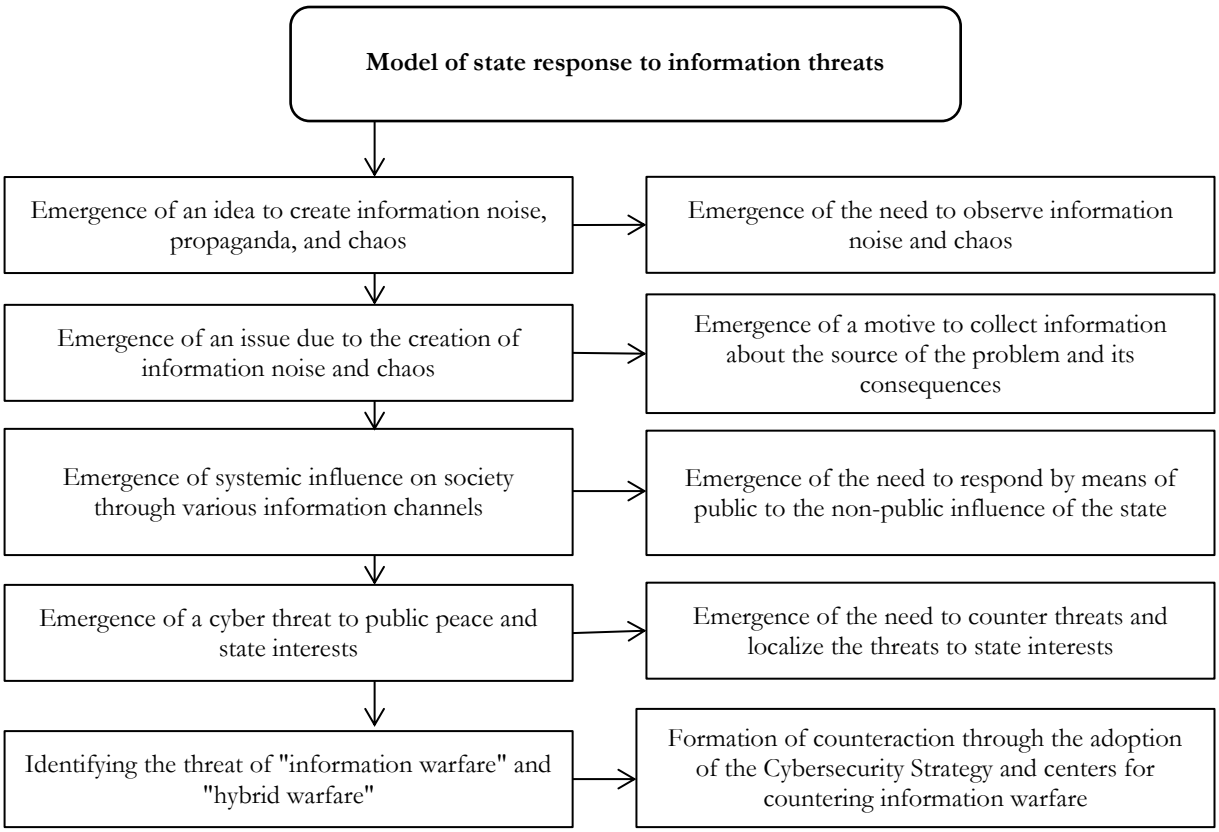

Figure 3. Model of state response to information threats
Source: compiled by the author.

As we can see from our constructed model, chronological information insecurity arises when a party wishes to introduce a certain level of chaos into society and conduct fake actions to destabilize peace and undermine the government's image in that territory. Of course, any news, even of a prejudiced nature, is within society's and the government's purview. It creates informational noise and chaos that should be responded to cautiously or localized immediately.

Information warfare and information terrorism are forms of violating a state's information security. E. Vozniuk believes that "information warfare is the tactical and strategic use of information for gaining an advantage. It can involve several types of activities and be carried out differently over decades" (Vozniuk, 2021, p. 119). "Information warfare is also known as cyber war, electronic warfare, and cyber-attack. Den Kyul from AON defined information warfare as a conflict or struggle between two or more groups in an information environment" (Nychiporchuk, Voznyuk, 2018, p. 68).

In the modern era, information warfare includes elements such as collecting tactical information, verifying the accuracy and reliability of information, spreading propaganda and disinformation to demoralize or manipulate opponents and society, and undermining the quality of the opponent's data. Possible forms of information warfare include using viruses or malware to carry out cyberattacks, exploiting network vulnerabilities, and stealing information through various unauthorized access methods. Yu. Bondar emphasizes that among modern manifestations of information warfare, information terrorism is the most extreme. He defines it as "the use of information technologies, media, and the dissemination of information to influence a chosen object and discredit it consciously" (Bondar, 2011, p. 1-28).

The more aggressive the actions of the party trying to introduce information insecurity into the space, the more robust the response of the state and its governing and law enforcement agencies should be to such actions. This is because information is an intellectual product, and network information transmission systems reach content users in a short time through the Internet. In this regard, L. Lyubokhinets and O. Poplavska point out that information security is essential for manipulators who want to influence persons, groups of people, corporations, or countries in some way. If, in the past, a strong and numerically large army with various types of weapons was needed to protect a country, now only a few highly qualified specialists who can manage information, transmit it as required, and direct it toward one goal are needed (Lyubokhinets, Poplavska, 2017, p. 94). We agree with these authors, as they provide the main basis for the motivation of the state to react promptly to information insecurity, which manifests itself in one way or another. During this period, the reason for creating information security arises.

We should delve deeper into the process of forming a country's information security. This process should be based on principles that make up an entire legal institution.

The principle of legality involves using information protection mechanisms and information security system management technology exclusively based on current legislation and the regulatory and legal framework regulating both social information relations and international

relations in the field of information cooperation. In this context, it should be understood that the legal rule limits the necessity: "What is not prohibited by law is automatically allowed," based on the conditions of a democratic state. Therefore, the need for legality is limited by the permission system for disseminating information.

The principle of the primacy of norms of international law over national legislation, in addition to the Constitution of Ukraine, in the information security system, will consist in the direct application of generally recognized principles and norms of international law, international treaties throughout the country at the level of the Constitution of Ukraine. In this context, it should be emphasized that the necessity of applying international norms on the territory of a specific country is determined by the specificity of the information resource that spreads without borders. Also, it can significantly influence events in a large region where various countries with different legal regimes and attitudes towards certain circumstances are located.

The principle of property rights in ensuring information security entails guaranteeing the rights of subjects of Ukraine to information, except for limitations provided by current regulatory acts. This institution is currently in the process of formation in Ukraine. In addition, it is mainly related not to a state of war but to an imperfect regulatory framework that should regulate the exchange of information between foreign partners regarding property objects.

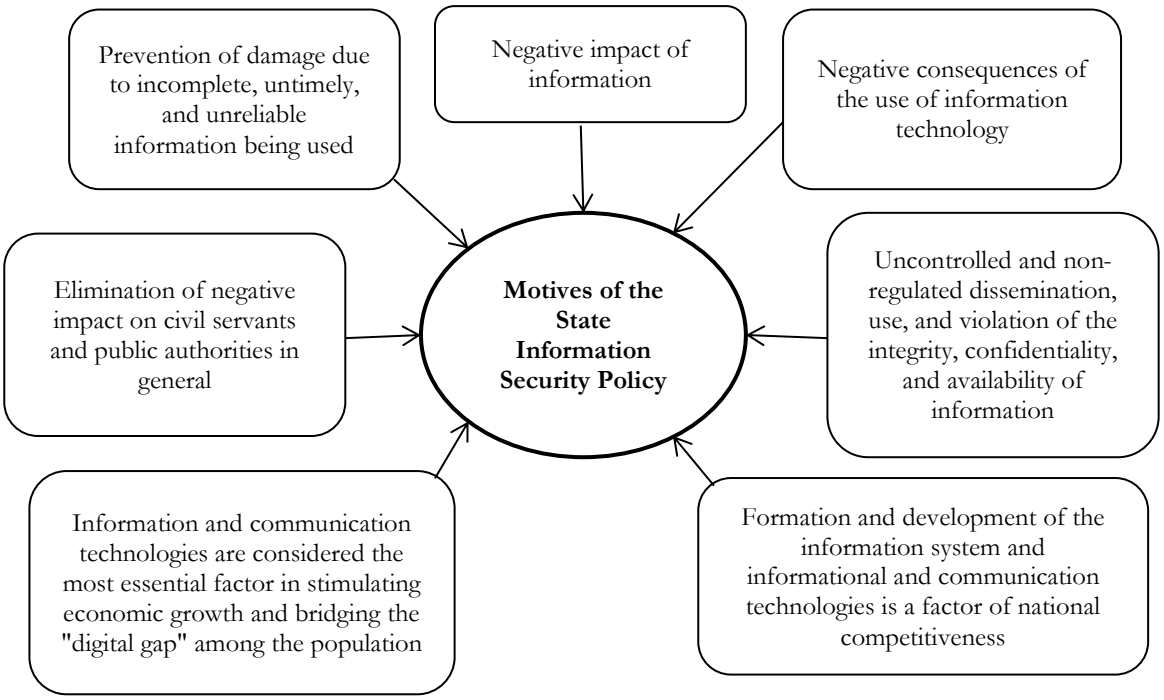

Figure 4. Motives of the State Information Security Policy
Source: compiled by the author based on (On the Basic Principles... for 2007-2015, 2007; Kobko, 2019, 46-46).

The principle of economic expediency of information security systems is based on measures and the necessity of maintaining the secrecy and confidentiality of information related to consumer property. It includes their cost based on legal requirements in the overall price of manufactured products. This primarily concerns classified state orders and contracts that shape mechanisms for ensuring information security and the country's national security. O. Oliinyk believes that the magnitude of economic damage and the severity of other negative consequences for vital national interests should be considered the main criteria for applying economic expediency to ensure information security (Oliynyk, 2012, p. 171).

The principle of unbiasedness in the information security system is fundamental and crucial. Only based on an unbiased assessment of actual and potential threats to information and its circulation, the state of the legal and organizational framework, as well as the actual capabilities of using material, technical, human, and financial resources, even in minimal necessary volumes and sufficient quantity, can information security or the mitigation of threats to its circulation be ensured. Additionally, as emphasized by V. Knyazev and V. Bakumenko, the principle of unbiasedness requires compliance with the requirements of unbiased regularities in all management processes, the verification of these regularities, and a thorough analysis of available capabilities, continuous monitoring of all relevant processes (Knyazev, Bakumenko, 2000, p. 355).

The principle of continuity of information security involves the daily, constant (uninterrupted) application of both general and specific measures and methods of information security at all stages of the life cycle of ensuring national security.

Thus, the described principles of implementing information protection of state and national interests should ensure the necessity of a systemic approach to this protection.

The sufficiency criterion of the state's information security policy should be based on society members' legal consciousness. As V. Lukyanova and A. Lautar emphasized, "There are various methods and means of ensuring information security." Ensuring information security in the state means "using all available methods and means to protect the information needs of society, individuals, and the state. The predominance of law in all activities, especially politics, is of utmost importance. Every subject of the information process must have the appropriate legal awareness, comply with the legislation, clearly understand the consequences of their actions for other subjects, and the degree of responsibility in case of violation of their vital interests. This is important because the use of specific forms and methods depends on whether information threats result from unintentional or deliberate actions of subjects of the information process" (Lukyanova, Lautar, 2013, p. 99-101). Therefore, we can understand here that the sufficiency criterion for measures to

ensure the state's information security is, on the one hand, the legal awareness of citizens affected by the hostile information environment and, on the other hand, the ability, adequacy, and timely awareness of government and law enforcement agencies of the depth, breadth, and territorial coverage of society by false information resources.

Rephrasing S. Budagovska and O. Kilievich, we can confidently state that information stability in society is "a complex combination of internally and externally oriented measures that, by reflecting the dialectic of the part and the whole, determine the essential features of endogenous socio-political actions at a particular moment of management system development on an innovative basis" (Budagovska, Kilievich, 1998, p. 50). With this in mind, we can propose a set of sufficiency criteria for state regulation of information development to implement the information security policy, namely:

1) Defining national external and internal political interests in the context of globalized world relations and, directly, global information markets.

2) Formulating parameters for Ukraine's information development model, considering the necessary focus on national interest and national information security resources.

3) Determining priorities and the scope of exclusively state regulation of information, intellectual, and technological development within the chosen national model and defining state national interests to ensure predictability and transparency in state relations with its internal partners.

6. Discussion

After considering the fundamental principles on which the protection of the information component of the state's national security should be based, we can note several controversial issues. Firstly, it is necessary to regulate the interaction of various subjects responsible for information protection within the state and establish a transparent hierarchical system that allocates access to different types of information. This includes publicly available information, information with restricted access, and classified information that significantly affects the state's national security. Secondly, it is crucial to regulate the interaction of various structures operating at international levels with specialized technologies for controlling information flows and preventing information intrusions, provocations, and exacerbations of "hybrid wars" based on the improper dissemination of unreliable information capable of causing significant impacts on public opinion.

Thirdly, Ukraine, in particular, should clearly regulate its information field protection system with the help of European-ready systems and institutions. It is especially relevant during the war with Russia since it fully exploits information attacks on Ukrainian and international society to discredit the government, lower its image, and sow doubts.

V. Kolyadenko believes that "creating a single information and communication space for Ukraine in the global information environment is especially necessary now. It will ensure Ukraine's full participation in the processes of information and economic integration of regions, countries, and nations. Information and communication processes contribute to the inclusion of Ukrainian society in the global political environment, where leading development standards are set by countries with strong democratic traditions" (Kolyadenko, 2002, p. 13). E. Vozniuk is convinced that the opportunities to improve Ukraine's information security should start with the initiation and strengthening of international cooperation with NATO, OSCE, EU, and UN in all areas, as well as the ability to defend one's position and interests in international negotiations, in all forms of cooperation, and international courts (Vozniuk, 2021, p. 121).

The sufficiency criteria for state influence on information protection of the territory and society, as well as the country's population, remains a subject of debate. In our opinion, the state has no clear upper limit in protecting its people and territory if this population is affected by information warfare or information terrorism. Besides, the state's measures are insufficient to eliminate the threat, even if human rights and freedoms previously proclaimed by the state are violated.

7. Conclusions

The national information space is a crucial political concept. It can be put in second place after the independence of the state's territory and its integrity. The state has to ensure the use of its own and external information fields in its interests and the interests of its citizens. If it fails to do so, its information space will be used against it. Ukraine approaches the control of its information space with a lack of seriousness, experiencing numerous breaches and information-related issues, inadequately addressing them in the conditions of "hybrid warfare," where the information battlefield is invisible, vast, and borderless. Nevertheless, its disruptions affect national security as a whole.

In the context of its security functions, the state's information policy defines the rules for the existence of the information flow sphere. Suppose the information system operates effectively

and benefits society. In that case, it allows for the rapid cultivation of a new political elite, enables it to discuss new projects actively, and promotes transparency in governance, bringing its actions closer to the population and making them public and accessible. According to the law of interaction between the government and people, communication between them should be adequate and commensurate with the applied efforts.

The absence of motivation, the level of necessity, and adherence to the principles and foundations of information security at the state level leads to foreign policy problems. However, while taking measures to protect the information field of the state and its interests, it is essential to adhere to sufficiency and optimality criteria for regulating the interaction between government and society from the perspective of "what is not prohibited and does not pose a societal danger is allowed." It is an approach followed in democratic countries that can control the information space through established regulatory frameworks and institutions in various sectors.

References

Bondar, Yu. (2011). Freedom of speech as a factor in information security. The Actual problems of international relations. *International Information Security: Contemporary Concepts and Practices.* 102(Part I). Kyiv. 127-129.

Budagovska, S., Kilievich, O. (1998). Microeconomics and macroeconomics, Kyiv, Osnovy, 910 p.

Concept of development of state information infrastructure. Official website of the State Committee for Communication and Informatization of Ukraine. Available at: http://www.stc.gov.ua/info/ (access date: 09/22/2023).

The doctrine of information security of Ukraine, (2017). App. By Decree of the President of Ukraine dated February 25, 2017, 47/2017. Available at: https://www.president.gov.ua/documents/472017-21374 (access date: 09/21/2023).

Knyazev, V., Bakumenko, V. (2000). Philosophical and methodological foundations of state-management decisions. *Bulletin of the Ukrainian Academy of Sciences*, 2, 341-357.

Kobko, E. (2019). Information security in the national security system: modernity and prospects. National Law Journal: Theory and Practice, 3, 46-50.

Kolesnyk, V. T. (2015). Conceptual model of national security of Ukraine. Imperatives of civilization development. Information security in the military sphere. Current state and development prospects: materials of the international scientific and practical conference, Kyiv, March 31, 2015. National. The University of Defense named after Ivan Chernyakhovskyi. K.: FOP OS Lipkan, p. 167-170.

Kolyadenko, V. A. (2002). Information and communication technologies as a factor of political modernization: thesis abstract for the degree of Candidate of Political Sciences: specialty 23.00.02 "Political institutions and processes," Odesa, 23 p.

Krynina, O. Yu. (2009). Definitions of the term "information war". New technologies, 3, 68-70.

Lukyanova, V., Lautar, A. (2013). Information security in the context of the development of information systems. Bulletin of the Khmelnytskyi National University. *Series "Economic Sciences"*, 2(3), 97-101.

Lyubokhinets, L. S., Poplavska, O. V. (2017). The world practice of ensuring information security in the modern globalized environment. *Business navigator*, 4-1, 93-97.

Moskalenko, A. (1998). Theory of journalism, Kyiv, 320 p.

Nychiporchuk, N. Vozniuk, E. (2018). The secret of the US success in the field of information security. International relations, public communications, and regional studies. 1(3), 66-71.

Oliynyk, O. V. (2012). Principles of ensuring information security of Ukraine. *Scientific Bulletin of Uzhhorod University*,"Law" series, 18, 170-173.

On the Basic Principles of Information Society Development in Ukraine for 2007-2015, (2007), Law of Ukraine dated January 9(537-V). *Information of the Verkhovna Rada of Ukraine*, 12(102).

On the Cybersecurity Strategy of Ukraine (2021). The decision of the National Security and Defense Council dated 05/14/2021. Available at: https://www.president.gov.ua/documents/4472021-40013 (access date: 09/21/2023).

On the main principles of ensuring cyber security of Ukraine (2017), Law of Ukraine No. 2163-VIII of October 5, 2017 (revision dated August 17, 2022). Information of the Verkhovna Rada of Ukraine. 45(403). Available at: https://zakon.rada.gov.ua/laws/show/2163-19#Text (access date: 09/21/2023).

On the Strategy of Economic Security of Ukraine for the period until 2025 (2021). Decree of the President of Ukraine, 347/2021 dated August 11. Available at: https://zakon.rada.gov.ua/laws/show/347/2021#Text (access date: 09/21/2023).

On the Sustainable Development Strategy "Ukraine - 2020": Decree of the President of Ukraine dated January 12, 5/2015. Available at: www.zakon.rada.gov.ua/go/5/2015 (access date: 09/22/2023).

Pocheptsov, H. G. (1999). Introduction to information wars. Kyiv University, Kyiv, 60 p.

Pocheptsov, H. G. (2001). Information & disinformation, Elga, Kyiv, 256 p.

Pocheptsov, H. G., Chukut, S. L. (2002). Information policy: Education. Manual, Part 1, UASU, Kyiv, 96 p.

Regarding the implementation of a unified information policy in the conditions of martial law. (2022). The decision of the National Security and Defense Council of Ukraine dated March 18, 2022: Decree of the President of Ukraine dated March 19, 152/2022. Available at: https://zakon.rada.gov.ua/go/152/2022 (access date: September 21, 2023).

Vetrov, K. Voznyuk, Y. (2019). Information Terrorism as a Modern Threat to Information Security of European States. *International relations, public communications, and regional studies*. 1(5), 34-42.

Vozniuk, E. (2021). SWOT-analysis of the state of information security of Ukraine. Scientific journal of the NPU named after M.P. Drahomanova. Series 22. Political science and teaching methods of socio-political disciplines, 22(30). Available at: https://doi.org/10.31392/pnspd.v22i30.1147