ppi 201502ZU4645
Esta publicación científica en formato digital es continuidad de la revista impresa
ISSN-Versión Impresa 0798-1406 / ISSN-Versión on line 2542-3185Depósito legal pp
197402ZU34

# CUESTIONES POLÍTICAS

Instituto de Estudios Políticos y Derecho Público "Dr. Humberto J. La Roche"
de la Facultad de Ciencias Jurídicas y Políticas de la Universidad del Zulia
Maracaibo, Venezuela

*Vol.40*

*Nº 73*
*Julio*
*Diciembre*
*2022*

Cuestiones Políticas Vol. 40, Nº 73 (2022), 901-918
IEPDP-Facultad de Ciencias Jurídicas y Políticas - LUZ

# Protection of the rights and legitimate interests of the individual in a hybrid war

**DOI: https://doi.org/10.46398/cuestpol.4073.52**

***Petro Rekotov*** *
***Viktor Nikitenko*** **
***Tetiana Korshykova*** ***
***Oleksandr Zherebko*** ****
***Ihor Samoilenko*** *****

## Abstract

The objective of the article was to reveal r the main topics related to the definition of «hybrid warfare» and «legal policy of the state in a hybrid war», «legal policy of the state in the field of cybersecurity». The need to finalize legislation on the Internet taking into account international human rights standards was emphasized. Given the categorical uncertainty and unwillingness of Ukraine's current legal framework to resist new threats in a hybrid war, it is advisable to terminologize and standardize the conceptual apparatus in the legal system of cybersecurity, harmonize national legislation with international acts, as well as promoteflexibility in relevant areas of activity. It is alsonecessary to legally regulate the use of the Internet to help increase the liability of providers and site owners for the location of inaccurate and deliberately harmful information, as well as to establish a mechanism to influence unscrupulous subjects of information law in cyberspace. It is concluded that a separate area in criminology should be the protection of information sources and information security issues in a hybrid war.

**Keywords**: information warfare; crime prevention; cybercrime; individual rights; legal policy.

* Candidate of legal sciences, Associate Professor, Associate Professor of the Department of Information Economics, Entrepreneurship and Finance at the Zaporizhzhia National University, Zaporizhzhia, Ukraine. ORCID ID: https://orcid.org/0000-0002-0378-378X

** Candidate of legal sciences, Associate Professor at the Department of legal support of business activity at the Kyiv National University of Trade and Economics; Kyiv, Ukraine. ORCID ID: https://orcid.org/0000-0002-1785-1819

*** Doctor of Philosophy, Lecturer at the Department of Criminalistics and Forensic Medicine of National Academy of internal Affairs, Kyiv, Ukraine. ORCID ID: https://orcid.org/0000-0001-9840-5230

**** Candidate of legal sciences, Head of the department of normative and methodical activity and standardization, Kyiv Scientific Research Institute of Forensic Expertise, Kyiv, Ukraine. ORCID ID: https://orcid.org/0000-0002-9740-4145

***** Chief forensic expert of the department of trasological, ballistic, explosive and weapons research of the laboratory of forensic research, Kyiv Scientific Research Institute of Forensic Sciences, Ministry of Justice of Ukraine, Kyiv, Ukraine. ORCID ID: https://orcid.org/0000-0001-6345-1456

Recibido el 18/03/2022 Aceptado el 14/05/2022

# Protección de los derechos e intereses legítimos del individuo en una guerra híbrida

**Resumen**

El objetivo del articulo fue revelar los principales temas relacionados con la definición de «guerra híbrida» y «política jurídica del estado en una guerra híbrida», «política jurídica del estado en el campo de la ciberseguridad». Se hizo hincapié en la necesidad de ultimar la legislación en Internet teniendo en cuenta las normas internacionales de derechos humanos. Dada la categórica incertidumbre y falta de voluntad del actual marco legal de Ucrania para resistir nuevas amenazas en una guerra híbrida, es aconsejable terminologizar y estandarizar el aparato conceptual en el sistema legal de ciberseguridad, armonización de la legislación nacional con actos internacionales, así como impulsar la reflexión en áreas de actividad relevantes. Tambien es necesario regular legalmente el uso de Internet para ayudar a aumentar la responsabilidad de los proveedores y propietarios de sitios por la ubicación de información inexacta y deliberadamente dañina, así como para establecer un mecanismo para influir en sujetos inescrupulosos del derecho de la información en el ciberespacio. Se concluye que un área separada en criminología debería ser la protección de las fuentes de información y los problemas de seguridad de la información en una guerra híbrida.

**Palabras clave:** guerra de la información; prevención del delito; ciberdelito; derechos individuales; política jurídica.

## Introduction

In today's world, the terms «information society», «information impact», «information technology» are increasingly used. These terms are widely used due to the need to exchange information between people and the processes of informatization of society. Currently, the process of information exchange is accelerating, attempts are being made to influence other people through information (Kamneva, 2016).

At the same time, the achievement of strategic goals (military, political, economic) of individual criminal states (their leaders) is achieved through information warfare - the process of suggestive influence on groups of people through specially prepared communication technologies and information materials. Today in everyday and scientific circulation the term «information war» is increasingly used, which in a broad sense is any negative information impact on the enemy, and in a narrow sense - a new one that does not fit into the international legal qualification, type or method of conduct. armed conflicts (Korotkiy and Koval, 2010).

Today, people are vulnerable to a large array of information that is aggressive, discriminatory, destructive, manipulative in nature and is the object of information warfare or even hybrid warfare, covering not only information but also economic, financial, political spheres, encroaching on liberal values, which are a sign of the XXI century, are anthropocentrism and sociocentrism. The purpose of hybrid methods and techniques is to instill in the minds of citizens a negative attitude and distrust of the government, contempt for national heroes, traditions, shrines, creating confrontation on religious grounds. Along with asymmetric conflicts and unconventional wars (situations where open hostilities are not taking place), there is also the notion of «hybrid wars», which are now increasingly used (Reeves and Barnsby, 2013).

The development of the system of protection of individual rights and freedoms, protection of public relations in the state is an integral part of the national policy of developed countries, and the effectiveness of such policy depends on the ability of governments to choose mechanisms for its implementation. A thorough study of this problem in the transformation of society requires a new approach to modern jurisprudence, which would provide a comprehensive study of tactics and strategies of legal policy, principles, goals and functions based on existing developments in lawmaking, value concepts and relevant methods of individual sciences (Rudanetska, 2014). Legal policy should guarantee the achievement of consensus between members of society, public authorities and the public, as well as non-governmental organizations (Ilyashko, 2017).

As practice shows, insufficient attention to the issues of parrying information threats can cause significant damage to the political system of any state up to the destruction of the state itself. The hybrid war against Ukraine requires the state to adequately counter and develop a certain policy to respond to challenges. Ukraine's policy in the context of European integration processes should be aimed at ensuring the rights, freedoms of man and citizen, harmonization of all spheres of state activity with international standards.

The legislation stipulates that one of the directions of the state information policy of the state is information security (On the national security of ukraine: law of ukraine, part 4, article 3; on the concept of the National program of informatization: the law of Ukraine, part 1 On the Concept of the National Informatization Program: Law of Ukraine). Information security is understood as the protection of the individual, society and the state from destructive and other negative influences in the information space (Gapeeva, 2017: 26), an integral part of the political, economic, defense and other components of national security (On the concept of the National informatization program: law of Ukraine, 1998). Information security is understood as the protection of the individual,

society and the state from destructive and other negative influences in the information space (Gapeeva, 2017).

As noted in the Strategy of Foreign Policy of Ukraine, approved by the Decree of the President of Ukraine, there are new challenges in the digital space, including the lack of clear legal regulation in this area, which leads to misuse of digital data to harm both individuals and states and international organizations. Among the means of hybrid warfare that the aggressor state uses against Ukraine and other states in the region are the use of energy as a means of pressure; interference in elections; disinformation and manipulation campaigns; cyberattacks on critical infrastructure, government agencies, financial institutions, etc. («On the strategy of foreign policy of Ukraine»: Decree of the President of Ukraine, 2021).

The state, despite the existence of internal conflict with the intervention of the aggressor country to it, does not deviated from the declared European values (Herasymchuk *et al*., 2021). But, hybrid wars combine different regimes of warfare, including criminal action (Gorbulin, 2017). Therefore, it is worth focusing on the role of crime in hybrid warfare and on ways to combat it both at the general legal level and by organizational means to combat cybercrime.

## 1. Methodology of the study

The methodological basis of the study is based on the methods of dialectical, formal-logical, historical, structural-functional, institutional analysis, as well as content analysis of legislative and regulatory acts and the method of evaluation of opinions. Using the dialectical method, the author's tasks to define the concept of «hybrid war», «state policy in a hybrid war» and «legal policy of the state in the field of cybersecurity» were solved. The formal-logical method allowed to reveal contradictions in the legislation, features of separate regulatory legal acts, and also helped to draw conclusions and to give offers concerning the further improvement of the legislation and the decision of the set tasks.

The application of the historical method allowed to reflect the historical need to adjust public policy in a hybrid war, to ensure cybersecurity. The structural-functional method allowed to consider the peculiarities of Ukraine's legal policy to protect the rights and legitimate interests of individuals in a hybrid war caused by the aggression of the Russian Federation as a whole system, to explore its structural elements and identify features of investigating crimes in cyberspace. With the help of the formal-legal method the definitions concerning the essence of research categories were substantiated, the conceptual-categorical apparatus was formed.

The comparative legal method was used in the study of domestic and foreign legislation on the legal regulation of protection of rights and legitimate interests in a hybrid war, in particular, in the investigation of certain criminal offenses in the field of cybersecurity in Ukraine. The method of system analysis and synthesis was used to compare the concepts of «hybrid war», «armed aggression», «individual rights», «state policy», «security», «cybersecurity». The institutional method of research is used in the work. At the same time, the methodology of the system analysis in relation to the object of the legal policy of the state to ensure the rights and interests of the person in the information war was made up of system, structural-functional and evolutionary methods. Statistical and sociological methods were used to obtain and analyze empirical data on the subject of research, characteristics of phenomena, analysis of law enforcement and substantiation of conclusions. The most important methodological role in the study was played by the conceptual provisions and the conceptual and categorical apparatus of the theory of state and law, international humanitarian law, constitutional law and criminal procedure.

## 2. Analysis of recent research

Analyzing the degree of scientific development of research problem, it should be emphasized that in general, the science of international law and the cycle of other legal sciences lacks an understanding of the concept of «hybrid war». Important publications on this topic have been made by such scholars as V. Gorbulin (Gorbulin, 2017), F. Hoffman (Hoffman, 2009), O. Ilyashko (Ilyashko, 2017), J. M**c**Cuen (M**c**Cuen, 2008), L. Veselova (Veselova, 2021), V. Vlasyuk, Y. Karman (Vlasyuk and Karman, 2021), R. Wilkie (Wilkie, 2009) and others.

Recognizing the importance of the contribution of these researchers in the development of these issues, it should be recognized that the problem of protection of the rights and legitimate interests of the individual in a hybrid war in the literature is not given enough attention. There is no comprehensive, systematic research, and most modern scientific work deals only with general issues of criminal law policy or its specific area.

Also, a thorough analysis of the works of scientists gives grounds to state the lack of unity in approaches to the specifics of the investigation of cybercrime related to the policy of information warfare. All the above, as well as insufficient development at the theoretical level of this issue and the presence of organizational and legal gaps in the study area, determines the relevance of the chosen topic and requires legal regulation of certain problematic aspects in a hybrid war on the basis of both legal sciences and modern science. opinions of related sciences.

## 3. Results and discussion

In jurisprudence, "hybrid warfare" is a fairly new concept, and therefore little studied. It has entered an active discourse in recent years in connection with Russian aggression. Ukraine faced the problem of defending state sovereignty and borders in the conditions of a hybrid war, which has other ways than, for example, the Second World War.

Therefore, it is necessary to rethink the phenomenon of war, its course and consequences, to react quickly, to develop radically new approaches. At the same time, it should be taken into account that in the latest war the use of information and communication technologies, highly qualified human resources, the art of international politics, re-equipment of the economy, etc. have become crucial. Hybrid warfare is a complex and inert process, it is not always controlled, it cannot be stopped "as instructed from above." Unlike the traditional wars of the past, it does not end with the signing of an armistice.

The current war on the territory of Ukraine is called "hybrid", presenting it as a new way of implementing aggressive policies. But almost all its tools (an attempt to consolidate its influence in Ukraine through the support of loyal Ukrainian political circles, the internal political division of Ukrainian society through propaganda, and finally open military intervention, attempts to present aggression as an internal civil conflict) were tried by Russian leaders from the seventeenth to the eighteenth centuries. This scenario was most clearly manifested in the activities of the Bolsheviks against the Ukrainian People's Republic during the Ukrainian Revolution of 1917–1921.

It should be emphasized that armed aggression is only one of the instruments of the Russian Federation's war against Ukraine, the last argument when all other means of subduing Ukrainians have exhausted themselves. Aggression is carried out in several dimensions: military, political, economic, social, humanitarian, information. Elements of hybrid warfare have long been propaganda based on lies, manipulation and substitution of concepts, denial of the very fact of war and the participation of the aggressor state in it; accusing Ukraine of its own crimes, distorting Ukrainian history; trade and economic pressure and energy blockade; terror and intimidation of citizens; cyberattacks and attempts to destabilize critical infrastructure.

Hybrid threats include a range of different regimes of warfare, including standard weapons, irregular tactics and formations, terrorist acts (including violence and coercion) and criminal disorder (The origins of the concept of a hybrid war, 2015). Threats can be more characterized as a hybrid balance of traditional and irregular strategies and tactics, it is decentralized planning and implementation, the participation of non-state actors using both simple and complex technologies (Reeves and Barnsby, 2013).

Some scholars point out that hybrid warfare combines military, quasi-military, diplomatic, informational, economic, and other measures to achieve strategic policy goals (Hoffman, 2009). It is characterized by such methods as bribery, intimidation, crime, kidnapping, looting, violence against civilians, seizure of state institutions, organization and conduct of terrorist acts (Martin van Creveld, 2018).

The American researcher J. McQueen sees in a hybrid war a combination of traditional and asymmetric forms of violence with the simultaneous involvement of the local population in the conflict and misleading the international community, or leveling its influence (McCuen, 2008). According to him, virtually any hybrid war combines traditional forms of violence, cyber warfare, terrorism, organized crime, irregular military formations and private military companies. American analyst R. Wilkie proposed to consider as a hybrid war a conflict in which the state or non-state group uses terrorist violence, irregular military, indiscriminate violence, criminals and mercenaries, in order to destabilize the political and economic status of the opponent (Wilkie, 2009).

Thus, considering the concept of "hybrid war", we can conclude that it means a modern type of war, where the conflict uses a variety of means of attack and defense of states that go beyond conventionally defined options and types of warfare. Scientists are already identifying a list of possible real weapons that can be used by the parties. The term weapon, in this case, includes not only material traditional weapons, but also model-organizational and informational weapons.

At the same time, despite the urgency of understanding hybrid warfare to characterize modern military conflicts, the definition of this term is absent both in the recently adopted Law of Ukraine "On National Security of Ukraine" (Law of Ukraine "On National security of Ukraine", 2018), which is a component of the concept of national security, which limits the scientific development of this phenomenon in the system of views on the nature and character of modern military conflicts, principles and ways to prevent their occurrence.

Thus, we see the need to form a conceptual and terminological apparatus for the legal provision of cybersecurity and its consistency not only with the terminology of current domestic legislation and international acts, but also with adequate content for the hybrid threat of cyber threat.

The law of armed conflict, which is synonymous with international humanitarian law or the law of war, is a significant part of all international law that regulates and controls the actions of the parties to a conflict. It consists of both contractual and customary rules. This right is a fundamental right that is binding on all parties to an armed conflict (Kudors, 2015).

The main purpose, as well as the humanitarian and functional significance of the law of armed conflict, is that this law guarantees protection for war victims, whether civilians, prisoners of war, wounded or sick, who will be determined whether acceptable measures of war have been applied, and no prohibited means were used. This specialized branch of law, which defines both state and individual obligations, limits the impact of war, and establishes clear rules for its conduct, in case of violation of which, international legal sanctions or prosecution of war crimes can be applied (Klimchuk, 2015).

The current state of international peace, under the influence of the constant growth of innovative technologies, development and slowing down of economies of various subjects of international law, strengthening of data transmission devices and other new means, is undermined by the discovery of a new phenomenon of "hybrid war". The problem arises in how one can determine the place of hybrid warfare in international law, especially given the current right to war and the law of war. Awareness of the existence of a new threshold of danger raises the level of defense of the party to which these tools are addressed (Vlasyuk and Karman, 2021).

Today there are a large number of international treaties and customary norms that regulate the issue of war - both its beginning and the rules of its conduct. They are given a significant role, but as it turned out, these rules are not able to regulate legal issues that arise in modern wars. Hybridization of war only exacerbates these already complex problems and may lead to the fact that the law of armed conflict will not matter and will not be able to resolve the legal issues of modern hybrid warfare, assuming that in such a situation there will be no legal control and protection of the parties.

Some scholars rightly point out that if the trend towards the development of the law of armed conflict as something outdated and irrelevant continues, participants in armed conflict, as well as the entire international community, will begin to consider international law as more anachronistic than the legal imperative (Reeves and Barnsby, 2013).

If the authority of law is reduced, traditional legal prohibitions will be violated with impunity, and only certain notions of morality will be able to somehow limit action during war. Opponents of the state and non-state will believe that the observance of such ancient legal norms contains significant shortcomings and can no longer regulate their actions. As a result, the parties to the conflict will ignore the obligations under the law of armed conflict and attribute titles to their actions as self-defense or manipulate the very content of the law of armed conflict through the strategic application of lawfare (asymmetric, hybrid warfare) (Kudors, 2015).

Modern international law does not include the concept of "hybrid war", which in turn leads to the corresponding consequences. The lack of

regulation of this newly discovered phenomenon accelerates the emergence of new means of attack in wars, for which the perpetrators cannot be held responsible due to the lack of norms that bind the parties.

The law of armed conflict was developed by the joint action of the international community, which was able to resolve the most pressing issues. Today, a new challenge has emerged - hybrid warfare. In order to prevent the possibility of undermining efforts to humanize war, the international community must recognize that the question of the effectiveness and practicality of the law of armed conflict must expand as a new "hybrid" type of war develops.

Ignoring this trend makes modern legal efforts ineffective, ineffective means of resolving modern armed conflicts, which continues to undermine confidence in the law of armed conflict. Instead of continuing outdated practices, the international community should push for the addition and incorporation of the concept of hybrid warfare and weapons into the law of armed conflict.

Whether through an international treaty or the formation of a new international custom, the international community must renew the law of armed conflict to resolve various issues, as created by hybrid warfare, while emphasizing that comprehensive humanitarian protection under the law of armed conflict is inviolable. At the same time, the disclosure of the concept of "hybrid war" in the context of international law should be carried out in inseparable connection with the realities of warfare, which go beyond the conventionally established standards and rules (Vlasyuk and Karman, 2021).

The main principles of the legal policy of the state in the temporarily occupied territories in a hybrid war include: the priority of human rights; legality; social conditionality; scientific validity; stability and predictability; legitimacy; morality; justice; publicity; combination of interests of the person and the state; compliance with international standards; objectivity; adequacy; optimality; expediency; systematicity; purposefulness; sequence; resource security; humanistic orientation and democratic nature of the tools.

In our opinion, the legal policy of the state in a hybrid war can be defined as part of public policy, which is a reasonable and consistent activity of public authorities, local governments to ensure an effective mechanism for legal regulation of public relations in the temporarily occupied territories in a hybrid war, is expressed in a set of ideas, measures, tasks, programs, guidelines implemented in the field of law and through law and is based on fundamental legal principles.

Implementation of the Strategy of Ukraine's foreign policy will be carried out in compliance with the following principles: compliance

with international law - compliance with generally accepted norms and principles of international law, fulfillment of Ukraine's international obligations under international treaties and membership in international organizations, compliance with international agreements; human-centeredness - recognition and affirmation of respect for human life and dignity, human rights and freedoms as the highest values; protection, promotion, promotion of rights and legitimate interests of Ukrainian citizens abroad, rights and legitimate interests of foreign Ukrainians in other states ("On the strategy of foreign policy activity of Ukraine" Decree of the President of Ukraine, 2021).

We believe that the content of the Strategy should include issues of cybersecurity in Ukraine in a hybrid war based on minimizing the risks of cyber threats by the aggressor through the implementation of a set of measures for the formation and implementation of public administration in this area to determine vulnerability and stability of society and state. In our opinion, the key measures of this Strategy, namely: raising awareness, ensuring resilience, prevention, crisis response and recovery, increasing cooperation with the European Union and NATO, as well as other foreign and international partner organizations.

One of the main tools of hybrid warfare is cyber attack, which can do as much damage as weapons of mass destruction. Any sophisticated cyber weapon can act as a platform that is first implemented in networks and computers, then performs spy functions, and at the right moment is activated and acts as a weapon that destroys military and civilian facilities and infrastructure. The peculiarity of virtual attacks is that it is very difficult to prove the involvement of a state in them. Thus, cyber warfare and cyber espionage are ideal weapons of hybrid warfare.

The main methods of cyberattack are: vandalism; cyber espionage or information gathering; propaganda; attacks to disrupt computers and local area networks; cyberattacks aimed at destroying the critical infrastructure of cities, industrial centers, disrupting transport, communications and other critical facilities.

Vandalism and propaganda in cyberspace in recent years have become one of the most effective ways of waging information warfare. As the experience of the «color» revolutions of the last decade shows, the Internet and social networks are becoming one of the most important fronts of psychological warfare. Also, the methods of information warfare in cyberspace are the creation of fake accounts, throwing false or biased information, coordinating anti-government speeches, conducting propaganda.

Cyber espionage is a very effective method of gathering classified information. It can be used to obtain a list of hostile agents or informants or to steal the latest developments in military or industrial technology. It

is believed that Chinese hackers are most actively involved in industrial espionage, most often the targets of their attacks are enterprises and research centers in the United States and Western Europe.

In recent years, Ukrainian courts have ruled on the following articles of the Criminal Code of Ukraine: 109 (actions aimed at forcible change or overthrow of the constitutional order or the seizure of state power); 110 (encroachment on the territorial integrity and inviolability of Ukraine); 111 (treason); 114-1 (obstruction of the lawful activities of the Armed Forces and other military formations); 161 (violation of equality of citizens depending on their race, nationality, religious beliefs, disability and other grounds); 258-2 (public appeals to commit a terrorist act); 295 (calls to take actions that threaten public order); 436 (propaganda of war) (Criminal code of Ukraine, 2001).

Most of the verdicts were handed down by the courts in relation to statements that affect the national security of Ukraine in cyberspace and the media. In particular, for encroaching on the territorial integrity and inviolability of Ukraine, actions aimed at forcible change or overthrow of the constitutional order. In 74 % of cases, defendants entered into agreements with the prosecutor, admitting their guilt. More than 80 % of cases resulted in courts releasing convicts from serving a probation period of one to three years (Mirny, 2021). This indicates that the state does not see for society a significant danger in the dissemination of this information, as well as danger from these people.

In some cases, the motivation of sentences in such criminal proceedings is inappropriate, and the assessment of the fact of a criminal offense is transferred to forensic experts who conduct forensic-linguistic, complex examinations and semantic-textual examination of written speech. Judges often cite information that has become the subject of a crime, refer to an expert opinion and impose a sentence, while the international standard is that if a court has to decide whether to restrict access to information, it must analyze it on its own. content and context to make decisions. Moreover, these examinations are conducted by institutions that are subordinate to the executive branch and therefore cannot be considered independent. This undermines the right to an impartial and fair trial.

Some scholars and experts focus on the formal approach of Ukrainian courts to national security. Thus, when passing sentences, courts impose the same penalties regardless of the size of the audience that is affected by illegal content. The verdicts do not reflect how the future fate of illegal information is resolved. In particular, 80 % of criminal proceedings ended on probation. Probation requires the convict to fulfill a number of obligations.

As a result, the court may order the offender to delete illegal information, to replace the conditional term with a real one. In our opinion, this is the protection of the state's interests in the conditions of information warfare. Also, experts of the coalition «For Free Internet» pointed out that the courts may use information from the portal «Peacemaker» as the only source of evidence. That is, the court does not assess such evidence either in terms of its reliability or in terms of belonging and admissibility (Mirny, 2021).

The importance of finalizing Internet legislation should also be pointed out. It is necessary to develop a law taking into account international human rights standards. Risks, Russia's military aggression against Ukraine, including in cyberspace, have demonstrated the importance of separate legal regulation.

The aggression of the Russian Federation in the form of a hybrid war clearly showed the low ability of Ukrainian law enforcement agencies to act systematically and effectively in the face of threats to internal security, revealed a lack of reliable mechanisms for coordination and coordination between them and showed unwillingness to respond to hybrid law enforcement system as a whole and its individual units and officials. In particular, the central offices of law enforcement agencies were unable to respond quickly and influence changes in the operational situation, and their territorial bodies and leaders - to take responsibility for making even perfectly legal decisions.

This was a consequence of the existing problems in ensuring public administration of law enforcement agencies, namely: the lack of a single strategic leadership of law enforcement agencies, which would be carried out in accordance with the general principles of the rule of law and international standards of law enforcement; secrecy from society and lack of effective public control over their activities, as well as lack of responsibility of both managers and ordinary law enforcement officers, their unwillingness to act exclusively in accordance with the law; excessively complex and cumbersome structure of law enforcement agencies with duplication and the presence of uncharacteristic functions; imperfections of current legislation in the field of internal security, lack of clear delineation of anti-terrorist, anti-sabotage and counterintelligence activities of law enforcement agencies and military formations, the presence of an excessive number of bylaws, contradictions, the Constitution and laws of Ukraine; low level of competence of the management staff, their corruption, use of positions not for the purpose of maintenance of public safety, and for the sake of personal enrichment; imperfect system of personnel selection and training, etc.

Therefore, within the main basic tasks of law enforcement agencies such as the protection of the constitutional order, state sovereignty and territorial integrity of the state, the fight against crime, protection of rights, freedoms and legitimate interests of citizens, society and the state as a whole, there

are new important tasks to combat hybrid threats: first, ensuring the internal security of the state by strengthening the effectiveness of the fight against the intervention of the secret services of the aggressor country in the internal affairs of Ukraine, including with espionage, destructive activities of agents of influence in state structures and civil society, all types of hostile intelligence, as well as by combating terrorism, separatism and criminal structures that threaten the internal security of Ukraine and contribute to the destabilization of society; secondly, achieving steadfast positions in the protection of national interests in the information and cyberspace, constant monitoring of the situation, effective and prevention of conflicts in interethnic, interfaith, interregional and other areas of national and social relations, promoting their stabilization; third, the protection of the national interests of the state at the international level through diplomatic, political, economic, energy, judicial and other methods.

In our opinion, an effective step in improving the public administration of law enforcement agencies capable of guaranteeing the security, rights and freedoms of citizens could be the creation of a state body responsible for coordinating strategic management in the country's internal security, counterterrorism, emergency prevention and elimination of their consequences.

The Security Service of Ukraine and the National Police of Ukraine will set up specialized units to investigate crimes committed in the context of armed conflict. Such structural units will be organized as part of the central offices of these entities, as well as their regional and territorial bodies in Donetsk and Luhansk regions. They will work directly with the Department for Supervision of Criminal Proceedings on Crimes Committed in the Armed Conflict of the Office of the Prosecutor General and the relevant departments in the Donetsk and Luhansk Regional Prosecutor's Offices. The need to create a single such system is long overdue, and specialization will improve the quality and efficiency of the investigation. At the same time, the investigation of war crimes, crimes against humanity, acts of aggression require a high level of special knowledge (Police and sbu will create special units for the investigation of crimes during armors).

The realities of the so-called "hybrid war" have posed a number of legislative and law enforcement challenges in the field of criminal law policy of the Ukrainian state, the answers to which have not yet been found. Peacetime legislation should ensure the regulation of legal relations in conditions of military aggression in the presence of an inevitable and immediate threat to the sovereignty and territorial integrity of Ukraine, human rights and freedoms.

One of the elements of evidence in criminal proceedings is the collection of evidence. But the inability of our pre-trial investigation bodies to conduct procedural actions in uncontrolled territories forces us to look for

alternative ways to solve the problem of documenting (proving) criminal proceedings on criminal offenses committed in those territories.

The use of evidence-based evidence in criminal proceedings from international human rights organizations monitoring human rights in areas of armed conflict and journalistic investigations into individual facts is difficult to overestimate. Another way out of this situation is to set up joint international investigation teams to investigate individual crimes. The current criminal procedure legislation provides such opportunities. Yes, Art. 571 of the Criminal Procedure Code of Ukraine stipulates that joint investigative teams may be established to conduct a pre-trial investigation of the circumstances of criminal offenses committed in the territories of several states, or if the interests of these states are violated. The establishment and operation of joint investigation teams is an important measure of international cooperation in criminal proceedings, which consists in the coordinated activities of representatives of the competent authorities of different states to investigate crimes of an international nature (Criminal procedure code of Ukraine, 2012).

Any criminal investigation or trial is a "fight for information". Insufficient information (lack of evidence or their falsity) complicates the process of establishing the fact of the crime, the perpetrators, the motives of the crime and so on. In such circumstances, it is important to obtain evidentiary information about the fact of the crime, the use of forensic and other special knowledge. The task of criminology is to develop and apply tools that allow you to collect, investigate, use evidence.

The task of criminology is to develop and apply tools that allow you to collect, investigate, use evidence. In modern conditions, criminology is designed to develop the latest tools aimed at combating organized and transnational crime, corruption, human trafficking, drug trafficking, terrorist financing and other criminal acts. A separate area in criminology should be the protection of information sources and information security issues. In the context of global threats and changing criminal manifestations, an important role should be given to the use of modern forensic knowledge. Means of criminology must meet information challenges, successfully combat crime in an information (hybrid) war.

In general, it should be noted that the problem of improving public administration of law enforcement in a hybrid war is still insufficiently studied and needs more detailed study and discussion. Ukraine will be able to counter hybrid threats only by radically reforming its own law enforcement system in the direction of strengthening the possibility of both vertical coordination of actions of all law enforcement agencies and horizontal ties between them.

## Conclusions

Legal policy of the state in a hybrid war – a type of public policy that is a reasonable and consistent activity of public authorities, local governments to ensure an effective mechanism for legal regulation of public relations in the temporarily occupied territories in a hybrid war, which is expressed in a set of ideas, measures , tasks, programs, guidelines implemented in the field of law and through law and is based on fundamental legal principles.

The information component of national security requires the formation of a secure cyberspace and the systematic implementation of legal instruments of a preventive nature. It is necessary to develop adequate mechanisms of legal regulation, determine the appropriate legal status of the national cybersecurity system in Ukraine, improve the forms and methods of legal regulation in the field of combating hybrid threats.

The formation of the national legal institute of cybersecurity is directly related to the development of international law in this area in the field of information and telecommunications security of society. The legal policy of the state in the field of cybersecurity is a legally regulated activity of cybersecurity entities aimed at ensuring the rights and freedoms of citizens, society and the state in the information space, preventing their violation, identifying cyber threats and restoring violated rights, freedoms and legitimate interests of individuals. carried out by means of international humanitarian law and national legislation with the possibility of applying coercive measures and bringing the perpetrators to justice.

According to the content, the Strategy of Ukraine's foreign policy should include Ukraine's cybersecurity in a hybrid war by minimizing the risks of the aggressor spreading cyber threats by implementing a set of measures to form and implement public administration in this area to determine vulnerability and stability of society and the state. The key measures of this Strategy are, namely: raising awareness, ensuring resilience, prevention, crisis response and recovery, increasing cooperation with the European Union and NATO, as well as other foreign and international partner organizations.

It is important to finalize the legislation on the Internet taking into account international human rights standards. Given the categorical uncertainty and unwillingness of the current legal framework of Ukraine to withstand new threats in a hybrid war, it is necessary to terminologize and standardize the conceptual apparatus in the legal system of cybersecurity, harmonization of terminology of national legislation with international acts. It is also necessary to legally regulate the use of the Internet to help increase the responsibility of providers and site owners for the placement of inaccurate and knowingly harmful information, as well as to establish a mechanism for influencing unscrupulous subjects of information law in cyberspace.

In the modern information society it is necessary to constantly, systematically and timely take effective measures to combat cybercrime in all spheres of public and state life, business and socio-humanitarian environment. Given Ukraine's course to enter the global information space, a national model for cybersecurity of enterprises, institutions and organizations needs to be built; coordination of efforts and interaction of law enforcement agencies, special services, the judiciary, as well as their proper staffing and logistics, exchange of information on the prevention and combating of such criminal offenses.

Given the cross-border nature of cybercrime, law enforcement cooperation in investigating such criminal offenses at the operational level needs to be established; creating and ensuring the functioning of the mechanism for resolving jurisdictional issues in cyberspace. A separate area in criminology should be the protection of information sources and information security issues. An important role should be given to the use of modern forensic knowledge, and the means of forensics should meet the information challenges, successfully combat crime in an information (hybrid) war.

## Bibliographic References

CRIMINAL CODE OF UKRAINE. 2001. No 2341-III. Available online. In: https://zakon.rada.gov.ua/laws/show/2341-14. Consultation date: 15/01/2022.

CRIMINAL PROCEDURE CODE OF UKRAINE. 2012. No 4651-V1. Available online. In: http://zakon.rada.gov.ua/go/4651-17. Consultation date: 15/03/2022.

GAPEEYEVA, Olga. 2017. Current issues of information security: the experience of the CSTO. Information dimension of hybrid warfare: the experience of Ukraine: materials of the International scientific-practical conference. NUOU. PP. 25–28. Kyiv, Ukraine.

GORBULIN, Vladimir. 2017. World Hybrid War: Ukrainian Front: monograph. Kyiv, Ukraine.

HERASYMCHUK, Serhiy; MATIYCHYK, Yaroslav; KHYLKO, Maksym; FYLYPENKO, Artem; SHELEST, Hanna; ZOLKINA, Mariya. 2020. "Rethinking Ukraine's deoccupation policy in the context of Russia's hybrid war against Ukraine". Available online. In: https://dif.org.ua/uploads/pdf/631759284601l3b4e9dcf21.35897876.pdf. Consultation date: 13/02/2022.

HOFFMAN, Frank. 2009. "Hybrid Warfare and Challenges" In: JFQ. No. 52, pp. 34-39.

ILYASHKO, Olexander. 2017. "Conceptual approaches to determining the legal policy of the state in a hybrid war" In: Scientific Bulletin of the National Academy of Internal Affairs. Vol. 104, No. 3, pp. 105-116.

KAMNEVA, Olena. 2016. "Information and psychological impact of the media on the mental state (on the example of a student sample)" In: Cybersecurity issues. 2016. Vol. 18, No. 5, pp. 51-52.

KLIMCHUK, Julia. 2014. Hybrid warfare as a form of armed conflict. In: Law 13. International law. In: http://www.rusnauka.com/34_NNM_2014/Pravo/13_179711.doc.htm. Consultation date: 15/01/2022.

KOROTKIY, Timur; KOVAL, Dmitry. 2010. "The concept of information warfare in international law" In: Almanac of International Law. Available online. In: http://nbuv.gov.ua/UJRN/amp_2010_2_29. Consultation date: 15/01/2022.

KUDORS, Andis. 2015. Interparliamentary Conference for the Common Foreign and Security Policy and the Common Security and Defense Policy. In: Hybrid War - A New Security Challenge for Europe. March 4-6. Riga. Available online. In: http://www.parleu2015.lv/files/cfsp-csdp/wg3-hybrid-war-background-notes-en.pdf Consultation date: 15/01/2022.

LAW OF UKRAINE. 1998. ON THE CONCEPT OF THE NATIONAL INFORMATIZATION PROGRAM. Information of the Verkhovna Rada of Ukraine. 1998. № 27. Art. 182.

LAW OF UKRAINE. 2018. ON NATIONAL SECURITY OF UKRAINE. Voice of Ukraine. № 22. Available online. In: http://zakon0.rada.gov.ua/laws/show/2469-19. Consultation date: 15/01/2022.

MIRNY, Mykola. 2021. How Ukraine punishes for illegal information on the Internet. Available online. In: https://www.ppl.org.ua/yak-ukra%D1%97na-karaye-za-nezakonnu-informaciyu-v-interneti.html. Consultation date: 15/01/2022.

McCUEN, John. 2008. Hybrid Wars. In: Military rewiew. MarchApril. Pp. 107-113.

ON THE DECISION OF THE COUNCIL OF NATIONAL SECURITY AND DEFENSE OF UKRAINE. 2021. "ON THE STRATEGY OF FOREIGN POLICY ACTIVITIES OF UKRAINE. Available online. In: https://zakon.rada.gov.ua/laws/show/448/2021#Text. Consultation date: 15/03/2022.

REEVES, Shane; BARNSBY, Robert. 2013. The New Griffin of War. Hybrid International Armed Conflicts. In: Academic joutnal "Harvard International Review". Available online. In: https://www.questia.com/library/journal/1G1-316203914/the-new-griffin-of-war-hybrid-international-armed. Consultation date: 15/01/2022.

RUDANETSKA, Oksana. 2014. Legal policy of the state in the transformation of society: theoretical and legal aspect. Lviv, Ukraine.

THE ORIGINS OF THE CONCEPT OF A HYBRID WAR. 2015. In: Electronic journal The Bell. 2015. Available online. In: http://www.thebellforum.com/showthread.php?t=130013. Consultation date: 15/01/2022.

The police and the Security Service of Ukraine will set up special units to investigate crimes during the armed conflict. Available online. In: https://www.ukrinform.ua/rubric-society/3280324-u-policii-ta-sbu-stvorat-specpidrozdili-z-rozsliduvanna-zlociniv-pid-cas-zbrojnogo-konfliktu.html. Consultation date: 15/03/2022.

VAN CREWELD, Martin 2018. "Transformation of War". Available online. In: http://loveread.ec/read_book.php?id=44369&p=81. Consultation date: 15/03/2022.

VESELOVA, Lilia. 2021. Administrative and legal bases of cybersecurity in the conditions of hybrid war. The dissertation on competition of a scientific degree of the doctor of legal sciences on a specialty 12.00.07 Administrative law and process; finance law; information law. Odessa State University of Internal Affairs. Odessa, Ukraine.

VLASYUK, Victor; KARMAN, Yaroslav. 2021. Some basics of the concept of "hybrid war" in international law. Available online. In: http://lcslaw.knu.ua/index.php/item/207-deyaki-osnovy-ponyattya-hibrydna-viyna-v-mizhnarodnomu-pravi-vlasiuk-v-v-karman-ya-v. Consultation date: 15/03/2022.

WILKIE, Robert. 2009. "Hybrid Warfare. Something Old, Not Something New" In: Air & Space Power Journal. Vol. 23, No. 4, pp. 13-17.

UNIVERSIDAD
DEL ZULIA

# CUESTIONES POLÍTICAS

**Vol.40 Nº 73**

*Esta revista fue editada en formato digital y publicada en julio de 2022, por el* ***Fondo Editorial Serbiluz, Universidad del Zulia. Maracaibo-Venezuela***

**www.luz.edu.ve**
**www.serbi.luz.edu.ve**
**www.produccioncientificaluz.org**