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.39 *Nº 69*

Julio
Diciembre
2021

Cuestiones Políticas Vol. 39, Nº 69 (Julio - Diciembre) 2021, 115-132
IEPDP-Facultad de Ciencias Jurídicas y Políticas - LUZ

Measures to combat cybercrime: analysis of international and Ukrainian experience

DOI: https://doi.org/10.46398/cuestpol.3969.06

Serhii Cherniavskyi *
Viktoria Babanina **
Oleksandr Mykytchyk ***
Liudmyla Mostepaniuk ****

Abstract

The article is dedicated to the study of the measures used to combat cybercrime in different countries. It is observed that the world's leading countries are actively expanding and creating units in the armed forces and intelligence services that should ensure the development of offensive capabilities in cyberspace. In particular, the operational cooperation of law enforcement agencies, such as Interpol, Europol and Eurojust, in the fight against cybercrime is being stepped up. Anti-cybercrime activities are carried out not only by individual states, but also by their blocs, including NATO. In Ukraine, unlike the developed countries of the world, measures to combat cybercrime are less developed. Despite the existence of special laws and strategies, in particular the Cyber Security Strategy of Ukraine, the fight against cybercrime is not effective due to the declarative nature of most of the provisions of this strategy. It is concluded that one of the problematic aspects of the phenomenon of cybercrime is the low level of education in information technologies of the population of Ukraine.

Keywords: cybercrime; cybersecurity countermeasures; cybercrime; information security; comparative law.

* Vice-Rector of National Academy of Internal Affairs, Doctor of Law, Professor, Kyiv, Ukraine. ORCID ID: https://orcid.org/0000-0002-2711-3828. Email: 0677443745@gmail.com

** Professor of Criminal Law Department of the National Academy of Internal Affairs, PhD in Law, Associate Professor, Kyiv, Ukraine. ORCID ID: https://orcid.org/0000-0003-4173-488X. Email: v774910@gmail.com

*** Professor of Criminal Law Department of the National Academy of Internal Affairs, PhD in Law, Associate Professor, Kyiv, Ukraine. ORCID ID: https://orcid.org/0000-0002-4973-2670. Email: mikitcik@bigmir.net

**** Associate Professor of Criminal Law Department of the National Academy of Internal Affairs, PhD in Law, Associate Professor, Kyiv, Ukraine. ORCID ID: https://orcid.org/0000-0003-2894-0654. Email: LMostepaniuk@ukr.net

Recibido el 14/03/2021 Aceptado el 14/06/2021

Medidas para combatir la ciberdelincuencia: análisis de la experiencia internacional y ucraniana

Resumen

El artículo está dedicado al estudio de las medidas utilizadas para combatir el ciberdelito en diferentes países. Se observa que los países líderes del mundo se están expandiendo activamente y creando unidades en las fuerzas armadas y los servicios de inteligencia que deberían garantizar el desarrollo de capacidades ofensivas en el ciberespacio. En particular, se está intensificando la cooperación operativa de los organismos encargados de hacer cumplir la ley, como Interpol, Europol, Eurojust, en la lucha contra la ciberdelincuencia. Las actividades contra el delito cibernético las llevan a cabo no solo los estados individuales, sino también sus bloques, incluida la OTAN. En Ucrania, a diferencia de los países desarrollados del mundo, las medidas para combatir el ciberdelito están menos desarrolladas. A pesar de la existencia de leyes y estrategias especiales, en particular, la Estrategia de seguridad cibernética de Ucrania, la lucha contra el delito cibernético no es eficaz debido a la naturaleza declarativa de la mayoría de las disposiciones de esta estrategia. Se concluye que uno de los aspectos problemáticos del fenómeno de la ciberdelincuencia es el bajo nivel de educación en tecnologías de la información de la población de Ucrania.

Palabras clave: ciberdelito; contramedidas de ciberseguridad; delitos informáticos; seguridad de la información; derecho comparado.

Introduction

Each state constantly balances between the principles of respect for human rights and freedoms, integration into the international community and the need to ensure economic growth and national security, including by restricting human rights and freedoms, establishing administrative forms of restricting business activities, protecting its own interests in the international arena.

The choice is made by both the population and public authorities, but in the list of areas no internal reasons should outweigh the need for international cooperation in combating crime, which should be based on the principles of openness, mutual assistance, activity in developing new forms of cooperation. International cooperation in the fight against cybercrime must be carried out on the basis of the participation of all countries, which is determined by the nature of the information itself, both the object of encroachment and the nature of the crimes committed.

Indeed, in today's world, all spheres of life are directly dependent on the operation of computer and information networks. However, the widespread use for information processing of computer technology with software that allows to relatively easy modify, copy and destroy information, increases the vulnerability of the information space.

Most users of information systems do not believe in cyberattacks without sufficient grounds for such belief, that is why they use the information space with ignorance of the limitations and threats to system security, creating threats for cybersecurity.

In today's world, information is the most important component of society. The transformation of post-industrial society into an information society means that information becomes global and meaningful both for the individual and for the state and society as a whole, everyone can seek, receive, store, use and disseminate information in any legal way, there are no borders for its flow. At the moment, information is recognized as one of the most important values, respectively, its protection is no less important than its receipt and transmission, therefore, in a digitalized society of the early XXI century the scope of risk changes.

All this suggests the need to coordinate joint efforts in the fight against cybercrime. For Ukraine, taking into account the ongoing integration processes, it is especially important to consider the world experience in the fight against cybercrime and apply it to increase security in the country. Therefore, the study of foreign experience and demonstration of own achievements in the fight against cybercrime is especially important for each country.

1. World experience in combating cybercrime

It is very important to understand the global nature of the cybercrime issue. Thus, cyberattacks already paralyze the work not only of private structures but also of state bodies, there is no state in the world that would be protected from such attacks. Not only hackers or their groups, but also individual states, terrorist and criminal groups are considered as probable sources of cyber threats. When developing tools and methods to combat cybercrime it should kept in mind the latency of such type of crime. According to experts, the latency of "computer crimes" in the US reaches 80%, in the UK - 85%, in Germany - 75%, in Ukraine - more than 90% (Statista, 2020).

According to the international cybersecurity service Symantec Security, about 556 million cybercrimes are registered worldwide each year, with losses of more than $ 100 billion (Belsky, 2014).

Cybercrime can violate the interests of both the state and the individual. Undoubtedly, the peculiarities of the functioning of information systems, especially the Internet, require the joint efforts of various actors, both public and private, to be aimed at solving cybersecurity issues (Rogovets, 2015). However, it is only the state that can and is able to effectively combat full-scale cybercrime, create the conditions for those who are most vulnerable to cybercrime attacks, to build more reliable information security system.

Currently, the world's leading countries are actively expanding and creating units in the armed forces and intelligence services, which should ensure the development of offensive capabilities in cyberspace. For example, in the United States, along with the National Cyber Security Center, the Joint Cyber Command has been formed within the Armed Forces, which should coordinate the efforts of all Pentagon structures in the course of hostilities, provide appropriate support to civilian federal agencies, and interact with similar agencies in other countries (US Department of Defense, 2009).

At the same time, these organizations are partially controlled agencies, as the supreme controlling structure is the National Security Council with a special committee, whose responsibilities include the implementation of information strategy (Djerf-Pierre, 2018), including the fight against cybercrime.

In the UK, cyber weapons programs are being implemented that will enable the government to withstand growing threats from cyberspace (Kessel and Mozur, 2016).

An e-mail security coordination group (ESCG) has been set up in Australia. The main task of this group is to create a secure and reliable electronic operational space for both public and private sectors (Sanders *et al.*, 2017).

Anti-cybercrime activities are carried out not only by individual states, but also by their blocs, including NATO. Thus, the importance of this problem is reflected in all the governing documents of the bloc, adopted in recent years. For the first time, NATO's strategic concept includes cyberspace as a new area of military alliance.

In other words, in the fight against cross-border crimes, which include a significant part of cybercrime, a special role is given to states, and only with well-coordinated law enforcement agencies of different countries it is possible to reduce the number of crimes committed in this area. International cooperation is carried out in several areas and involves, first of all, the creation of regulations and the development of general recommendations, as well as the introduction of effective models of organizational interaction between states. It should be borne in mind that the traditional mechanisms of international cooperation, including requests, mutual assistance and other similar tools used in the XIX century are inappropriate in an era when

crimes can occur from anywhere in the world at the speed of light (Wang, 2021).

Legal regulation of the fight against cybercrime is the basis of the entire system of combating cybercrime. The complexity of drafting international acts in general in the situation under consideration is further complicated by the fact that existing laws are difficult to apply when it comes to non-localizable attacks on a planetary scale, the evidence of which is scattered and virtual (Pozhuyev, 2016).

The international community at various levels has developed a number of acts relevant to the fight against cybercrime, with regional acts playing a special role, as global documents are currently difficult to create. At the same time, it is important to note the attempts of states to extend the norms of global international treaties to combat cybercrime or to conclude new treaties. For example, since organized crime groups can operate alongside individuals in cyberspace, it is possible to apply to them international treaties aimed at combating organized crime, in particular "the UN Convention against Transnational Organized Crime of 15 November 2000" (Butunbaev, 2020: 102). Also, the concept of the UN Convention on International Information Security was developed (Butunbaev, 2020). The main part of the document consists of five sections, the content of which is in a single compositional integrity.

It is important that in Art. 4 of the Convention the main threats to international peace and security in the information space are identified, eleven of which are basic and four additional. Among the basic are named, for example, the use of information technology and tools for hostile acts and acts of aggression; purposeful destructive influence in the information space on critical structures of another state; cross-border dissemination of information that contradicts the principles and norms of international law, as well as national laws of states. Again, the document does not mention such real threats to international security as the commission of cybercrime, the distribution of narcotic drugs and psychotropic substances, their analogues, as well as pornography, including child pornography. In addition, Art. 5 of the Convention is devoted to the basic principles of international information security.

Analysis of the principles mentioned above allows us to conclude that they can be divided into four groups:

1) principles of state participation in the system of international information security as a member of the international community.

2) principles that allow the state to preserve its sovereignty in the process of international cooperation in the fight against cybercrime.

3) principles of ensuring free information exchange between countries

4) the fourth group of principles establishes the nature of the interaction of the state and private entities in the considered relations.

At the same time, it should be noted again that the concept of the Convention does not prescribe in detail the principles of international cooperation in the fight against cybercrime, except for targeted counterterrorism.

The inclusion of section 5 "International cooperation in the field of international information security" in the concept of the Convention should be recognized as positive, but measures of international cooperation in this area are insufficient for the effective functioning of the system of international economic security. Such measures involve only the exchange of national concepts of security in the information space, the operational exchange of information on crisis events and threats in the information space and measures taken to resolve and neutralize them, consultations on activities in the information space. However, these forms do not take into account the need for operational cooperation of law enforcement agencies on a wide range of issues. Thus, the provisions of the concept of the UN Convention on International Information Security are quite compromising and focused primarily on the prevention of information wars, terrorism.

2. European programs to combat cybercrime

It should be noted that most of the specialized acts to combat cybercrime are acts of the European Union, which has one of the most developed information security systems in the world. In 2001, the European Commission presented a special communication containing proposals of a legal and organizational nature to combat cybercrime in the European Union (Zaporozhets, 2009).

Interpol's programs are built around the preparation of operations to combat new computer threats. They are aimed at:

- facilitating the exchange of information between member states in the framework of regional working groups and conferences.
- preparation of training courses for the creation and maintenance of professional standards.
- coordination and facilitation of international operations.
- creating a global contact list to investigate cybercrime.
- assisting member states in the event of cyberattacks or cybercrime investigations through databases.

- development of strategic partnership with other international and private sector organizations.
- detection of new threats and transfer of intelligence to member countries.
- ensuring the functioning of a secure web portal for access to operational information and documents.

Following a feasibility study by the sociological company Rand Corporation, the European Commission decided to establish a European Cybercrime Center (EC3) within the European Police Organization (Europol). The center is designed to act as a coordinator in the EU's fight against cybercrime, facilitating a faster response to online crime. It supports Member States and institutions of the European Union in building operational and analytical capacity for research and cooperation with international partners (Dremliuga *et al*., 2020). EC-3 officially began operations in January 2013 with a mandate to address policing in the following areas of cybercrime:

- crimes committed by organized groups in order to seize large criminal proceeds, such as online fraud.
- crimes that cause serious harm to the victim, such as the sexual exploitation of children online.
- crimes affecting critical infrastructures and information systems in the countries of the European Union (United Nations, 2021).

EC-3 seeks to become a focal point in the EU's fight against cybercrime by building operational and analytical capacity for research and cooperation with international partners in creating an EU cybercrime-free space. The European Cybercrime Center is based in The Hague (Netherlands), so the EC-3 can build on Europol's existing infrastructure and law enforcement network. The EC-3 Program Board assists EU governments in managing the fight against cybercrime (Europol, 2018).

The members of the EU-3 Program Board are currently:

1. EUCTF (European Union Cybercrime Task Force).
2. CIRCAMP (COSPOL project on child pornography on the Internet).
3. ENISA (European Network and Information Security Agency).
4. ECTEG (European Cybercrime Training and Education Group).
5. CEPOL (European Police College).
6. EUROJUST (European Organization for Judicial Cooperation).
7. CERT-EU (European Computer Security Responsibility Team).

8. International Criminal Police Organization - Interpol.
9. European Commission.
10. EEAS (European External Action Service) (Europol, 2018).

Overcoming the consequences of cybercrime and its prevention is a very popular topic for public services. Today, not all Member States have reached the level of know-how needed to start an effective fight against cybercrime. Cyber police units in most EU countries often do not have the hardware and software needed to perform even simple forensic examinations.

EC-3 promotes the development of Member States' capacity by linking EU funding to EU law enforcement. The high level of training of specialists in the fight against cybercrime will be the cornerstone of the new project. EC-3 will actively coordinate technology development and training under Horizon 2020 (Council of Europe, 2001).

Investigations of online fraud, child abuse and other crimes regularly open up hundreds of new victims of crime in Europe. Operations of this magnitude cannot be successfully completed by the national police force alone. This is where the European Cybercrime Center is of significant value.

Europol is a community of professionals in Europe for operational support, coordination and expertise in the field of cybercrime. The European Cybercrime Center provides wider joint activities in cooperation with EU Member States and other key stakeholders; non-EU countries; with international organizations; with governing bodies and Internet service providers, with companies dealing with Internet security of the financial sector; with academic experts; with civil society organizations.

In other words, the current trend in the international fight against cybercrime is to expand the scope of cooperation between states. The reality is the operational cooperation of law enforcement agencies in the fight against cybercrime (Interpol, Europol, Eurojust), the creation and use of a single database on cybercriminals, on committed and planned cybercrimes (primarily works 24/7). Note that the work of Interpol in terms of efficiency of information processing is less effective than specialized organizations of smaller scale.

3. Measures to combat cybercrime in Ukraine

Threats to Ukraine's national security and relevant state policy priorities in the areas of national and public security are defined in the Law of Ukraine "On National Security of Ukraine", National Security Strategy of Ukraine, Military Security Strategy of Ukraine, Cyber Security Strategy of Ukraine and other documents related to national security and defense and

are determined by the National Security and Defense Council of Ukraine, as well as approved by decrees of the President of Ukraine.

It should be noted that in accordance with the goals of the Strategy for the Development of the System of the Ministry of Internal Affairs of Ukraine until 2020 (hereinafter - the Ministry of Internal Affairs) it was planned to create a safe environment for the existence and development of a free society. It was assumed that the achievement of this goal was possible through the implementation of the following measures:

- formation and implementation of state policy in the field of internal affairs.
- strengthening public confidence in the bodies of the Ministry of Internal Affairs.
- ensuring the development of Ukraine as a secure European state, the basis of which are the interests of its citizens and the high efficiency of all components of the system of the Ministry of Internal Affairs (Ryazantseva, 2014).

The implementation of these measures for Ukraine is a serious stage in its development, as this Strategy will contribute to the implementation of European integration policy in the field of internal affairs. Thus, Ukraine will achieve the indicators necessary for Ukraine's full membership in the North Atlantic Treaty Organization.

Analysis of the provisions of this Strategy reveals that the approaches, which will ensure the implementation of its objectives, require clarification in connection with the declarative principles that they include. The point is that service to society (indicated as one of the tasks of the system of bodies of the Ministry of Internal Affairs) is already enshrined in the Constitution of Ukraine, and in this Strategy is an a priori postulate. The provisions of this Strategy require refinement in the direction of bringing them in line with the provisions of the Law of Ukraine "On National Security of Ukraine" (Verkhovna Rada, 2018). Thus, this Law defines national security as a state of protection of national interests of the individual, society, and the state. At the same time, the Strategy for the Development of the System of the Ministry of Internal Affairs of Ukraine until 2020 envisages the creation of a safe environment and the elimination of the negative impact of modern challenges to personal and social security.

Modern management practices and information activities that will be implemented during the implementation of the Strategy will require significant financial investments.

According to its developers, the source of replenishment of costs for the implementation of measures in the field of creating a safe environment, ensuring a balanced migration policy etc., will be the state budget, as well as

international technical assistance and other sources not prohibited by law. In this case, it is necessary to pay more attention during the implementation of the Strategy to the approaches aimed at involving society in the process of creating a safe environment, increasing intolerance to corruption and the development of democratic civilian control. This should have a positive effect on funding the implementation of the above measures, as well as ensure their support from society, which, in turn, will strengthen confidence in the bodies of the Ministry of Internal Affairs as a whole (Kopotun, 2020).

In the Criminal code of Ukraine, as cybercrimes are recognized such crimes in the field of use of electronic computers, systems, computer, and telecommunication networks:

1) unauthorized interference in the work of electronic computers, automated systems, computer networks or telecommunication networks (Article 361).
2) creation for the purpose of use, distribution or sale of malicious software or hardware, as well as their distribution or sale (Article 361-1).
3) unauthorized sale or dissemination of information with limited access, which is stored in computers, automated systems, computer networks or on the media of such information (Article 361-2).
4) unauthorized actions with information that is processed in computers, automated systems, computer networks or stored on the media of such information, committed by a person who has the right to access it (Article 362).
5) violation of the rules of operation of electronic computers, automated systems, computer networks or telecommunication networks or the procedure or rules for the protection of information processed in them (Article 363).
6) interference with the work of electronic computers, automated systems, computer networks or telecommunication networks by mass distribution of telecommunication messages (Article 363-1).

Article 361-1 of the Criminal Code of Ukraine provides for the creation, distribution, or sale of malicious software - a particular program or set of programs that interferes with the functioning of the computer, damages the data on it or leads to other undesirable consequences in the computer system (Verkhovna Rada, 2019).

Malware can take many forms and can be used as an aid in hacking and other cybercrimes (Nekit *et al.*, 2020). According to Article 361-2 of the Criminal Code of Ukraine, an offense is the unauthorized sale or dissemination of restricted information stored on computers or other

media. However, the sale and dissemination of such information need not result from the commission of the offenses set forth above.

"Computer" information with limited access is divided into confidential and classified. Confidential information contains information that is in the possession, use or disposal of individuals, disseminated at their request in accordance with the conditions provided by them. Classified information includes information that constitutes a state and other secret provided by law, the disclosure of which harms the person, society, and the state.

According to Article 362 of the Criminal Code of Ukraine, cybercrime is the unauthorized alteration, destruction or blocking of computer information. This article also penalizes unauthorized interception or copying of computer information if it has led to its leakage. Moreover, the subject of this crime is only persons who have the right to access such information.

Article 363 of the Criminal Code of Ukraine provides for such criminal acts as violation of the rules of operation of computers (which may be expressed in non-fulfillment or improper fulfillment of obligations to comply with the rules of operation of computers, for example, rules of hardware or rules of operation of their software, and violations the order or rules of information protection (non-fulfillment or improper fulfillment of the requirements of information protection established by legal acts), if it has caused significant damage committed by persons responsible for such operation or protection.

Article 363-1 of the Criminal Code of Ukraine provides for liability for intentional mass distribution of messages, carried out without the prior consent of the recipients, which led to the violation or shutdown of the computer. The messages in question are so-called "spam", i.e. the mass distribution of unsolicited e-mails. Due to the mass nature of spam messages, the latter complicate the work of information systems and resources, creating unnecessary overload for them, which may be the cause of their failure. "Spam" can also be a carrier of the previously mentioned malware and viruses (Bogutsky, 2018).

Information crimes, according to Ukrainian law, can take various forms and methods of commission. In addition, we can say that the actions committed by cybercriminals can be complex, i.e. constitute a set of cybercrimes that accompany and provide each other.

The social danger of cybercrime and the urgency of this problem is illustrated by such a phenomenon as cyberattack. Cyberattack - targeted (intentional) actions in cyberspace, which are carried out by means of electronic communications and aimed at achieving the following goals:

- violation of confidentiality, integrity, availability of electronic information resources processed (transmitted, stored) in communication and/or technological systems, obtaining unauthorized access to such resources.
- violation of security, sustainable, reliable, and regular operation of communication and/or technological systems.
- use of the communication system, its resources and means of electronic communications for cyberattacks on other objects of cyber defense (Bogush *et al*., 2014).

Cyberattacks, due to their specificity, are often aimed at automated and information systems of national importance. Examples of this are the well-known cyberattacks on energy companies in Ukraine on December 23, 2015, when criminals successfully attacked the computer control systems of three energy companies in Ukraine, or the cyberattack on December 17-18, 2016, when the substation "Northern" of the energy company " Ukrenergo ", which resulted in leaving consumers of certain districts of Kyiv without electricity (Kokhanovska, 2011).

In view of all the above, it can be concluded that cybercrimes do have a high degree of public danger, because the actions that constitute such crimes are quite difficult to implement, as they require special knowledge in the field of computer technology. This means that the use of existing methods of protection against them also requires a certain level of awareness in this area. Thus, one of the problematic aspects of the phenomenon of cybercrime is the low level of IT education of the population of different countries, in particular, Ukraine. The difficulty is that computer technology is quite difficult to master, so it is very important for the average citizen to know at least the simplest methods of protection that do not require deep specific knowledge.

4. Practical recommendations for the prevention of cybercrime

The activity of the world's leading countries in cyberspace, profound changes in domestic information policy and the formation of powerful transnational criminal groups specializing in cybercrime necessitate the development of priorities for the transformation of the domestic cybersecurity sector, taking into account the above trends.

Since the information technologies that exist at the moment allow us to both hide the location and use the data of others, the next steps are needed at the national and international levels.

At the national level:

1. Participation in the development of an international strategy to combat cyber threats and the creation of unified international legal mechanisms for regulating cyberspace with such statements:

    1) the common goal and direction of the Cyber Security Strategy is to determine the virtual security of the individual, organization and state by defining a system of priorities, principles and measures in the field of domestic and foreign policy, which should reflect all components of cyberspace.

    2) specific / private areas of the strategy need to determine the standards of cooperation of the information society - individuals, organizations, and the state in the field of cybersecurity. Such standards include:

        - rules for maintaining a balance between establishing liability for non-compliance with cybersecurity requirements, on the one hand, and the introduction of excessive restrictions - on the other.

        - priority of cybersecurity risks in accordance with the possibilities of cyber threats and the size of the negative consequences of cybersecurity incidents.

        - updating the means and methods of cybersecurity in order to counter the ever-changing cyber threats (Yarema, 2016).

2. Development and implementation of a multi-level institutional system of cybersecurity, which would include:

    1) scientific and analytical level, which would study the risks of cybersecurity in accordance with the possibilities of implementing cyber threats and the size of the negative consequences, updated the means and methods of cybersecurity.

    As the problem lies in the complexity of classifying threats that go beyond the territory of the state, it is necessary to emphasize the need for any state to develop measures to identify cyber threats, as well as their timely detection, prevention, protection and minimization of consequences.

    2) the executive level, which would coordinate in two directions - internal (between national structures responsible for detecting and combating cyber threats) and external, when coordination is carried out between national structures and similar foreign regional / international institutions (Hancock, 2000).

3. Increase capacity in the information sphere to counter electronic attacks.

It is necessary to strengthen domestic policy measures to stimulate the development of the technological component of cybersecurity to maintain a balance of power and counterbalance other likely "adversaries" in the field of cybersecurity.

4. Act and implement regional and international cooperation in the field of cybersecurity, tracking the activities of criminal, terrorist groups and individual hackers operating in cyberspace.

5. Act and take an active part in the development of international cooperation in the field of cyber threat detection, timely detection, prevention, protection, and minimization of consequences (Downing, 2005).

At the international level:

1. Development and implementation of an international agreement in the field of prevention and investigation of cyber aggression, as well as updating of the existing regulations;

2. Creation an international body with regional offices. This body should be the equivalent of the UN in cyberspace - UN Cyberspace (hereinafter - UNC), it should have several structures. There should be a scientific-analytical level, where the same functions should be performed as at the national level. In addition, there should be an executive level and a regional level that will allow in case of cyber-aggression to join the fight in time. It is also required that the activities of the UNC be carried out by 12 administrators, elected annually from the members of the UNC. Unlike the UN, there should be no privileged members, vetoes or permanent members. In the event of cyber-aggression, the UNC should establish a commission of inquiry from international, regional, and national representatives. The conclusions of the commission with the relevant evidence should be sent to the international court.

Conclusions

For Ukraine, entering a new stage of social development means an unalterable situation in which only improving the use of the information base of the Ukrainian nation and state, as well as the development of information production and social information communication systems, can ensure a proper position in international cooperation.

The key to this development is the organization of security of national information sovereignty for Ukraine both as an object of global information influences and as a full-fledged subject of international activity, international information exchanges are extremely important. The guarantor of the existence and development of national information resources in the context of global influences is the effective information security of our society.

The processes of globalization, catalyzed in recent decades by informatization based on electronic technologies, in addition to their positive significance for the development of progress cause new challenges and threats to the information infrastructure, national information sovereignty, identity, self-awareness, and for civilization - many opportunities for further development. Therefore, work to neutralize cyber threats as an important component of information security is the key to the effective use and long-term development of sovereign for each state, nation information arrays.

The development of effective tools for ensuring information sovereignty is an important condition for social development and a priority today. Issues of cyber security are extremely important for the Ukrainian state at the present stage, which is primarily due to the need to resist illegal encroachment on the information space of Ukraine, preservation of information resources, protection of the population from negative information influence and more.

In addition, a strategically recognized priority of Ukraine's foreign policy is European integration, which requires improving the regulatory framework for cyber security of Ukraine, which would meet not only international standards, but primarily Ukrainian national interests in the information sphere.

Defeat in information warfare, including cyber warfare, can inevitably lead to the disintegration of any state. In modern conditions, many important systems of the industrial and defense sector of the economy, such as the air traffic management system, energy and nuclear enterprises and the grid, working on the basis of information and communication technologies, pose potential risks due to their vulnerabilities to outside intrusion.

Bibliographical References

BELSKY, Yuriy. 2014. "On the definition of cybercrime" In: Legal Bulletin. Vol. 6, pp. 414–418.

BOGUSH, Volodymyr; KRYVUTSA, Volodymyr; KUDIN, Anton. 2014. "Information security: Terminological textbook" In: Kyiv: OOO DVK, p. 508.

BOGUTSKY, Pavlo. 2018. "Nonlinear rationality of the legal system" In: Law of Ukraine. Vol. 6, pp. 182–195.

BUTUNBAEV, Timur. 2020. "Features Of International Legal Cooperation In Combating Cyber Crime" In: International Journal of Advanced Research (IJAR). Vol. 8, No. pp. 05, 100-107. Available online. In: http://dx.doi.org/10.21474/IJAR01/10911. Consultation date: 15/06/2020.

COUNCIL OF EUROPE. 2001. European Convention on Cybercrime. Available online. In: https://www.europarl.europa.eu/meetdocs/2014_2019/documents/libe/dv/7_conv_budapest_/7_conv_budapest_en.pdf. Consultation date: 23/09/2020.

DJERF-PIERRE, Monika. 2018. "Squaring the circle: public service and commercial news on Swedish television" In: Journalism Studies. Vol.1, No.2, pp. 239-260.

DOWNING, Robert. 2005. "Shoring up the weakest link: What lawmakers around the world need to consider in developing comprehensive laws to combat cybercrime" In: Columbia journal of transnational law. Vol. 43, No. 3, pp. 705-762.

DREMLIUGA, Roman; DREMLIUGA, Olga; KUZNETSOV, Pavel. 2020. "Combating the threats of cybercrimes in Russia evolution of the cybercrime laws and social concern" In: Communist and post-communist studies. Vol. 53, No. 3, pp. 123-136.

EUROPOL. 2018. Internet Organised Crime Threat Assessment 2018. Available online. In: https://www.europol.europa.eu/activities-services/main-reports/internet-organisedcrime-threat-assessment-iocta-2018. Consultation date: 23/09/2020.

HANCOCK, Brian. 2000. "Getting the laws to help combat cybercrime (There's a grand idea)" In: Computer & security. Vol. 19, No. 8, pp. 669-670.

KESSEL, Jonah; MOZUR, Paul. 2016. How China Is Changing Your Internet. Available online. In: https://www.worldpressphoto.org/collection/storytelling/2017/29057/2017-how-china-is-changing-your-internet. Consultation date: 23/09/2020.

KOKHANOVSKA, Olena. 2011. "Legal regulation in the field of information relations" In: Kyiv: National Academy of Internal Affairs of Ukraine, p. 212.

KOPOTUN, Igor. 2020. "Expanding the Potential of the Preventive and Law Enforcement Function of the Security Police in Combating Cybercrime in Ukraine and the EU" In: TEM journal – Technology education

management informatics. Vol. 9, No. 2, pp. 460-468.

NEKIT, Kateryna; KOLODIN, Denis; FEDOROV, Valentyn. 2020. "Personal data protection and liability for damage in the field of the Internet of Things" In: Juridical Tribune. Vol. 10, No. 1, pp. 80-93.

POZHUYEV, Volodymyr. 2016. "Formation of the state information policy in the conditions of globalization" In: Humanitarian bulletin of the Zaporozhye state engineering academy. Vol. 43, pp. 4–12.

ROGOVETS, Vitaliy. 2015. "Information wars in the modern world: causes, mechanisms, consequences" In: Personnel. No. 5, pp. 10-17.

RYAZANTSEVA, Iryna. 2014. "Problematic issues of building a national cybersecurity system". In: Law and security: science magazine. Vol. 2, No. 53, pp. 140–144.

SANDERS, Karen; CANEL CRESPO, María José; HOLTZS-BACHA, Christina. 2017. "Communicating governments: a three-country comparison of how governments communicate with citizens" In: The International Journal of Press/Politics. Vol. 16, No. 4, pp. 82-96.

STATISTA. 2020. The level of penetration of the Internet in the world. Available online. In: https://www.statista.com/statistics/269329/penetration-rate-of-the-internetby-region/. Consultation date: 23/09/2020.

UNITED NATIONS. 2021. European Institute for Crime Prevention and Control, affiliated with the United Nations (HEUNI). Available online. In: https://www.unodc.org/unodc/en/commissions/CCPCJ/PNI/institutes-HEUNI.html. Consultation date: 02/03/2021.

US DEPARTMENT OF DEFENSE. 2009. Report on Strategic Communication. Available online. In: https://www.hsdl.org/?view&did=716396. Consultation date: 23/09/2020.

VERKHOVNA RADA OF UKRAINE. 2018. On National Security of Ukraine: Law of Ukraine of June 21, 2018 № 964-IV. Available online. In: https://zakon.rada.gov.ua/laws/show/2469-19#n355. Consultation date: 23/09/2020.

VERKHOVNA RADA OF UKRAINE. 2019. Criminal Code of Ukraine of November 28, 2019, grounds - 263-IX, 284-IX. Available online. In: https://zakon.rada.gov.ua/laws/main/2341-14. Consultation date: 23/09/2020.

WANG, Shun-Yung Kevin. 2021. "Collaboration between law enforcement agencies in combating cybercrime: implications of a Taiwanese case

study about ATM hacking" In: International journal of offender therapy and comparative criminology. Vol. 65, No. 4, pp. 390-408.

YAREMA, Oleksandr. 2016. "The subject of legal support of information security in information law" In: Scientific herald of the Lviv state university of internal affairs. No. 2, pp. 244–252.

ZAPOROZHETS, Olha. 2009. "Policy of the European Union in the field of information security" In: Current issues of international relations. Vol. 8, pp. 36-45.

UNIVERSIDAD DEL ZULIA

CUESTIONES POLÍTICAS

Vol.39 Nº 69

Esta revista fue editada en formato digital y publicada en julio de 2021, por el ***Fondo Editorial Serbiluz, Universidad del Zulia. Maracaibo-Venezuela***

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