Lykhova S.♦

DOI: 10.25108/2304-1730-1749.iolr.2022.67.104-110
UDC: 004.056.5:343.326 (045)

Analysis of cyber threats in the modern electronic world

Annotation:

Introduction. In modern conditions, the development of information technology leads to violations of the rights and freedoms of both individuals and states. **Purpose and objectives.** Investigate such elements of cyberthreats in the modern world as information threats (cyberthreats) terrestrial and in space. **Methods.** Developed general scientific methods of cognition, with which the author solves the issues of cognition, proof, investigation of space electronic crimes committed in cyberspace. **Results.** The author emphasizes the need for special research on space cybercrime, as such criminogenic phenomena threaten the national security of Ukraine. **Conclusions.** The author states that the current state of legislation on the prevention and combating of space cybercrime is insufficient, and therefore requires the adoption of relevant conventions and laws both at the global level and at the national level. The author proposes to develop interstate standards to ensure the cybersecurity of terrestrial and space cyberspace to guarantee the inalienable and inviolable constitutional rights and freedoms of man and citizen. And also to draw the attention of developers of the latest cybersecurity electronic tools, creative methods and grid technologies of electronic intelligence to the need to technologically prevent and counteract possible cyber threats of misuse of outer space and electronic intelligence in various spheres of terrestrial and space life. An international association of the world's leading e-States should create to form, develop and implement common security standards for the provision of e-trust services around the globe. In addition, the relevant international security organizations, agencies and institutions of the world need to develop an orderly legal, organizational and technological system to prevent and combat the harmful use of outer space and electronic intelligence at the national, regional and interstate (global) (transboundary, transnational, transnational), planetary, cosmic (near space, far space)).

Keywords: space cybercrime; electronic cyberspace; cybersecurity.

In modern conditions, the rapid development of information technology in the world and the need to exchange information through the use of the global information network Internetreally create a favorable climate for both terrestrial [8], and space electronic criminal inbreak: illegal access to public and private computer databases; databases of financial and credit institutions (internal banking computer systems); telephone communications; computer systems of enterprises; scientific institutions and educational establishments; misappropriation of funds from bank accounts of others, including in other countries [4, c. 9-17]. Recent cyberattacks on the Pentagon, pipeline transportation networks and other US critical infrastructures, disconnection of power supply systems in the Western regions of Ukraine, blocking of the airport in Warsaw, etc. already

♦ **Lykhova Sofiia** - Doctor of Law, Professor, Head of the Department of Criminal Law and Procedure, Faculty of Law, National Aviation University, Kyiv (Ukraine). E-mail: k_kpipp@ukr.net

specifically indicate the real existing terrestrial and space electronic threats, risks and dangers of global scale. World practice shows that cyber wars, cyber attacks, cyberbullying, cyberterrorism, cybercrime have now acquired not only cross-border, transnational, transcontinental, planetary, but also space [2, c. 14-15]. This is binding on the international community, given the possible global negative consequences of the world order of this extremely dangerous social phenomenon,constantly analyze, monitor such malicious intentions and control and minimize their encroachment on state and interstate legal, political, diplomatic, educational, scientific, economic, environmental, social and communication relations.

It should be noted that in order to overcome such extremely dangerous threats in Europe, a basic legal document was adopted in 2001 to prevent and combat international cyberterrorism and cybercrime in European countries.In particular, the Council of Europe Convention on Cybercrime of 23 November 2001 and the Additional Protocol thereto of 28 January 2003 were adopted.It is obvious that today this European convention is a strong foundation and an effective legal document for the use, further development and improvement of the relevant leading legislation in European countries.In our opinion, this convention today also needs to be improved with new ideas, which are due to modern trends in the civilizational development of electronic communication in the world.

An analysis of international jurisprudence shows the real facts of the emergence of space cybercrime in the world.In particular, it has recently become known that NASA is investigating the world's first computer crime committed in space (outer cyberspace). The basis for the investigation of this computer crime, committed in space cyberspace, was that the victim N. reported a space crime committed from space orbit by the American astronaut K., who was at that time on the space station [3, c. 2-4].

The real danger of malicious electronic actions in space electronic cyberspace, which is already real on the horizon today, is the possibility of electronic information cyber attack from space on terrestrial physical objects. The authors of the report “The Malicious Use of Artificial Intelligence: Forecasting, Prevention, and Mitigation” rightly warn that modern tools and grid technologies of electronic intelligence allow already today to get freely both into systems of ground establishments and the organizations, in particular, unmanned vehicles, and unmanned planes, trains, ships. Thus, it allows to actually manage them under a special code to commit malicious acts, which contributes to the real possibility of not only theft of property, resources, funds, but also the possibility of committing both terrestrial and space threats in the form of epidemics, accidents and catastrophes. Another dangerous example of space or electronic malicious activity may be the use of “drone armies” that can kill people with the help of the latest grid technologies for face recognition, voice, smell, and special behaviors, the study said. Thus, already today there is a real threat of creation and use both on Earth and in outer space (near and far) of electronic killer robots [9].

It is known that in order to implement the strategic objectives of combating space cybercrime and the formation of reliable space cybersecurity in the United Arab Emirates, the Dubai authorities announced the creation of a space court to regulate future civil relations and prevent violations in outer space in orbit [5].

Satellite technology, which is implemented on the basis of the Globalstar satellite network, used to provide quality services in the analyzed case, it seeks to maintain the connection of best practices as a leading global providers of reliable commercial satellite solutions used on our roads,

waterways and remote applications all over the world. Please note that Globalstar satellite solutions are provided by her our own network of satellites that are constantly operating and highly reliable.

Importantly, state-of-the-art Globalstar technology connects people on a daily basis through reliable satellite communications over an extremely clear and secure satellite network. Globalstar satellites provide reliability and performance around the world, connecting users in areas where traditional networks are unreliable or unavailable.Its portfolio of satellite products equips the field with voice and data services, commercial IoT (internet of things) and SPOT Business tracking and messaging products that cater to many companies, workers and leisure enthusiasts in remote business and entertainment applications.

It is known that, like “curved tubes” or mirrors in the sky, Globalstar satellites pick up signals from more than 80% of the Earth’s surface. Globalstar satellites transmit customer signals using CDMA (Code Division Multiple Access) technology to antennas on the appropriate terrestrial gateway, then the signals are transmitted over local networks. This highly efficient design offers the shortest connection latency and allows Globalstar to upgrade its terrestrial and satellite systems with the latest field technology. It should be noted that the new Globalstar Orbit satellite constellation and the new generation of terrestrial infrastructure provide exceptional quality and reliability of coverage and quality customer service.

Moreover, 24 Globalstar ground stations serve as a bridge between Globalstarsatellites and traditional communication infrastructure on six continents. This connection provides contacts with more than 120 countries around the world. The next-generation terrestrial infrastructure is based on the configuration of the Internet Protocol Multimedia Subsystem, which allows satellite network engineers to constantly adapt to changing user needs.

In fact, the Globalstar service operates far beyond terrestrial networks to provide quality traffic to many companies and employees who operate outside of periodic or inaccessible cellular coverage.

It is known that the world community at the dawn of the XXI century has finally entered the era of new innovative civilizational development of “Industry 4.0”, “Fourth Industrial Revolution” and “Knowledge Society” [6, c. 12-13]. The latest ideas, innovations, knowledge, and scientific developments have become the cornerstone, the fundamental basis for the development of culture, education, science, medicine, and the economy of the world's leading countries.

According to the Index of Information and Communication Technologies Development, published by the International Telecommunication Union in 2014, which includes 162 countries, the first 10 places are occupied: 1) Denmark; 2) the Republic of Korea; 3) Sweden; 4) Iceland; 5) Great Britain; 6) Norway; 7) the Netherlands; 8) Finland; 9) Hong Kong (China); 10) Luxembourg. The second ten includes the following developed countries: 11) Japan; 12) Australia; 13) Switzerland; 14) the United States of America; 15) Monaco; 16) Singapore; 17) Germany; 18) France; 19) New Zealand; 20) Andorra.

For comparison, here are a few more figures that apply to Eastern Europe. Belarus ranks 38th, Lithuania 40th, the Czech Republic 41st, Poland 44th, Slovakia 45th, Moldova 61st, Ukraine 73rd, and Armenia 74th. It is obvious that the 73rd place for Ukraine in the world ranking is quite low. This shows that Ukrainian realities need innovative development, and issues of global electronic communication in the context of sustainable development of the world require special research, in particular, the formation of conceptual foundations of the legal status of human relations and work.

Today, researchers seek to know both the distant past of human development and the distant

future of civilization. Yu. Harari believes that it is time to think about the present and look closely, to analyze what changes await us in the future. The author's plans are global in nature, and therefore in his research he draws attention to the main forces that shape societies around the world and are able to influence the future of our planet as a whole. Obviously, the observation and analytical generalization of the behavior of individuals and entire countries is a project that aims at a global perspective [7, c. 10-11].

Therefore, dreams, thoughts, ideas, innovations and know-how, which are covered in this study, without exaggeration, determine the agenda of development strategies to prevent and combat space and ground cyber threats to humanity in the third millennium.

This study raises a number of extremely important strategic issues that relate not only to the prospects of individual countries and regions, but also completely unconventional specific tasks of innovative development of cybersecurity, education, science, culture, medicine, economics and other areas of human life.

Based on these priorities, which are covered in this paper, we believe that the "Intelligence Industry", "Knowledge Industry" and "Global Innovation Communication" – are the modern locomotives of civilization, which identifies the latest areas of cybersecurity in space and terrestrial electronic space, and as well as the strategy, tactics and art of building a world order for a better secure future.

The main purpose of our study is to find a methodology for the formation of the latest security knowledge in space and terrestrial cyberspace and to develop a strategy for adapting modern knowledge, skills and abilities to the requirements and needs of Industry 4.0 and the fourth industrial revolution.

According to the defined concept, the results of the study have already been partially published in a number of scientific papers. In accordance with this goal, this study formulates the basic provisions for the formation of conceptual provisions of cybersecurity of electronic civilization and identifies the conceptual foundations of the innovative future of Ukraine [1, c. 14-15].

According to the chosen strategy of creative search, this study focuses on three different approaches to the development of the digital society – a philosophical, innovative, communication and cybersecurity, which simultaneously complement each other. The first is a philosophical worldview, which highlights the conceptual foundations of the formation and development of the digital society. The second is analytical (innovation-communication), which allows to assess the essential features of the development and implementation of innovative communication in the digital space. This approach allows us to understand the real possibilities of "Industry 4.0" and helps to develop recommendations to improve the efficiency of its operation. The third is communication and cybersecurity. It helps to determine the likelihood of the proposed changes and to anticipate possible cyber threats, cyber risks and cyber threats, and offers specific mechanisms, procedures and measures to prevent and counter these cyber threats.

The main characteristics of the desired independent, democratic Ukraine can be grouped into four spheres of life: political, economic, social and environmental.

In the political sphere, it is a true democracy to ensure constitutional human rights, freedom of speech, free elections at all levels, equality before the law, a strong and independent judiciary, and the distinction between business and politics.

In the economic sphere, it is competitiveness in domestic and foreign markets, knowledge-

intensive rather than energy- and resource-intensive structure of the economy, free market, high rate of innovation, professional management of enterprises, rapid gross domestic product growth, low inflation, material well-being, low unemployment (certain the unemployment rate is needed for labor mobility, for changes in the structure of the economy, enterprise restructuring, the introduction of new technologies).

In the social sphere, it is a high level of science and education, good health, sufficient wages and pensions, the opportunity to work in retirement and, most importantly, social justice by reducing the gap between the very rich and the very poor.

In the environmental sphere, this is a transition to a model of sustainable development. The biosphere in which we live (clean air, water and land, natural resources) is limited. It should be valued as "authorized capital" and not as annual income.

The above-stated provisions systematically set out the state worldview concept, as well as indicate what necessary specific actions and events should be implemented for the quality development of a sovereign and independent, democratic, social, legal Ukrainian state.

Thus, the above educational, scientific, legal, innovation-communication and resource guidelines allow us to formulate the latest concept, an effective platform for reliable protection against space and ground cyber threats to civilization in today's electronic world, which has long gone beyond our planet.

References

1. Bilenchuk P. *Stratehiia innovatsiinoi komunikatsii v suchasnomu tsyfrovomu sviti: pravove, naukove y resursne zabezpechennia* [Strategy of innovative communication in the modern digital world: legal, scientific and resource provision]. *Yurydychnyi Visnyk Ukrainy– Legal Bulletin of Ukraine*. 2018. No. 7(1180). P. 10-17 (in Ukrainian).

2. Bilenchuk P.D., Malii M.I. *Kosmichna y elektronna kiberzlochynnist: zahrozy i vyklyky novoho tysiacholittia* [Space and electronic cybercrime: threats and challenges of the new millennium]. *Yurydychnyi Visnyk Ukrainy– Legal Bulletin of Ukraine*. 2019, No. 40. P. 11-18 (in Ukrainian).

3. Bilenchuk P.D., Malii M.I. *Suchasni kompiuterni zlochyntsi ta kiberterorysty: novitni tekhnolohii na sluzhbi orhanizovanoho zlochynnoho svitu* [Modern cybercriminals and cyber-terrorists: the latest technology in the service of the organized crime world.]. *Biznes i bezpeka– Business and security*. 2019. No. 4. P.1-7 (in Ukrainian).

4. Lykhova S.Ia., Bilenchuk P.D. *Kosmichni i nazemni kiberzahrozy tretoho tysiacholittia: zasoby piznannia, dokazuvannia, rozsliduvannia* [Space and ground cyber threats of the third millennium: means of knowledge, evidence, investigation]. Naukovi pratsi Natsionalnoho aviatsiinoho universytetu. Seriia: Yurydychnyi visnyk "Povitriane i kosmichne pravo", Kyiv: NAU – Scientific works of the National Aviation University. Series: Legal Bulletin "Air and Space Law", Kyiv: NAU Publ., 2021. No. 2 (59). P. 9-17 (in Ukrainian).

5. *OAE stvoriuie pershyi u sviti kosmichnyi sud*. Veb-sait: Ukrinform [The UAE is creating the world's first space ship. Website: Ukrinform]. URL: https://www.ukrinform.ua/rubric-world/3183255-oae-stvorue-persij-u-sviti-kosmicnij-sud.html (in Ukrainian).

6. Sosnin O. *Ideolohiia «suspilstva znan»: novi zavdannia osvity i nauky* [The ideology of the «knowledge society»: new challenges of education and science]. *Yurydychnyi Visnyk Ukrainy – Legal Bulletin of Ukraine*, 2017. №17. P. 10-17 (in Ukrainian).

7. Kharari Yuval Noi. *21 urok dlia 21 stolittia* / per. z anhl. O. Demianchuka[Harari Yuval Noah. 21 lessons for the 21st century / trans. from English O. Demyanchuk]. Kyiv: Fors Ukraina Publ., 2018. 416 p. (in Ukrainian).

8. Lykhova S., Svintsytskyi A., Padalka A., Nizovtsev Y., Lyseiuk A. Utilization of Technologies of Digital Identification of the Person on the Image: Criminal Law Aspect. *Studies of Applied Economics*. 2021. No. 39 (9). (SCOPUS). URL: http://ojs.ual.es/ojs/ index.php/eea/article/view/5765.

9. The Malicious Use of Artificial Intelligence: Forecasting, Prevention, and Mitigation. February 2018. URL: https://img1.wsimg.com/blobby/go/3d82daa4-97fe-4096-9c6b-376b92c619de/downloads/MaliciousUseofAI.pdf?ver=1553030594217.

Лиховая С.Я.♦

DOI: 10.25108/2304-1730-1749.iolr.2022.67.104-110
УДК: 004.056.5:343.326 (045)

Анализ киберугроз в современном электронном мире

Аннотация:

Введение. В современных условиях развитие информационных технологий приводит к нарушениям прав и свобод как личности, так и государства. **Цель и задачи.** Исследовать такие элементы киберугроз в современном мире, как информационные угрозы (киберугрозы) наземные и космические. **Методы.** Разработаны общенаучные методы познания, с помощью которых автор решает вопросы познания, доказывания, расследования космических электронных преступлений, совершенных в киберпространстве. **Полученные результаты.** Автор подчеркивает необходимость специальных исследований космической киберпреступности, так как подобные криминогенные явления угрожают национальной безопасности Украины. **Выводы.** Автор констатирует, что современное состояние законодательства о предупреждении и борьбе с космической киберпреступностью является недостаточно совершеным, в связи с чем требуется принятие соответствующих конвенций и законов как на глобальном, так и на национальном уровне. Автор предлагает разработать межгосударственные стандарты обеспечения кибербезопасности наземного и космического киберпространства, гарантировать неотъемлемые и неприкосновенные конституционные права и свободы человека и гражданина. А также обратить внимание разработчиков новейших электронных средств кибербезопасности, креативных методов и грид-технологий электронной разведки на необходимость технологического предотвращения и противодействия возможнымкиберугрозам неправомерного использования космического пространства и электронной разведки в различных сферах земной и космической жизни. Международная ассоциация ведущих элек-

♦ **Лиховая София Яковлевна** – доктор юридических наук, профессор, заведующая кафедрой уголовного права и процесса юридического факультета Национального авиационного университета, Киев (Украина). E-mail: k_kpipp@ukr.net

тронных государств мира должна создать для формирования, разработки и внедрения единых стандартов безопасности для предоставления услуг электронного доверия по всему миру. Кроме того, соответствующим международным организациям, органам и учреждениям безопасности мира необходимо разработать упорядоченную правовую, организационную и технологическую систему предотвращения и пресечения вредоносного использования космического пространства и радиоэлектронной разведки на национальном, региональном и межгосударственном (глобальном) (трансграничный, транснациональный, трансконтинентальный), планетарный, космический (ближний космос, дальний космос)).

Ключевые слова: космическая киберпреступность; электронное киберпространство; кибербезопасность.

Библиография

1. Біленчук П. Стратегія інноваційної комунікації в сучасному цифровому світі: правове, наукове й ресурсне забезпечення. *Юридичний Вісник України*. 2018. №7(1180). С. 10-17.

2. Біленчук П.Д., Малій М.І. Космічна й електронна кіберзлочинність: загрози і виклики нового тисячоліття. *Юридичний Вісник України*. 2019, № 40. С. 11-18.

3. Біленчук П.Д., Малій М.І. Сучасні комп'ютерні злочинці та кібертерористи: новітні технології на службі організованого злочинного світу. *Бізнес і безпека*, 2019. №4. С.1-7.

4. Лихова С.Я., Біленчук П.Д. Космічні і наземні кіберзагрози третього тисячоліття: засоби пізнання, доказування, розслідування. *Наукові праці Національного авіаційного університету. Серія: Юридичний вісник «Повітряне і космічне право».* - Київ: НАУ, 2021. № 2 (59). С. 9-17.

5. ОАЕ створює перший у світі космічний суд. Веб-сайт: Укрінформ. URL: https://www.ukrinform.ua/rubric-world/3183255-oae-stvorue-persij-u-sviti-kosmicnij-sud.html

6. Соснін О. Ідеологія «суспільства знань»: нові завдання освіти і науки. *Юридичний Вісник України*. 2017. №17. С. 10-17.

7. Харарі Ювал Ной. 21 урок для 21 століття / пер. з англ. О. Дем'янчука. - Київ: Форс Україна, 2018. 416 с.

8. Lykhova S., Svintsytskyi A., Padalka, A., Nizovtsev, Y., Lyseiuk A. Utilization of Technologies of Digital Identification of the Person on the Image: Criminal Law Aspect. *Studies of Applied Economics*. 2021. № 39 (9). (SCOPUS). URL: http://ojs.ual.es/ojs/ index.php/eea/article/view/5765

9. The Malicious Use of Artificial Intelligence: Forecasting, Prevention, and Mitigation. February 2018. URL: https://img1.wsimg.com/blobby/go/3d82daa4-97fe-4096-9c6b-376b92c619de/downloads/MaliciousUseofAI.pdf?ver=1553030594217