Co-funded by
the European Union

EuroHybSec

Erasmus+
Jean Monnet
Programme

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
Національний університет «Острозька академія»

ЕРАЗМУС+ МОДУЛЬ ЖАНА МОНЕ
«Саморегульоване вивчення гібридних загроз
і європейської безпеки»
(Project number: 101081342 – EuroHybSec –
ERASMUS-JMO-2022-HEI-TCH-RSCH
https://eurohybsec.oa.edu.ua/)

РОЗВИТОК БЕЗПЕКОВИХ СТУДІЙ В УКРАЇНІ: ДОСВІД КРАЇН ЄС

МАТЕРІАЛИ
КРУГЛОГО СТОЛУ

17 вересня, 2024 р.

Острог
Видавництво Національного університету «Острозька академія
2024

УДК 355/359(477+4)
Р64

Рецензенти:

Роман Мартинюк, кандидат політичних наук, доцент кафедри державно-правових дисциплін Національного університету «Острозька академія»;

Оксана Матласевич, доктор психологічних наук, доцент, завідувач кафедри психології та педагогіки Національного університету «Острозька академія».

Р64 Розвиток безпекових студій в Україні: досвід країн ЄС: матеріали Круглого столу (м. Острог, 17 вересня, 2024 р.) / за ред. Едуарда Балашова, Дениса Гаврилюка. Острог: Видавництво Національного університету «Острозька академія», 2024. 36 с.

DOI 10.25264/17.09.2024-1

У збірнику представлені матеріали доповідей учасників Круглого столу на тему: «Розвиток безпекових студій в Україні: досвід країн ЄС»/ «Developing security studies in Ukraine: the experience of EU’s countries», який відбувся у Національному університеті «Острозька академія» в рамках виконання проєкту Еразмус+ Модуль Жана Моне «Саморегульоване вивчення гібридних загроз і європейської безпеки» / Erasmus+ Jean Monnet Module «Self-Regulated Studies of Hybrid Threats and European Security» (101081342 – EUROHYBSEC – ERASMUS-JMO-2022-HEI-TCH-RSCH).

В рамках круглого столу викладачі, науковці, фахівці та експерти у сфері вивчення гібридних загроз та безпекових студій представили доповіді, що стосуються досліджень безпекових студій в Україні з використанням досвіду ЄС. Круглий стіл був використаний як платформа для обміну знаннями та ідеями щодо розвитку та вдосконалення безпекових студій в Україні з використанням досвіду ЄС.

УДК 355/359(477+4)

Проф. Анатолій Худолій / Prof. Anatoliy Khudoliy,
Національний університет Острозька академія» (Україна) /
National University of Ostroh Academy (Ukraine)

GEOPOLITICAL TRANSFORMATION OF THE MODERN WORLD AS A FACTOR OF INFLUENCE ON THE INTELLIGENCE ACTIVITY OF THE UKRAINIAN STATE

Introduction.

Global problems are of a planetary nature, affecting the interests of all peoples of the world, need urgent solutions, and require collective efforts and joint action by all nations. Local military conflicts and hybrid wars on geopolitical and territorial grounds (for example, between Israel and Palestine, Ukraine and the Russian Federation) are one of the most complex global threats in the 21st century. After all, these confrontations have become a challenge for the whole world, as they threaten to completely destabilize the world order. The geopolitical development of modern societies has changed the priorities in global problems: some experts consider the energy and raw materials problem to be a priority, while others consider the geopolitical distribution of territories and spheres of influence in the world. Therefore, among the global problems of the last twenty years, peace and disarmament, environmental, food, demographic, energy and raw materials issues are most often mentioned. And among the global problems of the last 3 years is Russian aggression against Ukraine.

An analysis of the main trends in the current geopolitical situation shows that a new multipolar model of the world order is being formed, within which new centers of power are emerging alongside the United States, including China, the EU, India, Brazil, Russia, and others. The interests of each of these countries do not coincide in the political, economic, security and other spheres, which leads to confrontation between them at both the global and regional levels, and as a result – to increased global instability, wars or armed conflicts. At the same time, there is a decline in the effectiveness of leading international organizations, including the UN and the OSCE, in the political settlement of existing security problems. This is evidenced by the military conflicts in Georgia and Ukraine, as well as developments around Syria and Israel.

Because new threats to Ukraine's national interests never stop emerging, and world nations' foreign priorities keep changing, the DIU leadership pays extra attention to maintaining and improving of DIU staff's professionalism, development of the infrastructure. New areas of interests are constantly researched, international cooperation is actively maintained. In addition, the DIU directly contributes to the development of Ukrainian legislature on a regular basis.

Unprovoked Russian aggression against Ukraine caused significant changes in activity of Ukraine's military and intelligence service. The full-fledged war sparked by Moscow in 2022 set new goals not only for the Ukrainian militaries, but also for the defence intelligence of Ukraine. The DIU (Defence Intelligence of Ukraine) had to reevaluate its activities and make changes in approaches, functioning and carrying out of special military operations. All the activities of the DIU concerned the essence of its mission, tasks and values. The war waged by Moscow made corrections not only in functioning of the intelligence organization, but also in the life of the whole country, society, all Ukrainians.

Regarding the main tasks of intelligence, they are as following: timely providing consumers with intelligence information; promoting the implementation of the national interests of Ukraine; countering external threats to the Ukraine's national security in spheres determined by the law. The Defence Intelligence of Ukraine conducts intelligence in the defence, development of military capability, military and military-technical as well as cybersecurity areas [10]. There are differences in intelligence activities assessing them during the peaceful time and the warfare.

The warfare reshaped the perception and the attitude of the intelligence officers. As it is said in the definition of the tasks – We protect the national interests of Ukraine, counter threats to national security, and provide intelligence to the country's leadership and the Armed Forces of Ukraine. DIU conducts a wide range of operations: cyber space, marine and ground operations.

Since the beginning of the full-scale invasion, Ukrainian military intelligence specialists have conducted over a hundred large-scale cyber operations in the territory of the russian federation. Ukrainian specialists secretly extracted tens of terabytes of data about the enemy. This data is collected, analyzed, and used by the Defence Intelligence of Ukraine, the Security Service of Ukraine, and the Armed Forces of Ukraine to inflict damage on the enemy. Military intelligence specialists also engage in other types of cyber operations, the aim of which is to damage and destroy the enemy's equipment used for transmitting information or for the functioning of the financial and economic activities of specific institutions or companies [6].

For instance, in 2024 Ukrainian intelligence has again attacked the largest banks of the Russian Federation. The Defence Intelligence of Ukraine have carried out another DDoS attack on the Russian banking system. The operation disrupted the work of the largest banking institutions of the aggressor state, which support the activities of the occupation forces of the Russian armed forces. In particular, the cyberattack targeted Bank Rossiya, Tinkoff Bank, Gaz Bank, and the SBP payment system [4].

In late May, hackers from the Defense Ministry's Main Intelligence Directorate (GUR) launched a large-scale DDoS attack targeting Russian providers. Russians complain and call it "the most powerful in history." The attack left at least 250,000 subscribers in the temporarily occupied territories of Ukraine, including Crimea, without communication. Both the subscriber networks and the networks of operators that used the affected infrastructure were affected. According to the CEO of one of the Russian operators, most subscribers were left without communication for more than two days. Representatives of providers reported difficulties in communicating with subscribers, as they refused to provide operators with their up-to-date information for fear of fraud. In particular, 20% refused to modernize network equipment that could protect them from attacks in the future [2].

Russian companies have received letters reminding them of the inevitable reckoning for the war against Ukraine. Activists of the cyber community BO_Team together with the DIU specialists attacked facilities in the territory of the aggressor state of Russia. This was reported by the Defence Intelligence of Ukraine. “Destroying important data and equipment, paralyzing work, causing damage and creating a bad mood in Russia,” the statement said.

Over the past week of June 2024, cyber specialists together with the GUR destroyed: 1) more than 100 terabytes of data from OrbitSoft, a software developer that fulfilled contracts for the Russian occupation army; 2) all data on 8 servers of Orient Systems, a developer and supplier of navigation equipment. The company cooperated with Russian manufacturers of military equipment, including UAVs; 3) all data on 19 servers of Internet providers in the city of Nizhny Novgorod – Linktelecom NN and Access Telecom. “All subscribers of these providers have received letters reminding them of the inevitable reckoning for the war against Ukraine,” the statement added [1].

Naval Drones of the Defence Intelligence of Ukraine Dominate the Black Sea. A proud achievement of the DIU’s successful operations is the destruction of ships of the russian black sea fleet using the “Magura” unmanned marine vehicles. The boat was first presented at the International Defence Industry Fair (IDEF), which took place from 25 to 28 July 2023 in Istanbul, Turkey.

The first target of the DIU’s naval drones on May 24, 2023, was the russian reconnaissance ship “Ivan Khurs”, successfully attacked by three drones 140 km northeast of the Bosphorus Strait. On August 1, 2023, the 22160-project ship “Serhii Kotov” was sunk 340 km from Sevastopol. On November 10, 2023, as a result of an operation by Ukrainian military intelligence in Crimea, two russian boats sank: one from the older project 1176 “Acula”, and the other, newer one from project 11770 “Serna”. On February 1, 2024, six “Magura V5” drones attacked the russian missile boat “Ivanovets”. It sank, and all crew members (approximately 40 people) were killed. Several landing boats near the Black Sea were also destroyed. On February 14, 2024, a large assault ship “Cezar Kunikov” was sunk near Alupka. On March 5, 2024, “Group 13” the Special Forces unit of the Defence Intelligence of Ukraine finally sank the patrol ship “Sergey Kotov” of the black sea fleet of the russian federation. On May 6, 2024, in Narrow Bay, the unit of the Defence Intelligence of Ukraine “Group 13” destroyed the russian high-speed patrol boat of project 12150 “Mangust” using the strike sea drone “Magura V5”. On May 30, 2024, the Special Forces personnel from “Group 13” destroyed two russian border guard boats of the russia’s fsb type KS-701 “Tunets” and damaged two more vessels of the same type using the strike sea drones “Magura V5”. On June 6, 2024, the Special Forces unit of the 9th Department of the Defence Intelligence of Ukraine near the shores of the temporarily occupied Crimea successfully struck the russian raid tug of project 498 “Saturn” or “Protei” [7].

Long-Range Aviation is also a priority target for the DIU units. On January 14, 2024, as a result of a successful joint operation of the Defence Intelligence of Ukraine and the Air Forces of the Armed Forces of Ukraine, a russian long-range radar detection aircraft A-50U was destroyed, and its crew perished. An airborne command post the Il-22M was also shot down, which, despite severe damage, managed to land in Anapa. On April 19, 2024, a similar scenario unfolded 308 km away from the launch site of an anti-aircraft missile, resulting in the destruction of a russian strategic bomber Tu-22M3 [5].

The Defence Intelligence of Ukraine actively apply strike UAVs of reach the enemy everywhere. On April 17, 2024, special forces personnel of the Defence Intelligence of Ukraine attacked the 590th separate radio-technical node of military unit no. 84680 located in the russian town of kovylkino (mordovia) using UAVs. The over-the-horizon 29B6 “Container” radar with a detection range of 3,000 kilometres and a detection height of 100 kilometres was destroyed. The distance from the Ukrainian border to the impact site is approximately 680 kilometres.

On the night of 24 April, drones of the Defence Intelligence of Ukraine attacked the Novolipetsk Metallurgical Plant in the russian city of lipetsk. On May 27, a drone of the Defence Intelligence of Ukraine set a record for the range of flight and attacked a radar station in russia at a distance of over 1800 kilometres. It hit the "Voronezh M" radar in orsk, orenburg region of the russian federation.

On June 8, 2024, at the "Akhtubinsk" airfield in the astrakhan oblast of the russian federation, located 589 km from the line of contact, the most advanced multirole fighter of the aggressor state Su-57 was successfully hit, and another aircraft of the same class was damaged. This is the first case of hitting a Su-57 in history [8].

The Return of Control Over the "Boiko's Towers". In early September 2023, intelligence officers of the "Artan" Special Forces unit of the DEfence Intelligence of Ukraine carried out a daring operation and liberated the so-called "Boiko's Towers" – drilling gas production platforms on the Black Sea shelf between Zmiinyi Island and the western coast of Crimea, captured by the russians back in March 2014. In particular, control was regained over the drilling platforms "Petro Hodovalets" and "Ukraine", as well as the self-elevating drilling rigs "Tavrida" and "Sivash". During the operation, Special Forces men managed to capture valuable trophies: stocks of unguided aviation rockets (UAR) and destroy the "Neva" radar system, which tracked the movement of vessels in the Black Sea [9].

The DIU units participated in defence of Avdiivka, Vovchansk, in the Battle for Chasiv Yar. In May 2024 GUR drones had attacked a refinery and three military airfields in Russia. In particular, a Tu-22M3 bomber was damaged at the Olenya airfield [3].

Conclusions. Due to circumstances the DIU makes corrections in its activities. DIU is indispensable component of the Ministry of Defence of Ukraine. Its goals are shaped by interest and values of the Ukrainian state. The unprovoked aggression of the russian federation stimulated activities of the DIU, its methods, approaches and techniques that vary from special military operations to cyber space operations.

Improving effectiveness of its activities, the DIU fruitfully cooperates with its partners in Europe and around the world.

1. Holovchak Khrystyna. Khakery HUR atakuvaly rosiiski kompanii, yaki pidtrymuiut viinu. TSN. 29.06.2024. URL: https://tsn.ua/svit/hakeri-gur-atakuvali-rosiyski-kompaniyi-yaki-pidtrimuyut-viynu-2610819.html

2. Kuznietsova Kateryna. Naipotuzhnisha v istorii": khakery HUR zdiisnyly masshtabnu DDos-ataku proty provaideriv RF – ZMI. TSN. 01.07.2024.URL: https://tsn.ua/svit/naypotuzhnisha-v-istoriyi-hakeri-gur-zdiysnili-masshtabnu-ddos-ataku-proti-provayderiv-rf-zmi-2612019.html

3. Labiak Iryna. Zelenskyi nazvav dosiahnennia HUR v atakakh uhlyb Rosii. TSN. 29.07.2024. URL: https://tsn.ua/ato/zelenskiy-nazvav-dosyagnennya-gur-v-atakah-uglib-rosiyi-2629836.html

4. Poliakovska Tania. Ukrainska rozvidka zdiisnyla novyi kiberudar po naibilshykh bankakh RF. UNIAN. URL: https://www.unian.ua/war/ukrajinska-rozvidka-zdiysnila-noviy-kiberudar-po-naybilshih-bankah-rf--dzherelo-12757524.html

5. Destruction of Enemy Long-Range Aviation. DIU. URL: https://gur.gov.ua/en/content/znyshchennia-vorozhoi-dalnoi-aviatsii

6. Operations of Defence Intelligence of Ukraine In Cyberspace. DIU. URL: https://gur.gov.ua/en/content/operatsii-hur-v-kiberprostori

7. Naval Drones of the Defence Intelligence of Ukraine Dominate the Black Sea. DIU. URL: https://gur.gov.ua/en/content/morski-drony-hur--dominuiut-u-chornomu-mori

8. Strike UAVs of the Defence Intelligence of Ukraine Reach the enemy Everywhere. DIU. URL: https://gur.gov.ua/en/content/udarni-bpla-hur--dosiahaiut-voroha-skriz

9. The Return of Control Over the "Boiko's Towers". DIU. URL: https://gur.gov.ua/en/content/povernennia-kontroliu-nad-vyshkamy-boika

10. What we do. Defence Intelligence of Ukraine. Access mode: URL: https://gur.gov.ua/en//content/directions.html#tasks

Мгр. Магдалена Вронська / Mgr Magdalena Wrońska,
Університет Яна Кохановського у Кельце (Польща) /
Jan Kochanowski University in Kielce (Poland)

APPLICATIONS OF ARTIFICIAL INTELLIGENCE IN CYBERSECURITY AND DEFENSE OF UKRAINE

The purpose of this study is to highlight the economic aspects of using AI in cybersecurity within a highly responsible sector such as defense. The economic risks arising from improper implementation of artificial intelligence (AI) in defense and cybersecurity are multifaceted and can lead to significant financial and operational consequences. Incorrect deployment of AI algorithms, especially in sectors crucial to national security, can result in unpredictable complications [6]. As a result, these systems may become increasingly difficult to control, generating substantial operational and maintenance costs that may outweigh the initial technological benefits.

Artificial intelligence is one of the most rapidly developing technologies, with the potential to fundamentally transform nearly every aspect of operations [1]. An analysis of various definitions and concepts of AI reveals the key elements that characterize this field:

- Simulation of Human Intelligence: Most definitions emphasize that AI aims to mimic or replicate human intelligence in machines and computer systems [5].
- Learning and Adaptation Ability: AI systems are characterized by their ability to learn from experiences and adapt to new situations [10].
- Problem Solving: AI is designed to solve complex problems and make decisions in a manner similar to humans [1].

- Data Processing and Analysis: AI systems are capable of collecting, processing, and analyzing vast amounts of data to draw conclusions and make decisions [9].
- Interaction with the Environment: AI can respond to its environment, both physical and digital [11].

The costs of implementing artificial intelligence (AI) in defense are significant and include both technology and infrastructure expenses and risk management. From an economic perspective, it is crucial to ensure that AI implementation processes are closely monitored and that systems are optimally adapted to specific defense requirements. Neglecting these aspects can lead to excessive financial burdens that exceed the planned benefits of using new technologies. One of the key problems in high-responsibility sectors such as defense is the failure to adapt AI systems to actual needs, which often results in inefficiency and cost escalation. The costs of implementing AI depend largely on the chosen implementation model. Companies can use ready-made solutions available on the market, which are cheaper but less flexible, or decide to create their own models, which requires larger investments and a longer implementation time [2]. Examples of companies from the defense sector show that even a five-month implementation period is the norm, especially for more complex, customized AI systems.

Additionally, one of the main risks is the insufficient understanding by decision-makers of what problems AI is supposed to solve. Many AI projects fail due to a lack of adequate data or a poor fit between technology and real user needs. Organizations can spend significant resources on advanced algorithms that do not deliver tangible results, ultimately leading to wasted resources [6].

Another major challenge is the operational costs associated with ensuring the security and control of autonomous systems. The need for a constant human presence in the decision-making process to avoid risks related to the reliability and ethics of using AI in armed conflicts further increases operational expenses. Long-term savings can result from the automation of logistics processes, resource management, and intelligence analysis, but implementation costs are high enough to limit the scale of projects in the short term [6].

Another important factor influencing costs is the need for data infrastructure. In defense, as in other sectors, data collection and management are key, but many companies indicate that the lack of consistent data systems significantly increases the costs of implementing AI. Challenges related to data integration can lead to delays and additional costs related to infrastructure modernization [8].

The economic risks resulting from the improper implementation of artificial intelligence (AI) in the defense sector are significant and can lead to serious financial and reputational losses.

Another problem is the risk associated with AI model errors, which can lead to inadequate decisions, especially in critical defense systems. For example, models can inadvertently discriminate against certain user groups or incorrectly process data, which can consequently create security gaps that can be exploited by adversaries. It is crucial to implement broad risk control mechanisms throughout the AI development cycle, which will allow for more effective identification of threats, such as data errors or lack of transparency in decisions made by algorithms. Companies that neglect such mechanisms risk both their finances and reputation, which in the case of defense applications can lead to catastrophic consequences [8].

The implementation of AI in the defense sector can contribute to increased innovation and stimulate economic development. AI has the potential to increase productivity not only in the defense sector itself, but also in other sectors of the economy through effective process automation, data analysis, and decision support. Modern AI technologies, unlike previous solutions, require lower capital outlays due to the possibility of using data and cloud services, which can accelerate adaptation in various industries [7]. Economic benefits resulting from the use of AI in defense also include the development of technology companies and the creation of new jobs in fields related to research, software development, and cybersecurity [3].

Inadequate implementation of AI is associated with the possibility of data and privacy breaches. AI can be misused in cyberattacks, which causes financial losses related to the need to rebuild systems and protect information. Companies and military institutions that implement AI without proper security measures may become targets of attacks, which in the context of the war in Ukraine could have catastrophic consequences for the country's defense [4].

1 A. Jabłoński, M. Jabłoński, Sztuczna inteligencja (ai) w kształtowaniu cyfrowych modeli biznesu pozytywnie wpływających na zmiany klimatyczne, Wyższa Szkoła Bankowa w Poznaniu, Poznań 2021

2. A. Singla, A. Sukharevsky, L. Yee and other, The state of AI in early 2024: Gen AI adoption spikes and starts to generate value QuantumBlack, AI by McKinsey and McKinsey Digital, 2024

3. B. Pavel, I. Ke, M. Spirtas and other, AI and Geopolitics How Might AI Affect the Rise and Fall of Nations?, Objective Analysis. Effective Solutions,-Published by the RAND Corporation, 2023

4. D. Broom, AI: These are the biggest risks to businesses and how to manage them, World Economic Forum, 2023

5. D.A. Agbaji, B.D. Lund, N. R. Mannuru, Perceptions of the Fourth Industrial Revolution and Artificial Intelligence Impact on Society, "arXiv (Cornell University)" 2023, vol. 1

6. F.E. Morgan, B. Boudreaux, A.J. Lohn and other, Military Applications of Artificial Intelligence Ethical Concerns in an Uncertain World, Published by the RAND Corporation, Santa Monica, Calif, 2020, s. 85

7. J. T. Gonzales, Implications of AI innovation on economic growth: a panel data study, Journal of Economic Structures, Article number: 13, 2023

8. R. Doucette, S. Hilaire, V. Marya and other, Digital: The next horizon for global aerospace and defense, McKinsey&Company, 2021

9. K. Różanowski, Sztuczna inteligencja rozwój, szanse i zagrożenia, "Zeszyty Naukowe Warszawskiej Wyższej Szkoły Informatyki" 2007, nr 2

10. R. Stępień, Możliwości zastosowania sztucznej inteligencji i blockchain w działalności archiwalnej. Przegląd doświadczeń zagranicznych, "Archeion" 2021, nr 122

11. W. Robaczyński, Sztuczna inteligencja–przedmiot badań czy podmiot kontrolowany. Prawo wobec rozwoju technologii, "Kontrola Państwowa" 2022, nr 407

Д-р. Ярослав В. Пшибитньовський /
Dr. Jarosław W. Przybytniowski,
Університет Яна Кохановського у Кельце (Польща) /
Jan Kochanowski University of Kielce (Poland)

RISK OF ENVIRONMENTAL DISASTERS UNDER THE CONDITIONS OF LOCAL SECURITY CONSTRUCTION

Introduction.

In the market of industrial clients in the European Union, as well as in Poland, information related to the risk of formation of ecological risks has not yet been disseminated. The study has a scientific and research character and is a prelude to the research being carried out, in the field of the emergence of ecological risks, taking into account pro-ecological revenues and expenditures by governmental institutions. The research is conducted on secondary as well as primary statistical data from official websites and surveys. The research is conducted on the territory of Poland, broken down by voivodeship. Thus, the scientific and research objective of the study is to seek to understand and analyse the risks of environmental disasters under conditions of sustainable development and the associated expenses, as well as to draw attention to one of the methods of financing these risks – environmental insurance. The author also drew attention to potential environmental risks, the costs of restoring the polluted environment to its original form at the institutional level. To carry out the research, statistical methods were used: spatial-differential.

Keywords: risk, environmental hazards, sustainability, Zero Waste, environmental insurance, spatial differentiation

The course of research

The risk of causing environmental damage is a new challenge for public administration, as well as for insurers, not only in Poland but also in the European Union (EU). Environmental protection directed at the revenues and costs resulting from the necessity to: appear this risk, reduce the negative impact on the environment, restore the environment to its previous state and prevent or remedy environmental damage is a relatively new issue. Indeed, environmental remediation is costly and lengthy. The disregard of this topic by public administration, regardless of the level of management, may result in significant financial complications, not only for enterprises but also for budgets: municipalities, districts or voivodeships themselves.

The construction of the article is subordinated to the hypothesis that the appropriate level of revenues and outgoings related to the appearance of ecological risks, as well as the appropriate construction of insurance contracts, can be a method of appropriate financing of these risks, at the level of governmental and pro-governmental institutions. Thus, the author argues that the appropriate level of income and outgoings associated with economic insurance are an important method of counteracting the effects of the emergence of risks of ecological damage in the aspect of sustainable development, for entities and persons interested and not interested in the emergence of these risks.

According to scientists, ecological damage is the negative environmental impact caused by excessive pollution of the environmental components: air, water and soil, or by changes in the ecosystems within the range of the perpetrator B [2, 3].

Reflections on risk and uncertainty theory in economic theory indicate [6], że *istota polega na sprzeczności tych zjawisk w odniesieniu do racjonalnych zachowań gospodarczych, czyli niepewność jest czymś innym niż ryzyko. Problem niepewności w rzeczywistości ekonomicznej występuje, kiedy podejmujący decyzję nie zna konsekwencji jego wyboru, np. działania sił przyrody niemożliwych do przewidzenia, a nawet do rozpoznania. Spowodowało to, że badania nad zjawiskiem ryzyka i niepewności* *zaowocowały wypracowaniem modeli i teorii ekonomicznych dopiero w drugiej dekadzie dwudziestego wieku («that the essence lies in the contradiction of these phenomena in relation to rational economic behaviour, i.e. uncertainty is something different from risk. The problem of uncertainty in economic reality occurs when the decision-maker does not know the consequences of his or her choice, such as the action of natural forces impossible to predict or even to recognise. This led to research into the phenomena of risk and uncertainty resulting in the development of economic models and theories only in the second decade of the twentieth century».).*

Environmental risks are associated with activities whose effects result in adverse changes to the environment and vary considerably in scope and degree of impact, ranging from sudden phenomena such as accidents or incidents to long-term phenomena such as damage to building infrastructure due to landslides, adverse effects on the health of the population. *In view of the diversity of environmental risks, they can be subdivided and a distinction can be made between environmental risks sensu stricto (environmental risks), i.e. the possibility of a deterioration in the level of environmental quality, a violation of the natural balance or the occurrence of a natural disaster, and risks sensu largo comprising health, cultural, material and financial risks.*

According to D. Maśniak [4], the sources of environmental risk are the use of the environment, the introduction of changes to it, the action of natural forces of nature and the use of legal and administrative instruments. On the other hand, Insurance risk – is the uncertainty about a specific event under conditions of two or more possibilities. In this sense, it is a measurable uncertainty as to whether the intended purpose of an action will be achieved. The second definition focuses attention on issues of insurance practice, stating that a risk is an insured person or insured entity [6].

In their paper E. J. Vaughan, T. Vaughan [9] gave some of the most common definitions of insurance risk, including: – risk is the chance of loss occurring – it is the possibility or probability that something will happen, or as the degree of that probability. The first of these meanings treats risk as the chance of loss, which is not measurable. The chance of loss is quantifiable as a percentage or fraction [8].

When analysing the essence of ecological risk, it is important to note that there is often no possibility of compensating the damage in relation not only to specific persons, but also to objects. Thus, in current law there is the principle that the «polluter pays». This principle means that environmental damage is the financial responsibility of the polluter [1, 11].

The table below presents a basic classification of ecological damage:

Table 1: Ecological damage (caused by environmental impact)

Environmental damage	**Szkoda na osobie lub na mieniu**
Environmental costs – borne by the state or municipality	Environmental costs – borne by the entity
Loss of benefits associated with environmental pollution – borne by the state or municipality	Loss of benefits associated with environmental pollution – borne by the entity
Impairment or damage to the environment as: • a common good – borne by the state, or • a public good – borne by the state or municipality	1. Bodily injury, 2. Death, 3. Damage to natural resources – used by the individual

Source: studies after: Maśniak D., 2003, p. 119.

Environmental damage can be considered as environmental damage – destruction or disturbance of natural assets, which are elements of the environment; personal damage – death, bodily injury, damage to health; property damage – destruction or damage to property values, consumer or production property, and loss of benefits [7, 5].

Thus, we can say that ecological insurance is an important economic instrument creating, firstly: the possibility of minimising the social costs of environmental protection, and secondly: complementing or strengthening the action of legal and administrative tools, these mechanisms create incentives for compliance with legal and administrative requirements and, within the limits of the law, enable enterprises to take decisions related to environmental protection, taking into account the economic benefits they achieve. It should be borne in mind at this point that the function and purpose of environmental insurance should be the environmental liability of economic operators. Accordingly, insurers should assume part of the responsibility by offering companies adequate insurance coverage. From the point of view of clients and their risks, it is reasonable to expect protection for two types of liability – civil and administrative.

Conclusions of the research:

1. Insurance practice and literature on the subject treat ecological insurance very narrowly – extensive treatment of insurance – only as a source of compensation for environmental damage.

2. The role of insurance in assisting the market expansion of those involved in eco-development is overlooked.

3. Insurance is mainly seen as a method: providing compensation for damage and the financial consequences of environmental degradation, without seeing the possibility of involving them in the development process of those whose economic activity prevents disruption to the ecosystem.

4. In environmental policy, economic insurance as a method of reducing the financial impact of environmental disasters in the operation of economic and market mechanisms, creates:

a) the possibility of minimizing the social costs of environmental protection,

b) the role of complementing or reinforcing the operation of legal and administrative tools. These mechanisms create incentives for compliance with legal and administrative requirements and, within the limits of the law, enable enterprises to make decisions related to environmental protection, taking into account the economic benefits they achieve.

1. Adamowicz M. (2004), *Integration of agricultural and environmental policies as a way for sustainable development of rural areas*, CEESA – Central and Eastern European Sustainable Agriculture, www.ceesa.de/NitraPapers/Adamowicz.pdf

2. Baranowska-Dutkiewicz B., (1993), *Problem ubezpieczeń ekologicznych na tle zagrożeń środowiskowych*, Wiadomości Ubezpieczeniowe 1993 nr 10-12

3. Graff Zivin, J., Hsiang S., and Neidell M.. (2018), *Temperature and human capital in the short- and long-run*. Journal of the Association of Environmental and Resource Economists,5: pp. 77–105.

4. Maśniak D., (2003), *Ubezpieczenia ekologiczne*, Zakamycze, Kraków.

5. Pizer, W.A., and Sexton S., (2019), *The distributional impacts of energy taxes*, Review of Environmental Economics and Policy, Vol 13(1): pp. 104–123.

6. Przybytniowski J.W., (2014), *Risk of Natural Catastrophes and Ecological Safety of a State*, Polish Journal of Environmental Studies, Vol. 23, No. 3, pp. 1025-1031.

7. Ranson, M., (2014), *Crime, weather and climate change*, Journal of Environmental Economics and Management, Vol. 67(3): pp. 274–302: https://doi.org/10.1016/j.jeem.2013.11.008.

8. Śliwiński A.,(2002), *Ryzyko ubezpieczeniowe : taryfy – budowa i optymalizacja*, Poltext, Warszawa, p. 10-30.

9. Vaughan, E J; Vaughan, T M., (1999), *Fundamentals of risk and insurance*, John Wiley & Sons, Inc. Canada, Eighth edition, pp. 1025-1031.

10. Willet A., (1901), *The Economic Theory of Risk Insurance*, Studies in history, economics and public law, ed. by the Faculty of political science of Columbia University – vol. XIV, no. 2,, New York.

11. Wu M., Zhan Y., Liu Y, Tian Y., (2022), *Evaluation of the Effects of the Ecological Environmental Damage Compensation System on Air Quality*, y. Forests, 13, 982, pp. 3-13; https://doi.org/10.3390/f13070982

Д-р. Павел Джєканський / Dr. Paweł Dziekański,
Університет Яна Кохановського у Кельце (Польща) /
Jan Kochanowski University of Kielce (Poland)

Д-р. інж. Маркета Шимкова / PhDr. Ing. Markéta Šimková,
Vysoká škola DTI (Словацька Республіка/ Slovak Republic)

ECONOMIC CHALLENGES FOR REGIONAL SECURITY UNDER CONDITIONS OF GREEN TRANSFORMATION OF THE LOCAL ECONOMY (POLISH AND CZECH REPUBLIC EXPERIENCE)

Economic security is a broad concept. It is a state of reality in which it is possible to sustainably develop the economy and ensure an adequate standard of living for citizens through uninterrupted access to raw materials, markets, capital, modern technology, or information [26]. Economic, social, and political realities dictate that security should be treated as an overriding human need understood as the absence of something that is necessary to preserve life, develop, or maintain a social role [24, 11].

Security and development are two fundamental dimensions of the existence of individuals and entire communities. These two dimensions condition each other; without security, one cannot dream of development, while development facilitates the provision of security. The effectiveness and efficiency of security formation depend to a large extent on the rational recognition and use of many variables [13]. Development and security are complex processes that are difficult to assess unambiguously (e.g., due to access to detailed, homogeneous variables for all units under study). They can be characterized on the basis of variables depicting the demographic situation and labor market, social potential, economic structure, technical infrastructure, and the state and protection of the environment. The complexity of phenomena is increasing; their uncertainty is increasing, which makes the quality of human decisions increasingly dependent on the quality of the information they have [12].

As pointed out by P. Churski and his co-authors (2013), M. Stanny and W. Strzelczyk (2015), or P. Dziekańskii and P. Prus (2020), the element that affects development opportunities is financial potential. D. Milczarek (2005) points to the importance of local potential in the development process, i.e., geographical, demographic, economic, social, etc. elements. I. Kiniorska (2014) distinguishes three types of it: demographic, economic, and infrastructural. When looking at the potential and possibilities of the local economy, it is necessary to diagnose the intangible and tangible factors of development. P. Churski and all (2021) point to the need to redefine the factors of local (regional) development in the interpretation of socio-economic development processes. The economic security of a region can be defined as a state of certainty in the functioning of the local economy and economic development and achievement of economic goals.It promotes the creation of conditions for economic stability, socio-economic development, economic growth, high competitiveness and innovation of the economy, development of socio-economic infrastructure, reduction of poverty, and social exclusion. Economic security is often defined in a triad of three components: financial, raw materials, and food [17, 13].

Treating the economic security of the local economy as a balance of development needs and opportunities to meet them, it is expedient to distinguish four areas of functioning of its determinants, i.e., development opportunities and needs, infrastructure, and financial resources. Sources of threats to economic security can be unfavorable proportions in the creation and distribution of gross domestic product, erroneous directions of the country's financial and economic policies, the resources and structure of the country's natural wealth, infrastructure [7], the state and structure of natural, property, and human resources, the ability to absorb demographic changes, and the degree of energy security [9, 16]. Energy is a specific resource considered to be of great strategic importance (including in terms of economic security). Energy supply interruptions are extremely disruptive and can cause economic paralysis as well as social and political consequences [3]. An improved state and increased sense of security (including economic security) among the public can also result from an increased quality of life. Economic security is defined as a phenomenon related to the stability of material condition and the ability to provide financing regarding basic expenses [6, 18].

A synthetic measure can be used to compare which risks have the greatest impact on economic security. It is an instrument for monitoring and modeling the performance of local authorities, an indicator of economic evaluation under the dynamics of changes in economic and social phenomena, a decision-making measure, and a measure of the economic situation of the unit. On the basis of the synthetic measures determined, it is also possible to assess the structure of the local economy, the level of development of units, the degree of inter-group differentiation, the quantitative distance in the spatial level of units and separate groups, or the level of economic security. It allows to indicate its specialization and key and peripheral areas [2, 1].

The synthetic measure (as an element of monitoring the situation of the studied object) will allow a multidimensional and comprehensive look at the level of the phenomenon in the studied units, conduct comparative analyses, and linearly order the objects, that is, build a ranking in spatial as well as temporal terms [20, 28]. It makes it possible to carry out an assessment using an unlimited number of criteria, the degree of legibility of the results obtained is high, and it allows the results to be presented in numerical form [27, 19]. The quantification of a complex phenomenon with a single numerical value, which facilitates all comparisons and synthesizes partial images about the areas under study, can be considered a benefit in this regard. It can be a helpful tool for local governments assessing the accuracy of past decisions and the effectiveness of past regional management instruments. Its value depends on the number and type of variables adopted for the study [22, 8].

Economic security is determined by the region's economic potential, its size, the structure of the economy and its competitiveness. The basis of economic security is based on the expectation of changes in the structure of consumption, growth of entrepreneurship and economic activity. The economic security of the countries of Central and Eastern Europe (as well as their regions) is strengthened by the high level of concentration of markets, the numerical and qualitative potential of the population, the aspirations of societies and the political position in the region. Implemented development strategies contribute to the use of endogenous potential and the growth of economic importance of the economies of these countries (as well as regions) [23].

1. Balabán M., Pernica B. (2015). *System bezpieczeństwa Republiki Czeskiej: problemy i wyzwania*. Praga: Uniwersytet Karola w Pradze, Wydawnictwo Karolinum.

2. Bąk A. (2018). Zastosowanie metod wielowymiarowej analizy porównawczej do oceny stanu środowiska w województwie dolnośląskim, *Wiadomsoci Statystyczne*, Rok LXIII, 1 (680).

3. Brodny J., Tutak M. (2021). The comparative assessment of sustainable energy security in the Visegrad countries. A 10-year perspective, *Journal of Cleaner Production*, Volume 317, 2021, 128427.

4. Churski P., Borowczak A., i inni (2013). *Czynniki rozwoju obszarów wzrostu i obszarów stagnacji gospodarczej w Polsce*, Poznań: Uniwersytet im. A. Mickiewicza.

5. Churski P., Herodowicz T., Konecka-Szydłowska B., Perdał R. (2021). Rethinking Regional Development Factors. In: P. Churski, T. Herodowicz, B. Konecka-Szydłowska, R. Perdał (Eds.), *European Regional Development* (pp. 97-150). Cham: Springer. https://doi.org/10.1007/978-3-030-84659-6_4.

6. Churski, P. (2008). *Czynniki rozwoju regionalnego i polityka regionalna w Polsce w okresie integracji z Unią Europejską*. Poznań: Wydawnictwo Naukowe Uniwersytetu im. Adama Mickiewicza.

7. Ciszek M. (2013). Filozofia ujmowania zagrożeń ekonomicznych dla bezpieczeństwa narodowego RP i stabilności wewnętrznej państwa. *Doctrina. Studia społeczno-polityczne*, 10.

8. Dziekański P. (2024) *Green economy in the context of local financial and demographic differences*, Kielce-Łódź: Wydawnictwo Naukowe ArchaeGraph.

9. Dziekański P. (2014). Bezpieczeństwo ekonomiczne wyzwaniem współczesnego regionu – próba oceny syntetycznej. *Kultura Bezpieczeństwa. Nauka – Praktyka – Refleksje, 16*, 121-140.

10. Dziekański P., Prus P. (2020). Financial Diversity and the Development Process: Case study of Rural Communes of Eastern Poland in 2009–2018. *Sustainability*, 12, 6446.

11. Eichler J. (2004). *Stosunki w zakresie bezpieczeństwa międzynarodowego*. Praga: Oeconomica.

12. Jajuga K. (1993). *Statystyczna analiza wielowymiarowa*, Warszawa: Wyd. Naukowe PWN.

13. Jaźwiński I. (2011). Determinanty kształtowania polskiego bezpieczeństwa gospodarczego. Wybrane aspekty, *Przegląd Strategiczny*, nr 1.

14. Jaźwiński I. (2019). Bezpieczeństwo ekonomiczne regionów w polityce społeczno-gospodarczej państwa. *Review of Law, Business and Economics*. doi: 10.31743/ppe.9943.

15. Kiniorska I. (2014). *Potencjał rozwojowy obszarów wiejskich woj. świętokrzyskiego a polityka spójności*, In: W. Kamińska, K. Hoffner (ed.), *Polityka spójności a rozwój obszarów wiejskich. Stare problemy i nowe wyzwania*, Warszawa: PAN KPZK. t. CLVI.

16. Koďousková H., Lehotský L. (2021). Energy poverty in the Czech Republic: Individual responsibility or structural issue?, *Energy Research & Social Science*, Volume 72, 101877.

17. Korenik S. (2003). *Dysproporcje w rozwoju regionów Polski – wybrane aspekty*. Wrocław: Wydawnictwo Akademii Ekonomicznej im. Oskara Langego we Wrocławiu.

18. Kośny, M. (2013). *Determinanty bezpieczeństwa ekonomicznego rodzin*. Wrocław: Wydawnictwo Uniwersytetu Ekonomicznego we Wrocławiu.

19. Kozera A., Wysocki F. (2016). Problem wyznaczania współrzędnych obiektów modelu w metodach porządkowania liniowego obiektów. *Res. Papka. Wrocław Univ. Econ.*, 27.

20. Malina A. (2004). *Wielowymiarowa analiza przestrzennego zróżnicowania struktury gospodarki polski według województw*, Kraków: Wyd. AE w Krakowie.

21. Milczarek D. (2005). Potencjał Unii Europejskiej w stosunkach międzynarodowych (część 1). *Studia Europejskie*, nr 1, 9-18.

22. Nermend K. (2015). Wielokryterialna metoda wektora preferencji jako narzędzie wspomagające proces decyzyjny, *Przegląd Statystyczny*, R. LXII, zeszyt 1.

23. Niedziółka D. (2021), Uwarunkowania bezpieczeństwa ekonomicznego państw Europy Środkowej i Wschodniej, *Rocznik Instytutu Europy Środkowo-Wschodniej*, 19 (2021), z. 1.

24. Stachowiak Z. (2012). *Teoria i praktyka mechanizmu bezpieczeństwa ekonomicznego państwa. Ujęcie instytucjonalne*. Warszawa: Wyd. AON.

25. Stanny M., Strzelczyk W. (2015). Zróżnicowanie przestrzenne sytuacji dochodowej gmin a rozwój społeczno-gospodarczy obszarów wiejskich w Polsce, *Roczniki Naukowe Stowarzyszenia Ekonomistów Rolnictwa i Agrobiznesu*, tom XVII, zeszyt 4.

26. Szubrycht T. (2006). Współczesne aspekty bezpieczeństwa państwa, *Zeszyty Naukowe Akademii Marynarki Wojennej*, rok XLVII NR 4 (167).

27. Wysocki F. (2010). *Metody taksonomiczne w rozpoznawaniu typów ekonomicznych rolniczych i obszarów gospodarstwie wiejskim*, Poznań: Wydawnictwo Uniwersytetu Przyrodniczego w Poznaniu.

28. Zeliaś A. (ed.) (2000). *Taksonomiczna analiza przestrzennego zróżnicowania poziomu życia w Polsce w ujęciu dynamicznym*, Kraków: Wyd. AE w Krakowie.

Д-р. Сара Бондессон / Dr. Sara Bondesson,
Шведський університет оборони (Швеція) /
Swedish Defense University (Sweden)

EXPERIENCES FROM RESEARCH COLLABORATION BETWEEN UKRAINE AND SWEDEN

In times of war, universities serve not only as educational institutions but also as crucial pillars of societal resilience. They provide a sense of normalcy, offering hope and aspirations for the future, and play a vital role in the post-war rebuilding of a country. Beyond their academic function, universities offer tangible resources such as housing, mobilization of volunteers, and logistical support. However, despite their practical and symbolic importance, these institutions remain potential targets for an invading force and are often overlooked in crisis and war preparedness planning. Understanding how universities adapt and build resilience in the face of war is crucial, as the lessons learned from Ukraine may be applicable in other conflict-affected contexts.

Motivated by a desire to contribute meaningful support to Ukrainian colleagues, this research initiative was developed within the framework of the REACT – Resilience and Adaptive Capability in Training: Higher Education Institutions in Ukraine In Light of the Russian Invasion project.

The research project brings together a team of three Sweden-based researchers and eight junior researchers from Ukraine. It is funded by the Swedish Institute and SEDU and is designed to provide both training and collaborative research opportunities. The project is structured into multiple phases, covering training, data collection, analysis, and mentorship.

During 2023–2024, the Ukrainian researchers underwent extensive training in qualitative interview methods and ethnographic rapid assessment techniques. This training equipped them with the necessary skills to conduct fieldwork, after which eight researchers were selected for employment within the project. Their primary responsibilities included gathering empirical data, participating in analytical discussions, and contributing to writing and publishing research findings. The selected participants represent a diverse range of disciplines, including political science, psychology, and journalism.

The empirical phase of the study focused on investigating how Ukrainian universities are responding to the realities of war. In the early summer of 2024, the research team conducted field visits to various institutions, where they interviewed representatives from academic and administrative spheres. In total, 50 interviews were conducted across 20 universities, including:

– Poltava National Technical Yuri Kondratuyk University;

– Bohdan Khmelnytsky National University of Cherkasy;

– Ternopil Volodymyr Hnatiuk National Pedagogical University;

– Ivan Franko National University of Lviv;

– Taras Shevchenko National University of Kyiv;

The interviewees included university administrators, professors, and students, providing a comprehensive perspective on institutional responses to war. Currently, the Ukrainian researchers are engaged in transcribing and analyzing the collected data, with ongoing guidance and mentorship provided by Swedish team members. The collaboration between the researchers and project coordinator remains active, ensuring continuous feedback and academic support throughout the research process.

The research collaboration between Swedish and Ukrainian scholars presents numerous opportunities for both sides. The partnership fosters a win-win exchange of knowledge, broadens the reach of research findings, and strengthens language and academic networks between the two countries. The insights gained through this study contribute not only to the understanding of Ukrainian higher education under war conditions but also offer valuable lessons for crisis management in academic institutions worldwide.

However, the project has also faced several challenges. While the Ukrainian researchers demonstrated strong proficiency in conducting interviews, transitioning from data collection to structured academic writing has proven more difficult. Like many ethnographers, they struggle with synthesizing large amounts of qualitative material into cohesive narratives. Additionally, their heavy teaching loads and other professional obligations limit the time available for writing and analysis.

External factors have also posed significant difficulties. Frequent blackouts disrupt communication and slow the research process, making coordination between team members challenging. Maintaining a consistent interview guide across nine researchers, each with different academic backgrounds and personal research interests has been another obstacle. Furthermore, translation and transcription of interviews have proven to be extremely time-consuming, requiring meticulous review and verification to ensure accuracy.

Despite these challenges, this research collaboration represents a significant step toward strengthening academic ties between Ukraine and Sweden. Conducted within the framework of the REACT project, it provides an in-depth examination of how Ukrainian universities are navigating war-related disruptions while continuing their educational mission. By documenting the resilience and adaptability of Ukrainian universities in wartime, this project not only contributes to the field of security studies but also provides practical insights for academic institutions facing crises. The knowledge gained through this initiative has the potential to shape future strategies for safeguarding higher education institutions in conflict zones, making it a valuable endeavour for both Ukrainian and European academic communities.

Поліна Полякова / Polina Poliakova,
Національний університет Острозька академія» (Україна) /
National University of Ostroh Academy (Ukraine)

IS TELEGRAM A HYBRID THREAT FOR UKRAINE?

Recently, the head of the Main Directorate of Intelligence of the Ministry of Defense of Ukraine, Kyrylo Budanov, stated that Telegram is a threat to the national security of Ukraine [6]. In turn, Andriy Yusov compared the messenger to the «darknet» [10]. This caused a wave of curiosity among its consumers and caused a number of discussions on so cial networks. In this thesis, I would like to analyze why Telegram can be dangerous for Ukrainians and why it is so difficult for us to stop using the messenger.

Telegram is a Russian cross-platform messenger, according to the Ukrainian Wikipedia [8]. It is interesting that according to the Russian Wikipedia Telegram is not mentioned as russian social network [8].

Yehor Aushev, CEO of Cyber Unit Technologies and an expert in cyber security, says that although Telegram is a free platform, more than a billion dollars have been invested in its development from banks financed precisely from the Russian Federal Reserve. «The question arises, why do they invest there if they don’t make money from it? It turns out that this is a strategically important platform», says Aushev [7].

The founder of Telegram is Pavlo Durov, a Russian-French businessman and programmer. He was born and started his business in Russia, but eventually moved to France. Recently, he was arrested by the French special services at the Paris airport due to the disruption of his social network. This was reported by the French TV channels LCI and TF1.

After the arrest of the owner, Telegram actively began to cooperate with the French services, as reported by the publication

Libertation. Previously, the messenger ignored any requests from government authorities, so now in France it was called «Opening the door» [3]. From this, we can assume that Durov himself could forbid employees to cooperate with the authorities of any country. However, as early as 2021, the Russian pseudo-president declared that there was an "agreement" with Telegram. This leads to the idea of selling the information of the messenger users to the Russian special services, which also applies to Ukrainians.

In the conditions of war, the sale of information about Ukrainian users is a threat. Russian special services can use it for their own purposes. In particular, we can follow this already, using the example of a large number of account hacks in Telegram itself. Fraudsters or hackers use various methods to gain access to a user's personal information. One of them is a mailing with a request to vote for a girl in a dance contest, after which a request to confirm login to the Telegram account appears. After receiving confirmation, fraudsters gain access to all personal correspondence and contact details and can use them for their own purposes [11].

Even more dangerous is the spread of disinformation and fakes in the messenger. Nowadays, this is quite a popular problem. Unfortunately, many Ukrainians don't check the information they consume on the Internet and this causes some chaos. Telegram is a platform where there are many ways to provide information: general chats, Telegram channels with news, various groups, etc. Their number is very large, so it is difficult to control them. But such information spreads very quickly.

Many of these channels are anonymous, which gives more opportunities to carry out illegal activities using Telegram. On this platform, in addition to normal communication, there is the following: drug and weapons trade, distribution of various types of pornography, materials about racism, violence, terrorism, and others. The New York Times writes about it [5]. Telegram is an ideal platform for organizing such crimes, as it provides many opportunities and freedom of use.

The owner of the company, Pavlo Durov, said: «Were it entirely up to us, we would always give our users what they ask for: access to uncensored information and opinions so that they can make their own decisions».

In this way, Durov allegedly shows respect for the decision and choice of users. He ignores all requests from the state bodies, government agencies and special services regarding his crimes on his platform. This is clearly perceived as support for such actions.

So, in this case, permissiveness gives rise to arbitrariness.

Of course, each of the listed problems applies to each country. However, in today's conditions, the greatest threat to Ukraine is russia. Telegram's cooperation with russian special services was not confirmed by the messenger's management. However, researchers think otherwise. In February, Forbes cited a number of arguments confirming close ties with the Russian Federation. From the servers used by the platform to Putin's public statements, all this is evidence that Telegram is closely cooperating with the aggressor state [1].

Pavlo Durov stated that Telegram is a messenger independent of any government. However, the main servers used by the platform are located in Russia, Russian companies are involved in the transmission of users' network traffic, the president of the Russian Federation declares good cooperation with Telegram, and groups discussing resistance that is not beneficial for Russia are blocked by the program's administration. All this points to the danger for users all over the world, as their private information can be in the hands of the Russian special services at any moment.

According to the Kyiv International Institute of Sociology polls, the first place among messengers in Ukraine is Viber, the second is Facebook Messenger, and the third is Telegram [4]. Even though Viber also has dubious roots, there is no such permissiveness as in Telegram. That is why Telegram poses a much greater threat.

To solve this problem, Ukrainian services tried to contact the platform since it does not have a representative office in Ukraine. Appeals to Remy Vaughn, a representative of Telegram, turned out to be fruitless, as the platform ignored any requests from the Ukrainian authorities. The very existence of the so-called Remy Vaughan is not proven.

Therefore, Ukrainian lawmakers proposed to solve this problem through legislation. In March, the Ukrainian parliament registered the «Draft of the Law on Amendments to Certain Laws of Ukraine on the Regulation of Activities of Information Sharing Platforms Through which Mass Information is Disseminated», which should regulate the activities of all online platforms on the territory of Ukraine. It is currently at a hearing in the Ukrainian parliament. However, experts already see some potential problems with this.

Previously, no state had the experience of dealing with such problems at the legislative level. Only recently, the countries of the European Union adopted several acts similar in content. However, they are currently in the «testing mode», so Ukraine will not be able to immediately create an effective law to regulate the activities of the platforms. «The main regulatory act in the EU is the Digital Services Act. And it sets out a series of due diligence obligations that apply to platforms. Mostly they relate to transparency...», – says Maksym Dvorovy, head of the «Digital Rights» department of the «Digital Security Laboratory» public organization [2]. Another obstacle here is that Ukraine is not yet a member of the EU. This prevents joining the European legal system.

In any case, it takes time.

«If the network does not come into contact with the regulator, then the only possible way to fight against malicious content is to block the network as a whole. Telegram belongs to those social networks that are extremely reluctant to cooperate with regulators», says Nikita Poturaev, head of the Verkhovna Rada of Ukraine Committee on Humanitarian and Information Policy [2]. «Telegram is unpopular in Europe... This network has become hyper-popular in our country precisely since the full-scale invasion of russia», says Ihor Rozkladai, the chief media law expert of the Center for Democracy and Rule of Law.

«But the problem is that Telegram is not under the jurisdiction of the EU, so influencing it is not easy», says Ihor Rozkladai. — And especially in Ukraine. Any regulation aims to establish the rules of the game and the ability of the state to enforce these rules of the game. Telegram, by all accounts, is managed from Russia. Accordingly, Ukraine has no means of control, there are no representatives of this network here. What can be done? Block the platform entirely through communication tools and block the app in the Apple and Google stores. But is society ready for this?» [2]. Precisely because of the unpreparedness of society, no one is doing this yet. First of all, we will look for ways to establish communication with the platform. Only after a certain number of unsuccessful attempts, it will be possible to act with such a radical method.

In fact, a big problem in Ukraine, which concerns not only Telegram, is the information hygiene of Ukrainians. Many citizens do not check information, take any news seriously and do not know how to use critical thinking to distinguish between truth and lies. I believe that this is the key thing that Ukrainians need to be taught now. The experience of the hybrid war in Ukraine showed us how easy it is to manipulate society with the help of informational factors. That is why society should always be prepared for such manipulations. This will ensure the absence of chaos, which will facilitate work in critical situations for the state and its citizens.

So, Telegram is a platform that enables the development of a large number of threats to Ukraine. The biggest of them in modern times is the spread of disinformation in Ukrainian society. This becomes a big obstacle to continuing the fight against such a powerful enemy as Russia. Ukrainians should learn information hygiene in order not to become a victim of an information war.

1. Cyber Division, ICWR Cyber Warfare Research Institute. Telegram risks. Is it safe to use the messenger and is it connected to the FSB and GRU of the Russian Federation? Specialists of the Cyber Division and the ICWR Cyber Warfare Research Institute tell the story. *Forbes*. URL: https://forbes.ua/innovations/riziki-telegram-chi-bezpechno-koristuvatisya-mesendzherom-ta-chi-povyazaniy-vin-z-fsb-ta-gru-rf-rozpovidayut-fakhivtsi-cyber-division-ta-institutu-doslidzhennya-kiberviyni-icwr-19022024-19311.

2. Dankova Natalia. Telegram in Ukraine: cannot be regulated, not ready to block. *ms.detector.media*. URL: https://detector.media/rinok/article/219977/2023-11-30-telegram-v-ukraini-regulyuvaty-ne-mozhna-zablokuvaty-ne-gotovi/.

3. Judicial cooperation: since the arrest of Pavel Durov, the sudden about-face of Telegram in France. *Liberation*. URL: https://www.liberation.fr/societe/police-justice/cooperation-judiciaire-depuis-linterpellation-de-pavel-dourov-la-soudaine-volte-face-de-telegram-en-france-20240910_36YZVT65HBADBII5HWNGG554FE/#mailmunch-pop-1146266.

4. Oleksandr Bevzyuk-Voloshchyn. What are the most popular mobile apps? *Kyiv International Institute of Sociology.* URL: https://kiis.com.ua/?lang=ukr&cat=reports&id=1027.

5. Paul Mozur, Adam Satariano, Aaron Krolik, Steven Lee Myers. How Telegram Became a Playground for Criminals, Extremists and Terrorists. *The New York Times*. URL: https://www.nytimes.com/2024/09/07/technology/telegram-crime-terrorism.html.

6. Roman Petrenko. Budanov: Telegram is a threat to national security. *Ukrainska Pravda*. URL: https://www.pravda.com.ua/news/2024/09/7/7473898/.

7. Semenyuta Iryna, Gala Sklyarevska. Telegram addiction: how to legally and technically tame the Russian messenger. *ms.detector.media.* URL: https://ms.detector.media/trendi/post/34676/2024-04-16-telegram-zalezhnist-yak-yurydychno-y-tekhnichno-pryborkaty-rosiyskyy-mesendzher/.

8. Telegram – Wikipedia. *Wikipedia – the free encyclopedia*. URL: https://ru.wikipedia.org/wiki/Telegram.

9. Telegram – Wikipedia. *Wikipedia*. URL: https://uk.wikipedia.org/wiki/Telegram.

10. Valentyna Troyan. Intelligence representative: Telegram is often used as a legalized darknet. *Institute of Mass Information*. URL: https://imi.org.ua/news/yusov-telegram-chasto-vykorystovuyetsya-yak-legalizovanyj-darknet-i61448.

11. Yuliia Abramova. A new fraudulent scheme: users massively report the hacking of Telegram accounts. *tsn.ua.* URL: https://tsn.ua/ukrayina/nova-shahrayska-shema-koristuvachi-masovo-povidomlyayut-pro-zlam-akauntiv-v-telegram-2587962.html.

ЗМІСТ / CONTENT

Наукове видання

РОЗВИТОК БЕЗПЕКОВИХ СТУДІЙ В УКРАЇНІ: ДОСВІД КРАЇН ЄС

Матеріали Круглого столу
(м. Острог, 17 вересня, 2024 р.)

Редактори: *Е. М. Балашов, Д. А. Гаврилюк*

Комп'ютерна верстка *Н. О. Крушинської*

Формат 60х84/16. Ум. друк.арк. 2,09.
Зам. № 5–25. Гарнітура «Cambria».

Оригінал-макет виготовлено у видавництві
Національного університету «Острозька академія»,
Україна, 35800, Рівненська обл., м. Острог, вул. Семінарська, 2.
Свідоцтво суб'єкта видавничої справи РВ № 1 від 8 серпня 2000 року.