38

Revista Científica

General José María Córdova

Revista Colombiana de Estudios Militares y Estratégicos
Colombian Journal of Military and Strategic Studies

ESCUELA MILITAR DE CADETES
"General José María Córdova"

ESMIC
SELLO EDITORIAL

Vol. 20, Núm. 38
abr-jun / 2022
Bogotá D.C., Colombia

ISSN 1900-6586 (impreso)
ISSN 2500-7645 (en línea)

Revista Científica

General José María Córdova

(Revista Colombiana de Estudios Militares y Estratégicos)
ISSN 1900-6586 (impreso) - ISSN 2500-7645 (en línea)
Volumen 20, número 38, abril-junio 2022

INDEXADA EN

Scopus, DOAJ, Google Scholar, Publindex, SciELO Citation Index (WoS), SciELO, Redalyc, REDIB, Latindex, CLASE, CIRC, MIAR, BASE, NSD, Ebsco, Suncat, WorldCat, Wilbert, Rev Sapiens, ERIH PLUS, Journal TOCs, FLACSO (LatinRev)

ESMIC
SELLO EDITORIAL

Miles Doctus

Esta página queda intencionalmente en blanco

Revista Científica

General José María Córdova

(Revista Colombiana de Estudios Militares y Estratégicos)
ISSN 1900-6586 (impreso) - ISSN 2500-7645 (en línea)
Volumen 20, número 38, abril-junio 2022

La **Revista Científica General José María Córdova** (Revista Colombiana de Estudios Militares y Estratégicos) es una publicación académica de acceso abierto, revisada por pares y editada trimestralmente por la Escuela Militar de Cadetes "General José María Córdova" (ESMIC), *alma mater* de los oficiales del Ejército Nacional de Colombia, a través de su Sello Editorial ESMIC.

Escuela Militar de Cadetes
"General José María Córdova"
Calle 80 # 38-00. Bogotá D.C., Colombia
Teléfono: +57(1) 377 0850 Ext. 1104
Web oficial:
https://www.revistacientificaesmic.com
Contacto:
revistacientifica@esmic.edu.co

Revista Científica General José María Córdova
(Revista Colombiana de Estudios Militares y Estratégicos)

Enfoque y alcance

La Revista Científica General José María Córdova (RCGJMC) es una revista interdisciplinaria, con un enfoque en las ciencias sociales (Clase 5I01, OCDE / UNESCO). Publica resultados de investigación en estudios militares y estratégicos. Este campo se centra en el análisis de escenarios de incertidumbre en seguridad y defensa para proporcionar a un amplio número de lectores, incluidos decisores políticos, miembros de las Fuerzas Armadas, profesionales, educadores, investigadores y estudiantes de las ciencias sociales, una comprensión del uso legítimo del poder y su adecuada aplicación en relación con los intereses nacionales, en beneficio de la formulación de políticas y la gestión pública.

Misión y visión

La RCGJMC explora perspectivas teóricas y prácticas innovadoras en cuanto al estudio del poder y su aplicación legítima en la defensa de los intereses nacionales. De esta forma, busca aportar a la construcción de una cultura estratégica, en la que se articule el uso de los medios disponibles con las formas de empleo de las capacidades nacionales para lograr los fines esenciales del Estado. La RCGJMC, como publicación interdisciplinar, es un proyecto líder en la región de Latinoamérica y el Caribe, en el que convergen múltiples perspectivas académicas y experiencias profesionales que contribuyen al fortalecimiento del pensamiento y la cultura estratégica, a la optimización de la administración pública, al robustecimiento de la democracia y a la defensa de los derechos humanos.

Orientación temática

Los contenidos de la RCGJMC están enmarcados en los siguientes ejes temáticos y disciplinas correspondientes: 1) Educación y doctrina (ciencias militares); 2) Política y estrategia (ciencia política); 3) Seguridad y defensa (relaciones internacionales); 4) Justicia y derechos humanos (derecho); 5) Fuerzas Armadas y sociedad (historia y geografía); 6) Inteligencia y logística (administración); y 7) Industria y tecnología (economía).

Responsabilidad de contenidos

La responsabilidad por el contenido de los artículos publicados por la RCGJMC corresponde exclusivamente a los autores. Las posturas y aseveraciones presentadas son resultado de un ejercicio académico e investigativo que no representa la posición oficial ni institucional de la Escuela Militar de Cadetes "General José María Córdova", el Ejército Nacional de Colombia o el Ministerio de Defensa Nacional.

Indexación

La RCGJMC se encuentra incluida en los siguientes Sistemas de Indexación y Resumen (SIR): Scopus, DOAJ, Google Scholar, Publindex, SciELO Citation Index (WoS), SciELO, Redalyc, REDIB, Latindex, CLASE, CIRC, MIAR, BASE, NSD, Ebsco, Suncat, WorldCat, Wilbert, Rev Sapiens, ERIH PLUS, Journal TOCs, FLACSO (LatinRev).

Envío de propuestas

La RCGJMC fomenta la presentación de propuestas originales correspondientes a los ejes temáticos y disciplinas descritas anteriormente. Todos los envíos deben seguir las instrucciones para autores disponibles en https://revistacientificaesmic.com/index.php/esmic/about/submissions, y deben enviarse electrónicamente a https://revistacientificaesmic.com/index.php/esmic/login

Tabla de contenido

Revista Científica General José María Córdova
(Colombian Journal of Military and Strategic Studies)
Bogotá D.C., Colombia

Volume 20, Number 38, April-June 2022, pp. 243-244
https://dx.doi.org/10.21830/19006586.954

Editorial: Protection of national security in information and cyberspace

Editorial: La protección de la seguridad nacional en la información y el ciberespacio

Andrii Svintsytskyi
Guest Editor
Ukrainian Scientific and Research Institute of Special Equipment and Forensic Expertise
of the Security Service of Ukraine

Andres Eduardo Fernandez-Osorio
Editor in Chief Revista Científica General José María Córdova
Escuela Militar de Cadetes "General Jose Maria Córdova", Bogotá D.C., Colombia

Dear colleagues and interested readers,

We are honored to present a dossier of the *Revista Cientifica General Jose Maria Cordova* (Colombian Journal of Military and Strategic Studies) on the *protection of national security in information and cyberspace*, led by Dr. Andrii Svintsytskyi from the Ukrainian Scientific and Research Institute of Special Equipment and Forensic Expertise of the Security Service of Ukraine as a guest editor.

Over the last few decades, information technologies have increasingly developed and deeply integrated into almost all spheres of life, including entertainment, everyday life, production, finance, security, and defense. Naturally, this progress in digital technologies has not been overlooked by criminals who have found various methods to interfere in the work of automated information systems (cyber-attacks), including malicious software.

The evolution of cyber-attacks has proceeded gradually, and the danger of these attacks has increased. As a result, the current scale of criminal acts in cyberspace has acquired the characteristics of real wars; this provides the basis to consider these actions by criminal hacker groups as cyber wars.

Contact: Andres Eduardo Fernandez-Osorio ✉ andres.fernandez@esmic.edu.co

The state develops its own cyber security system to counter cyber threats. In Ukraine, a system of specialized agencies has been created to ensure cyber security. These agencies include The State Service of Special Communication and Information Protection of Ukraine, the Computer Emergency Response Team of Ukraine (CERT-UA), the subdivisions of the cyber police, the Department of Counterintelligence Protection of State Interests in the Sphere of Information Security of the Security Service of Ukraine, and the National Coordination Center for Cyber Security of the National Security and Defense Council of Ukraine.

However, investigators, prosecutors, advocates, judges, and other judiciary parties usually do not possess the deep knowledge in the sphere of cyber technology as experts. Therefore, forensic experts are intrinsic in countering cyber threats, particularly in investigating cybercrimes. Although the smallest in employee numbers, The Ukrainian Scientific and Research Institute of Special Equipment and Forensic Expertise of the Security Service of Ukraine is responsible for the greater part of the assignments set before the Security Service. It plays a significant role in forensic and forensic support of cybercrime investigation and countering cyber threats in Ukraine. The institute is accredited according to the international standard ISO / IEC 17025 in computer and technical examinations. It actively participates in implementing international standards for cyber incident investigations into the Ukrainian regulatory framework and develops scientific and methodological materials for examinations in the investigation of cybercrime.

We encourage you to consider this information in a more detailed manner through the scientific papers prepared by several fellow scientists from different Ukrainian academic institutions. We hope the reading process is interesting and insightful.

DOSSIER

Esta página queda intencionalmente en blanco

Revista Científica General José María Córdova
(Colombian Journal of Military and Strategic Studies)
Bogotá D.C., Colombia

Volume 20, Number 38, April-June 2022, pp. 247-264
https://dx.doi.org/10.21830/19006586.898

International and national standards on societal information security

Normas internacionales y nacionales sobre seguridad de la información en la sociedad

Sofiia Lykhova and Viktoriia Sysoieva
National Aviation University, Ukraine

Liudmyla Servatiuk and Oleksandr Shamsutdinov
National Academy of the Security Service of Ukraine, Ukraine

Dariia Hurina
Ministry of Internal Affairs of Ukraine, Ukraine

Abstract. This research focuses on information security as a social state, its aspects and characteristics, information security standards, and its impact on improving the information security process. It emphasizes the multidisciplinary nature of the issue of information security. Several methods are employed in this study, including formal-logical and system-structural methods, methods of generalization, and comparative law. Documentary analysis is used to examine the regulatory framework concerning information security and the main international and national information security standards. Three levels of information security are identified –personal, social, and state. It concludes that the levels differ depending on their degree within the information space.

Keywords: information space; information technology; policy management; public information; state security

Resumen. Esta investigación se enfoca en la seguridad de la información como estado social, sus aspectos y características, las normas de seguridad de la información y su impacto en la mejora del proceso de seguridad de la información. Hace énfasis en el carácter multidisciplinar de la seguridad de la información. El estudio emplea varios métodos, entre ellos el formal-lógico y el sistémico-estructural, los métodos de generalización y el derecho comparado. El análisis documental es utilizado para examinar el marco normativo de la seguridad de la información y las principales normas internacionales y nacionales en la materia. Se identifican tres niveles de seguridad de la información: la personal, la social y la estatal. Se concluye que los niveles difieren según su nivel dentro del espacio de la información.

Palabras clave: espacio informático; gestión de políticas; información pública; seguridad del Estado; tecnología de la información

Section: Dossier • Scientific and technological research article

Received: November 29, 2021 • Accepted: March 3, 2022

Contact: Sofiia Lykhova ✉ lykhova8138@edu.cn.ua

Introduction

Society has entered the era of global information relations. Consequently, safeguarding its information security is becoming the priority mission of modern states, along with protecting the national information space. However, the existing global and regional information confrontations, destructive communicative influences, the clash of multi-vector national information interests, and the spread of information expansion and aggression significantly complicate the fulfillment of this task and indicate the multifold nature of information security.

Information security is not a constant characteristic of a specific process or phenomenon. Its features include dynamism, multidimensionality, and uncertainty. Thus, developments concerning the management component and the technical characteristics of the information space, which provide for the study of this issue by technical disciplines, are constant. International standardization organizations, in particular, pay a great deal of attention to the information security management system. At the same time, legal sciences study many legal aspects of information security, particularly criminal, administrative, and civil law.

There is no consolidated view on the content of this concept in scientific literature, reiterating information security's multidimensionality. Thus, reducing information security to information protection is unbefitting; this concept is broader in nature. It is a multifold area of activity that requires a system-integrated approach. Defining information security requires determining its most essential features, considering the constant dynamics of information systems. It should be considered through the unity of signs such as state, features, and the management of threats and dangers, where the latter provides for choosing the optimal way to eliminate and minimize the impact of negative consequences (Galkin et al., 2020).

Ukrainian legislation defines *information security* as a state of protection of vital human, society, and state interests, preventing harm due to incompleteness, untimeliness, and unreliability of the information used; negative information impact; negative consequences of information technology use; unauthorized dissemination, use, and integrity violation, confidentiality, and information availability. The legislation on information should aim to consolidate the state's information policy. The policy should provide for a guaranteed level of national security in the information sphere, including a steady development of information technologies and protection tools, the exclusion of monopoly in this area, the prevention of the development of destructive information technologies, and the protection of copyrights.

Given that information and communication technologies are now used in all spheres of human life, there is an urgent need to ensure societal information security. A system

of legal rules regulating relations in the information sphere is being developed to achieve and maintain an appropriate level of information security in society (Kniazieva et al., 2021). Moreover, state administration bodies' main directions of activity are being determined. Bodies and forces ensuring information security and a mechanism for monitoring their activities are being formed or transformed. To effectively ensure such security, it is important to approve its standards, which is a process that combines technical and legal components. This work is devoted to the legal aspects of the study of information security standards in society.

Due to the increased urgency of this problem, many domestic and foreign scientists have focused their research on information security. The legal aspect of the problem is particularly highlighted in works by Dovgan and Tkachuk (2019), Kuzmenko (2010), Marushchak (2010), and Ovsyannikov et al. (2015). These and other authors have made significant contributions to the development of information security. However, legal scholars continue to overlook the issue of standards for its provision.

The need for information security

This study was conducted using general scientific and specific scientific methods. The object of the article's research is presented, considering the research methodology. Three levels of methodology are generally accepted in legal research: fundamental (philosophical), general scientific, and specific scientific. With the help of the fundamental level of methodology, the most general principles and methods were ensured, which were further specified at the general scientific level.

The formal-logical, historical, system-structural, and generalization methods are worth noting among the general scientific methods used in the study. These methods are fundamental because they can be found in all fields of science and can help operations with the information presented in the research. The levels of information security and types of standards for its provision were identified using the system-structural method (Orlovskyi et al., 2018). The formal-logical method was used to analyze existing information security standards. Lastly, the positions of scientists on the researched problems were systematized and analyzed using the generalization method.

The study also used specific scientific methods, that is, methods specific to legal science, including comparative law, documentary, and statistics. To fully explore the delineated object, it is necessary to use the above methods comprehensively. The comparative legal method was used to analyze the regulatory framework for information security, and the documentary method was used to examine the international and national standards of information security.

The empirical basis of the study was examples of the application of international and national standards for information security by organizations, bodies, and institutions. The normative basis of the study included international regulations, Ukrainian legislation, and international and national standards in information security.

In the context of globalization and informatization, information security is becoming an urgent and critical task for every state. Ukraine is no exception. Even the Constitution of Ukraine (Article 17) states that ensuring information security is the State's most important function, a matter concerning the entire Ukrainian people (Constitution of Ukraine, 1996). In terms of solving this problem in Ukraine, several legal documents exist to firstly determine the general principles of information security and ways to improve it.

For example, the Law of Ukraine *On Basic Principles of Information Society Development in Ukraine for 2007-2015* defines the following ways to solve the problem of information security:

- Creating a fully functional State information infrastructure and ensuring the protection of its critical elements;
- Increasing the coordination level of State bodies' activities in identifying, assessing, and forecasting threats to information security, preventing such threats, and avoiding their consequences, as well as implementing international cooperation on these issues;
- Improving the information security regulatory framework, particularly in protecting information resources, combating computer crime, protecting personal data, and managing law enforcement activities in the information sphere;
- Deploying and developing the National system of confidential communication as a modern secure transport base capable of integrating territorially distributed information systems in which confidential information is processed (Law of Ukraine, 2007).

It is evident that the State is thorough in defining ways to ensure information security. However, it should be noted that information security as a phenomenon is not static. Just as information and communication technologies do not stand still, the state of protection of vital interests of man, society, and the state is constantly changing. Therefore, even if we can say that the state of information security has been achieved in a specific area at a specific time, it does not mean that this same condition will be maintained in subsequent periods. Information technologies are constantly evolving and improving, leading, among other things, to the emergence of new threats to information security. Therefore, it is necessary to pay attention to information security's instability. In addition, the state of security depends on many factors –both internal and external. The influence of these factors determines the presence or absence of information security.

However, it should be noted that such dynamism, multidimensionality, and uncertainty are not unique to information security. One must agree with the authors of the article, *The Negative Impact of Corruption on the Economic Security of States*. They rightly note that the threat to economic security is usually considered an undesirable but, at the same time, an integral part of the economic system, which operates in difficult competitive conditions, represented by a multifactorial, dynamic, and uncertain external environment (Akimova et al., 2020). All this indicates that information security standards cannot remain stable for a long time; they must be constantly revised, amended, and the old standards replaced by new ones.

Problems of scientific-theoretical reasoning

Kuzmenko (2010) distinguishes three levels of information security. They are as follows:

- Personal level (formation of rational, critical thinking based on the principles of freedom of choice);
- Social level (formation of high-quality information-analytical space, pluralism, multichannel information retrieval, and independent powerful mass media owned by domestic owners);
- State-level (information and analytical support of state bodies, information support of domestic and foreign policy at the interstate level, system of information protection with limited access, and counteraction to offenses in the information sphere –computer crimes).
- In turn, Ovsyannikov et al. (2015) consider information security as guaranteeing the state of security depending on the type of threats, which include:
- Individuals, society, state from the influence of poor-quality information;
- Information and information resources of the organization from the illegal influence of third parties;
- Information rights and freedoms of man and citizen.

These scientists noted that individuals' information security is characterized as a state of protection of the individual, various social groups, and associations of people from influences against their will and desire to change mental states and psychological characteristics, modify behavior, and restrict freedom of choice. State (society) information security is characterized by the degree of protection of the state (society) and the stability of the main spheres of life (economy, science, technosphere, management, and military affairs, among others); relatively dangerous information impacts (including destabilizing, destructive, and affecting state interests.) on the implementation and extraction of information. The State's information security is determined by the ability to neutralize such

influences. Organization information security is the purposeful activity of its bodies and officials using permitted forces and means to achieve the organization's information environment's state of security, ensuring its normal functioning and dynamic development (Ovsyannikov et al., 2015).

In this regard, Marushchak (2010) adds that the problems of scientific and theoretical justification of the feasibility of legal regulation of public relations, arising from the information security of the individual, society, and state, are not only relevant; they are also practical. After all, for example, the regulation of relations on the dissemination of information on the Internet can occur both with the state's participation (both in China) and without legal influence. However, the level of protection of information interests of the state, and in many cases –society and individuals– may differ depending on the presence (absence) of legal regulation. Ensuring the safety of a person is very important in this aspect because an individual's life and health are the highest social value.

Guarantees for human security are a broad concept in which legal aspects are closely intertwined with philosophical, social, and even medical aspects. For example, the authors of the article, *Biomedical Ethics and Human Rights in the Context of Innovation and Information Development of Society*, note that biomedical ethics is a science of morality, through which human security guarantees are established, and moral and ethical barriers are created, supported by legal acts. The purpose of bioethics is to prevent harm to a person in need of medical care and protect rights and interests (Kalyuzhny et al., 2020; Vakulyk et al., 2020).

In determining the methods of legal regulation of public information and security relations, the conceptual difference between the principles of information security resources and the security of the state's information space should be considered. Marushchak (2010) considers these the main objects of information security, the basis of the information sovereignty of Ukraine. To ensure the security of the information space, it is necessary to strictly adhere to the constitutional principles of freedom of speech and the right to information. Meanwhile, to ensure the security of information resources, integrity, accessibility, and completeness of information are among the key aspects. Therefore, the method of legal regulation to ensure the security of information resources should be predominantly imperative, as it mainly concerns the protection of the right to information with limited access, while in ensuring the state's security of information space, it should be dispositive, as it relates to freedom of information, ways to obtain and disseminate information (Marushchak, 2010). In this work, we concede with the scientist's position on the delimitation of areas of regulation of public information and security relations. Indeed, significant restrictions on the rights and freedoms of citizens, especially in ensuring the security of the state's information space, will unlikely solve this problem entirely.

Information security is a component of the country's national security system. Ensuring the society's information security implies the protection of political, social, and economic interests. Given its importance, the international community has long heeded the development and improvement of standards for its provision (Chyzhmar et al., 2019).

Regarding information security standards, it is worth noting that the etymological meaning of the word *standard* is a norm or *sample*. On this matter, there is a broad and narrow interpretation of the term in science. In a broad sense, a standard is a particular sample, standard, or model against which other objects are compared and gauged. In the narrow sense, a standard is a normative or technical document that establishes norms, rules, and requirements for an object of standardization. Furthermore, it is worth considering this term's unregulated use in this sphere when analyzing the concept of information security standards.

The first problem that scientists face in studying the legal component of information security is defining *information security*. At the same time, one of the most controversial issues among scientists concerns information security. They recognize the state's interests in the information sphere and the information rights of citizens and society. However, they only recognize information security in information and telecommunications systems. Given the diversity in composition and content of information security objects, considering the leading scientists' positions on this issue is crucial. An important area of research involves determining the relationship of identical concepts used in current legislation that creates an ambiguous understanding of information security's structure. For example, the concept of *information security* is defined as the security of devices, processes, programs, environment, and data that ensure the integrity of information processed, stored, and transmitted. *Network security* is defined as measures to protect local computing networks from unauthorized interference with their functioning or attempts to disrupt the normal operation of its elements. The term *Automated System Data Security* (AS Data Security) is used to describe the quality of organizing access to data, protecting it from unauthorized use, intentional or unintentional distortion, or destruction. These definitions disagree with the definition of *information security* and the generic concept of *information security of telecommunications networks* as the ability of telecommunications networks to protect against destruction, distortion, blocking of information, or unauthorized leakage or violation of its routing (Marushchak, 2010). Unfortunately, this vagueness in terminology can lead to misinterpreting concepts.

Solodka (2013) notes that developed countries have established relations in this area, even before adopting legislation on personal data security. Ensuring proper protection of personal data is provided for in the EU-Ukraine Association Agenda, the EU Visa Liberalization Action Plan for Ukraine, and the draft of the EU-Ukraine Association Agreement. However, the legal institution of personal data in domestic information leg-

islation is still in its infancy. Even after adopting the Law of Ukraine, *On Personal Data Protection*, Ukraine's legislation does not establish and, according to some scientists, cannot establish a well-defined list of information about an individual, the data considered personal, and how to apply the Law's provisions to various situations. This is particularly so when processing personal data in information (automated) databases and files of personal data that may arise in the future due to changes in public life. Under national law, personal data is information or a collection of information about an identified individual or one that can be specifically identified (Solodka, 2013). This definition does not improve specificity and may lead to a subjective interpretation in deciding whether a person's right to privacy has been violated.

In this regard, Ovsyannikov et al. (2015) draw attention in their article to the interests of the state in the information sphere. They include creating conditions for the harmonious development of the state's information infrastructure, implementing constitutional rights and freedoms of man and citizen in the interests of strengthening the constitutional order, upholding the country's sovereignty and territorial integrity, and establishing political and social stability, economic prosperity, unconditional implementation of laws, and support for international cooperation through partnership. The state carries out its activities through the relevant bodies, citizens, and public organizations and associations with the appropriate powers, according to the law. The state system is the most important part of the information security system of the individual, society, and the state. The main tasks of this system include detecting and forecasting destabilizing factors and information threats to the individual, society, and state's vital interests, implementing operational and long-term measures to prevent and eliminate them, and creating and maintaining forces (Ovsyannikov et al., 2015). Thus, State regulation of information security at all levels reflects the state of its provision. Ensuring information security depends on the national measures, whether the information and communication space will be protected, the citizens' security guarantees will be observed, and so on. At the state level, regulations are adopted to regulate this area of public relations.

There is also a position in legal science that maintains that the wording of the right to information and its restrictions (Articles 5, 6 of the Law, *On Information*, Article 6 of the Law, On *Access to Public Information*) do not meet international standards. Article 10 of the European Convention states that everyone has the right to freedom of expression. This right includes the freedom to hold opinions and receive and impart information and ideas without interference by public authorities and regardless of frontiers. However, these domestic laws do not address the exercise of the right to information irrespective of state borders; this is relevant in the age of the Internet. Furthermore, laws such as the Law of Ukraine *On Information*, *On State Secrets*, *On Access to Public Information*, *On Personal Data Protection*, and *On Banks and Banking* classify some information as *closed*, setting re-

strictions on the right of access to information. However, there are conflicts in these laws. For example, in the Law of Ukraine, *On Banks and Banking*, there is a conflict between the definition of *banking secrecy* and the list of information attributed to it. It should be noted that no list exists of information that can be classified as a trade secret; this complicates the exercise of a person's right to access information (Solodka, 2013). Thus, it can be stated that the Ukrainian national legislation has some gaps in the field of information security and regulation of public relations that arise in this sphere.

Dovhan and Tkachuk (2019) note that developing and adopting appropriate legislation is necessary to ensure information security. The basic principles of the construction of such a law, as well as information security activities, should firstly include the priority of human and civil rights and freedoms, a principle enshrined in International Law, reflecting the essence and limits of information security activities, and fundamental in the Doctrine of Information Security of Ukraine and observance of human rights and freedoms in the information sphere referring to the primary national interests of our country. The second principle involves the individual, society, and state's balance of interests. It is also provided by the Doctrine of Information Security of Ukraine. It follows the first because the legitimacy of each person's interests extends to the rights and freedoms of others and the interests of society and the state. These rights and freedoms ultimately caused the restrictions associated, for example, with the protection of state secrets and protection of personal data. The third principle, also following the previous principle, is the compliance of security measures with the degree of threats. Measures befitting the threats' actual level should be applied to prevent and eliminate them in the information sphere, with the minimum restrictions on the rights and freedoms of citizens. The fourth involves the state's monopoly on developing and producing special means of informational influence, including informational-psychological influence. In the conditions of Russian aggression, this means the prohibition in Ukraine of specific harmful information and inhumane informational-psychological technologies, which many lawyers rightly call information weapons. The fifth involves transparency and control of civil society in the field of information security. Namely, and following the Law of Ukraine *On Access to Public Information*, any information on the activities of public administration and local government to ensure information security is open and accessible to citizens unless they constitute a state secret or other secret provided by law. The last principle involves the obligation to involve public organizations in information security activities. This principle, which follows from the previous, and the principle of balanced interests of man, society, and the state, allows for public evaluation of bills related to the information sphere, fully taking into account the interests of various segments of the population to improve the quality of relevant legislation (Dovgan & Tkachuk, 2019). We acquiesce with the opinion of these scientists. Today, Ukraine has an urgent need to consolidate the general princi-

ples of information security at the legislative level. However, the development of such legislation should be approached with a clear understanding that information security is a dynamic, multifactorial phenomenon, and predicting how threats and challenges to information security will change in the future is challenging.

In the narrow sense, information security standards are represented by international and national standards of individual countries. Information security requirements to protect information or its properties are defined within the framework of international (ISO standards) and national standards (State Standards of Ukraine and Normative documents of technical information protection). In English standards, this is a classic Systemic-Institutional Alignment (SIA) model for ensuring the requirements of confidentiality, integrity, and availability of information. The requirement of observability (accountability) is made separately. The requirement of confidentiality applies to information; all others apply to both the information and the system as a whole. Three components are also considered for targeted application (protection and prevention mechanism) of information security standards within a certain model in information and telecommunication systems: hardware, software, and communication components (Ovsyannikov et al., 2015).

Organizations and standards to ensure information security

International standards of information security are normative documents developed by the International Organization for Standardization (ISO). The ISO is an independent, non-government organization made up of members from the national standards bodies of 165 countries. Its members play a vital role in how we operate, meeting once a year for a General Assembly that decides our strategic objectives. In Geneva, Switzerland, its Central Secretariat coordinates the system and runs day-to-day operations, overseen by the Secretary-General (International Organization for Standardization, 2021a). The ISO's primary goal was to promote international trade; however, the scope of its activities has expanded significantly with the development of information technology. To this end, this organization has developed the following standards to ensure information security:

- ISO/IEC 27033-3: 2010 *Information technology. Security techniques. Network security. Part 3: Reference networking scenarios. Threats, design techniques, and control issues*. It addresses the issues of possible threats, design and management methods, and possible threats for each scenario. It provides a detailed guide to dealing with security threats and the security and control design techniques needed to minimize the associated risks (International Organization for Standardization, 2010).
- ISO/IEC 27036-3:2013 *Information technology. Security techniques. Information security for supplier relationships. Part 3: Guidelines for information and commu-*

nication technology supply chain security. This document provides product and service acquirers and suppliers in the information and communication technology (ICT) supply chain with guidance on gaining visibility into and managing the information security risks caused by physically dispersed and multi-layered ICT supply chains. It also guides on responding to risks stemming from the global ICT supply chain to ICT products and services that can have an information security impact on the organizations using these products and services. These risks can be related to organizational as well as technical aspects (e.g., insertion of malicious code or presence of the counterfeit information technology (IT) products) and integrating information security processes and practices into the system and software lifecycle processes (International Organization for Standardization, 2013b).

- ISO/IEC WD 27036-1:2021 *Cybersecurity. Supplier relationships. Part 1: Overview and concepts*. This standard, as well as the previous one, concerns information security of information and communication technologies of the supply chain (International Organization for Standardization, 2021b).
- ISO/IEC 27002:2013 *Information technology. Security techniques. Code of practice for information security controls*. This document gives guidelines for organizational information security standards and information security management practices, including the selection, implementation, and management of controls considering the organization's information security risk environment(s). It is designed to be used by organizations that intend to: select controls within the process of implementing an Information Security Management System based on ISO/IEC 27001; implement commonly accepted information security controls; develop their own information security management guidelines (International Organization for Standardization, 2013a). It should be noted that this standard is currently in use, but another draft standard is being considered, which will replace this one.
- ISO/IEC TR 27016: 2014 *Information technology. Security techniques. Information security management. Organizational economics*. This document provides guidelines on how an organization can make decisions to protect information and understand the economic consequences of these decisions in the context of competing requirements for resources. This document is applicable to all types and sizes of organizations and provides information to enable economic decisions in information security management by top management who have responsibility for information security decisions (International Organization for Standardization, 2014).

- ISO/IEC 27035-3:2020 *Information technology. Information security incident management. Part 3: Guidelines for ICT incident response operations*. This document gives guidelines for information security incident response in ICT security operations. It does this by firstly covering the operational aspects in ICT security operations from a people, processes, and technology perspective. It then further focuses on information security incident response of ICT security operations, including information security incident detection, reporting, triage, analysis, response, containment, eradication, recovery, and conclusion (International Organization for Standardization, 2020).
- International standardization of the components of the information security management system forms three areas of development in this sphere:
- The group of standards: *Security Methods* - ISO/IEC 27000-ISO/IEC 27037;
- The group of standards *Methods and means of security* - ISO/IEC 15408 (*General criteria*, three parts), ISO/IEC 13335 (five parts), and ISO/IEC 18045;
- The group of standards *Management and audit of information technology* (CobIT, ITSM, ITIL, among others) (Ovsyannikov et al., 2015).
- In addition to the international standards developed by ISO specialists, there is a list of international cybersecurity standards developed by specialists of the British Standards Institute (BSI).
- BS 7799-1: 2005 — British standard BS 7799 first part. BS 7799 Part 1 is the Code of Practice for Information Security Management (Practical Rules for Information Security Management) describes the 127 control mechanisms needed to build an organization's information security management system based on the best examples of world experience in this field. This document is a practical guide to creating an information security management system.
- BS 7799-2: 2005 — British standard BS 7799 is the second part of the standard. BS 7799 Part - Information Security Management - The information security management system specification defines the specification of the information security management system. The second part of the standard is used as a criterion in the official certification procedure of the organization's information security management system.
- BS 7799-3: 2006 — British standard BS 7799 is the third part of the standard. A new standard in the field of information security risk management (Wikipedia, 2021).

These are the main international standards used by world organizations and institutions to ensure information security in their activities.

At the national level, many countries have developed their own information security standards, which are mandatory in a specific area. According to Ukrainian legislation, the standards of other countries may be applied in Ukraine in the prescribed manner by referencing them in national and other standards if their requirements do not contradict the legislation of Ukraine.

It is also possible to apply the official translation of international standards at the national level. For example, there is an identical translation of the relevant international standard in the State Standard DSTU ISO / IEC 27001: 2015 *Information technology. Methods of protection. Information security management systems. Requirements*. The specified State standard contains, among other things, a broad list of safety measures. These applicable measures include:

- Principles of information security management,
- Information security organizations,
- Security of human resources,
- Resource management of the information security management system,
- Access control,
- Cryptography,
- Physical security and infrastructure security,
- Operational safety,
- Communication security,
- Issues of acquisition, development, and maintenance of information systems,
- Relationships with suppliers,
- Information security incident management,
- Aspects of information security of business continuity management, and
- Compliance with certain requirements (National Standard of Ukraine, 2016).

According to Ovsyannikov et al. (2015), the application of the DSTU ISO/IEC 27001 for banking structures is mandatory and discretionary for structures with other activities. Additionally, harmonization is required with international standards ISO/IEC 27005: 2008 *Information Security Risk Management* and ISO/IEC 27003: 2010 *Guidelines for the implementation of information security management system* to implement the requirements of the information security management system in Ukraine. The first standard provides a framework for determining the approach to risk management depending on the scope of the information security management system, the scope of information security risk management or industry, and the process of information risk assessment, which involves the following two stages: 1) Information risk analysis (identify and quantify assets) - threats, existing means of control, vulnerabilities, and consequences; 2) Information risks assessment - risk management based on an iterative approach to its

assessment to obtain an acceptable value. The second standard describes the information security management system's specification and design process from the beginning of the design to the submission of the plans for implementing the system. The purpose of the standard is to provide practical assistance in implementing the information security management system within the organization following ISO/IEC 27001: 2005. The Informatization Department of the National Bank of Ukraine implements the information security management system and risk assessment methodology based on the ISO/IEC 27003: 2010 standard, *Guidelines for implementing the information security management system* according to the National Bank of Ukraine's industry standards, considering the peculiarities of banking and requirements of the National Bank of Ukraine on information security (Ovsyannikov et al., 2015). These recommendations indicate that implementing information security management standards cannot be a one-off action. In fact, it is a continuous process of developing, implementing, operating, monitoring, reviewing, maintaining, and improving the information security management system. The *plan – execute – check – act* is applied in the modeling processes of the information security management system (National Bank of Ukraine, 2011). These recommendations determine the procedure for preparing the implementation of the information security management system, describing the existing infrastructure and security measures, and proposing risk analysis and assessment in the banking system of Ukraine.

Regarding other branches of management and societal life in general, the legal basis for information security (security of information resources) is contained in a system of documents, including the Constitution of Ukraine; Laws of Ukraine (*On Information*, *On the Protection of Information in Information and Telecommunication Systems*, *On Basic Principles of Information Society Development in Ukraine*, and *On Fundamentals of National Security of Ukraine*); Presidential and Cabinet of Ministers normative legal acts (National Security Strategy, Doctrine of Information Security of Ukraine, Concept of Technical Protection of Information in Ukraine, and Regulations on Technical Protection of Information in Ukraine); international and state standards defining the relationship between various ministries, agencies, and other Government agencies in terms of information security; and normative documents of the system of technical protection of information and departmental regulations within their responsibility. According to information security standards, an information and telecommunication system is considered protected if it meets the established requirements and guarantees for ensuring the confidentiality, integrity, accessibility, and monitoring of information assets. Undoubtedly, the scientists Ovsyannikov et al. (2015) are correct in stating that information security is a highly complex problem. Ensuring information security requires a comprehensive approach to security tools development at both the organizational and technical levels and management to provide a mechanism that allows the implementation of information

security. Information security management is a part of the general management system whose purpose is to ensure the confidentiality, integrity, and accessibility of information assets (documents, media, applications, information systems, and staff knowledge). It implies implementing the company's security policy on an ongoing basis and its constant updating (Ovsyannikov et al., 2015). The previously mentioned documents primarily define the objects of protection involved in ensuring information security, how to analyze existing threats, challenges, risks, and most importantly, the security measures.

The development and implementation of information security standards are essential for creating a reliable and modern model for protecting personal data and information. Information security standards are designed to minimize risks and threats in the information space locally and internationally.

Conclusions

In conclusion, it should be noted that the information security problem is not limited to the technical or legal component. The information and communication spaces are not limited by state borders, and therefore ensuring information security is a strategic transnational task. In Ukraine, information security is ensured at the Constitutional level, providing for its protection. However, Ukraine merely entering the international system of information security standardization and certification is insufficient. National information security measures ensure the level of information and communication space protection; thus, regulations are adopted to regulate this area of public relations at the national level.

Because information security has a dynamic rather than static character, adopted standards do not remain relevant for long. The main international and national standards of information security considered in this work indicate that their approval is usually conditioned by the development of information technologies, the emergence of new information threats, and the increasing menace of information risks. Today, global information security is ensured through compliance with a number of international ISO standards, establishing the procedure for analysis and assessment of information risks and methods for combating them.

The adoption of the international standards and their supporting documents makes it possible to lay the foundations for implementing a new direction of standardization. In Ukraine, the development of a unified regulatory framework in information security can also ensure a high level of standards governing the conduct of certification tests and, as a result, increase confidence in the security of IT products and systems.

In addition to the analysis of information security standards, a comprehensive, system-forming legislative act that ensures a unified strategy for implementing state policy in the field of information security should be developed and enshrined at the legislative level.

Disclaimer

The authors declare no potential conflict of interest related to the article.

Funding

The authors do not report sources of funding for this article.

About the authors

Sofiia Lykhova received her Ph.D. in Legal Sciences in 2006. She graduated as a Professor of Criminal Law and Procedure in 2013. She is the Head of the Department of Criminal Law and Procedure of the National Aviation University.

https://orcid.org/0000-0002-5678-5869 - Contact: lykhova8138@edu.cn.ua

Liudmyla Servatiuk received a Ph.D. in Administrative Law and Process in 2009. She graduated as an Associate Professor of Constitutional, Administrative, and International Law. She has authored 44 scientific papers. She actively researches issues concerning the Ukrainian State Border Guard Service and other law enforcement agencies, national security issues, and border management.

https://orcid.org/0000-0002-0315-8829 - Contact: servatiuk8138@sci-univ.com

Oleksandr Shamsutdinov is a Professor at the National Academy of Security Service of Ukraine in Kyiv. He received an MS and Ph.D. in Law from the National Academy of Security Service of Ukraine in Kyiv. He is a researcher on Criminal Law, Information Safety and Security, and Biosecurity.

https://orcid.org/0000-0001-8820-4558 - Contact: shamsutdinov8138@neu.com.de

Viktoriia Sysoieva is an Associate Professor at the Department of Criminal Law and Process at the National Aviation University in Kyiv. Her expertise includes Law Enforcement and research work organization. She is a researcher on Criminal Law, current criminal law issues, modern crime detection factors, and crime prevention.

https://orcid.org/0000-0001-7913-1676 - Contact: sysoieva8138@acu-edu.cc

Dariia Hurina received Ph.D. in Law. She is the Deputy Head of the Laboratory of Educational and Scientific Work of the Ministry of Internal Affairs of Ukraine. Her expertise includes Law Enforcement, teaching, and research activities. Her research focuses include forensic examination, expert offense prevention, and accounting examination.

https://orcid.org/0000-0002-3692-4614 - Contact: hurina8138@edu-knu.com

References

Akimova, L., Litvinova, I., Ilchenko, H., Pomaza-Ponomarenko, A., & Yemets, O. (2020). The negative impact of corruption on the economic security of states. *International Journal of Management, 11*(5), 1058-1071. https://doi.org/10.34218/IJM.11.5.2020.097

Chyzhmar, Y., Rezvorovich, K., Orlovskyi, R., Kysylova, K., & Buhaichuk, K. (2019). State employment service: European approaches to providing electronic services. *Journal of Legal, Ethical and Regulatory Issues, 22*(6), 1-7.

Constitution of Ukraine. (1996). Law of Ukraine of 28.06.1996, No. 254k/96-VR. Article 7. Verkhovna Rada of Ukraine (Parliament of Ukraine). https://zakon.rada.gov.ua/laws/show/254%D0%BA/96-%D0%B2%D1%80#Text

Dovgan, O.D., & Tkachuk, T.Yu. (2019). Conceptual principles of legislative support of information security of Ukraine. *Information and Law, 1*(28), 86-99. https://doi.org/10.37750/2616-6798.2019.1(28).221314

Galkin, A., Popova, Y., Kyselov, V., Kniazieva, T., Kutsenko, M., & Sokolova, N. (2020). Comparison of urban conventional delivery and green logistics solutions. Paper presented at the *Proceedings - International Conference on Developments in eSystems Engineering, DeSE, 2020-December* (pp. 95-99). Liverpool: Institute of Electrical and Electronics Engineers Inc. DOI: 10.1109/DeSE51703.2020.9450776

International Organization for Standardization (2021b). Cybersecurity. Supplier relationships. Part 1: Overview and concepts (SO/IEC 27036-1:2021). https://standards.iteh.ai/catalog/standards/iso/9bd-2dee7-5278-4b19-a629-1231f50ddfbe/iso-iec-27036-1-2021

International Organization for Standardization. (2010). *Information technology — Security techniques — Network security — Part 3: Reference networking scenarios — Threats, design techniques and control issues* (ISO/IEC 27033-3:2010). https://www.iso.org/standard/51582.html

International Organization for Standardization. (2013a). *Information technology. Security techniques. Code of practice for information security controls* (ISO/IEC 27002:2013). https://www.iso.org/ru/standard/54533.html

International Organization for Standardization. (2013b). *Information technology. Security techniques — Information security for supplier relationships — Part 3: Guidelines for information and communication technology supply chain security* (ISO/IEC 27036-3:2013). https://www.iso.org/ru/standard/59688.html

International Organization for Standardization. (2014). *Information technology. Security techniques — Information security management — Organizational economics* (ISO/IEC TR 27016:2014). https://www.iso.org/ru/standard/43756.html

International Organization for Standardization. (2020). *Information technology. Information security incident management — Part 3: Guidelines for ICT incident response operations* (ISO/IEC 27035-3:2020). https://www.iso.org/ru/standard/74033.html

International Organization for Standardization. (2021a). *About Us*. https://www.iso.org/about-us.html

Kalyuzhny, R., Makeieva, O., & Shapenko, L. (2020). Biomedical ethics and human rights in the context of innovation and information development of society. *Journal of History Culture and Art Research*, *9*(1), 96-106. https://doi.org/10.7596/taksad.v9i1.2537

Kniazieva, T. V., Shevchenko, A. V., Shevchenko, A. V., Yaroshenko, O. M., Inshyn, M. I., & Yakovlyev, O. A. (2021). Current trends in the formation and development of insurance marketing in Ukraine. *Risk Management and Insurance Review, 24*(3), 279-292. DOI: 10.1111/rmir.12185

Kuzmenko, A.M. (2010). Peculiarities of problems of legislative provision of information security of the state, society and citizen in the conditions of information-psychological confrontation. *Journal of Kyiv University of Law, 4*, 317–321. http://kul.kiev.ua/images/chasop/2011_1/315.pdf

Law of Ukraine. (2007). No. 537-V. *On Basic Principles of Information Society Development in Ukraine for 2007–2015*. Verkhovna Rada of Ukraine http://zakon2.rada.gov.ua/laws/show/537-16.

Marushchak, A.I. (2010). Research of information security problems in legal science. *Legal Informatics, 3*(27), 17-21. http://ippi.org.ua/ai-marushchak-doslidzhennya-problem-informatsiinoi-bezpeki-u-yuridichnii-nautsi

National bank of Ukraine. (2011). Letter No. 24-112 / 365. *Regarding the implementation of the information security management system and risk assessment methodology in accordance with the standards of the National Bank of Ukraine*. https://zakon.rada.gov.ua/laws/show/v0365500-11#Text.

National Standard of Ukraine. (2016). *Methods of protection of the information security management system*. UkrNDC. https://www.assistem.kiev.ua/doc/dstu_ISO-IEC_27001_2015.pdf

Orlovskyi, R., Shapoval, R., & Demenko, O. (2018). Possibilities of adapting the typologies of the international standards for establishing criminal liability for corruption-related crimes in Ukraine. *Journal of Eastern European and Central Asian Research, 5*(2). DOI: 10.15549/jeecar.v5i2.230

Ovsyannikov, V.V., Dekhtyar, S.V., Palamarchuk, S.A., Chernysh, Y.O., & Shemendyuk, O.V. (2015). Analysis of regulatory, legal, organizational, and technical aspects of information security. *Modern Information Technologies in the Sphere of Security and Defense, 3*(24), 187-193. https://doi.org/10.33099/2311-7249/2015-24-3-187-193

Vakulyk, O., Petrenko, P., Kuzmenko, I., Pochtovyi, M., & Orlovskyi, R. (2020). Cybersecurity as a component of the national security of the state. *Journal of Security and Sustainability Issues, 9*(3), 775-784. https://doi.org/10.9770/JSSI.2020.9.3(4)

Wikipedia. (2021). *BS 7799*. https://en.wikipedia.org/wiki/BS_7799

Revista Científica General José María Córdova
(Colombian Journal of Military and Strategic Studies)
Bogotá D.C., Colombia

Volume 20, Number 38, April-June 2022, pp. 265-285
https://dx.doi.org/10.21830/19006586.899

Economic security through criminal policies: A comparative study of Western and European approaches

La seguridad económica a través de las políticas criminales: estudio comparativo de los enfoques occidental y europeo

Olena S. Oliinyk
Department of Criminal Law, National Academy of Internal Affairs, Ukraine

Roman M. Shestopalov
Sumy State Pedagogical University named after A.S. Makarenko, Ukraine

Volodymyr O. Zarosylo, Mykhaylo I. Stankovic & Sergii G. Golubitsky
Interregional Academy of Personnel Management, Ukraine

Abstract. The article aims to identify the factors that have the greatest impact on economic security. Based on the study of legislative acts of the countries of the European Union, the United States, and relevant scientific literature, an analysis is made of the current situation in the field of economic security, exploring its constituent elements and factors influencing the security of the economy. Among them are ecology, the fight against crime, the financial and taxation spheres, innovative development, and the element itself as a component of the considered social relations, processes, among others. The article outlines the key areas of public relations and other factors that influence the situation's state concerning the issue addressed.

Keywords: corruption; economic interest; economic relations; national security; public relation; taxation

Resumen. El objetivo del artículo es identificar los factores que más influyen en la seguridad económica. A partir del estudio de los actos legislativos de los países de la Unión Europea, de los Estados Unidos y de la literatura científica pertinente, se analiza la situación actual en el ámbito de la seguridad económica, examinando los elementos que la componen y los factores que influyen en la seguridad de la economía. Entre ellos se encuentran la ecología, la lucha contra la delincuencia, las esferas financieras y fiscales, el desarrollo innovador, la unidad en sí y como componente de las relaciones sociales consideradas, los procesos, entre otros. El artículo esboza las áreas clave de las relaciones públicas y otros factores que influyen en el estado de la situación en el tema.

Palabras clave: corrupción; fiscalidad; interés económico; relaciones económicas; relaciones públicas; seguridad nacional

Section: Dossier • Scientific and technological research article
Received: November 3, 2021 • Accepted: January 27, 2022

Contact: Olena S. Oliinyk ✉ oliinyk8179@sci-univ.com

Introduction

The processes taking place today in society closely link social life and processes in the economy, ecology, the fight against crime, and the field of innovation development, among others. This connection first manifests itself in the fact that no social relation can exist independently. For example, the economic security of an agrarian country depends on the state of its natural resources and the effective use of environmental elements. However, individuals have only recently begun to understand the importance of preserving the integrity of lands, the balance of water resources, and flora and fauna, even at the interstate level. Until recently, there was widespread confidence in the inexhaustibility of the land resource, its limitless use, and self-restoration of fertile properties, despite the emerging discussions on the lack of fresh water and contamination of the ozone layer in the last century.

The purely consumeristic attitude towards the components of the environment has led to their partial loss and exacerbated the need to strengthen the accountability for acts committed resulting in the physical destruction of fertile lands, pollution of water resources, mass disappearance of representatives of the animal and plant world, and the emergence of threats to life, the health of people, or the environment (Savchenko et al., 2017). Such threatening consequences are especially terrible for those countries where the agrarian sector occupies a decisive position in the economy. If a country lacks its own resources, including the natural ones, the government should orient the economy towards another direction of state development, for example, active trading, investment, or the innovative activity of entrepreneurship in the region.

Economic security refers to the access to resources, finances, and markets needed to maintain an acceptable level of prosperity and government. However, the whole idea of economic security is extremely controversial and politicized. In the capitalist system, the concept itself is fraught with contradictions and complications, not least because market participants must feel insecure; if they fail to do so, the market will not achieve its effectiveness. Thus, the idea of economic security is in the dark, as well as the highly political debate on international political economy regarding the nature of the relationship between the political structure of anarchy and the economic structure of the market. The main opposing positions reflect different views on whether some states and societies or markets should be given priority and whether private entities have their own security requirements, which should be weighed against the market decision. The positions are as follows.

Mercantilists and neo-mercantilists place politics first, seeing the state as the embodiment of the social and political goals for which wealth is created and the security necessary for firms and markets to function. From this point of view, economic security is simply part of a broader priority given to national security, and economic success is usually

disregarded. Liberals place the economy first, arguing that the economy should be at the heart of the social fabric and that the market should function as freely as possible without government intervention. The state is needed to ensure legislative and military-political security and support the social fabric in those areas where the market cannot.

From this point of view, the main object of economic security is the development of rules that create the mobility of factors between national economies. However, it can also be argued that liberalism is the protection of the position of the capitalist elite. Liberals value economic efficiency and view economic relations with a positive quantity of shared gains. Socialists are somewhere in between, arguing that the economy is at the heart of the entire social fabric and that, to the extent that states can circumvent this logic, their task is to tame the economy to the social and political goals of justice and fairness. To socialists, security is focused on the economically weak and against the strong (Buzan et al., 1998).

In order to develop the strategy and boundaries of protecting economic security as a whole, as well as its separate elements, it is, first of all, necessary to clearly identify the object of such protection and the methods by which such protection will be carried out. The problems of ensuring economic security, structure, and development strategies in post-Soviet and EU countries have been considered by such scholars as Pasternak-Taranushenko (2002) and Zhalilo (2001).

In their work, Kryshevych et al. (2018) point out that the national economy of any state is a complex economic, social, organizational, scientific, and technological system. It has a general economic potential, among which natural resources, industry, labor, science, and technology stand out. As seen from the above definitions, the category under consideration includes both the conditions and the quality of the system of economic functioning.

Thus, in our study, under economic security, we consider the complexity of the official state bodies' effective measures to provide stability to external and internal threats. We also characterize the national economy's ability to expand self-reproduction to meet the needs of citizens, society, and the state at a specific level and time interval, as well as the state of the economy, which provides sufficiently high and stable economic growth, effectively satisfying economic needs.

It should not be forgotten that economic security is an integral part of national security, which protects the vital interests of people, citizens, society, and the state. It provides sustainable development of society, modern detection, prevention, and neutralization of real and potential threats to national interests.

Components of economic security

Among the factors that ensure (affect) the state of economic security, the state usually refers to the following:

- Financial (achievement of the most effective use of resources):
- Political and legal (observance of the current legislation, comprehensive legal support of the legal activity of entrepreneurship);
- Intellectual and personnel (preservation and development of the intellectual potential of entrepreneurship and effective personnel management);
- Techno-technological (degree of conformity of applied technologies of entrepreneurship to the modern world analogs providing optimization of resource expenditures);
- Information (effective informational and analytical support of the entrepreneurial economic activity);
- Ecological (observance of the current ecological norms);
- Power (providing physical security of entrepreneurship employees). (Buzan et al., 1998)

Concerning the political and legal component of the economic security of entrepreneurship, in this case, it should be noted that the latter provides for protection against excessive tax pressure (which will be discussed below), volatile legislation, and ineffective work of the legal department of entrepreneurship. It defines the environment in which businesses operate and the "game rules" for them. The legal component is the comprehensive legal protection of the company's activities in observance of the current legislation. The legal hazards for entrepreneurship are:

- Insufficient legal protection of the entrepreneurship's interests in contracts and other business documentation;
- Low quality of legal service employee's maintenance of the relevant business entity and mistakes in the recruitment of the personnel of this service;
- Violation of the entrepreneurship and its employees' legal rights;
- Deliberate or unintentional disclosure of commercially important information, among others. (Zavadska, 2018)

Among the external threats of political and legal security in entrepreneurship are frequent government changes, instability of the taxation system, excessive state interference in business affairs. Other serious threats to the companies' activity include the lack of legal guarantees in case of forcible alienation of property and blocking of entrepreneurship accounts (so-called raiding). In turn, entrepreneurship's internal legal and regulatory threats include harmful, ill-conceived rules of internal regulations, positions, instructions, orders, and decisions of the labor collective. The overall process of ensuring the political and legal component of economic security is based on a typical scheme that covers the following elements (actions) of organizational and economic orientation:

- Analysis of the threats of negative influences;
- Assessment of the current level of security;
- Planning a set of measures to increase this level;
- Implementation of resource planning;
- Planning of the work of the enterprise's (organization) relevant functional units;
- Operational realization of the proposed set of measures to ensure an adequate level of
- security.

The main reasons for the occurrence of internal negative influences can be:

a) Low qualification of the relevant business entity's legal service and mistakes in the recruitment of personnel for this service;
b) Insufficient financing of legal support of entrepreneurial or other activities;
c) The enterprise's (organization) reluctance or inability to actively influence the external political and legal environment of its activity.

The causes of external negative influences are mostly of a double nature:

1) Political: a) collision of interests of social groups (groups) of the population with economic, national, religious, and other motives; b) military conflicts (actions); c) economic and political blockade, embargo; d) financial and worldwide political (international) crises.
2) Legislative and legal: a) The parties (public movements) in power's realization of their political and other goals; b) Change of the provisions of the current legislation on property, economic and labor law, taxation, among others.

Assessment of the enterprise's (organization) current level of political and legal security is conducted in several areas:

1) The level of organization and quality of work to ensure this component of the overall level of economic security;
2) Budget-resource support of works;
3) The efficiency of the activities of the relevant subdivisions of economic entities. (Pasternak-Taranushenko, 2002).

The general process of protecting the legal component of economic security is based on a typical scheme that covers the following elements (actions) of organizational and economic orientation. It includes the analysis of the threats of negative influences; assessment of the current level of security; planning a set of measures to increase this level; resource planning; planning of the work of the relevant functional divisions of the entrepreneurship; operational realization of the proposed set of measures to organize the proper level

of security. The following must be noted to ensure the entrepreneurship's compliance with the current ecological standards.

Technological catastrophes arise due to physically depreciated fixed assets, unplanned shutdown of electricity, or employees' low qualifications and irresponsibility. Environmental damage can significantly affect the firm's financial condition; for example, events such as a lawsuit for violations of environmental legislation or an accident with environmental consequences at the enterprise causing financial and environmental losses measured in cash. Other events include environmental damage caused by a company employee's loss of health; reduced production and sales can also affect the company's financial position in a somewhat slower way. However, environmental damage involving a person's loss of health cannot be measured in cash; compensation must be determined subjectively. Because environmental damage to the firm may be uncovered or partially covered, it is a significant source of danger for the organization (Ruslan et al., 2020).

The organization itself can become a source of danger to the environment as a result of economic activity. Internal factors that impair environmental safety include mistakes made at the design stage of new products harmful to human health. At the development and introduction stage of new technologies, these hazards can include fines for pollution of the environment and illegally created landfills. The ecological component involves complying with current environmental norms minimizing losses from the pollution of the environment.

The issues around guaranteeing a society's ecological safety by economic entities engaged in industrial and commercial activities can be solved only by developing and carefully observing national (and international) maximum permissible concentration norms of harmful substances that enter the environment and observing environmental parameters in production (Lavrentieva et al., 2020). However, these measures, including wastewater treatment plants and related efficient, environmentally friendly technologies, require additional costs. Therefore, production companies will not voluntarily comply. The only factor that prompts entrepreneurship to fulfill ecological production rules is the use of tangible fines for violating national environmental legislation.

The algorithm of the process of providing the ecological component of economic security involves the following sequential actions:

1) Calculating the measures' effectiveness map to ensure the ecological component of economic security, according to the organization's reported data on financial and economic activities;
2) Analyzing the performed calculations and the development of recommendations for improving the effectiveness of the activities undertaken;
3) Developing alternative scenarios for the implementation of planned activities;

4) Selecting a priority scenario based on a comparison of planned performance calculations;
5) Submitting the selected planned scenario as part of the general plan for guaranteeing economic security in the functional planning units of the organization's financial and economic activity;
6) Practically implementing the planned activities in the course of the entity's activity. (Kryshevych et al., 2018)

The effective informational and analytical support of the economic activity is a systematic approach to determine the level of economic security of industrial entrepreneurship in the process of information and analytical support. This process can be carried out based on financial information and other industrial economic security components, including social, political, ecological, and demographic production. There is a need for a comprehensive assessment of the level of economic security to optimize the approaches to maintaining the proper state of entrepreneurship security. Therefore, a list of information classified as commercial secrets should exist to resolve the issue at the level of the law. This information should not contain state secrets or harm the interests of society; it should relate to the organization's production activity, have effective or potential commercial value, create competitive advantages, and have access restrictions.

The previous should be considered when creating a list of the enterprise's commercial secrets. The enterprise's legal regime of commercial secrecy provides constitutional guarantees that entitle the entity to own, use, and dispose of intellectual property rights at its own discretion, determining the business entity's competence regarding commercial secrets. Usually, the state protects information containing commercial secrets through criminal law. The same approach to understanding the conceptual apparatus to draw up regulations should ensure such measures' effectiveness, within the limits of one state and at the international level.

Financial factor of economic security

Thus, as we noted, the financial factor of the state's economic security achieves the most effective use of various kinds of resources at the disposal of one or another state. A special effort in developing the modern economy and ensuring its security is to increase the role of banks in creating the necessary resources for the implementation of innovation policies. To ensure innovation in the development of the international economy, it is necessary to create new production capacities and renewal of fixed assets, crucial for increasing labor supply, productivity, resource conservation, and product competitiveness (United Nations, 2021). These transformations require major innovations, investments, and the provision of appropriate funding sources. In connection with this, the question arises on bank loans as sources of funding for projects.

Given the objective need to attract investment and resources for innovative programs and projects in the priority directions of worldwide economic development, the issue of activating commercial banks in the investment market has received a special character and significance (Zavadska, 2018; Bogatyrev et al., 2019). Zachosova and Babina (2006) highlight the significant role of banking institutions in securing economic security, indicating that political, social, and financial crises can seriously harm both the economy of an individual state and the global economy. In addition, the scientists point out in their research that destructive processes that may occur during the functioning of the financial market should be timely determined by government regulators. Usually, the country's National (Central) banks perform this function with the National Commissions, which are called to implement state regulation in the field of financial services markets, and the National Securities and Stock Market Commissions. Among the negative factors that influence the work of financial institutions (banks), scientists name:

- A decrease in the level of active and passive banking services operations;
- Fluctuations in exchange rates;
- Client and their own bank employee frauds;
- Low quality bank assets;
- Lack of proper due diligence of clients' financial security;
- Attempts to expand the lending volumes;
- Information leaks on management and investment;
- Financial decisions from insiders;
- Loss of consumers in competitions;
- Intruder attacks on branches and banks branches, especially in regional departments with poor physical protection;
- Cyberattacks;
- Corruption and false regulator actions, among others. (Zhalilo, 2001)

A number of these problems can be solved by increasing the criminal liability for certain socially dangerous acts that have the highest level of risk. Thus, actions such as cyberattacks on financial institutions are subject to criminalization or its enhancement. These actions not only interest the financial institution; they also interest its clients, who can be seriously affected. To optimize this issue's solution, it is necessary to clearly outline the actions that fall under the notion of "cyberattack" and identify the culprits of such unlawful conduct (Indicators, 2021). Especially because information security is an integral part of national security and, at the same time, an important part of its own sphere, it is also determined as one of the main functions of the state.

Information security is a state of protection of the national interests of any state in the information sphere from threats to individuals and society, and the state through

incompleteness, lack of timely information, unauthorized dissemination and use of information, negative informational influence, and negative consequences of the functioning of information technologies. Today, the information component does not exist outside general national security, and national security will not be comprehensive without information security. Similar crimes encroach on the order of information relations established in society and are committed using electronic computers (computers, systems, and computer networks). Today's cybercrime is widespread (Tatsyi et al., 2010). Moreover, there is no unified and clear definition of the concept under study, both in national and international legislation. The fundamental basis of a high-quality fight against cybercrime is understanding the essence of processes in the functioning of the information space of a particular state.

Therefore, for qualitative scientific and practical comprehension of this problem, it is necessary to determine the essence of the terms used by allocating a conceptual apparatus in the field of cyberspace. However, no clear definition of "cybercrime" was established in the Convention on Cybercrime of November 23, 2001 (Council of Europe, 2001) document. It did imply, however, that cybercrime is the deliberate use of an illegally imposed authority, violence, destruction, or penetration into a cyber system, provided that such actions caused death or damage to a person or persons, material damage to property, civil disorder, or significant economic damage. The document mentions four types of computer crimes: illegal access, unlawful interception, data interference, and interference with the system and establishes the means of cybercrime as computer systems, computer data, information technology services, and traffic data. Cyberspace allows attackers to manipulate information and society's perception at its discretion. Terrorist acts can be implemented with unprecedented efficiency, complicating the task of identifying intruders.

It can first be argued that cybercrime poses a real threat not only for any corporation or private person's individual or computer network but also for an entire state's information and communication systems and, therefore, should be qualified as modern forms of commission aggression. Secondly, given this crime's transnational nature, it is appropriate to establish closer cooperation between national law enforcement agencies and the relevant competent bodies of the international community to achieve the most effective results in combating this negative phenomenon. Thirdly, because many cases of damage to critical infrastructure objects were caused by the lack of well-trained cybersecurity personnel, the qualification level of this personnel must be updated periodically. Moreover, measures should be considered to eliminate illiteracy in the field of cybercrimes in the population.

Lastly, the analysis of international practice in this direction has demonstrated the negative aspects of the continuous computerization and automation of the industrial, banking, and social sectors of the state infrastructure. The violation of their work through

large-scale cyberattacks can lead to irreparable consequences in loss of strategically important information, resources, funds, and human lives. Therefore, the activities of these structures are currently relevant to the development of high-quality and effective preventive measures against cybercrime. Economic security, as such, is impossible without an active counteraction to the processes and socially dangerous phenomena mentioned above. Among the essential factors of an economic nature is the position on observance by all participants in public relations of various types of financial discipline, for example, concerning the payment of taxes. Thus, the current activity of registering fictitious companies worldwide as a means of tax evasion has become increasingly threatening. Producing required documents "on request" has created a separate segment of the economy with a high level of organization and conspiracy.

These socially dangerous acts, which in most countries are recognized as crimes, seriously damage the state's economic security because of the negative impact on tax and budgetary policies, social security, the development of priority economic sectors, and military capabilities, among others; they are also a significant obstacle to ensuring equal conditions. Moreover, such unequal pre-conditions also reject potential investors for which compliance with the law is one of the main principles of business organization (Minchenko et al., 2018).

Crimes as factors of economic destabilization

Tax evasion as a destabilizing factor

Let us look at, for example, the Spanish Criminal Code's wording on tax evasion. In Art. 305, "On felonies against the Exchequer and the Social Security," it establishes that criminal responsibility occurs for any action or omission, leading to losses to the budget by way of non-payment, debt cancellation, or reimbursement (Legislationline, 1998).

The sanction of the article provides for punishment in the form of deprivation of liberty from one to four years with a fine of six times the number of assessed sums. At the same time, this article contains an incentive clause providing exemption from criminal liability if a person has not been informed of a tax audit process or that such a review has been initiated. Normally, the state prosecutor or procedural representative of autonomy administration or the local administration must file a complaint or a statement against that person before the prosecutor's office, and this office or the investigating judge acts, making the person aware of the initiation of an investigation (Legislationline, 1998). In the United States, Germany, and Spain, tax evasion is most often attributable to inconsistencies in total property status, the declared income, and the questionable nature of transactions. In tax cases, the tax legislation in the United States and other developed countries' carries a presumption of innocence, demonstrating their trust in the taxpayers

and allowing the latter the opportunity to refuse information that may be used against them during a trial.

The US legislation not only criminalizes non-payment of taxes; it even criminalizes actions aimed at attempting to evade taxation. The very procedure for collecting tax arrears prompts the payer to cooperate; the tax authorities' main purpose is filling the budget, not bringing taxpayers to liability. This approach is realized by introducing the order by which the payer repeatedly sends claims for payment of taxes, which they can appeal to the tax authority or the court. The taxpayer's property can be arrested; however, this can be canceled before the start of tenders in the event of repayment of arrears. Moreover, the payment of arrears with deductions excludes prosecution and eludes criminal liability (Minchenko et al., 2018).

Corruption as a factor in the destabilization of economic relations

The globalization of the economy, which today has a very active influence on the development of society, influences processes under consideration. Thus, global changes that accompany world economic relations between its participants, from international communities to small companies and consumers, are positive and negative. In the context of exacerbation of socio-economic, political, legal, environmental, financial, and other relations between world countries in the framework of the implementation of active integration processes at the international level, it is important to study and assess the negative effects of the economic nature of globalization. The economic consequences of globalization directly impact the global community, changes in macroeconomics, microeconomic implications, economic development of countries and their associations, the environment, finance, migration processes, and political environment, among others.

Underestimation of the negative impact of globalization in the world community can lead to large-scale crises in the world economy, the destruction of global economic interactions under the pressure of negative consequences (Shopina et al., 2017). Corruption remains a negative factor in the development of economic relations both within the country and beyond. Although this socially negative phenomenon is not a separate aspect of our study, the following should be noted. In the scientific environment, corruption is defined as:

1) Abuse of state power by state officials, political, and civil servants to illegally enrich themselves or their subordinates;
2) The activities of state-authorized persons aimed at abuse of power and position to accept material goods, services, benefits, or other tangible or intangible effects from individuals and legal entities, and bribing of officials;
3) Bribing of civil servants by legal entities and individuals encroaching upon normatively established social relations in the field of civil service;

4) The use of an official of the state's power and management of his/her official position for personal enrichment;
5) Abuse of management by authorities in favor of personal or group interests;
6) A social phenomenon that covers the entire set of corruption actions related to the illegal use of persons authorized to perform public functions of the authorities, the official authority, the appropriate facilities to satisfy the personal interests or interests of the third party and other corruption offenses, which create conditions for committing or concealing corruption (Inshyn & Moskalenko, 2018).

From the previous, three groups of definitions concerning the complex definition of corruption can be distinguished. The first group of definitions refers to public ethics. In this case, *corruption* is defined as the ethical mutual distribution of interests between the public and private space. The second group of definitions refers to corruption issues regarding the transparency of the state's activities. Finally, there is the third group of definitions that is proposed as basic: corruption is one of many parts of a more complex criminal phenomenon, which is an economic crime (Savchenko et al., 2018). In their work, Semchuk et al. (2018) note that corruption has existed since ancient times, since the emergence of the state and the creation of its bodies with authority and administrative powers. The authors emphasize that the characteristic feature of this phenomenon is its harm in the legal, social, economic, and other aspects.

In addition, the authors emphasize that corruption is a phenomenon that is constantly evolving, transforming, and adapting to modern conditions and developing legislation, society, and state, while its essence and negative influence remain unchanged. Thus, according to a survey conducted by the investment company Dragon Capital (Kyiv) and the European Business Association, this phenomenon is widespread. In Ukraine, for example, there is practically no trust in the authorities, judicial authorities, and law enforcement agencies. The Interfax-Ukraine[1] news agency issued a press release of a report in which respondents used a 10-point scale to rate relevant obstacles in this regard. The monopolization of markets and seizure of power by oligarchs placed third in the ranking (5.9 points), while the military conflict with Russia and the unpredictable exchange rate (by 5.6 points) occupied the fourth and fifth positions, respectively.

The repressive actions of law enforcement bodies occupied the sixth position (Ivanova et al., 2020) (4.6 points), based on the large-scale illegal actions of the Public Prosecutor's Office, the Security Service, and the police. Other positions belonged to the constant change of the statutory regulation, the complex administration of taxes, and

1 Ukrainian news agency founded in 1992. The agency publishes 52 information products on political and economic issues.

currency restrictions (Yunin et al., 2018). Kuzmenko et al. (2018) noted that the most damaging effects of the spread of corruption on the European state economy are:

1) The expansion of the shadow economy, leading to the reduction of tax revenues to the budget. As a result, the state loses the financial levers of economic governance, and social problems are exacerbated by the budget deficit.
2) The brake down of the competitive market mechanism. Often the winner is not the one who is competitive but the one able to obtain benefits illegally. This leads to a reduction of the market, a decrease in its efficiency and the discrediting of the idea of market and competition.
3) The deceleration in the emergence of effective private owners, primarily because of a breach of the privatization procedure and artificial bankruptcies, usually associated with the bribing of officials.
4) The inefficient use of budget funds, in particular, when distributing government orders and benefits, further complicating budget problems in the country.
5) Price increases due to "corruption costs." As a result, consumers are suffering.
6) Business entities do not believe in the ability of the authorities to establish, control, and adhere to fair rules of the market game.
7) The investment climate leads to degradation and unresolved problems of overcoming the fall in the countries of production and reconstruction of fixed assets.

The shadow economy's main causes are those previously mentioned. They include the imperfection of legislation, which is subject, among others, to tax pressure, confusion in the tax administration, the lack of assistance in obtaining tax breaks, lobbying the interests of business groups, and the closeness to power. Tylchyk et al. (2018) add that another socially dangerous phenomenon negatively affecting the state of economic security is the legalization of the proceeds of crime as an aspect or component of the shadow economy itself. By analyzing the laws defining measures to counteract the legalization (laundering) of proceeds from crime we can conclude that they actually emphasize that the negative phenomenon and the shadow economy are not identical. Some publications note that the sign of the shadow economy is an indication of the illegality of the origin of the monetary sum, including its mathematical expression (Tagarev, 2010). Thus, according to the authors, the legalization of shadow capital introduces it into the legal sphere of economic activity with a view to legitimate accumulation, that is, the receipt of "purified income."

Indeed, each state has a single, functioning anti-corruption strategy (program) that includes comprehensive measures, usually approved at the state level. At the same time, the importance of establishing liability, commensurate with the harm caused by bribes

and payoffs, should not be diminished. In the face of these actions, the rules of liability are established, firstly, by prohibiting the conduct and establishing good conduct. Secondly, they can act as a preventive measure or incentive to refrain from unlawful actions, and thirdly, they can accomplish their direct function, repress, which also "works" in a certain way. Returning to the analysis of criminal legislation in Europe, we can conclude that most have criminalized various forms of bribery –both receiving and issuing a bribe (Melnyk et al., 2021). Consequently, foreign criminal law operates with the terms of "active and passive" bribery; there is a more detailed regulation of liability for passive bribery than active.

Active bribery in the international experience

According to Article 21 of the UN Convention Against Corruption (2003), active bribery can be defined as

> (a) "the promise, offering or giving, directly or indirectly, of an undue advantage to any person who directs or works, in any capacity, for a private sector entity, for the person himself or herself or for another person, in order that he or she, in breach of his or her duties, act or refrain from acting;
>
> (b) The solicitation or acceptance, directly or indirectly, of an undue advantage by any person who directs or works, in any capacity, for a private sector entity, for the person himself or herself or for another person, in order that he or she, in breach of his or her duties, act or refrain from acting". (p. 12)

The term "active bribery" is used in the Framework Decision of the Council of the European Union No. 2003/568 / IPU on combating corruption in the private sector (Verkhovna Rada of Ukraine, 2003). According to Article 2 of this document, active corruption is an act consisting of promising, soliciting, or providing, directly or through a third party, to a person who, on any basis, has a leading function or work in favor of an organization related to the private sector, an unlawful gain any character assigned to such person or a third party in order to violate their obligations, such person committed or refrained from committing a certain action.

The positive aspect of the criminal law of western European states is that, compared with US law, the regulation of criminal measures to prevent active commercial bribery in Italy, France, and Germany is quite stable. In France, before 1992, the guilty were prosecuted under Articles 177-183 of the Criminal Code of 1810. In Italy, significant changes in the Criminal Code of 1930 concerning official crimes were introduced only in 1990. In many European countries, the criminalization of active commercial bribery is closely linked to the establishment of liability for organized crime, drug trafficking, and money laundering, in which corruption is considered an essential (qualitative) sign. Most clearly, this is seen from the experience of Italy. Experts from the Italian Parliament believe that

corruption in state and municipal government bodies has reached unprecedented proportions, corporate corruption is rampant among corrupt officials, and the law of "immortality" (duty of silence) is in effect.

Article 322, "Incitement to corruption," in the Criminal Code of Italy (2022), establishes liability for active commercial bribery, implying responsibility even for offering a bribe. The severity of the punishment for committing this socially damaging act depends on whether it involves actions within the scope of official duties or actions not provided for by them. That is, if it is beyond the limits of the rights and duties assigned to a person by position, the punishment is more severe. In 1999, for example, the Criminal Code of Switzerland introduced a new section (1 called "Bribery." It consists of two main points:

1) Bribery of a Swiss official. Giving a bribe;
2) Bribery of an official of a foreign state.

Here, private individuals bribing officials performing public functions are equated with officials of an international organization bribing officials of a foreign state. According to various articles, punishment applies in the following cases: a) a proposal for improper benefits, its promise, or provision in connection with official activities (bribery), b) an action or inaction contrary to the duties of an official (provision of benefits); c) accepting a bribe; and d) acceptance of benefits. In Swiss criminal law (similar to Germany), the notion of an official socially dangerous act in the context of bribery includes socially dangerous acts that may be carried out in the future, at the time of the bribe, and issuing a bribe (Vystavna et al., 2018). Because it is unknown what this act may involve and when it can occur, the "just in case bribe" is criminalized in these countries.

Active bribery in the Criminal Code of Belgium is defined as an act committed directly or through an intermediary's actions consisting of offering, promising, or rendering unlawful benefits to a person holding a directorial or managing position or a representative or employee of an individual or legal entity. It is performed for themselves or in the interests of a third person for the commission or non-execution of actions within the limits of the powers of such persons, or through such powers, without the corresponding agreement or notice to the board of directors, the general meeting of shareholders socket (principal), or employer.

Croatian criminal law on liability for corrupt bribery of a private law official is established in the Criminal Code and the Criminal Law Act of legal entities for the commission of criminal offenses. In the Criminal Code of the Republic of Croatia (2011), in the chapter on crimes committed in the field of official activity, there is no special rule that establishes responsibility for corrupt bribery of a private person. Instead, such rules (active and passive bribery) are contained in Chapter 28, "Criminal offences against official duty," where articles 294(20) and 294(3) under "Giving a Bribe" provide for criminal

liability for receiving and offering bribes in the course of economic and other transactions. In accordance with this norm, active bribery is defined as the provision of gifts or any other benefit, the promise of such items to the authorized person in exchange for the commission acts or provision of services by such a person that are beneficial to one side and harmful to the one represented by the person receiving such a benefit.

Criminal punishment is also the provision of such items through intermediaries (§1). The commission of such actions on mutually beneficial terms is also a criminal offense but it is punishable less strictly (§2) (CMS Law, 2018). In the United States, for example, liability is established by special laws for both physical and legal persons. Thus, anyone who gives, offers, promises anything valuable to a public official or a candidate for this post can be held responsible for giving a bribe. This action has the following aim: 1) to influence official actions on decisions within the individual's competence; 2) influence the official commit, assist in committing, conspire, permit any fraudulent action, or create an opportunity for deception; 3) to incline an official to action or inaction in violation of the official's legal duties. Punishment for those who give and those who receive a bribe is a fine of up to $10,000 or imprisonment for up to two years (Jiménez, 1998).

Thus, it can be concluded that the concept of "active bribery" includes an offer or a promise to render unlawful benefits and give an unlawful benefit to the official of a private right for that person's performance or non-performance of certain actions (in exchange), using the person's official powers. Consequently, illegal rendering or attempting to grant another person an unjustified advantage when accessing a public contract or setting up public service entrepreneurship is punishable. In general, European criminal law draws attention to the fact that the sanctions provided for all types of bribery are strict. They involve, as a general rule, imprisonment and monetary fines; however, the "gap" between the lower and upper limits of the relatively defined sanctions is often quite significant. It is typical that in some countries the types and sverity of punishment for receiving and giving a bribe are the same (Part 1 of Article 331 and Part 1 of Article 333 of the Criminal Code of Germany, Articles 432-11 and 433-1 of the Criminal Code of France; 321 CC of Italy) (Zitryak, 2021).

A selective study of foreign experience in establishing criminal responsibility for active commercial bribery shows the main features and trends of criminalization and penalization of bribery. Most of the examined criminal codes of foreign states criminalize offering a bribe, as well as its offer or promise. The scope of criminally-related bribery is not limited to the public sector; the law also addresses commercial and public relations. In some states, individuals and legal entities are the subjects of responsibility for active bribery. Sanctions against criminals are quite harsh, sometimes set at the level of responsibility of the bribe-taker, an obvious reflection of the view that bribery is a mutual agreement between two parties. Therefore, both parties are accountable for the social risk,

and responsibility should not differ materially. Currently, the international (transnational) nature of corruption involving the bribing of foreign officials and the harm caused by socially dangerous acts, especially in economic relations between economic entities, is criminalized (Zitryak, 2012).

Indeed, at the end of the twentieth century, the world community recognized that corruption is a global problem for every country, which needs to be addressed. The result was the adoption of several international legal acts (mandatory and recommended) prepared and adopted by the Organization of the Nations, the Organization for Economic Cooperation and Development, the Organization of American States, the Council of Europe, the European Union, among others. International instruments differ in scope; however, they have one aim: to establish common standards for combating corruption through the provision of anti-corruption legislation at the national level (Kryshevych et al., 2018). Thus, as evidenced by European and international experience, aimed at protecting business entities during their activities in the private and public sectors, the criminalization of illegal socially dangerous acts of private and public law officials is not overlooked. It is a significant factor, which will further normalize the economic situation and ensure economic security both in a single state and worldwide.

Conclusion

In this article, we have examined various factors and aspects that, in one way or another, affect the development of national and international economic relations. Based on this, the following conclusions have been drawn.

First, economic security is the key to the successful development of any state. The vector of this development should aim to ensure the state's sustainable development, the implementation of structural reforms, and, consequently, the improvement of living standards. Secondly, a macroeconomy that is capable of ensuring stability, sustainable economic growth, favorable conditions for economic activity, and a transparent tax system needs to be restored. Thirdly, the vector of provision is to provide the state, businesses, and security of citizens protection of investments and private property. Each country must become a state capable of defending its borders and securing peace within its territory and the European region. Fair and impartial justice, urgent purges of power at all levels, and ensuring the effective implementation of the fight against corruption should be the decisive basis for security.

Fourthly, more severely repressive effects on tax evasion measures are required to help fill the budget. More effective regulation of the activities of state financial control agencies is required to ensure the legality of regulation of relations in the field of public relations and their coordination. The international community should assist States in creat-

ing the legal framework for the financial control of the participation of society. Successful work in the given direction is considered an increase in the number of services provided by the financial control authorities impersonally, that is, through a computer network. In addition, with the increase of such a list, the level of responsibility for violation of financial and tax discipline should increase. Fifthly, it is necessary to create a high-quality normative-legal act at the level of international cooperation based on the integrated application of various spectra of expert assessments, addressing anti-corruption and financial expediency and the legal, independent, scientific, linguistic, social, and other. At the same time, it should be noted that the aspects, factors, and instruments mentioned and studied here have a direct or indirect impact on the provision of economic security, different in nature. These issues will not be covered and solved at the level of a single comprehensive normative act.

Sixth, given the previous, it should be reiterated that resolving the problems of effective counteraction to corruption, which has tightly captured the state and non-state sector of practically every developed state, depends largely on how properly and deeply we understand its essence. Understanding the essence of corruption is extremely important in the theoretical and practical sense. Therefore, the approach to solving this problem must be justified by theoretical developments. Moreover, "pilot" projects should be actively introduced in individual states or regions to confirm or deny the authenticity (validity) of the theory of mechanisms for combating this negative phenomenon, as corruption offenses in the field of economics. Lastly, ensuring the protection of the natural environment as an important component of economic security should not be called into question. There is a need to develop a single codified act to regulate the protection of objects of the natural environment; given their close interconnection, it is impossible to separate its constituent borders of the state.

Therefore, given the importance of the issues raised in the study, it should be emphasized that the aspects considered are rather ramified, complex, and diverse. In itself, the provision of economic security at the state, intergovernmental, and international levels require extraordinary efforts, strong cooperation of interested actors in public relations, and the involvement of specialists from various fields. Moreover, it is important to note that developing a single normative act (convention) with the issue raised *a priori* is impossible. In this case, a comprehensive approach to the issue is vital. Its result should be the development of the entire complex (system) of normative acts aimed at improving methods, forms, and measures to solve the problem of ensuring economic security comprehensively. The provided acts should be appropriate mechanisms and adequate methods (following the specifics of the region or country) to influence the resolution of public issues in this area qualitatively.

Disclaimer

The authors declare no potential conflict of interest related to the article.

Funding

The authors do not report sources of funding for this article.

About the authors

Olena S. Oliinyk is a Ph.D. in Legal Science from the Dnipropetrovsk State University of Internal Affairs. She is an Associate Professor and Professor at the Department of Criminal Law of the National Academy of Internal Affairs. A researcher in criminal law in the Ukraine, environmental protection, and corruption crimes.

https://orcid.org/0000-0002-2519-8370 - Contact: oliinyk8179@sci-univ.com

Roman M. Shestopalov is a Ph.D, in Law. Senior Lecturer at the Department of Law and Methods of Teaching Jurisprudence. Participated in the international internship "Innovations in the field of higher vocational and professional education in the digital environment of transformation," representing Sumy State Pedagogical University named after A.S. Makarenko.

https://orcid.org/0000-0003-3397-2482 - Contact: shestopalov8179@edu-knu.com

Volodymyr O. Zarosylo is a Ph.D. in Legal Science. A Professor, Head of the Department of Law Enforcement and Anticorruption Activity at the Interregional Academy of Personnel Management. Scientific and pedagogical activity from 1999 to the present. For the last 5 years, he has prepared 6 monographs, 5 textbooks and 20 scientific articles.

https://orcid.org/0000-0001-6538-7515 - Contact: zarosylo8179@acu-edu.cc

Mykhaylo I. Stankovic is a Ph.D. in Law. Associate Professor of the Department of Law Enforcement and Anticorruption Activity. He heads the legal consulting center, "Central Legal Clinic," at the Interregional Academy of Personnel Management, Ukraine. Researcher in criminal procedure and criminology, forensic examination, and operational and investigative activities.

https://orcid.org/0000-0002-3903-9362 - Contact: stankovic8179@edu.cn.ua

Sergii G. Golubitsky is a Ph.D. in Law and an Associate Professor. He works at the Department of Law Enforcement and Anticorruption Activity in the Interregional Academy of Personnel Management.

https://orcid.org/0000-0003-4164-9052 - Contact: golubitsky8179@neu.com.de

References

Bogatyrev, I., Topchiy, V., Koropatnik, I., Kotliarenko, O., & Kofanov, A. (2019). Problems and Perspectives for Attracting Investments in Economy of Ukraine. *Investment Management and Financial Innovations*, *16*(2), 195-205. http://doi.org/10.21511/imfi.16(2).2019.17

Buzan, B., Waever, O., & Wilde, J. D. (1998). *Security: A new framework for analysis*. Lynne Rienner Publishers.

CMS Law. (2018). *CMS Guide to Anti-Bribery and Corruption Laws*. June. https://cms.law/en/media/local/cms-cmno/files/news-information/brochures/cms-guide-to-anti-bribery-and-corruption-laws-2018?v=5

Council of Europe. (2001). *Convention on Cybercrime* (ETS No. 185). https://www.coe.int/en/web/conventions/full-list?module=treaty-detail&treatynum=185

Criminal Code of Italy. (2022). *Incitement to corruption*. Article 322. https://www.altalex.com/documents/news/2014/10/14/dei-delitti-contro-la-pubblica-amministrazione

Criminal Code of the Republic of Croatia. (2011). *Criminal offences against official duty*. Chapter 28. Legislationline. https://www.legislationline.org/download/id/7896/file/Croatia_Criminal_Code_2011_en.pdf

Indicators. (2021). *Fragile States Index*. The Fund for Peace. https://fragilestatesindex.org/indicators/

Inshyn, M., & Moskalenko, O. (2018). Ensuring freedom of labor in Ukraine in the context of labor emigration. *Baltic Journal of Law and Politics, 11*(2), 1-31. https://doi.org/10.2478/bjlp-2018-0009

Jiménez, L. (1998). The Inter-American Convention Against Corruption. *Proceedings of the ASIL Annual Meeting*, 92, 157-162. https://doi.org/10.1017/S0272503700057803

Ivanova, H., Podoliaka, S., Aliieva-Baranovska, V., Vasyliev, V., & Liudvik, V. (2020). Administrative and Legal Support for Functioning of the Agro-Industrial Complex of Ukraine. *Journal of Legal, Ethical and Regulatory Issues, 23*(4), 1-7.

Kryshevych, O., Terzi, O., & Starytska, O. (2018). Key development factors for the Ukrainian economy. *Baltic Journal of Economic Studies*, *4*(4), 194-201. https://doi.org/10.30525/2256-0742/2018-4-4-194-201

Kuzmenko, O., Drozd, O., & Chorna, V. (2018). Financial control as a means of countering economic corruption in Ukraine. *Baltic Journal of Economic Studies*, *4*(4), 233-237. https://doi.org/10.30525/2256-0742/2018-4-4-233-237

Lavrentieva, O., Pererva, V., Krupskyi, O., Britchenko, I., & Shabanov, S. (2020). Issues of shaping the students' professional and terminological competence in science area of expertise in the sustainable development era. Paper presented at the E3S Web of Conferences, 166. https://doi.org/10.1051/e3sconf/202016610031

Legislationline. (1998). *On felonies against the Exchequer and the Social Security*, *Article 305.* Criminal Code of Spain. p. 93. https://www.legislationline.org/documents/section/criminal-codes

Melnyk, D.S., Parfylo, O.A., Butenko, O.V., Tykhonova, O.V., & Zarosylo, V.O. (2021). Practice of the member states of the European Union in the field of anti-corruption regulation. *Journal of Financial Crime*, (pre-print). https://doi.org/10.1108/jfc-03-2021-0050.

Minchenko, S., Oliinyk, O., & Borovyk, A. (2018). Tax Avoidance as a Threat to Economic Security: Ways and Methods of Counteraction (Domestic and Foreign Experience). *Baltic Journal of Economic Studies*, *4*(3), 172-178. https://doi.org/10.30525/2256-0742/2018-4-3-172-178

Pasternak-Taranushenko, G.A. (2002). *Economic security of the state. Static of the process of securing*. Kyiv: Kondor. https://www.lvduvs.edu.ua/documents_pdf/biblioteka/nauk_konf/konf_22_04_2016.pdf

Ruslan, K., Inshyn, M., Dmytro, S., Yelena, T., & Olena, A. (2020). Occupational safety and health of factory workers in European countries in the nineteenth century: Historical and legal analysis. *Labor History, 61*(3-4), 388-400. https://doi.org/10.1080/0023656X.2020.1775796

Savchenko, A., Babikov, O., & Oliinyk, O. (2017). Comparative and Legal Analysis of Criminal and Legal Protection of Individual Components of Natural Environment: European Experience. *Journal of Advanced Research in Law and Economics*, *8*(7), 2219-2226. https://doi.org/10.14505/jarle.v8.7(29).21

Savchenko, L., Subbot, A., & Demianchuk, Y. (2018). Influence of Corruption on the Economic Development of Ukraine in Terms of Reformation: A Retrospective Analysis. *Baltic Journal of Economic Studies*, *4*(3), 276-282. https://doi.org/10.30525/2256-0742/2018-4-3-276-282

Semchuk, Z., Zharovskaya, I., & Merdova, O. (2018). Corruption as a Negative Social Phenomenon Hindering the Economic Development of the State. *Baltic Journal of Economic Studies*, *4*(4), 295-300. https://doi.org/10.30525/2256-0742/2018-4-4-295-300

Shopina, I., Oliinyk, O., & Finaheiev, V. (2017). Globalization and its negative impact on the global economy. *Baltic Journal of Economic Studies*, *3*(5), 457-461. https://doi.org/10.30525/2256-0742/2017-3-5-457-461

Tagarev, T. (2010). *Building integrity and reducing corruption in defence: A compendium of best practices.* NATO-Geneva Centre for the Democratic Control of Armed Forces. https://www.dcaf.ch/sites/default/files/publications/documents/Compendium_Building_Integrity_and_Reducing_Corruption_in_Defence.pdf

Tatsyi, V., Getman, A., Ivanov, S., Karasiuk, V., Lugoviy, O., & Sokolov, O. (2010). Semantic network of knowledge in science of law. Paper presented at the Proceedings of the IASTED International Conference on Automation, Control, and Information Technology - Information and Communication Technology, ACIT-ICT 2010 (Novosibirsk, June 15-18) (pp. 218-222). Novosibirsk: ACIT-ICT.

Tylchyk, O., Dragan, O., & Nazymko, O. (2018). Establishing the ratio of concepts of counteraction to legalization (Laundering) of illegally-obtained income and counteraction to the shadow economy: The importance for determining performance indicators of the European integration processes. *Baltic Journal of Economic Studies, 4*(4), 341-345. https://doi.org/10.30525/2256-0742/2018-4-4-341-345

United Nations (2003). *Convention Against Corruption*. Article 21. https://www.jus.uio.no/lm/un.against.corruption.convention.2003/portrait.pdf

United Nations (2021). *Approach to human security*. Human Security Course. https://humansecuritycourse.info/module-1-the-concept-of-human-security/un-approach/

Verkhovna Rada of Ukraine. (2003). *Framework Decision of the Council of the European Union No. 2003/568 "On combating corruption in the private sector."* http://zakon3.rada.gov.ua/laws/show/994_945

Verkhovna Rada of Ukraine. (2006). United Nations Convention against Corruption. http://zakon4.rada.gov.ua/laws/show/995_c16

Vystavna, Y., Cherkashyna, M., & van der Valk, M. R. (2018). Water laws of Georgia, Moldova and Ukraine: Current problems and integration with EU legislation. *Water International, 43*(3), 424-435.

Yunin, O., Sevruk, V., & Pavlenko, S. (2018). Priorities of economic development of Ukraine in the context of European integration. *Baltic Journal of Economic Studies*, *4*(3), 358-365. https://doi.org/10.30525/2256-0742/2018-4-3-358-365.

Zachosova, N., & Babina, N. (2018). Identification of threats to financial institutions' economic security as an element of the state financial security regulation. *Baltic Journal of Economic Studies, 4*(3), 80-87. https://doi.org/ 10.30525/2256-0742/2018-4-3-80-87

Zavadska, D. (2018). Determining the role of banks in the financing of innovative development processes of the economy. *Baltic Journal of Economic Studies*, *4*(3), 68-73. https://doi.org/10.30525/2256-0742/2018-4-3-68-73

Zhalilo, Y. (2001). Strategy for ensuring economic security of Ukraine. Priorities and problems of implementation. In *Strategy of National Security of Ukraine in the context of world community experience*. Kyiv: Satsanga. https://iie.org.ua/wp-content/uploads/2019/02/Harazishvili_monograf_2019-ost.pdf

Zitryak, V.Ya. (2012). Foreign experience of criminalization of active bribery. *State and Law, 56*, 444-449. http://dspace.nbuv.gov.ua/handle/123456789/64415

Esta página queda intencionalmente en blanco

Revista Científica General José María Córdova
(Colombian Journal of Military and Strategic Studies)
Bogotá D.C., Colombia

Volume 20, Number 38, April-June 2022, pp. 287-305
https://dx.doi.org/10.21830/19006586.903

The system of cybersecurity bodies in Ukraine

El sistema de organismos de ciberseguridad en Ucrania

Andrii V. Svintsytsky
Ukrainian Scientific and Research Institute of Special Equipment and Forensic Expertise of The Security Service of Ukraine, Ukraine.
University of the State Fiscal Service of Ukraine, Ukraine

Abstract. This article describes Ukraine's cybersecurity system, its place, and its role in a single configuration of national security. The methods used include formal-dogmatic, comparative-legal, sociological, and hermeneutics. The research revealed that effective cybersecurity must be addressed comprehensively, requiring coordinated action at the national, regional, and international levels to prevent, prepare, and respond to incidents by the government, the private sector, and civil society.

Keywords: cyber defense; cybersecurity; cyberspace; cyber strategy; national security

Resumen. Este artículo describe el sistema de ciberseguridad de Ucrania, su lugar y papel en un complejo único de la seguridad nacional. Los métodos utilizados son el formal-dogmático, el comparativo-legal, el sociológico y el hermenéutico. La investigación reveló que la ciberseguridad efectiva debe ser abordada de forma integral, requiriendo una acción coordinada a nivel nacional, regional e internacional para prevenir, preparar y responder a los incidentes por parte del gobierno, el sector privado y la sociedad civil.

Palabras clave: ciberdefensa; ciberespacio; ciberestrategia; ciberseguridad; seguridad nacional

Section: Dossier • Scientific and technological research article
Received: November 30, 2021 • Accepted: February 12, 2022

Contact: Andrii V. Svintsytskyi ✉ svintsytskyi19@neu.com.de

Introduction

The law "On the Basic Principles of Cyber Security of Ukraine" (Law of Ukraine No. 2163-VIII, 2017) was adopted relatively recently, in 2017; however, the system of bodies addressing cybersecurity was formed long before. In 2007, the *State Special Communications and Information Protection Service (Derzhspetszviazok)* was established based on the dissolved Ukrainian Security Service's *Department of Special Telecommunication Systems and Information Protection* (Law of Ukraine No. 2163-VIII, 2006). It included the State's Special Communications Administration's *Department of Information and Telecommunication Systems Security*, later renamed the *State Cyber Protection Centre*.

In the same year, the *Computer Emergency Response Team* (CERT-UA) was established within the Department. Two years later, in 2009, this response team was accredited by the *Forum for Incident Response and Security Teams* (FIRST). In 2010, it became clear that the existing range of tasks was too considerable for one unit. Thus, two separate entities, part of the State's Special Communications Administration, were created based on the dissolved *Information and Telecommunication Systems Security Department*, namely, *the State Special Communications Information Security Department* and the *Special Information and Telecommunication Systems Department.*

In the same year, the former was renamed the *State Center for Information Resources Protection* (Boyarchuk et al., 2021). In 2012, developing international cooperation, CERT-UA received accreditation from the specialized security agency of the International Electrotechnical Commission (IEC), the *International Multilateral Partnership Against Cyber Threats* (IMPACT). In 2015, the need arose to regulate cybersecurity issues in Ukraine legislatively. Accordingly, the decision of the Board of the State Special Communications Administration[1] was adopted; it reorganized the State Special Communications Service's *State Center for Information Resources Protection* into the *State Cyber Protection and Countering Cyber Threats Centre* of the same State service.

The adoption of the law on the basic principles of cyber security (Law of Ukraine No. 2163-VIII, 2017) prompted a need to reorganize, restructure the staff, and redistribute the areas of responsibility of the *State Cyber Protection Centre* according to the law. The process lasted for two years. Finally, by decision of the Board of the State Special Communications Administration[2], the State's Special Communications' *Cyber Protection Centre and Countering Cyber Threats Centre* was reorganized into the *State Cyber Protection Centre of Special Communications and Information Protection Service* (abbreviated: *Center for Cyber Protection of the State Special Communications*). In 2019, the abbreviated

1 Decision of the Board of the State Special Communications Administration of 01/07/2015.
2 Decision of the Board of the State Special Communications Administration No. 01/01 / 01-3729 of July 26, 2018.

name was changed to the *State's Cyber Protection Centre of Special Communication and Information Protection Service* (SCPC).[3] In October 2020, a new edition of the *State Cyber Protection Centre of Special Communication and Information Protection Service* regulation was approved.[4]

According to the mentioned law on the basic principles of cyber security in the Verkhovna Rada of Ukraine (Law of Ukraine No. 2163-VIII, 2017), the main tasks of CERT-UA are as follows:

1. Collecting and analyzing data on cyber incidents, maintaining the State register of cyber incidents;
2. Providing practical assistance to the owners of cybersecurity objects on the prevention, detection, and elimination of cyber incidents on these objects;
3. Organizing workshops on cybersecurity concerning ensuring the national cybersecurity system and owners of cybersecurity objects;
4. Preparing and posting recommendations for combating modern types of cyberattacks and cyber threats on websites;
5. Interacting with law enforcement bodies, informing them promptly about cyberattacks;
6. Cooperating with foreign and international organizations on cyber incident responses, particularly concerning the participation of FIRST security incident response teams, including the payment of annual membership fees;
7. Collaborating with CERT-UA and other enterprises, institutions, and organizations carrying out activities related to cyberspace security regardless of ownership;
8. Processing information received from citizens on cyber incidents concerning cybersecurity objects;
9. Assisting State bodies, local governments, military formations established under the law, enterprises, institutions, and organizations regardless of ownership, as well as citizens of Ukraine in addressing cyber protection and combating cyber threats.

Structural units for combating cybercrime before the reformation

In 2010, cybercrime units appeared in the law enforcement bodies' structures. On the basis of the Ukrainian Ministry of Internal Affairs' *Department for Combating Crimes Related to Human Trafficking* and other relevant departments/units of the Ministry of Internal

3 Through order of the State Special Communications Administration No. 168 of March 25, 2019.
4 Through order of the State Special Communications Administration No. 686 of 26.10.2020.

Affairs of Ukraine in the Autonomous Republic of Crimea, oblasts of Ukraine, Kyiv, and Sevastopol, the *Department for Combating Cybercrime and Human Trafficking* was established, directly governing the units for combating cybercrime and human trafficking of the Ukrainian Internal Affairs bodies (Order No. 581, 2010).

According to its regulation, the *Department for Combating Cybercrime and Human Trafficking* was an independent structural unit of the Central Office of the Ministry of Internal Affairs of Ukraine, authorized to carry out operational and investigative activities. The Department carried out its activities on a linear and zonal principle based on a combination of unity of command and collegiality, long-term and current planning, considering scientific recommendations and best practices, including international. Following the mentioned regulation, the Department's primary operational and service tasks were the following:

- Providing organizational and practical support in implementing State policy to prevent and combat crimes committed involving high information technology and telecommunications networks, human trafficking, illegal migration, crimes against morality, crimes in the field of employment abroad, illegal adoption, violation of the law procedure for transplantation of human organs or tissues, forcible donation, and counteraction to legalization (laundering) of proceeds from these crimes.
- Implementing organizational and practical measures to detect and stop organized groups and criminal organizations' criminal activity, primarily of a transnational nature, and individuals specializing in the commission of crimes, the detection and cessation of which falls within the competence of the Department, an organization of operative support of criminal cases of the specified category.
- Organizing subordinate units' operational and service activities to detect and stop crimes, ensuring the prosecution of organized group members or individuals committing these crimes, identifying areas of work and priorities for subordinate units, finding effective means and methods of implementing the tasks assigned to them, ensuring organizational and methodological support for their activities to detect and stop crimes of this category.
- Developing and taking measures to improve forms and methods of operational and investigative activities of subordinate units, providing them with practical assistance in organizing work to detect and stop crimes, and solving other operational and service tasks.
- Ensuring control over the activities of business entities in employment mediation abroad, tourism entities, marriage, modeling bodies, as well as information market and telecommunication services business entities and representatives of interested ministries or other central executive bodies.

- Establishing confidential cooperation according to the legislation of Ukraine voluntarily with individuals able to cover the illegal activities of organized criminal groups and persons involved in the commission of crimes.
- Considering and disseminating positive experiences on recommendations of foreign law enforcement bodies on the detection, documentation, and investigation of such crimes in the fight against crime, together with higher education institutions of the Ministry of Internal Affairs and the Prosecutor General's Office.
- Organizing interaction with the Ukrainian Parliament Commissioner for Human Rights, other-state, non-state institutions, and international organizations engaged in combating cybercrime and human trafficking. Participating in international, interregional meetings, conferences, and seminars on problematic issues related to these types of crimes. (Order No. 494, 2012).

As shown, the Department's area of work was quite excessive, which is not surprising, given its name, which combined the fight against cybercrime and human trafficking. Moreover, these areas were poorly interconnected, barring the fact that the crimes related to "trafficking in human beings" could use some computer technology, for example, placing ads on the Internet to buy/sell human organs or advertise intimate services. Evidently, the same technology could be used to commit other crimes. Therefore, it is not surprising that two years later, the *Department for Combating Cybercrime of the Ministry of Internal Affairs of Ukraine* and units for combating cybercrime in the Main Department of the Ministry of Internal Affairs and regional departments in the Ministry of Internal Affairs were established.

The Department for *Combating Cybercrime of the Ministry of Internal Affairs of Ukraine* (UBK in Ukrainian) was an independent structural unit within the criminal police of the Ministry of Internal Affairs, which, according to the legislation of Ukraine, ensured the implementation of State policy and operational and investigative activities. According to the Ministry of Internal Affairs of Ukraine's Order No. 988 of 30/10/2012, "On the Organization of the Department for Combating Cybercrime and units for combating cybercrime of the Main Department and regional departments of the Ministry of Internal Affairs" (Order No. 988, 2012), the UBK's main tasks were to participate in the creation and implementation of State policy to prevent and combat the following:

- Criminal offenses using computing machinery (computers), computer systems and networks, and telecommunication networks;
- The mechanisms of preparation, commission, or concealment of criminal offenses involving the use of computing machinery (computers), computer systems and networks, and telecommunication networks. These activities in-

clude payment systems and the circulation of illegal information through these means, as well as economic aspects like financial and trade transactions carried out through telecommunication networks or computer networks and countering prohibited economic activities in this area (e-commerce), the provision of telecommunication services, and fraud and money laundering of proceeds from the above criminal offenses.

- As stipulated by applicable law, assist other units of the Ministry of Internal Affairs in the prevention, detection, and termination of criminal offenses and pre-trial investigations.

Cybersecurity-ensuring bodies' competence delimitation

During the reform of the internal affairs bodies in 2015, the *Cyber Police Department* was established within the National Police of Ukraine. According to the regulation approved by the Ministry of Internal Affairs through Order No.85 of 10/11/2015, this Department is an interregional territorial body of the Ukraine National Police, which is part of its criminal police. According to the legislation of Ukraine, it is responsible for ensuring the implementation of State policy in combating cybercrime and organizes and carries out operational and investigative activities.

This regulation also defines the *Cyber Police Department's* main tasks. They include participating in creating and implementing State policy to prevent and combat criminal offenses and the mechanism of preparation, commission, or concealment involving the use of computing machinery (computers), systems, computer networks, and telecommunication networks. It also assists other units of the National Police in preventing, detecting, and stopping criminal offenses as stipulated by applicable law. The cyber police's tasks include:

- The employment of the State policy in combating cybercrime;
- Providing the public with early warning on new, emerging cybercriminals;
- Introducing software to systematize cyber incidents;
- Responding to foreign partners' requests, coming through the channels of the 24/7 Network of National Contact Points (Cyber Police of Ukraine, 2020).

According to the ex-Minister of Internal Affairs Avakov (2015), the purpose of the cyber police is to restructure and develop units of the Ukraine Ministry of Internal Affairs. Moreover, it is responsible for the training and operation of highly qualified specialists in expert, operational and investigative police units involved in combating cybercrime, able to apply the latest technologies at a high professional level in operational and service activities. In addition, it must ensure the gradual transformation of the current model into

an innovative human rights body, which will respond instantly to cybercrimes and cyber threats and, following best world standards, will carry out international cooperation to neutralize transnational criminal groups. Avakov (2015) explained the cyber police's seven main tasks:

1. Implementing State policy against cybercrime.
2. Countering cybercrime in the following contexts:

   Payment systems:

   - Skimming - illegal copying of the contents of the magnetic stripe tracks (chips) of bank cards;
   - Cash trapping - ATM theft of cash by installing a special retaining pad on the ATM tent;
   - Carding - illegal financial transactions using a payment card or its details, which are neither initiated nor confirmed by its holder;
   - Unauthorized debiting of funds (payment) from bank accounts using remote banking systems.

   E-commerce and business:

   - Phishing - extortion of logins and passwords to e-wallets, online auction services, money transfers, or exchanges from Internet users;
   - Online fraud - the seizure of citizens' funds through online auctions, online stores, websites, and telecommunications;

   Intellectual property:

   - Piracy - illegal distribution of intellectual property on the Internet;
   - Card sharing - providing illegal access to satellite and cable TV;

   Information security:

   - Social engineering - a technology of the management of people in the Internet space;
   - Malware - the creation and spread of viruses and malicious software;
   - Illegal content - content that promotes extremism, terrorism, drug addiction, pornography, the cult of cruelty, and violence;
   - Refilling - illegal substitution of telephone traffic.
3. Providing early warning to the public on the emergence of the latest cybercrime.
4. Introducing software to systematize and analyze information on cyber incidents, cyber threats, and cybercrimes.
5. Responding to requests from foreign partners received through the channels of the 24/7 Network of National Contact Points.

6. Training police officers in the use of computer technology for combating crime.
7. Participating in international operations and cooperation in real-time and ensuring the functioning of the network of contact points between 90 countries.

Cyber police personnel consists of re-certified employees of the Ministry of Internal Affairs' anti-cybercrime units, selecting only those meeting cyber police officer requirements. In addition, nationwide cyber police recruitment was held to select the best cybersecurity specialists on a competitive basis (Bezzubov et al., 2017; Vystavna et al., 2018). In 2012, the *Department of Counterintelligence Protection of the State's Interests in the Sphere of Information Security of the Security Service* (DKIB SBU in Ukrainian) was established within the Ukraine Security Service (Presidential Decree No. 34, 2012). The DKIB SBU is an operational unit of the Ukraine Security Service, the scope of which includes ensuring the State's information security. The Security Service's *Counterintelligence Protection of the State's Interests in Information Security Department* is responsible for the State's security in the information and cyber spheres. It coordinates and controls the activities of regional bodies and central departments units of the Security Service. Within the limits of its competence, it submits proposals on the issuance of acts binding on public administration bodies, enterprises, institutions, organizations, and citizens to the President of Ukraine (Bilous, 2019).

The Department was established and developed with the assistance of the NATO-Ukraine Cybersecurity Trust Funds; especially favored by the fund was the Cyber Security Situation Centre. The hardware and software for the Centre's functioning were received in July 2017 as part of the first stage of implementing of the NATO-Ukraine Trust Fund on Cyber Defense Agreement. The Centre's grand opening took place with the participation of the Head of the Security Service of Ukraine, V. Hrytsak, on January 25, 2018 (Press center of the Security Service of Ukraine, 2018). The main tasks of the Cyber Security Situation Centre are as follows:

- Preventing, detecting, stopping, and disclosing crimes against the peace and security of humankind committed in cyberspace;
- Carrying out counterintelligence and operative search measures aimed at combating cyberterrorism and cyber espionage;
- Carrying out confidential reviews of the preparation level of critical infrastructure facilities for possible cyberattacks and cyber incidents;
- Combating cybercrime, the consequences of which may threaten the vital interests of the State;
- Investigating cyber incidents and cyberattacks on State electronic information resources, critical information, and infrastructure;

- Ensuring the response to cyber incidents concerning State security (Novikovas et al., 2017).

From 2017 to 2018, the Centre's specialists recorded and averted more than 50 cyberattacks of varying degrees of sophistication, some of which could have been much worse than the notorious "Petya-A" (Klimchuk, 2018). There is a plan to introduce similar units in regional security bodies in addition to the central Cyber Security Situation Centre. The first regional Cyber Security Situation Centre was established in Dnipro in November 2018. Six months later, with the participation of the Deputy Head of the Security Service of Ukraine, Oleg Frolov, a regional cybersecurity center was opened in Odesa.

International cyberlearning took place on different cybersecurity subjects in preparation for the 2019 parliamentary elections in Kyiv. The training was organized within the framework of the EU "Strengthening Cyber Security in Ukraine before the Elections" project, supported by the Estonian Center of Eastern Partnership (ECEAP) in cooperation with CybExer Technologies. The purpose was to collect the latest European experience in securing electoral processes and information in cyberspace. The cyberlearning sessions were attended by both European cybersecurity experts and Ukraine representatives, including specialists of the Security Service of Ukraine, the State Service for Special Communication and Information Protection, the cyber police, and the Central Election Commission of Ukraine. The training's virtual infrastructure enhanced the experience of counteracting hackers in conditions as close as possible to real situations (Krupskyi et al., 2019).

Among the Security Service's *Counterintelligence Protection of the State's Interests in the Sphere of Information Security Department's* achievements is the discontinuation of a powerful hacker group in July 2019, conducted jointly with US partners. The criminal hacker group based in Ukraine provided virtual services to other computer criminals, effectively creating the conditions for them to carry out illegal activities on the Internet without hindrance. The Ukraine citizen, the group's organizer, acquired his first hacking experience in Moscow in the mid-2000s. In 2007, the group provided services to hackers from other countries via Ukrainian networks. A large data center located on the private territory near Odesa was discovered during operational activities and further investigative actions. According to the acting Head of the Ukraine State Security Service, M. Kuleshov, almost one and a half hundred servers with thousands of hacker resources were confiscated. Some of them remained encrypted, configured so as not to keep traces of criminal activity (Press center of the Security Service of Ukraine, 2019).

The most recent of Ukraine's cybersecurity bodies is the *National Coordination Center for Cybersecurity of the National Security and Defense Council*, established in 2016. In the same year, the *National Coordination Centre for Cybersecurity* regulation was approved (Decree No. 96/2016, 2016). According to this regulation, this Centre is a work-

ing body of the Ukraine National Security and Defense Council, with a wide range of tasks, including:

1. Analyzing:
   - The state of cybersecurity;
   - The results of the review of the national cybersecurity system;
   - The cybersecurity-ensuring individual's level of preparation to perform tasks on combating cyber threats and implementation of measures to prevent and combat cybercrime;
   - The state of financial and organizational support of programs and measures for implementing State policy in cybersecurity in Ukraine;
   - The fulfillment of the legislation requirements on the cyber protection of State electronic information resources, information, and critical information infrastructure, as well as the requirements for protection established by law;
   - Data on cyber incidents related to State information resources in information and telecommunication systems;
   - Staffing of the national cybersecurity system to propose improvements;
2. Participating in the development of sectoral cybersecurity indicators;
3. Forecasting and identifying potential and real threats in cybersecurity in Ukraine;
4. Developing conceptual principles and proposals for State cybersecurity to improve the effectiveness of measures to identify and eliminate factors posing potential and actual threats in cybersecurity, preparation of draft programs, and plans to prevent and neutralize them;
5. Generalizing international experience in cybersecurity;
6. Ensuring the development and implementation of information exchange mechanisms required for cybersecurity-ensuring organizations to respond to cyberattacks and cyber incidents and eliminate their factors and negative consequences;
7. Providing the operational, information, and analytical support of the National Security and Defense Council on cybersecurity;
8. Developing and submitting proposals to the National Security and Defense Council on:
   a. Determining Ukraine's national interests in cybersecurity, priority areas, conceptual approaches to the formation and implementation of State policy concerning safe cyberspace and its use in the interests of an individual, society, and the State;
   b. Implementing systemic measures to strengthen the security and defense capabilities of sector entities in the fight against military cyber threats, cyber espionage, cyberterrorism, cybercrime, and ensuring cyber protection of State

electronic information resources, the protection required by law, and critical information infrastructure;

c. Implementing measures to ensure cyber protection of critical infrastructure and the protection of technological processes in production in the real sector of the economy;

d. Improving the cybersecurity regulatory framework in Ukraine, in particular the legal regulation of the areas of responsibility of the security and defense sector, ensuring Ukraine's cybersecurity and the interaction mechanisms between them;

e. Ensuring the development of State information infrastructure;

f. Coordinating activities of the entities in the security and defense sector that ensure cybersecurity in Ukraine;

g. Assessing the mutually agreed deployment of the Ukraine Armed Forces' cybersecurity units, other military formations, and special purpose law enforcement bodies formed under the laws of Ukraine, ensuring their preparedness to perform tasks under martial law in states of emergency or crises that threaten Ukraine's national security;

h. Overseeing the actions by national security subjects to improve cooperation with international organizations in cybersecurity and ensure the protection of Ukraine's national interests at the international level;

i. Setting priorities for attracting international technical assistance in cybersecurity;

j. Implementing State support measures for scientific institutions and organizations of strategic importance to the State's cyber defense, conducting scientific research involving cybersecurity and cyber defense for the needs of national security and defense;

k. Increasing the effectiveness of the implementation of military and technical policy and cooperation in cyber defense;

l. Strengthening the State's cyber defense capabilities, transfer of the national communication system, strategic national automated control systems, government networks, communication and weapons control systems, information and telecommunication networks, and systems of military administration to operate in a special period, mobilization of additional resources for organizing operations in cyberspace;

m. Improving the creation of domestic software products to protect the State's information resources, including the national operating system and national antivirus software.;

9. Monitoring the development and implementation of national standards and technical regulations for information use and communication technologies, harmonized with EU and NATO standards;
10. Defining ways, mechanisms, and means of solving problems that arise during the State's cybersecurity policy implementation;
11. Ensuring control over the status of decisions of Ukraine's National Security and Defense Council on State cybersecurity issues, enacted by Presidential decrees;
12. Studying international experience concerning the creation and operation of national cybersecurity systems, their dissemination among organizations and institutions, and monitoring their implementation in Ukraine;
13. Participating in the organization and conduction of interethnic and interagency cyberlearning training and the development of relevant methodological documents and recommendations (Presidential Decree No. 242, 2016).

The investigation of cybercrimes is entrusted to the investigative units of the National Police (Law of Ukraine No. 4651-VI, 2012), and forensic support for the investigation is provided by units of computer and telecommunication examinations of forensic institutions in Ukraine.

Problematic issues in combating cyber threats in Ukraine

It should be noted that the concept of "cybercrime" is not laid down in Ukraine's Criminal Code; however, it appears in other regulations, in particular, in the Law of Ukraine "On the Basic Principles of Cyber Security of Ukraine" (Law of Ukraine No. 2341-III, 2001). These crimes are combined in Section XVI: "Criminal offenses in the use of computers, systems, and computer networks, and telecommunication networks" in the Criminal Procedure Code of Ukraine. These crimes include the following:

- Article 361. Unauthorized interference in the work of computing machinery (computers), automated systems, computer networks, and telecommunication networks.
- Article 361-1. Creation for the use, distribution, or sale of malicious software or hardware.
- Article 361-2. Unsanctioned sale or distribution of information with limited access stored in computers, automated systems, computer networks or on data storage devices.
- Article 362. Unauthorized actions on the information processed on computing machinery (computers), automated systems, computer networks, or on the data storage devices by individuals with the right to access it.

- Article 363. Violation of operation rules of computing machinery (computers), automated systems, computer networks, or telecommunication networks or the order and rules of the information protection processed in them.
- Article 363-1. Obstructing the function of computers, automated systems, computer networks, or telecommunication networks through the mass dissemination of telecommunication messages.

As can be seen from the above articles of the Criminal Code, one of the Ukrainian legislation's problems is the lack of a clear definition of "cyberterrorism." Given the danger to the public posed by obstructing the State's critical information systems infrastructure, many scholars consider it necessary to legislate criminal liability for a new type of particularly dangerous crime –cyberterrorism. Instead, Art. 258 of the Criminal Code addresses responsibility for "classic" terrorism; therefore, the position on the introduction of a new *corpus delicti* is ambiguous.

Several arguments favor a separate crime because the means of committing "ordinary" terrorism and cyberterrorism can differ, and the instruments of these crimes and their preparation are miscellaneous (Britchenko et al., 2018). All this leads to several tactics of investigation, different types of examinations that need to be appointed, and different specializations of law enforcement officers (investigators, operatives, specialists, experts), among others. Thus, the idea of separating cyberterrorism as an individual crime is well-founded and validated.

In June 2015, the Parliamentary Assembly of the Council of Europe adopted Resolution 2070 (2015) on "Increasing cooperation against cyberterrorism and other large-scale attacks on the Internet." It calls on the Council of Europe member states to define cyberterrorism and establish accountability for its activities. Thus, several bills on amendments to the Criminal Code of Ukraine were prepared following this resolution (UNIAN, 2015).

The draft "On Amendments to the Criminal Code of Ukraine (on enhancing liability for cyberterrorism and cybercrimes)" No. 2328a of July 10, 2015, initiated by Myrnyy (2015), provides for part two of Art. 258 of the Criminal Code. It states:

> 2. The same actions committed repeatedly, or for a previous conviction by a group of persons or if they are connected with unauthorized intrusion into the work of electronic processing machines (computers), violating the law on automated systems, computer networks, or high-risk electric circuits or if they have caused significant property damage or other severe consequences –shall be punishable by imprisonment for a term of seven to twelve years with or without confiscation of property. (p.1; author translation)

Meanwhile, Article 361 was proposed, supplemented with new parts (three and four) stating the following:

> 3. Actions provided for in parts one or two of this article, if they involve unauthorized interference with the operation of electronic processing machines (computers), any act or omission in the operation of automated systems, computer networks, or electronic communications of high-risk telecommunication networks, which caused significant property damage or other serious consequences –shall be punishable by imprisonment for a term of seven to twelve years with or without confiscation of property.
>
> 4. The acts provided for in parts one, two, or three of this article, which caused the death of a person –shall be punishable by imprisonment for a term of ten to fifteen years or life imprisonment with or without confiscation of property. (pp. 1,2; author translation)

The bill of Ukraine "On Amendments to the Criminal Code of Ukraine on Establishing Liability for Cyberterrorism"[5] (Aryev, 2015) proposes introducing a new article in the Criminal Code of Ukraine, namely Article 258-6, Cyberterrorism.

> 1. Cyberterrorism, that is, the intentional attack on information processed by a computer, computer system, or computer network that endangers human life and health or leads to other serious consequences if such actions have been committed out of political motives, for violating public safety, intimidating the population, provoking a military conflict –shall be punishable by imprisonment for a term of five to ten years with or without confiscation of property.
>
> 2. The same acts performed repeatedly or by a group of persons by prior conspiracy shall be punishable by imprisonment for a term of seven to twelve years with or without confiscation of property.
>
> 3. The commitment of an act of cyberterrorism that has resulted in injury, trauma or death shall be punishable by imprisonment for a term of ten to fifteen years, or life imprisonment, with or without confiscation of property.
>
> 4. A person or group of persons who participated in the preparation of an act of cyberterrorism, but who voluntarily warned the law enforcement agency and if their actions led to the prevention of an act of terrorism, shall be released from criminal liability if their actions do not constitute another crime (pp. 3-5; author translation).

To date, the amendments to the Criminal Code of Ukraine have not been adopted. However, the criminalization of cyberterrorism through the amendment to the Criminal Code is extremely important. It will provide legislative protection to automated information and telecommunication systems. Moreover, it will protect State electronic registers and databases and critical national information infrastructure.

As Nizovtsev (2017) notes, both bills show shortcomings. According to Draft Law No. 2328a, there are amendments to the second part of Art. 258 of the Criminal Code, and parts three and four are added to Art. 361 of the same Code. At the same time, the adoption of the specified bill could produce a conflict between part two of Art. 258 and

5 No. 2439a of July 24, 2015.

part three of Art. 361 of the Criminal Code. Similarly, there could be a conflict between the proposed Bill No. 2439a's articles 258-6 and 361. According to the scientist, the optimal option is the introduction of parts three and four to Art. 361 of the Criminal Code, as provided by Bill No. 2328a. Furthermore, the concept of "cyberterrorism" should be enshrined in a separate regulation, for example, in Ukraine's Cybersecurity Strategy. It should be noted that Nizovtsev's (2017) proposal has, in fact, been partially implemented; the term "cyberterrorism" has been enshrined in a separate legislative act, namely, the Law of Ukraine "On Basic Principles of Ensuring Cyber Security of Ukraine." It provides the following definition: "Cyberterrorism is a terrorist activity carried out in cyberspace or with its use" (Gnatenko et al., 2020). Nevertheless, the allocation of cyberterrorism as a separate crime has not yet occurred.

These are not the only issues in countering cyber threats in Ukraine. As noted by Peresada and Hobby (2020), several factors hamper the effective functioning of the above services. The first one is the problem of coordinating law enforcement bodies and legal regulations concerning the bodies' areas of responsibility to avoid duplicating powers, procedures, and means of a comprehensive response to cybersecurity threats. Secondly, the prevention of these crimes is not sufficiently effective. The third one involves technical equipment. Orlov and Onishchenko (2014) note that the high level of cybercrime is due to several reasons. However, law enforcement bodies' are limited due to the lack of special technical equipment such as modern computer equipment and computer technology, knowledge and skills to detect and investigate cybercrime, tactics, and techniques, given the limited access to these modern methods, and overall deficient information culture.

Furthermore, they are faced with limited training covering a wide range of law enforcement bodies and judges to bring the perpetrators to justice and the victims' distrust of law enforcement bodies. Lastly, national legislation focuses mainly on cybersecurity and cyber defense concerning the State and public systems, including telecommunications, leaving technical and public information resources insufficiently protected and not in line with current trends in the fight against cybercrime. This effort requires the further expansion of law enforcement areas to include private computer networks and individual personal computers. There are no small or insignificant casualties in cyberwarfare; personal computer devices and networks can serve as a training ground to prepare for large-scale cyberattacks on government structures and livelihoods.

The issue of coordination and division of areas of responsibility is urgent. For example, when a cybercrime activity is detected, the *Department of Counterintelligence Protection of the State's Interests in the Sphere of Information Security* officers must provide the National Police investigators materials to further the operative support of the investigation. However, the National Police's structure has its own units with very similar functions – the cyber police.

Another significant problem is the insufficient number of highly qualified personnel; this applies to the cyber police staffing and the *Department of Counterintelligence Protection of the State's Interests in the Sphere of Information Security* (Shopina et al., 2020). In-depth knowledge is vital when investigating crimes involving the latest cyber technologies and should not be limited to merely specialized operatives and forensic experts. Modern information technology must also be understood by the investigator, prosecutor, and judge for an investigation to be effective. After all, without understanding the nuances of computer technology and their attackers' "hacking," the investigation can only be protracted for a long time or closed without bringing the perpetrators to justice.

Given the above, we propose creating specialized investigative units to investigate cybercrimes and the relevant units in the prosecutor's office. The specialization of judges would also be relevant. At the same time, the described vertical of specialized bodies do not require the same degree of independence as, for instance, the anti-corruption vertical (meaning the National Anti-Corruption Bureau, the Specialized Anti-Corruption Prosecutor's Office, and the High Anti-Corruption Court).

Another significant problem in ensuring cybersecurity in Ukraine is the lack of scientific research in this area (Ilchenko et al., 2021). On the state of implementation of the Cybersecurity Strategy, approved by Presidential Decree No. 96 (2016), the National Security and Defense Council's decision of May 14, 2021, concluded that certain indicators do not surpass 40 percent. Insufficient scientific support is considered one of the main reasons for this outcome. Mainly subjects of the security and defense sector took part in this strategy's implementation; other state bodies, scientific institutions, and the public were all but excluded. Thus, educational and scientific institutions were underrepresented in implementing tasks related to developing scientific potential and the spread of cyber literacy (Presidential Decree No. 447, 2021).

During the international scientific and practical conference "Countering Cyber Threats in the Modern Security Environment: Current Issues in Theory and Practice," organized by the Ukrainian Scientific and Research Institute of Special Equipment and the Security Service Forensic Expertise of the National Security and Defense Council, it was noted that research in cybersecurity in Ukraine has been of unsystematic and episodic nature in recent years. A significant number of scientific papers were limited to proclaiming the importance of cybersecurity without specific weighty proposals of engineering, technical, organizational, or other nature. Therefore, a joint effort was proposed between the Ukrainian Scientific and Research Institute of Special Equipment and the Forensic Expertise of the Security Service to introduce a platform for the continuous exchange of experience and achievements in cybersecurity (UTRPI, 2021).

Conclusion

An entire system of specialized bodies for cybersecurity has been created in Ukraine. In addition, non-specialized bodies are also involved; "ordinary" investigators carry out the investigation of cybercrime under the procedural supervision of the prosecutor's office. At the same time, there are several problems in ensuring cybersecurity in Ukraine. These are the lack of highly qualified personnel, the lack of cyber specialization of investigators and prosecutors, the inconsistencies of legislation with modern realities, the difficulty in organizing the interaction of the related entities mentioned, and the lack of research and development. As a way to solve these problems, we have proposed to create specialized investigative units and relevant units of the prosecutor's office to investigate cybercrimes and introduce the appropriate specialization of judges. Furthermore, to coordinate scientific developments, we proposed creating a platform for ongoing exchange of experience and achievements in cybersecurity –a cybersecurity research center– based on the Ukrainian Research Institute of Special Equipment and the Forensic Expertise of the Security Service of Ukraine.

Disclaimer

The author declares no potential conflict of interest related to the article.

Funding

The author does not report sources of funding for this article.

About the authors

Andrii V. Svintsytskyi is a Ph.D. in Law, Director of the Ukrainian Scientific and Research Institute of Special Equipment and Forensic Expertise of the Security Service of Ukraine, and Associate Professor at the Department of Criminal Law and Criminology of the University of the State Fiscal Service of Ukraine. Honored Lawyer of Ukraine.

https://orcid.org/0000-0002-9801-0535 - Contact: svintsytskyi19@neu.com.de

References

Aryev, V.I. (2015). *On Amendments to the Criminal Code of Ukraine on Establishing Liability for Cyberterrorism*. Bill No. 2439a (July 24, 2015). Verkhovna Rada of Ukraine. http://w1.c1.rada.gov.ua/pls/zweb2/webproc4_1?id=&pf3511=56183

Avakov, A. (2015). Cyberpolice (reforms). *Ukrainian Truth in social media.* https://blogs.pravda.com.ua/authors/avakov/561a92c183c27/

Bezzubov, D., Ihonin, R., & Diorditsa, I. (2017). Cyberthreats as a component of threats in the contemporary world (a legal aspect). *Journal of Advanced Research in Law and Economics, 8*(7), 2086-2093. https://doi.org/10.14505/jarle.v8.7(29).04

Bilous, I.A. (2019). *Socio-Legal Support of Information Security of Ukraine* [Abstracts by Kharkiv, December 2019, pp. 120-124]. Scientific seminar on information aggression of the Russian Federation against Ukraine. Kharkiv National University of the Air Force named after Ivan Kozhedub.

Boyarchuk, R., Khudyntsev, M., Lebid, O., & Trofymchuk, O. (2021). *Organizational and technical model of national cybersecurity and cyber protection*. CEUR Workshop Proceedings. http://ceur-ws.org/Vol-2923/paper5.pdf

Britchenko, I., Monte, A. P., Kryvovyazyuk, I., & Kryvoviaziuk, L. (2018). The comparison of efficiency and performance of Portuguese and Ukrainian enterprises. *Ikonomicheski Izsledvania, 27*(1), 87-108.

Cyberpolice of Ukraine. (2020). *About the unit*. https://cyberpolice.gov.ua/contacts/

Gnatenko, K. V., Yaroshenko, O. M., Inshyn, M. I., Vapnyarchuk, N. M., & Sereda, O. H. (2020). Targeted and effective use of state and non-state social funds. *International Journal of Criminology and Sociology, 9*, 2861-2869. https://doi.org/10.6000/1929-4409.2020.09.350

Ilchenko, M., Uryvsky, L., & Osypchuk, S. (2021). The main directions of improving information and communication technologies in the global trends. In Ilchenko, M., Uryvsky, L., Globa, L. (Eds.) *Advances in Information and Communication Technology and Systems*. [Lecture Notes in Networks and Systems, vol 152]. Springer. https://doi.org/10.1007/978-3-030-58359-0_1

Klimchuk, A. (2018). *Information and Cyber Security in the Modern World: Experience of the SSU*. Liga.net. https://www.liga.net/politics/opinion/informatsionnaya-i-kiberbezopasnost-v-sovremennom-mire-opyt-sbu

Krupskyi, O. P., Dzhusov, O., Meshko, N., Britchenko, I., & Prytykin, A. (2019). Key sources when formulating competitive advantages for hotel chains. *Tourism, 67*(1), 34-46.

Law of Ukraine No. 2163-VIII. (2006). *On the State Service for Special Communications and Information Protection of Ukraine*. Verkhovna Rada of Ukraine. https://zakon.rada.gov.ua/laws/show/2163-19#Text

Law of Ukraine No. 2163-VIII. (2017). *On the Basic Principles of Cyber Security of Ukraine*, Verkhovna Rada of Ukraine. https://zakon.rada.gov.ua/laws/show/2163-19#Text

Law of Ukraine No. 2341-III. (2001). *Criminal Code of Ukraine*. Verkhovna Rada of Ukraine. https://zakon.rada.gov.ua/laws/show/2341-14#Text

Law of Ukraine No. 4651-VI. (2012). *Criminal Procedure Code of Ukraine*. Verkhovna Rada of Ukraine. https://zakon.rada.gov.ua/laws/show/4651-17#Text

Myrnyy, I.I. (2015). *On Amendments to the Criminal Code of Ukraine (on enhancing liability for cyberterrorism and cybercrimes)*. Bill No. 2328a (July 10, 2015). Verkhovna Rada of Ukraine. http://w1.c1.rada.gov.ua/pls/zweb2/webproc4_1?id=&pf3511=55972

Nizovtsev, Yu.Yu. (2017). Regarding Legal Regulation in the Field of Counteraction to Unauthorized Interference in the Work of Information and Telecommunication Systems. *Forensic Bulletin*, 1(27), 54-62. http://elar.naiau.kiev.ua/bitstream/123456789/16433/1/Visnik_1-27-2017-54-62.pdf

Novikovas, A., Novikoviene, L., Shapoval, R., & Solntseva, K. (2017). The peculiarities of motivation and organization of civil defence service in Lithuania and Ukraine. *Journal of Security and Sustainability Issues, 7*(2), 369-380.

Order No. 494. (2012). *About the organization of activity of Management of fight against cybercrime of the Ministry of Internal Affairs of Ukraine and divisions of fight against cybercrime GUMVD, UMVD*. Ministry of Internal Affairs of Ukraine. https://ips.ligazakon.net/document/view/mvs308?an=1&ed=2012_05_31

Order No. 581. (2010). *About the organization of activity of Department of fight against cybercrime and human trafficking of the Ministry of Internal Affairs of Ukraine and divisions of fight against cybercrime and human trafficking GUMVD, UMVD*. Ministry of Internal Affairs of Ukraine. https://zakon.rada.gov.ua/rada/show/v0581320-10#Text

Order No. 988. (2012). *About the organization of activity of Management of fight against cybercrime of the Ministry of Internal Affairs of Ukraine and divisions of fight against cybercrime GUMVD, UMVD*. Ministry of Internal Affairs of Ukraine. https://ips.ligazakon.net/document/view/mvs308?an=1&ed=2012_05_31

Orlov, O.V., & Onishchenko, Yu.M. (2014). Organizational and Normative-Legal Bases of Fight Against Cybercrime. *Public Administration: Improvement and Development*, *4*. http://www.dy.nayka.com.ua/?op=1&z=715

Peresada, O.M., & Hobby, Y.S. (2020). Legal and Organizational Problems of Combating and Combating Cybercrime. *Modern Problems of Legal, Economic, and Social Development of the State* [Thesis Add. International. Scientific-Practical Conf. (November 2020, pp. 152-153)]. Kharkiv: Ministry of Internal Affairs of Ukraine, Kharki National University of Internal Affairs.

Presidential Decree No. 242. (June 7, 2016). *On the National Cyber Security Coordination Center*. President of Ukraine Official website. https://www.president.gov.ua/documents/2422016-20141

Presidential Decree No. 34 (September 25, 2012). *On Amendments to the Decree of the President of Ukraine of March 27, 2005 No.1860.* President of Ukraine Official website. https://www.president.gov.ua/documents/342012-13995

Presidential Decree No. 447. (June 14, 2021). *Decree of the National Security and Defense Council of Ukraine of June 14, 2021 "On the Cyber Security Strategy of Ukraine."* President of Ukraine Official website. https://www.president.gov.ua/documents/4472021-40013

Presidential Decree No. 96. (February 15, 2016). *On the decision of the National Security and Defense Council of Ukraine of January 27, 2016 on the Cyber Security Strategy of Ukraine*. President of Ukraine Official website. https://www.president.gov.ua/documents/962016-19836

Press center of the Security Service of Ukraine. (2018). *The head of the Security Service of Ukraine opened the Situational Center for Cyber Security*. https://sbu.gov.ua/ua/news/1/category/2/view/4318#.OD1o8ogT.dpbs/

Press center of the Security Service of Ukraine. (2019). *SBU jointly with foreign colleagues blocks activity of powerful hacker group* [video]. https://sbu.gov.ua/en/news/1/category/21/view/6281#.iPzWFbSO.dpbs

Resolution 2070. (June 26, 2015). *Increasing co-operation against cyberterrorism and other large-scale attacks on the Internet*. Parliamentary Assembly. http://assembly.coe.int/nw/xml/XRef/Xref-XML2HTML-en.asp?fileid=21975&lang=en

Shopina, I., Khomiakov, D., Khrystynchenko, N., Zhukov, S., & Shpenov, D. (2020). Cybersecurity: Legal and organizational support in leading countries, NATO and EU standards. *Journal of Security and Sustainability Issues, 9*(3), 977-992. https://doi.org/10.9770/jssi.2020.9.3(22)

UNIAN. (2015). The Council proposes to establish criminal liability for cyberterrorism. http://www.unian.ua/politics/1106141-u-radi-proponuyut-vstanoviti-kriminalnu-vidpovidalnist-za-kiberterorizm.html

UTRPI. (2021). *International scientific and practical conference "Countering cyber threats in the modern security environment: current topics of theory and practice."* June 1 to 31. Ukraine. https://utrpi.org.ua/mizhnarodnoyu-naukovo-praktychnoyu-konferentsiyeyu-protydiya-kiberzagrozam-u-suchasnomu-bezpekovomu-seredovyshhi-aktualni-pytannya-teoriyi-ta-praktyky-zavershyvsya-misyats-kiberbezpekyyakyj-z-1-po-31/

Vystavna, Y., Cherkashyna, M., & van der Valk, M. R. (2018). Water laws of Georgia, Moldova and Ukraine: Current problems and integration with EU legislation. *Water International, 43*(3), 424-435. https://doi.org/10.1080/02508060.2018.1447897

Esta página queda intencionalmente en blanco

Revista Científica General José María Córdova
(Colombian Journal of Military and Strategic Studies)
Bogotá D.C., Colombia

Volume 20, Number 38, April-June 2022, pp. 307-321
https://dx.doi.org/10.21830/19006586.897

International experience in conflict resolution: US-China conflict of interests

La experiencia internacional en la resolución de conflictos: el conflicto de intereses entre Estados Unidos y China

Nina F. Rzhevska and Nataliia P. Borotkanych
National Aviation University, Ukraine

Abstract. This article aims to characterize international political conflicts that have lasted for millennia on a civilizational, social, or geopolitical basis, which are insufficiently studied and analyzed despite their duration. This study aims to find an effective way to resolve a conflict of interests using the example of the US-China conflict. The authors determine that researchers of this issue must engage both the methodological and their political position, presenting a personal view. This study states the importance of understanding how best to avoid and, at some stage, try to prevent the spread of conflict.

Keywords: China; conflict management; international conflict; international organizations; national interest; United States

Resumen. Este artículo pretende caracterizar los conflictos políticos internacionales que se han prolongado durante milenios sobre una base civilizacional, social o geopolítica, que son insuficientemente estudiados y analizados a pesar de su duración. Este estudio pretende encontrar una forma eficaz de resolver un conflicto de intereses utilizando el ejemplo del conflicto entre Estados Unidos y China. Los autores determinan que los investigadores de esta cuestión deben emplear tanto lo metodológico como su posición política, presentando una visión personal. Este estudio afirma la importancia de comprender la mejor manera de evitar y, en algún momento, tratar de prevenir la propagación del conflicto.

Palabras clave: China; conflicto internacional; Estados Unidos; gestión de conflictos; interés nacional; organizaciones internacionales

Section: Dossier • Scientific and technological research article
Received: November 29, 2021 • Accepted: February 18, 2022

Contact: Nina F. Rzhevska ✉ rzhevska8125@edu.cn.ua

Introduction

All state actors of the modern international community make maximum efforts to prevent and predict all the possible causes of international conflicts. New alliances are formed to combat existing threats, and specific reforms are made. International and regional organizations, together with states, are joining forces to combat the spread of these deadly disputes (United Nations, 2021). However, more developed countries cope better and more efficiently.

Nevertheless, differences in mandates, relevant areas of activity, bureaucracy, national interests, and conflicting views on conflict prevention limit effective multilateral action and prevent the parties from joining forces to achieve a common positive outcome. The main reason for failures is, firstly, that each state conducts unilateral activity and pursues only its national interests. It is worth noting that the only common feature of conflict management policies in developing countries is the willingness to link their security policies to development and cooperation. Almost all forces, marked by positive dynamics, seek to play an active role in developing cooperation as an integral part of their policy to find its mission in global governance. However, these forces are not the only bloc (Syrotiuk & Oliynyk, 2021).

Their understanding of conflict management depends to a large extent on strategic culture, historical/cultural proximity to particular regions, and the interests/priorities of national security and foreign policy (Stockholm International Peace Research Institute, 2019). Even though growing forces hold to different approaches and practices to conflict resolution, they have the ability and potential to unite based on shared global interests and under the auspices of international organizations, including the United Nations (Gros, 2021). With the emergence of new security threats provoked by violent non-state actors, and the increasing number of factors that lead to controversies worldwide, the conflicts themselves are changing (Ackermann, 2003). Accordingly, large and developing countries have to manage them differently. In today's complex, unsecured environment, developing countries face several challenges, affecting both their approaches to conflict resolution and the tools they use to manage those conflicts. The current unstable security environment calls for stronger cooperation in diplomatic and military control (Leonova, 2014).

Dorussen and Clayton (2018) stated that managing international conflicts is not aligned with a single policy and can be successfully carried out without coordination between traditional and higher or middle states in the global and regional institutional environment. In the current global governance structure, international conflict management requires a new and more effective institutional framework, new concepts, and a new division of roles between traditional and non-traditional actors (Nazarovska, 2012). In this regard, developing countries can act more quickly and actively in building peace if they use UN initiatives. The initiatives are not based on peacekeeping; they apply existing

conflict management tools and create new tools and mechanisms for conflict management (Smidt, 2020; Stockholm International Peace Research Institute, 2021).

Compared to previous decades, international security issues are now being addressed in more detail and need to be addressed urgently in the short term. Therefore, it is necessary to study how recently occurred "new generation conflicts" have developed in the context of modern transformations in the international environment (Khovpun et al., 2019). A successful example of such a confrontation and attempts to resolve it is the conflict of interests between the two leading countries of the world –the United States and China. Relations between these states have remained one of the most difficult among bilateral relations in the international environment. Over the past 30 years, they have undergone dramatic transformations from hostility and conflict to open dialogue and constructive cooperation (Yuan, 2016). The two great powers have found common ground on trade, investment, and recently security. However, key political issues remain unresolved, and states continue to be on hold (European Commission, 2019).

The rivalry between the two states has become a paradigm of international relations that shapes the actual political, military, and economic development of many other leading countries, and it is likely to continue. However, there is a risk; the strategic rivalry between the United States and China can turn into a multilevel global conflict that poses economic and military threats. China is becoming an economic center, a military power in Asia, and a potential rival to the United States. The conflict between the United States and China is an example of an incredibly complex and multilevel bilateral relationship. The main reason for the long-lasting conflict between the states is that the United States sees the growing influence of China's foreign policy as a threat to America's dominance in the international system (Yuan, 2016). In addition, China is now the only country that could threaten the status of the United States, which, in turn, could shake the stability of the international system as a whole. China's growing ambitions and preferences may make the system incapable of reaching an understanding of governance and leadership, and the world may face a repeat of a world war.

Most experts view US-China relations through the prism of rivalry, given that both states are interested in strengthening their influence. Moreover, their interests and needs are very intertwined. The above may be why this conflict is the most successful example of "new generation conflicts," characterized by a partial lack of balance of power and the focus on their goals. It is worth noting that the conflict between the United States and China affects almost all spheres of activity, from political to economic. The Taiwanese scientist, Ying-Ming Lee (2011), states that the features of the relations between the two countries are fierce competition, complex cooperation, mutual restriction, and interconnectedness, indicating a completely new era in the formation of the international relations system. According to Lee (2011), the modern world is almost in a state of soft war, differ-

ent from the former hard ones. Sino-American relations cannot become confrontational, like Soviet-American relations during the Cold War. Nor can they be allied like US relations with Japan, Europe, and Britain (Kapitonenko, 2020).

There is no doubt that the settlement of any conflict, especially at the interstate level, involves a strategy. Therefore, its resolution requires, first of all, understanding the reason for its lack of resolution and further development. It is a known fact that the United States and China have constantly been trying to establish relations through peace talks. Unfortunately, new obstacles appear every year that hinder settling the conflict between the states. The issue of security acquires incredible significance in the conflict of interests between the United States and China. China seeks increasingly to ensure its security, especially to prevent offensives from the sea, where the United States remains the absolute world leader after World War II (China Office of the Historian, 2021; Central Intelligence Agency, 2020).

The United States has also accused China of exporting dangerous weapons and missile technology to countries such as Pakistan and North Korea. However, tensions have eased somewhat with China's recent announcement of a plan to limit missiles and other dual-use technologies exports. However, given the United States' plan to build a missile defense system, China's eagerness to improve its nuclear capabilities will significantly influence the beginning of difficult times for the international environment (Chunshan, 2021). The security dilemma is one of the most complicated issues in current relations between countries in terms of international relations. The essence of the dilemma is that the more one state is armed to ensure national security, the more other states feel threatened and begin to arm themselves as well. Such a situation calls into question any peace agreements and destroys trust between states.

It is worth noting that relations between states are often influenced by external sources. For example, the war on terrorism, which, unfortunately, remains one of the most crucial problems of our time, has provided Sino-US relations with a firmer footing (Johnson, 2017), somewhat increasing the potential for a successful and sustainable dialogue. Thus, common strategic concerns on terrorism have led to tangible cooperation where China has supported the US-led campaign in Afghanistan, the exchange of intelligence, and repression against Islamic separatists in western China.

However, the basis for negative development remains. A single case could shift relations in another direction, like a downed spy plane or a statement by the President of Taiwan in favor of independence. This instability remains a flaw in relations and US policy towards China in general. In this case, the settlement of the conflict largely depends on the stability or instability of the existing system of international relations and economic or social factors rather than the influence of external factors (Kniazieva et al., 2021). First of all, resolving any conflict depends on whether the states involved strive to ensure a peaceful existence for themselves and others (China Office of the Historian, 2021). The United

States will always speak out for its interests and values in relations with China, including its areas of trade, international security, and human rights. Furthermore, one should not be afraid of a strong and prosperous China; the best way to make China an enemy is to treat it as an enemy.

By 2021, China and the United States had already managed to build a relationship benefiting both countries and enhancing Asia and the world's stability. Enhanced ties and collaboration have allowed for the development of a stream of ideas, overcoming the United States' mistrust and misunderstanding of China while encouraging growth and, where possible, political change in both countries. Many Americans tend to think of US-China relations in terms of one issue like trade, Taiwan, or human rights. However, without diminishing the importance of these specific issues, American politicians should not allow any of these issues to dominate, disrupt, or disrupt any relationship.

There are so many questions ahead that will result in difficult periods and a clash of opinions. China is a large country with a growing economy, the future of which can be marked by both development and turmoil. If we pursue a policy that reflects the breadth of common interests between the two nations, we can hinder the turmoil that has plagued relations between the two nations over the past 30 years (Kurnishova, 2017).

As for the foreign intervention in the conflict between the United States and China, it is necessary to remember that Sino-US rivalry has a significant impact on the European Union and its member states. Europe's attitude toward China has become more critical. Other countries no longer see China as merely a negotiating partner for different interests or an economic competitor. The gap between Europe and China is enormous in matters of values, political system, and international order. Therefore, no matter how formidable the efforts are, overcoming such a gap is extremely difficult. Europe's relations with the United States as a strategic partner have been and will remain much closer. Furthermore, US policy is now aimed directly at attracting more and more participants who could take the American side (Coppieters et al., 2004). Thus, the strategic rivalry between the United States and China risks escalating into a multi-layered global conflict, which poses an economic and military threat. Compared to previous decades, the issue of constant interaction between states has become more critical. If economic and security interests are on an entirely new footing, the level of integration may decline to such an extent that it can turn into a kind of deglobalization (Yelchenko, 2017).

If the strategic rivalry between the United States and China is transformed into protracted global conflicts, it will lead to a kind of deglobalization. It will result in two parallel orders, one dominated by the United States and the other by China. If the conflict between the two countries continues to escalate and accelerate the bipolarization of the international system, the basis for global multilateralism may disappear. Moreover, the global conflict between the United States and China will compel Germany and the

European Union to rethink the extent to which and under what conditions they should support the United States against China. One thing is clear; the strategic rivalry with China will form the primary vector of US foreign policy.

Materials and methods

Settling most conflicts is impossible without the use of special methods to determine and understand the nature of a conflict and provide its possible recurrence in the future (Nye, 2008; Wallensteen & Möller, 2003; Yeremeeva, 2017). The Pareto principle or the 80/20 is one of the effective methods used to analyze a conflict situation; it states that 80% of the result is 20% of the effort for many phenomena. The principle is named after Vilfredo Pareto, an Italian economist who noticed in 1895 that about 80% of Italy's land belonged to 20% of the population. The initial purpose of applying this principle is to resolve the internal conflict between the population and ruling elites.

Its main characteristics are as follows. First, the results are achieved through less effort; the greatest labor costs are simultaneously a ballast and the basis for building the final result. Secondly, pre-predicted results often become irrelevant as soon as they are achieved in practice. The main task is to make the correct final choice and apply it in the actual course of the conflict, meaning that the most satisfactory result can be achieved by choosing the correct minimum of specific actions from the hundreds proposed. The Pareto principle is a method for eliminating unnecessary actions to obtain the optimal solution (Koch, 1999).

To develop this method, one should first determine the main reasons, problem, and objective. In this case, the problem was the conflict of interest between the United States and China. The main reasons were the struggle for leadership in the international environment and the formation of a "new world order." Thus, the participants in the conflict were the United States, China, and international organizations. Our objective was to find the best solution to the conflict using the Pareto principle. Table 1 summarizes the above.

Table 1. Participants in the conflict

Main Participants	Reasons	Objectives
The United States	State aims for world leadership and winning over more territories through diplomacy.	Strengthen its position globally and end the conflict.
China	Dissatisfaction with US policy and the desire to satisfy its national interests.	End of the conflict. Obtain superpower status and recognition in the international arena.
International organizations	The emergence and development of an increasing number of international conflicts. Interest in a peaceful settlement of the conflict.	Final settlement of the conflict through peace negotiations between the states, preventing its spread worldwide.

Source: Created by the authors.

Using the Pareto optimality principle, we chose the optimal solution for this problem, working out previously defined alternatives. The solution alternatives were the following:

A1- The cessation of extreme influence on states directly dependent on US foreign policy.
A2- Reforming the existing security system in the states.
A3- Ending the use of force to combat growing challenges and threats.
A4- Revision of each state's foreign policy.
A5- Introduction of new ways to combat the growing influence of foreign countries.
A6- Ensuring the continued peaceful existence of the state through reforms.
A7- Application of preventive conflict prevention methods.
A8- Increase the number of peacekeeping missions to assist states in conflict.
A9- Development of each state's latest methods of conflict prevention.

In order to evaluate the effectiveness of one or another of the above solutions, we needed certain evaluation factors - criteria. From a number of criteria, we selected five main criteria and based our research on them. We identified the following among them:

K1- Time spent searching for ways to resolve the conflict.
K2- Psychological readiness of the population and the state.
K3- The potential expended trying to prevent conflict.
K4- Economic benefits for both states.
K5- The impact of alternatives on the further development of events

Table 2 shows the solution alternatives vis-a-vis the criteria.

Table 2. Solution alternatives

	K1	K2	K3	K4	K5
A1	7	8	6	7	10
A2	9	7	9	6	8
A3	5	10	7	8	5
A4	8	9	10	6	9
A5	4	6	4	9	6
A6	6	8	8	10	10
A7	5	7	9	7	8
A8	10	9	7	9	7
A9	8	5	8	6	9

Source: Created by the authors

The following certain values were determined for the criteria:

8:(8+10+9+7+9) = 0.18
10:43=0.23
9:43=0.20
7:43=0.16
9:43=0.20

Table 3 presents the values obtained for the alternatives using the formula: An* βn

Table 3. Values of alternatives

	K1	K2	K3	K4	K5
A1	1.26	1.84	1.2	1.12	2
A2	1,62	1.61	1.8	0.96	1.6
A3	0.9	2.3	1.4	1.28	1
A4	1.44	2.07	2	0.96	1.8
A5	0.72	1.38	0.8	1.44	1.2
A6	1.08	1.84	1.6	1.6	2
A7	0.9	1.61	1.8	1.12	1.6
A8	1.8	2.07	1.4	1.44	1.4
A9	1.44	1.15	1.6	0.96	1.8

Source: Created by the authors.

Through this principle, we identified the primary and secondary alternatives. We also constructed a hierarchy of alternatives using additive and multiplicative criteria. The additive criterion was established by adding the results of the values of the alternatives obtained by the criteria:

A1= (1.26+1.84+1.2+1.12+2):65.91(sum of alternatives) = 0.112
A2= 7.59:65.91=0.115
A3= 6.88:65.91=0.104
A6=8.12:65.91=0.123
A7=7.03:65.91=0.106
A8=8.11:65.91=0.123
A9=6.95:65.91=0.105

The resulting hierarchy constructed was: A6; A8; A2; A1; A7; A9; A3.

To establish the multiplicative criterion, we multiplied the results of alternative values obtained by the criteria.

A1= 6.23:47.06=0.132
A2= 7.21:47.06=0.153
A3= 3.7:47.06=0.078
A6= 10.17:47.06=0.216
A7=4.67:47.06=0.099
A8=10.5:47.06=0.223
A9=4.58:47.06=0.097

The resulting hierarchy constructed was A8; A6; A2; A1; A7; A9; A3.

Results

The data obtained indicate that the additive criterion slightly differs from the multiplicative. The difference lies in the alternative values. For example, the additive criterion shows that alternatives 8 (0.123) and 6 (0.123) are equal. Thus, it is better to apply either A8 or A6 at first; however, the order in which they are used is inconsequential. The multiplicative method shows a difference between the values in A8 (0.223) and A6 (0.216). Consequently, the hierarchy of applying alternatives will change as follows: A8 must precede A6. Therefore, it is necessary to act according to the multiplicative method, which most clearly indicates the order of alternatives and is more sensitive to them. Thus, there must be improvements in the activities of peacekeeping organizations responsible for resolving international conflicts. The United States is the main proponent of fighting for the rights of nations and resolving international conflicts. However, it now faces the essential task of encouraging China to move toward prosperity, freedom, and international cooperation, while recognizing its influential role in the world. The United States and China continue to alternate common interests and misunderstandings on many issues. If both parties commit, based on the experience of the last 30 years, they will manage to build a relationship characterized by depth, openness, and common interests.

A detailed study of the causes and nature of international conflicts allows for predicting and preventing further similar international conflicts and finding effective ways to resolve existing international conflicts. The priority in settling any international conflict task is understanding that they have different dimensions and demonstrate different degrees of suitability for their management. General strategies or approaches applicable in some conflicts may not apply at all in others. Therefore, it is necessary to consider and offer recommendations on the effectiveness of entirely different conflict management methods and strategies and how they can be used to influence the cessation of protracted or even unresolved conflicts.

Understanding that international conflicts do not manifest themselves in a series of separate, unrelated episodes is equally important. Conflicts have a past, which, to some

extent, should help to explore the root causes of disputes. States involved in the conflict should rely on experiences and consider the mistakes that have led to the conflict, its uncertainty, or repetition. Finally, one should remember that conflict management is a rational and conscious decision-making process. The parties of a conflict (with or without the assistance of other states and international organizations) must take steps to transform, deescalate, or end the conflict conventionally. The range of methods and tools for long-term conflict management is broad, including coercive measures, third-party intervention, and multilateral conferences. An effective way to choose the most effective method of resolving an international conflict can be to divide existing methods into unilateral, bilateral (negotiations), and multilateral (third-party intervention). Also important is the role of factors influencing the response choice to the conflict and how certain specific conditions affect the choice of a particular method of conflict management or its final outcome.

In modern conditions, states-parties to conflicts strive to solve this problem through peace negotiations. However, there are currently conflicts at such a stage that traditional negotiations are not enough. Thus, states must sacrifice much of their potential to even have the opportunity to try to resolve a specific dispute. Therefore, strategies should be considered and developed for both conflict prevention and resolution in the event of their occurrence. It is expedient to regard the factors that influence the management of international conflicts.

Furthermore, the nature of the international system, the conflict, and the internal characteristics of the states involved should also be included. The nature of the international system influences the expectations of states and the strategies they can use to overcome a conflict. Features such as the polarity of the international system, coordination patterns, and allocation of opportunities are associated with different approaches to conflict resolution.

Undoubtedly, the approach to the settlement of international conflicts characteristic of recent years will remain the most effective way to prevent their occurrence. This approach is negotiation by which conflicting parties can neutralize their differences through consensus. This technique is a method to fight the conflict or reach an agreement even before the conflict. There are many methods to effectively contest the enemy state and many tips on how to behave in the course of both negotiations and military confrontation. However, the best way to counter international conflicts is undoubtedly to prevent them. In this context, the states' readiness and desire to prevent any disputes play a significant role. However, not all states are willing to sacrifice, for example, their principles and existing laws and directions to simply avoid conflicts with other countries.

Therefore, the main point of positive change may be third parties, which are interested states and international organizations. For instance, organizations like the United

Nations need to push harder for foundations of peace and security, development, and human rights to shift from their current –largely reactive– position to a conflict-oriented approach. Conflict prevention should be understood in terms of outbreak prevention, as well as a continuation, escalation, and recurrence of conflict. Moreover, peacekeeping and sustainable development must function as a single rather than two separate areas as they used to be in the past. Currently, the UN and the World Bank are conducting a joint flagship study on international conflict prevention in an effort to help the system move in a new direction.

Thus, states should primarily understand and sense their potential to prevent and counteract international conflicts. At some stage, they should be ready to mind the interests of other states and not only their national interests, so they can join forces and help resolve a particular international conflict.

Discussion

In studying the emergence and development of international conflicts in constructing a modern system of international relations, an attempt was made to determine the essence and main types of international conflicts. This study identifies the leading causes of conflicts and problems in international conflict prevention, describing the most effective models of conflict resolution using the example of two leading states. The best ways to resolve the international conflict were selected at the final stage of the study, providing detailed insight. This article offers insights into the most successful methods for finding the best ways to resolve international conflicts: the criterion analysis and the Pareto principle. They enabled examining the causes of the emergence and spread of conflicts and choosing the most effective way to counteract and prevent modern international conflicts, using the conflict of interest between the United States and China as an example.

An international conflict should be considered the interaction of two or more elements of the international relations system in pursuit of mutually exclusive or mutually incompatible goals. In international political conflicts, which arise primarily between states and intergovernmental organizations, all the interests of societies are combined and have the most straightforward expression (Galkin et al., 2020). In interstate relations, one can find manifestations of the most general patterns of conflict that affect the course of world development as a whole. The nature of international conflicts has changed significantly since the founding of the United Nations 75 years ago. Currently, conflicts are usually less deadly and often waged between national groups rather than states. Murders are becoming more common in some parts of the world, while gender-based attacks are on the rise.

There are no simple explanations for the causes of conflicts and how they can escalate violence. Understanding the dynamics of internal conflicts requires considering

many specific factors, such as poverty, rapid population growth, the availability of resources, and discrimination against minorities and other social groups. At the present stage, the direct causes of the emergence and development of international conflicts can be economic, territorial, political, ethnic, and even value differences. The process of globalization has influenced the increase in conflicts based on value differences (Chyzhmar et al., 2019). Automatically it has reduced the distance between countries and peoples of different cultures, forcing them to interact more closely and regularly; the greater the involvement of participants in joint activities, the greater the opportunities for conflict (Orlovskyi et al., 2018).

There are many tools used today by the parties to resolve a conflict. In most cases, they are independent or interacting with the United Nations and regional organizations. However, the most effective means is to avoid conflict. In other words, states simply ignore or abandon the conflict, choosing a method where the discomfort of confrontation exceeds the potential reward for resolving the conflict. Improvements in conflict resolution practices have given rise to new methods based on a drastic change in the quality of the situation, often using a third party or some other form of external action. Surprisingly, the United States is the primary propagator of the idea of a democratic system, constantly trying to disseminate its hypotheses on the protection of citizens, civil society's rights and freedoms, and the law as the highest value for all (Nye, 2008). Under these auspices, the United States often acts as a direct mediator in resolving some international conflicts.

It is worth noting that despite successful peacekeeping missions in various countries worldwide to resolve existing conflicts, the United States continues to be a participant in one of the most difficult bilateral conflicts today. The main reason for the long conflict between the states is that the growing influence of China's foreign policy is currently seen in the United States as a threat to its dominance in the international system. Indeed, China is the only country today that could threaten the United States' status, shaking the stability of the international system as a whole. Therefore, as a leading state and a determinant of the main trends in international relations, the United States should become an example and a driving force for other states regarding the emergence and spread of new international conflicts.

It is worth emphasizing the constant and continuous transformation of the conflict between the United States and China. At present, predicting further developments between the two specific states and the world, as a whole is highly challenging. The only viable solution would be the relentless desire to prevent the emergence of even the slightest controversy in the international environment and the development of a concrete plan to settle conflict in the event of its uncontrolled spread. Currently, the influence of globalization, regionalization, and democratization constantly changes the traditional range of international system elements. Given the fundamental changes in the role of state sovereignty, we can conclude there is a fundamentally new system present.

Conclusion

This study has revealed that China's assertive foreign policy and military stockpile challenge US supremacy and power, despite their common interests and intensive cooperation in global and regional issues. The conducted research attempted to determine the best ways to overcome international conflicts using the example of the conflict of interests of these two leading countries. Finally, the article offered some methods to counteract and prevent similar conflicts in the future. The key conclusions of this research are as followings:

1. The primary task in settling any international conflict is to consider that international conflicts have different dimensions and demonstrate different degrees of suitability for their management.
2. In any existing models, maintaining stability will occur through the management of international conflicts; the primary purpose is to maximize their constructive functions. This management is enabled by traditional settlement procedures, considering structural features of the post-bipolar international system.
3. The most effective model for resolving international conflicts is still the negotiations model, based on the equality of conflicting countries that brings them to the status of partners.
4. To avoid the emergence and spread of international conflicts in the future, states should consider the development dynamics of the policies of neighboring states and partner states, as well as their own foreign policy, and respond to new challenges in the international environment in a timely manner.

Disclaimer

The authors declare no potential conflict of interest related to the article.

Funding

The authors do not report sources of funding for this article.

About the authors

Nina F. Rzhevska is a Ph.D. in Political Science from the Taras Shevchenko National University of Kyiv, Ukraine, and a Ph.D. in Political Science from the Ivan Franko National University of Lviv. She is head of the department at National Aviation University, Ukraine. A researcher in strategic prognostications in foreign politics, peacekeeping, and geopolitical conflicts.

https://orcid.org/0000-0003-2911-3001- Contact: rzhevska8125@edu.cn.ua

Nataliia P. Borotkanych has a Master's degree in Foreign Policy from the Diplomatic Academy of Ukraine and a Ph.D. in History of Space Exploration. She is an associate professor at the National Aviation University, Ukraine. Researcher and teacher on international institutions, international conflict resolution, science, and space diplomacy.

https://orcid.org/0000-0002-6991-9838 - Contact: borotkanych8125@neu.com.de

References

Ackermann, A. (2003). The Idea and Practice of Conflict Prevention. *Journal of Peace Research*, *10*(3), 339-347. https://doi.org/10.1177%2F0022343303040003006

Central Intelligence Agency. (2020). *The CIA World Factbook 2020-2021.* New York: Skyhorse Publishing

China Office of the Historian. (2021). *A guide to the United States history of recognition, diplomatic, and consular relations, by country, since 1776. China.* https://history.state.gov/countries/china

Chunshan, M. (2021). *China-US relations: Views from China*. The Diplomat. https://thediplomat.com/2021/04/china-us-relations-views-from-china/

Chyzhmar, Y., Rezvorovich, K., Orlovskyi, R., Kysylova, K., & Buhaichuk, K. (2019). State employment service: European approaches to providing electronic services. *Journal of Legal, Ethical and Regulatory Issues, 22*(6), 1-7. https://www.abacademies.org/articles/State-employment-service-European-approaches-to-providing-electronic-services-1544-0044-22-6-444.pdf

Coppieters, B., Emerson, M., Huysseune, M., Kozviridze, T. & Noutcheva G. (2004). *Europeanization and conflict resolution: case studies from the European periphery.* Academia Press.

Dorussen, H., & Clayton, G. (2018). Political initiatives and peacekeeping: Assessing multiple UN conflict resolution tools. *Peace Economics, Peace Science and Public Policy, 24*(4), 1-5. https://doi.org/10.1515/PEPS-2018-0026

European Commission. (2019). *EU-China strategic outlook: Commission and HR/VP contribution to the European Council*. Press release https://ec.europa.eu/commission/presscorner/detail/en/ip_20_1600

Galkin, A., Popova, Y., Kyselov, V., Kniazieva, T., Kutsenko, M., & Sokolova, N. (2020). Comparison of urban conventional delivery and green logistics solutions. In *Proceedings - International Conference on Developments in eSystems Engineering, DeSE* (Liverpool, December 2020) (pp. 95-99). Liverpool: Institute of Electrical and Electronics Engineers Inc. https://doi.org/10.1109/DeSE51703.2020.9450776

Gros, D. (2021). The US-china technology conflict: The causes. In R.N., Choudhury (Ed.). *The China-US trade war and South Asian economies* (1st ed., pp. 217-228). Routledge.

Johnson, J. (2017). Washington's perceptions and misperceptions of Beijing's anti-access area-denial (A2-AD) 'strategy': Implications for military escalation control and strategic stability. *The Pacific Review, 30*(3), 271-288. https://doi.org/10.1080/09512748.2016.1239129

Kapitonenko, M. (2020). USA against China. How will the new confrontation affect Ukraine? *Interfax-Ukraine News Agency.* https://ua.interfax.com.ua/news/blog/708525.html

Khovpun, O.S., Zavydniak, V.I., Zavydniak, I.O., Kovtun, V.M., Zhuravel, Y.V. (2019). International legal norms as a source of criminal procedural law. *Journal of Advanced Research in Law and Economics, 10*(5), 1466–1476. https://journals.aserspublishing.eu/jarle/article/view/4832

Kniazieva, T. V., Shevchenko, A. V., Shevchenko, A. V., Yaroshenko, O. M., Inshyn, M. I., & Yakovlyev, O. A. (2021). Current trends in the formation and development of insurance marketing in Ukraine. *Risk Management and Insurance Review, 24*(3), 279-292. https://doi.org/10.1111/rmir.12185

Koch, R. (1999). *The 80/20 principle, expanded and updated: the secret to achieving more with less paperback*. New York: Broadway Business.

Kurnishova, Yu. (2017). *USA - China. Conflict in three dimensions*. Institute for Social and Economic Research (February 22). https://iser.org.ua/analitika/ssha-kitai-konflikt-u-troh-vimirah

Lee, Ying-Ming. (2011). The development of cross-straits relations. http://dspace.nbuv.gov.ua/bitstream/handle/123456789/31209/07-Lee2.pdf?sequence=1

Leonova, O. (2014). "Soft power": Tools and Factors of Influence. *Observer*, 3, 18-28. https://i-sng.ru/observer/observer/N3_2014/018_028.pdf

Nazarovska, I. (2012). The Main Subjects of Preventive Diplomacy. *Current Issues of International Relations*, *108*(1), 114-121. http://journals.iir.kiev.ua/index.php/apmv/article/viewFile/284/256

Nye, J. S. (2008). *Understanding international conflicts. An introduction to theory and history* (7th ed.). Harlow: Longman.

Orlovskyi, R., Shapoval, R., & Demenko, O. (2018). Possibilities of adapting the typologies of the international standards for establishing criminal liability for corruption-related crimes in Ukraine. *Journal of Eastern European and Central Asian Research, 5*(2). https://doi.org/10.15549/jeecar.v5i2.230

Smidt, H.M. (2020). United Nations Peacekeeping Locally: Enabling Conflict Resolution, Reducing Communal Violence. *Journal of Conflict Resolution*, *64*(2-3), 344–372. https://doi.org/10.1177%2F0022002719859631

Stockholm International Peace Research Institute. (2019). *SIPRI yearbook. armaments, disarmament and international security*. Oxford University Press.

Stockholm International Peace Research Institute. (2021). Stockholm International Peace Research Institute. https://www.sipri.org/yearbook/2021

Syrotiuk, Yu. & Oliynyk, Yu. (2021). *War index. Yearbook 2020*. Kyiv: Ukrayinski Studiyi Stratehichnykh Doslidzhen. https://ussd.org.ua/wp-content/uploads/2021/01/2021_01-indekc-3_web.pdf

United Nations. (2021). *A new era of conflict and violence*. https://www.un.org/en/un75/new-era-conflict-and-violence

Wallensteen, P. & Möller, F. (2003). *Conflict prevention: methodology for knowing the unknown*. Uppsala University.

Yelchenko, V. (2017). Letter dated 3 February 2017 from the Permanent Representative of Ukraine to the United Nations addressed to the Secretary-General. *United Nations Security Council* (February 6). https://undocs.org/en/S/2017/108

Yeremeeva, I.A. (2017). Actual Problems of Determining the Essential Characteristics of the International Conflict. *S.P.A.C.E. Society, Politics, Administration in Central Europe: Electronic Scientific-Practical Journal*, *3*, 58-61. http://dspace.onua.edu.ua/handle/11300/7905

Yuan, J. (2016). Averting US–China conflict in the Asia–Pacific. *International Affairs, 92*(4), 977-986. https://doi.org/10.1111/1468-2346.12662

Esta página queda intencionalmente en blanco

Revista Científica General José María Córdova
(Colombian Journal of Military and Strategic Studies)
Bogotá D.C., Colombia

Volume 20, Number 38, April-June 2022, pp. 323-339
https://dx.doi.org/10.21830/19006586.904

States' main directions and forms of international cooperation against transnational economic crimes

Principales orientaciones y formas de cooperación internacional de los Estados contra los delitos económicos transnacionales

Volodymyr I. Zavydniak, Iryna O. Zavydniak, Liubov V. Omelchuk, Lilia V. Polunina and Tetiana M. Suprun-Kovalchuk
University of SFS of Ukraine, Ukraine

Abstract. The current state of economic crime is characterized by stable growth, the structural diversity of new types of encroachments, a high latency level, and increased damage, making the topic under consideration relevant. This article studies the interaction of different states' legal systems in regulating international cooperation against transnational economic crimes and outlines the range of public relations arising from such activities under international public law. It employs a set of general scientific and special methods in the modern science of international public law to achieve the scientific objectivity of the results. Finally, it outlines the main trends in combating transnational economic crime at the international level.

Keywords: economic activity; international crimes; international relations; public law; transnational crimes

Resumen. El estado actual de la delincuencia económica, caracterizada por un crecimiento estable, la diversidad estructural de nuevos tipos de usurpación, un alto nivel de latencia y un incremento en los daños, hace que el tema que se examina sea relevante. Este artículo estudia la interacción de los sistemas jurídicos de los distintos Estados en la regulación de la cooperación internacional contra los delitos económicos transnacionales y esboza el abanico de relaciones públicas que se derivan de tales actividades en el marco del Derecho internacional público. El estudio emplea un conjunto de métodos científicos generales y específicos de la ciencia moderna del Derecho internacional público para lograr la objetividad científica de los resultados. Por último, este expone las principales tendencias en la lucha contra la delincuencia económica transnacional a nivel internacional.

Palabras clave: actividad económica; delitos internacionales; delitos transnacionales; derecho público; relaciones internacionales

Section: Dossier • Scientific and technological research article

Received: November 30, 2021 • Accepted: February 12, 2022

Contact: Volodymyr I. Zavydniak ✉ zavydniak8194@edu-knu.com

Introduction

In the context of globalization, crime goes beyond one state, destabilizing individual countries and the international legal order as a whole. The steady growth of international crime deepens the importance of international legal cooperation in the fight against it. The phenomenon of international crime is not a feature of modernity. It has occurred at different times and cultures, with various political and economic roots. However, at the present stage, international crime has become a global problem requiring a response from the world community and a targeted global legal effort in the fight against crime (Pozigun, 2021).

Although there has been significant progress in various spheres of public life in the XXI century, social progress has also been manifested in destructive, criminal, and dangerous phenomena that threaten humankind's sustainable development. The wide-spreading phenomena include terrorism, separatism, seizure of sovereign states' territories, increased economic crime, legalization (laundering) of proceeds from crime, fraud with financial resources, and cybercrime. Ukraine is increasingly becoming an object of interest for international criminal groups, particularly concerning money laundering, illegal migration, and trafficking of human beings, weapons, dangerous materials, and drugs. Therefore, it is expedient to study the problems of international cooperation between states in combating crime, its directions, and forms.

Today, many experts have noted a tendency for economic crime to transcend the state, becoming more transnational and even globally threatening in many cases. At the same time, the essence of the very concept of "transnational crime" has changed significantly. Transnational crimes were previously understood as a crime-set of strictly international character, posing an increased danger to the world community and harming interstate relations and peaceful cooperation between states, organizations, and citizens of different countries. Today, transnational crime has taken other forms. An appropriate interpretation would be the illegal commercial activity of criminal corporations in several states' economic, financial, trading, and other spheres of public life involving prohibited goods and services. In this regard, transnational crimes are spreading persistently, mainly extending beyond national borders. Given this worldwide trend, the United Nations has defined *transnational crimes* as offenses committed in one or more states, where a substantial part of their preparation, planning, direction, or control takes place in another state. In other words, offenses committed in one state with significant consequences in another. Accountability for such crimes is determined mainly by the states' national criminal law.

The urgency of combating this category of crimes nationally and abroad is determined by the scale of criminal groups' activities. In other words, it is determined by the scale and degree of organization currently supranational, requiring joint efforts by the

competent agencies, including law enforcement agencies around the world. At the same time, the trans-nationalization of crime marks the expansion of international cooperation in this area, that is, the involvement of organized "national" criminal elements in the activities of criminal groups in other countries.

International cooperation in the fight against crime is based on a system of principles that reflects both the common interest of the international community and the national interests of states as subjects of international law. Achieving a balance between the various actors' international law interests in the fight against crime is the key to effective cooperation and the peaceful coexistence of members of the international community. In the system of modern international relations, the basic principles of international law are fundamental and universally binding. They apply to all areas of international relations, including relations arising in international cooperation in the fight against crime.

The scale and global consequences of international offenses require establishing relations between states and international organizations to combat such negative manifestations. Accordingly, throughout the history of cooperation by international law subjects in combating crime, a fairly large array of international law, principles, and mechanisms for the prevention, counteraction, cessation, and investigation of international offenses has accumulated.

Establishing cooperation in combating international offenses began with the emergence of relations between the top developed countries, concluding in the first bilateral agreements on the extradition of criminals. In the future, the development of international relations in the fight against crime will occur within the context of developing international law. Each historical period has posed new challenges to the international community and required a joint effort to solve economic, political, and social issues and, in particular, to combat international offenses.

Scholars such as Tatsienko (2018a; b), Polianska (2018), Pidhorodynska (2015), Poplavsky (2019), and Woodwood and Zharovskaya (2020) have focused their scientific works on international cooperation between states against transnational economic crimes. However, this article studies the interaction of different states' legal systems concerning the regulation of international cooperation to combat transnational economic crimes, outlining the range of public relations arising from such activities that fall under international public law.

Materials and methods

The research methods were chosen considering the study's goals and objectives, object, and subject. To achieve the results' scientific objectivity, the authors resorted to general scientific and specific methods used in the modern science of international public law.

The historical-legal method was used to study the emergence of international legal cooperation in the fight against crime. It allowed the authors to identify the main stages of its development and examine international legal cooperation in the fight against crime in response to global challenges and the genesis of international criminal law. The formal legal method was used to analyze the international treaties, international legal customs, general principles of law, acts of international organizations, decisions of international judicial bodies, and other sources of international criminal and public law. Similarly, the dialectical method was used to determine the directions and forms of international criminal law and international legal cooperation in the fight against transnational crime and establish their subject composition.

The comparative legal method enabled determining the legal characteristics of international criminal law's sources as the central manifestation of international legal cooperation in the fight against transnational economic crimes. The authors used the theoretical modeling method to substantiate the existence of customary international law, general principles of law, and court decisions in the legal component of said cooperation, recognized by most countries' international treaties and decisions. The comprehensive analysis method allowed determining the actual content, main trends, and current state of international legal cooperation in the fight against crime. This method allowed the authors to identify legal, political, and economic factors that influence its implementation in the context of globalization and the features of international law implementation on a national scale, such as the implementation of international agreements on combating crime in Ukraine.

Moreover, the authors examined the approaches of international legal science to international cooperation and international legal cooperation, generalizing the scientific positions on international crime, transnational crime, and their features and proposing their definitions and the definition of international legal cooperation in the fight against crime. Furthermore, formal and logical methods (induction and deduction, analysis and synthesis, proof and refutation, generalization, among others) were used to identify the main shortcomings of the theory and current legal regulation of international cooperation in combating transnational economic crime in the context of globalization and national implementation of international law.

The classification criteria applied to the types of international agreements regulating international cooperation in the fight against crime included the number of participants, scope of cooperation, subject of regulation, time, territorial distribution, availability of control mechanism, ties, and subject composition. This classification helped delimit its directions, forms, and principles of international criminal law. The legal nature of the principles of international legal cooperation in the fight against crime was revealed based on the axiological approach. Because the international legal cooperation discussed in the article

represents a complex structured system of interconnected elements, the system-structural method played a crucial role in developing this scientific paper. Furthermore, the method allowed defining this legal category as a legal activity and identifying other branches and institutions of public international law to combat crime.

Results

The fight against crime is one of the priority areas of international cooperation. Its growth and internationalization have turned this struggle into one of the leading social problems, and its solution requires the cooperation of states. The principal modern areas of cooperation between states in the fight against crime are the following:

- The joint identification of the range of generally dangerous acts that require joint efforts to stop them;
- A mutual exchange of information on committed crimes and criminals;
- Assistance in searching for criminals in the state's territory and their extradition to the interested international law subjects;
- The joint study of crime and methods for combating it;
- The execution of specific instructions on criminal procedure issues;
- The creation of international agreements on combating certain types of international criminal acts; and
- The states' participation in international organizations specializing in the fight against crime.

This cooperation involves standardizing the qualification of international crimes and providing mutual legal assistance in criminal cases, including extradition. It also involves coordinating efforts and measures to prevent and stop crimes, combating specific categories of the most dangerous crimes, performing joint investigation tactical tasks (searching for hiding criminals, stolen items, and others), and combating transnational crimes in particular spheres of activity (transport, foreign trade), and ensuring punishment (Guliyeva et al., 2018). The authors highlight the following objectives of international cooperation in the fight against crime:

- Cooperation at the interstate level;
- Creation of international coordinating bodies;
- Cooperation at the level of individual agencies combating international and transnational crime; and
- Interaction between law enforcement agencies of neighboring regions of two or more countries.

Thus, international cooperation in the fight against crime requires the comprehensive coordination of actions of sovereign states and international organizations to develop

and coordinate measures to prevent and detect particular types of crimes and identify, detain, and bring offenders to justice. It also provides for defining goals and objectives to minimize transnational and domestic illegal acts. Based on the above, and according to Shkurko (2019), the forms of said cooperation are as follows:

- Coordination of actions to combat crime (exchange of information);
- Signing agreements on combating international crimes and crimes of an international nature;
- Legal assistance in criminal cases and conducting operational and investigative measures;
- Conducting investigative actions and crime prevention;
- Joint measures to stop criminal acts and bring the perpetrators to justice.

The basis for the states' international cooperation in this area implies a system of specific criteria, standards, and international principles that define the organization's essence and the states' and international organizations' activities in the fight against international crime. International cooperation against crime is a complex system of relations that includes coordinated policies, legislation, law enforcement, organizational and administrative, informational, and research activities of states represented by state bodies and officials. It also involves the activities of international organizations on crime prevention and handling of offenders. Such cooperation aims to improve international law in this area and achieve the coherence of states' actions –represented by their law enforcement agencies– in investigating criminal offenses. Implementing international cooperation in the fight against crime requires specific areas and forms. However, an analysis of legislation and scientific works reveals the lack of a unified and harmonized approach to their understanding (Dei et al., 2020a).

International legal norms in the specified field include multilateral conventions on combating international crimes, agreements on legal assistance in criminal cases, and agreements governing the activities of relevant international organizations. Some examples are the International Convention of December 14, 1973, on the Prevention and Punishment of Crimes against Internationally Protected Persons, including Diplomatic Agents (United Nations General Assembly, 1973), the Convention on Laundering, Search, Seizure, and Confiscation of Proceeds of Crime - Strasbourg, November 8, 1990 (United Nations General Assembly, 1990).

Cooperation between states in the fight against crime is carried out based on multilateral (within international organizations) and bilateral principles. Therefore, the UN's General Assembly and Economic and Social Council (ECOSOC) sessions address various issues in the fight against crime. The UN Congress on Crime Prevention is convened once every five years, the UN Committee on Crime Prevention and Control meets once

every two years, and the UN's Office for Crime Prevention and Criminal Justice is permanently operational. Bilateral agreements establish more specific forms of cooperation in the fight against certain types of crime.

Setting aside the doctrinal issues of transnational organized crime, one can easily note that it differs from the usual organized criminal activity with only one feature –the crime is committed both inside and outside national borders. In this regard, the following was stated in the Eighth UN Congress in Havana:

> Organized crime poses a direct threat to national and international security and stability and is a frontal attack on political and economic authorities, as well as a threat to the state itself. It disrupts the proper functioning of social and economic institutions and compromises them, leading to a loss of confidence in democratic processes. It undermines the development process and nullifies the progress achieved. It sacrifices the populations of entire countries and exploits human weakness while making a profit. It encompasses, envelops and even enslaves entire sections of society in various interconnected criminal enterprises. (United Nations, 1991; p. 7).

With the emergence and growth of transnational and organized forms of criminal crime, terrorism, and international terrorism, public and national security are at risk. Crime in the world has quadrupled in the last 30 years. According to the United Nations, since the late '90s, crime has increased an average of 5% per year worldwide, while population growth has been 1%. Accordingly, national and international methods and means of crime control, suppression, and the fight against it have begun to improve. Therefore, the urgent task of criminal law science is the development of scientifically sound recommendations for improving criminal law measures to combat crime driven by the needs of society and the growing threat of international crime (Lloyd et al., 2012).

According to Tatsienko (2018b), any state, even an economically developed one, cannot effectively combat transnational crime alone; this requires broad international cooperation. The UN Secretary-General Kofi Annan (2000) stated the following in this regard during the Millennium Summit:

> In 1945, the founders of the United Nations established an open system of international cooperation. The system worked and made globalization possible. As a result, everyone exists in the global world. Responding to these shifts is the central challenge facing world leaders. In this new world, groups and individuals are increasingly interacting directly across borders without state involvement. This poses a certain threat. Crime, drugs, terrorism, pollution, disease, weapons, refugees, and migrants are all moving in both directions at a faster pace and on a larger scale than in the past. People feel the threat posed by events unfolding far away from them. They react more sharply to injustice and cruelty in some countries and expect states to take some action in this regard. (p. 2)

On the other hand, new technology is also being developed for mutual understanding and joint action. To obtain the best of globalization and avoid the worst, we must

learn to lead better nationally and lead together internationally (Annan, 2000). Thus, international organizations, especially the United Nations, have an important role in consolidating and coordinating countries' efforts to combat transnational crime at the national and international levels. Within the framework of this authoritative universal intergovernmental organization, special bodies have been set up to appoint countries to increase the effectiveness of cooperation in the fight against crime and, to a greater extent, in the field of lawmaking. The Vienna Declaration on Crime and Justice: Meeting the Challenges of the Twenty-first Century, adopted at the Tenth United Nations Congress on the Prevention of Crime and the Treatment of Offenders (April 10th to17th, 2000), points to the need for closer coordination and cooperation between states (United Nations General Assembly, 2000). This cooperation should provide for solving the global crime problem, strengthening the internal systems of criminal justice, and national capacity in the field of international cooperation (Zavidnyak, 2021).

The increased social danger is the fundamental feature characterizing transnational crimes. This social (material) feature of the crime primarily determines its object, which is the presence of harmed public interests. First of all, transnational crimes are crimes, the commission or threat of which concern several states (the whole community). Secondly, their signs or the countermeasures against them should be enshrined or required in international agreements. Transnational crime also has a territorial feature, which is provided for in international agreements in which states define the scope of cooperation in the fight against crime. According to Article 3, paragraph 2 of the UN Convention against Transnational Organized Crime, a crime is transnational if it is committed in more than one state; committed in one state, but a substantial part of its preparation, planning, management, or control takes place in another state; committed in one state, but with the participation of an organized criminal group that carries out criminal activity in more than one state; or committed in one state, but its significant consequences occur in another (Wright, 2011).

Responsibility for these crimes is determined mainly by the states' national criminal law. However, the urgency to combat them, both nationally and abroad, is determined by the scale of activity of criminal groups and the supranational scale and degree of organization that requires the joint efforts of competent agencies and law enforcement agencies worldwide, cooperating in the fight against crime (Gerasymenko, 2021). Both the transnationalization of crime and its current trends and factors drive the expansion of international cooperation in this area. Moreover, the differentiation of the latter is necessary to clarify the prospects of such cooperation and improve its legal regulation (Nurullaev, 2020).

Transnational economic crime is an example of how criminals worldwide come together to make a profit. Transnational crime includes the most severe types of crime, such

as human trafficking, drug trafficking, arms trafficking, counterfeiting, corruption, cyberterrorism, money laundering, and theft and removal of works of art. Recently, modern transnational crimes have become more frequent, including cyberterrorism, kidnapping, and other crimes in cyberspace (Cherniavskyi et al., 2019). The number of methods employed to combat transnational crime compellingly proves that criminals involved in this area are not limited to one type of crime; they specialize in many at once. Thus, money from cybercrime, counterfeiting, and trafficking in stolen art is used to finance other terrorist activities, like human trafficking. Unfortunately, academic research today lags behind reality; therefore, it has not definitively explained the concept of transnational economic crime. Moreover, there is no clear definition of the boundaries and directions of transnational economic crime, significantly complicating the scientific analysis of the phenomenon under consideration. Therefore, it is impossible to develop a clear and transparent doctrine to combat transnational economic crime. Thus, clear and consistent actions must be developed to combat this phenomenon (Polyanska, 2016).

For a long time, transnational economic crime failed to attract enough attention from the political or scientific spheres. Seemingly, the interest became apparent only in the early 1970s, when outbreaks of international crime became widely known thanks to the media. However, transnational economic crime has now threatened individual states, their economies, and populations, which according to the authors, is the true reason for the interest in the problem. Experts explain that the problematic essence of this phenomenon is increased by the geographical distance in relation to the commission of crimes and the frequency of criminals' operations that go beyond regional and national borders. The preconditions for this phenomenon are believed to be the world community's tendency towards the globalization of modern socio-economic development. This tendency creates a level of interdependence between individual national economies and a qualitatively new phenomenon –the global economy (Reznik et al., 2020). The process of globalization affects all areas of economic relations, changing their quantitative and qualitative parameters. Therefore, economic globalization is also qualitatively changing the nature of crime, which is increasingly associated with violations of the laws of more than one country (Dei et al., 2021).

Transnational organized economic crime has not been overcome in the 21st century; it has even taken on a new dimension –new types of transnational economic crime. In fact, some states have begun to use the latest experience of transnational crimes to act against other countries, using crimes such as cyberterrorism. The intensification of the fight against transnational crime in the last decade is bearing very modest fruit. To make it more effective, the world states must jointly develop legislative, organizational, social, and moral-ethical measures, persistently implementing them using, among other things, coercive measures of influence. However, despite a recent trend towards the convergence

of legal systems that reflect integration processes in the economy, significant differences between legal systems (including the fight against economic crime) persist. Therefore, the creation of international documents on combating international economic crime is a challenging process (Poplavsky, 2019).

The UN Convention against Transnational Economic Crime of November 15, 2000, also provides an indicative list of crimes that fall under the definition of *transnational economic crime*. These include participation in an organized criminal group (Article 5), money laundering (Article 6), corruption (Article 8), and obstruction of justice (Article 23). However, the Convention neither explains the term *transnational economic crime* nor crimes included in this concept. This oversight greatly complicates the work of the relevant authorities investigating transnational economic crimes. Furthermore, the Convention also fails to consider the following factors when describing specific measures to combat transnational economic crime: the number of transnational economic crimes that are currently a major problem, the problems considered transnational economic crimes (e.g., smuggling), and new transnational crimes related exclusively to cyberspace, including cyberterrorism (Tatsienko, 2018a).

Transnational economic crime can be defined as criminal activity in the legal field and illegal economic activities in the fields of production, exchange, distribution, and consumption of material goods and services. The previous includes illegal activities under the guise of legal activities (Pidhorodynska, 2015) carried out in two or more states. These criminal activities require proper planning and preparation and a developed structure. They are driven by self-centered motives, profit, and a specific purpose –the commission of crimes, especially serious crimes. The perpetrators of these crimes are aware of their danger and illegality and consciously seek their consequences (Pidhorodynska, 2015).

With the previous in mind, the authors conclude that the fight against transnational economic crime can be achieved by exposing the illegal economic activities and legal entities that cloak them, obstructing the transport of relevant products across the borders of different states and blocking the money-transfer channels for such economic activities. The best results can be obtained if all these measures are carried out simultaneously; however, this involves complex coordination efforts between all law enforcement agencies and departments within a single country and between the different states. Currently, the significant difference in the criminal procedure legislation among states creates criminal procedure issues at the preliminary investigation and trial stages (Dei et al., 2020b).

The mutual recognition of results of forensic examinations as judicial evidence would be an important means to increase law enforcement agencies' effectiveness in joint investigations. Investigative actions in other countries and the development of common international requirements for evidence would also have a positive effect. The authors also believe that creating international tribunals on organized crime at the UN or oth-

er intergovernmental organizations is necessary to neutralize the criminal structures and prosecute criminal cases of crimes committed simultaneously in several states. Noting the serious and growing threat of international organized crime to the EU's very existence, it has adopted several legal acts to combat corruption in the private sector, money laundering, illegal insider dealing, fraud, and other related crimes (Polianska, 2018).

However, even within the EU, there is no single strategy to combat transnational economic crime; thus, no effective system exists to combat such crimes. The purpose of transnational crimes in the economic sphere is profit; this is inherent in all types of transnational crime (including those not regarded as economic). It is relevant in addressing transnational economic crime. The overlapping of profits can lead to the reduction and even cessation of criminal acts, as criminal acts become unprofitable. This effect should be considered when exploring the fight against transnational economic crime. The Internet, including its untraceable parts (the so-called Darknet), and many state-of-the-art communications, such as Viber or Telegram, have greatly increased the ability to establish private contacts between citizens of different countries and even different continents. Thus, transnational organized crime groups have more opportunities for trafficking.

Discussion

Ukraine is an active participant in international cooperation to promote peace, human rights, freedoms, and combating crime. Under its international legal obligations in combating crime, Ukraine implements its provisions into national legislation and cooperates with other states in this area. However, the effectiveness of implementing these commitments depends on the state of national legislation governing the State-authorized bodies' international cooperation, their interaction mechanisms, and real actions in international cooperation with states and other subjects of international law. International cooperation in the fight against crime is also influenced by the International Criminal Court and the development of cooperation within international organizations involved in crime-fighting activities, improving domestic criminal procedure and criminal activity investigation legislation, and borrowing best practices in international cooperation. The provisions of Ukraine's current legislation, in particular, and others under the rules of law, have been combined into a domestic legal institution of international cooperation in criminal proceedings, given Ukraine's participation in international cooperation at the universal and regional levels (Woodwood & Zharovskaya, 2020).

The growing level of crimes in this category is one of the factors driving the increased importance of international cooperation in the fight against economic crime and the related investigation of criminal proceedings. According to scientists from different countries, the highest growth rates in this category occur in economic crimes, with up to 10-15% per year. This situation is associated with the proliferation of new means to com-

mit economic crimes, including the use of existing and modified market relations and the active development of information (computer) technology. The outlined tendencies are typical for Ukraine as well. The transition from a rigid centralized government model to free-market relations has significantly changed the Ukrainian society's economic, social, and legal system. The rapid development of foreign economic relations, the domestic currency market, and the recognition of the primacy of international law, on the one hand, contributes to the fuller integration of the State into the world economic, financial, and legal spheres. On the other, it creates a number of negative phenomena and trends; the most dangerous is the intensification of criminalization of society and the economy in particular. This trend is due to a set of economic, social, and other factors whose elimination is beyond society's power as a whole at the present stage, as they occur in all spheres of public life and are associated with social contradictions that remain unresolved (Stelmakhov & Bondarchuk, 2018).

In addition, many powerful criminogenic factors in our country catalyze the global trend of quantitative and qualitative changes in economic crime. For example, the mass negative socio-psychological and moral condition and the decline of spiritual values have drawn a large part of the population into illegal relations. Moreover, Over the last five years, there has been a general decline in living standards, unemployment is on the rise, the gap between the rich and the poor has widened, and the middle class is dwindling, all stabilizers of the criminogenic situation.

Another trend determining the internationalization of economic crime is the growing number of organized criminal groups. According to the World Economic Forum (2019) in Davos, Ukraine was ranked 113th out of 137 countries with the highest level of organized crime in 2018-2019. Law enforcement agencies uncovered 230 organized criminal groups in 2019, reaching 308 in 2020. Despite significant human and natural resources, Ukraine's economic indicators are fairly low; therefore, the active growth of organized crime, and other factors, have become a threat to the State's national security. As organized crime transcends national borders, transnational criminal organizations are increasingly comparable to transnational corporations. As we can see, the current state of economic crime is characterized by stable growth dynamics, the structural diversity of new types of encroachments, and a high level of latency that increase the damaging consequences (Yaroshevskaya & Stetsenko, 2021).

Most economic crimes occur in the financial and credit system, the fuel and energy sector, the consumer market, and the foreign economic sphere. Organized criminal activity for profit is often not limited to any one type of illegal activity. An example of its *complex* nature is the criminal car business. These activities include the theft of vehicles, attacks on passengers to seize vehicles, obtaining illegal insurance compensation for allegedly stolen cars (fraud), car smuggling, customs duties evasion for imported vehicles for the purposes of stealing, making vehicles, and the sale of stolen vehicles, among others.

New categories of economic crimes have emerged in the course of radical changes in the State's economy. Counteracting these activities is hindered by significant law enforcement and organizational difficulties.

Tax-related crimes, for example, have become widespread in recent years; according to experts, the State annually receives only half of the budgeted tax revenues. The most criminogenic areas include credit banking and tax systems. Typical tax crimes include the non-crediting of currency to authorized bank accounts, the transfer of foreign exchange earnings abroad in violation of the established procedure and without the permission of the National Bank of Ukraine, the use of transfer pricing, the illegal export of capital under fictitious agreements, and the concealment of income received in Ukraine by foreign legal entities and individuals. As investigative efforts show, one of the main obstacles to the normal investigation of the crimes outlined above is the lack of an effective Ukrainian legal framework in the field of international cooperation.

The analysis of current trends in economic crime reveals that international cooperation in criminal procedure is a complex systemic phenomenon today. Thus, Ukraine's current legislation proceedings on transnational economic crimes cannot be ensured without external cooperation, including collecting evidence abroad, criminal prosecution, human and civil rights and freedoms protection in criminal proceedings, damages compensation, and possible property confiscation. These criminal procedural functions are implemented to some extent by pre-trial investigation bodies, the prosecutor's office, and the court during pre-trial investigation and court criminal proceedings (Legan, 2021).

Thus, the following areas of combating transnational crime are relevant to Ukraine. They involve a global call to update the United Nations Convention against Transnational Economic Crime significantly and include crimes presently recognized by the international community as transnational economic crimes, mainly smuggling and cyberterrorism. Ideally, the goal should be to create an adequate international legal act covering all areas of combating transnational economic crime. A similar single legal act should also be adopted at the EU and other intergovernmental association levels. In addition, a single system of evidence collection for transnational criminal groups should be introduced. An intergovernmental tribunal should be established to hear criminal proceedings when the activities of a transnational criminal group are exposed in several countries. It should also be legislated at the international level. These regulations should define transnational economic crime to develop a common legal doctrine for all countries to combat this threatening phenomenon.

Countering cyberattacks and cyberterrorism

Unfortunately, Ukraine is nearly defenseless in this direction. This condition must be corrected as soon as possible. In the event of an escalation of hostilities, a conventional enemy can paralyze the country's banking system in a matter of hours, leaving citizens without

electricity and communications, among others. Therefore, much more attention should be paid to areas including electronic surveillance systems and banking control against money laundering. Considering that the main purpose of transnational economic crimes is profit, the creation of a situation in which the costs of committing an economic crime exceed the possible profit should be the main goal of combating transnational economic crime. Countering transnational economic crime can be achieved in different ways; among them, exposing illegal economic activities and legal entities that conceal these activities, preventing the transport of relevant products across different states' borders, and blocking these economic activities' money transfer channels. All these methods involve both coordinating different states' departments and agencies' activities and interstate cooperation at different levels.

Conclusions

Globalization positively changes the economy and politics, making the international community more connected and interdependent with all its participants. Globalization made it possible to build strong international legal cooperation in the fight against crime. However, among the positive consequences, there are negative ones –new types, forms, and methods of transnational crime. They require a continuous update of international cooperation's legal and institutional mechanisms to combat crime. This study has shown that the development of international legal cooperation in the fight against crime requires programming to at least assess further crime development and ensure the inevitability of punishment.

Transnational economic crimes transcend a state's borders; thus, they can destroy the world economy, lead to poverty, and provoke other types of crime in countries. This study proved that the world has yet to develop effective strategies to combat this phenomenon. The government of one state alone is incapable of coping with crimes by its forces, no matter its means and resources. It must resort to some form of international cooperation to fight against transnational economic crimes. In light of the above, the fight against economic crime is one of the priority areas of international cooperation. Further research should aim to improve the international legal regulation for combating transnational economic crime.

Considering the circumstances that determine the prospects for international cooperation in the investigation of transnational economic crimes indicates that, on the one hand, its development is determined by quantitative and qualitative changes in economic crime. On the other, it is defined by the requirements of international treaties and the criminal procedural legislation of Ukraine. Global trends in economic crime and its genesis in Ukraine, moving towards these trends, drive the expansion of the domestic criminal process of international cooperation with the competent authorities of foreign countries.

In conclusion, the following means stand out in the fight against transnational economic crime. These are exposing illegal economic activities and legal entities that conceal these activities, preventing the transport of relevant products across the different states' borders, and blocking these economic activities' channels of money transfer. It is clear that the best results can be obtained if all these measures are carried out simultaneously; however, this involves complex coordination between all law enforcement agencies and departments within one country and between the relevant services of different states.

Disclaimer

The authors declare no potential conflict of interest related to the article.

Funding

The authors do not report sources of funding for this article.

About the authors

Volodymyr I. Zavydniak is a Ph.D. in Legal Sciences, Professor of the Department of Criminal Procedure and Criminology at the University of SFS of Ukraine. He is the author of approximately 100 research and methods papers. He is a researcher on international cooperation, case law, and other issues on criminal procedure.

https://orcid.org/0000-0001-9874-0346 - Contact: zavydniak8194@edu-knu.com

Iryna O. Zavydniak is a Ph.D. in Law, Associate Professor of the Department of Criminal Procedure and Criminology at the University of SFS of Ukraine. She is the author of 46 research and methods papers. She is a researcher on international cooperation and investigating transnational economic crimes.

https://orcid.org/0000-0003-4513-6529 - Contact: ir-zavydniak8194@acu-edu.cc

Liubov V. Omelchuk is a Ph.D. in Law, Associate Professor of the Department of Criminal Procedure and Criminology at the University of SFS of Ukraine. She is a researcher on developments in the methodology for investigating criminal offenses against the life and health of an individual and criminal offenses in the field of economic relations.

https://orcid.org/0000-0001-8489-3237 - Contact: omelchuk8194@sci-univ.com

Lilia V. Polunina is a Ph.D. in Law, Associate Professor of the Department of Financial Investigations at the University of SFS of Ukraine. She is the author of 35 research papers, including 19 conference papers. She is a researcher in investigation methods and forensics of criminal offenses in commercial and banking secrets.

https://orcid.org/0000-0002-0946-3568 - Contact: polunina8194@neu.com.de

Tetiana M. Suprun-Kovalchuk is a Ph.D. in Law, Associate Professor of the Department of Criminal Law and Criminology at the University of SFS of Ukraine. She is the author of approximately 60 research papers and a researcher on methods of responsibility for

committing corruption offenses and comparative characteristics of domestic and international anti-corruption legislation.

https://orcid.org/0000-0002-3387-3698 - Contact: suprun-kovalchuk8194@edu.cn.ua

References

Annan, K. (2000). *Address at the opening of the signing conference for the United Nations Convention Against Transnational Organized Crime*. United Office on Drugs and Crime. December 12. Palermo. https://www.unodc.org/unodc/en/about-unodc/speeches/speech_2000-12-12_1.html

Cherniavskyi, S.S., Golovkin, B.N., Chornous, Y.M., Bodnar, V.Y., & Zhuk, I.V. (2019). International cooperation in the field of fighting crime: directions, levels and forms of realization. *Journal of Legal, Ethical and Regulatory Issues, 22*(3), 1-11.

Dei, M. O., Matvieieva, H., Dorofeieva, L. M., Burdin, L. Yu., & Durnov, M. S. (2020a). Due process of law in Ukraine's national legal doctrine through the lens of ECHR practice. *Gênero E Direito Magazine, 1*(01). Periodicojs. https://www.periodicojs.com.br/index.php/ged/article/view/36

Dei, M. O., Myronets, O. M., Korolchuk, O. L. Butenko, O. V., & Slabetskyi, O. N. (2021). Participants and Victims of Armed Conflicts and Hostilities Rehabilitation. *The Journal of Nervous and Mental Disease*, *210*(3), 156-162. https://doi.org/10.1097/NMD.0000000000001430

Dei, M., Rudenko, O. & Lunov, V. (Ed.). (2020b). *Association agreement: driving integrational changes.* Ottawa: Accent Graphics Communications & Publishing.

Gerasymenko, O. (2021). Preconditions of administrative responsibility: doctrinal issues. *Journal of International Legal Communication, 1*(1), 102-111. https://doi.org/10.32612/uw.27201643.2021.1.pp.102-111

Guliyeva, A., Britchenko, I., & Rzayeva, U. (2018). Global security and economic asymmetry: A comparison of developed and developing countries. *Journal of Security and Sustainability Issues, 7*(4), 707-717. https://doi.org/10.9770/jssi.2018.7.4(8)

Legan, I. M. (2021). The main directions and forms of international cooperation in preventing and combating transnational crime. *Current Issues of State and Law, 1*, 89-93. https://doi.org/10.32837/apdp.v0i90

Lloyd, P., Simmons, B. A., & Stewart, B. M. (2012). Combating transnational crime: The role of learning and norm diffusion in the current rule of law wave. *The Dynamics of the Rule of Law, 2*, 153-180. https://doi.org/10.1017/CBO9781139175937.011

Nurullaev, I. O. (2020). International cooperation in the fight against crime as an integral part of the legal regulation of public international law. *Law and Public Administration, 1*, 243-249. https://doi.org/10.32840/pdu.2020.1-1.37

Pidhorodynska, A. B. (2015). International cooperation in criminal proceedings: concepts and procedural forms. *Scientific Bulletin of Kherson State University. Series: Juridical Sciences*, *4*(3), 114-118. http://nbuv.gov.ua/j-pdf/Nvkhdu_jur_2015_4%283%29__29.pdf

Polianska, V. (2018). Issues of European cooperation in combating transnational organized economic crime. *Scientific Bulletin of the National Academy of Internal Affairs, 108*(3), 67-79. https://scientbul.naiau.kiev.ua/index.php/scientbul/article/view/942/950

Polyanska, V.S. (2016). Origins and development of transnational organized crime in the field of economy in Ukraine. *Law Forum, 1,* 151–156. http://www.irbis-nbuv.gov.ua/cgi-bin/irbis_nbuv/cgiirbis_64.exe?I21DBN=LINK&P21DBN=UJRN&Z21ID=&S21REF=10&S21CNR=20&S21STN=1&S21FMT=ASP_meta&C21COM=S&2_S21P03=FILA=&2_S21STR=FP_index

Poplavsky, I. (2019). Problems of public regulation of activity international cooperation in the fight against organized crime. *Aspects of Public Administration, 7*(1), 5-13. https://doi.org/ 10.15421/15191

Pozigun, I. (2021). Rule of law implementation into the administrative process in Ukraine. *Journal of International Legal Communication, 1*(1), 73-80. https://doi.org/10.32612/uw.27201643.2021.1.pp.73-80

Reznik, O., Getmanets, O., Kovalchuk, A., Nastyuk, V., & Andriichenko, N. (2020). Financial security of the state. *Journal of Security and Sustainability Issues, 9*(3), 843-852. https://doi.org/10.9770/jssi.2020.9.3(10)

Shkurko, V. I. (2019). Some issues of combating transnational crime as a threat to the world economy in the context of globalization. *Economic Security of the State: Theory and Practice, 1*, 104-108. https://doi.org/10.32850/sulj.2019.1-26

Stelmakhov, V. Y., Bondarchuk, V. Y. (2018). Ways to overcome transnational organized crime. *International Scientific Electronic Journal, 5*. Nauka Online. https://nauka-online.com/wp-content/uploads/2018/05/Stelmahov-Bondarchuk.pdf

Tatsienko, V. (2018a). The urgency of research on the issue of transnational crime. *Financial Law, 12*, 244-248. http://pgp-journal.kiev.ua/archive/2018/12/46.pdf

Tatsienko, V. (2018b). The relevance of research on combating transnational economic crime. *Entrepreneurship, Economy and Law, 12*, 244-248. https://www.twirpx.com/file/3064474/

United Nations General Assembly. (1973). *Convention on the Prevention and Punishment of Crimes against Internationally Protected Persons, including Diplomatic Agents*. Zakon.rada.gov. https://zakon.rada.gov.ua/laws/show/995_389#Text

United Nations General Assembly. (1990). *Convention on Laundering, Search, Seizure and Confiscation of the Proceeds from Crime*. Zakon.rada.gov. https://zakon.rada.gov.ua/laws/show/995_029#Text

United Nations General Assembly. (2000). *Vienna Declaration on Crime and Justice: Meeting the Challenges of the Twenty-first Century*. Unodc.org. https://www.unodc.org/documents/commissions/CCPCJ/Crime_Resolutions/2000-2009/2000/General_Assembly/A-RES-55-59.pdf

United Nations. (1991). *Eighth UN Congress on the Prevention of Crime and Treatment of Offenders*. Unodc.org. https://www.unodc.org/documents/congress/Previous_Congresses/8th_Congress_1990/028_ACONF.144.28.Rev.1_Report_Eighth_United_Nations_Congress_on_the_Prevention_of_Crime_and_the_Treatment_of_Offenders.pdf

Woodwood, K, Zharovskaya, I. (2020). Fundamentals of cooperation between states in the fight against transnational organized crime: legal aspects. *Particulars of Legislative Adaptations of the Republic of Moldova and Ukraine to the Legislation of the European Union, 1,* 150-154. https://ibn.idsi.md/sites/default/files/imag_file/150-154_19.pdf

World Economic Forum. (2019). *Annual Report 2018–2019*. Weforum.org. https://www3.weforum.org/docs/WEF_Annual_Report_18-19.pdf

Wright, G. (2011). Conceptualising and combating transnational environmental crime. *Trends in Organized Crime, 14*(4), 332-346. https://doi.org/10.1007/s12117-011-9130-4

Yaroshevskaya, T. V., Stetsenko, K. O. (2021). International cooperation in the fight against crime. In *Materials of the 1st International Scientific and Practical Conference "Enforcement of Law Fight Against Crime in Ukraine and in the World: Problems and Ways to Solve Them."* (94-98). Dnipro: The Dnipro Humanitarian University

Zavidnyak, I. O. (2021). Factors determining the need for international cooperation in the investigation of economic crimes of a transnational nature. *Irpin Law Journal: Scientific Journal, 1*(5), 198-203. https://doi.org/10.33244/2617-4154.1(5).2021.198-203

Esta página queda intencionalmente en blanco

Revista Científica General José María Córdova
(Colombian Journal of Military and Strategic Studies)
Bogotá D.C., Colombia

Volume 20, Number 38, April-June 2022, pp. 341-353
https://dx.doi.org/10.21830/19006586.896

Agent-based models: an effective tool in Ukrainian state formation and legal regulation

Modelos basados en agentes: una herramienta eficaz en la formación del Estado y la regulación legal ucraniana

Oleksandr A. Lyubchik
Luhansk State University of Internal Affairs named after E.O. Didorenko, Ukraine

Olha S. Yadlovska
Dnipropetrovsk State University of Internal Affairs, Ukraine

Sergii Y. Vavzhenchuk
Taras Shevchenko National University of Kyiv, Ukraine

Olena Korolchuk
Uzhhorod National University, Ukraine

Oleksandr O. Stakhiv
Oles Honchar Dnipro National University, Ukraine

Abstract. This article explains the essence of the agent-based model method that simulates artificial societies to substantiate the thesis on its feasibility and scientific usefulness in lawmaking and law enforcement in Ukraine and research in the legal field. The primary research method used is synthesis, which allows combining components of a complex phenomenon and obtaining synthetic knowledge, which expands previous experience and constructs something new. Moreover, it allows going beyond the existing basis and drawing far-sighted conclusions, forecasting the directions of effective state formation and legal regulation in Ukraine.

Keywords: law enforcement; lawmaking; law enforcement; simulation; strategic planning

Resumen. Este artículo clarifica la esencia del método de modelos basados en agentes que simulan sociedades artificiales para fundamentar la tesis sobre su viabilidad y utilidad científica en la elaboración y aplicación de leyes en Ucrania y en la investigación en el ámbito jurídico. El principal método de investigación utilizado es la síntesis, que permite combinar los componentes de un fenómeno complejo y obtener un conocimiento sintético, que amplía la experiencia previa y construye algo nuevo. Además, permite ir más allá de la base existente y sacar conclusiones con visión de futuro, pronosticando las direcciones de la formación efectiva del Estado y la regulación legal en Ucrania.

Palabras clave: aplicación de la ley; legislación; modelos basados en agentes; planificación estratégica; simulación.

Section: Dossier • Scientific and technological research article
Received: November 29, 2021 • Accepted: February 12, 2022

Contact: Oleksandr A. Lyubchik ✉ lyubchik8123@neu.com.de

Introduction

The rapid development of digital technologies in recent years has provided humanity the opportunity to use them to resolve the most complex and important problems. Globalization, population growth, the escalating struggle for resources, and economic, environmental, and political crises, among other modern challenges, exist in every society, driving the search for new approaches to their solution. As a result, forecasting and planning any state's economic, political, legal, social, and environmental development strategy has become more complex and substantive.

States with numerous crisis phenomena, including Ukraine, cannot afford to make mistakes when planning their strategic and tactical (regional) development. Therefore, implementing agent-based models (ABM) can be key to seeing the state apparatus of Ukraine in practice by creating *artificial societies* that mimic the formation and development of various social phenomena that require state influence. Furthermore, this method can help solve legal issues and scientific problems in the field of legal research.

Academician Makarov (2006) argues that cognition through construction –through development– is the primary method of studying society. According to Istratov (2006), agent-based economic models represent the economy as several agents independently deciding on their livelihoods, employment, exchange of resources, communication, and others. The rules of interaction between agents in most agent-based model construction and study efforts are straightforward; however, the results are quite meaningful. Agent-based modeling is a relatively young branch of knowledge whose development has been driven by the rapid development of computer technology. However, to date, models have not been built to cover all areas of human activity simultaneously or at least a large number of them.

Currently, in Ukraine, there is very little research on the use of ABM in state forecasting and legal regulation; however, it is a promising and highly effective area of research. This is evidenced in studies like Remarks on the foundations of agent-based generative social science (Epstein, 2006); Faraway, so close: coupled climate and economic dynamics in an agent-based integrated assessment model (Lamperti et al., 2017); and Socio-natural and socio-ecological-economic models created using the method of agent modeling and Agent modeling of socio-political systems and processes: the history of development and prospects for practical application (Ageeva, 2018; 2019). Other studies that have obtained important and useful conclusions in this area include the article: Agent-based modeling of mutual influence between horizontal-vertical greenery systems and air pollutants using the city of Yerevan, Armenia, as a case study (Akopov et al., 2020).

Regarding the essence and features of agent-based models and their possible application to predict socio-economic phenomena have been studied by experts in various fields of knowledge, namely: Ageeva (2019); Bakhtizin (2015); Makarov (2006); Istratov

(2006); Sushko (2012); Chekmareva (2016); Epstein (2006), Chyzhmar et al. (2019), Lamperti et al. (2017), Vakulyk et al. (2020), and others. For the most part, these studies have tried to predict social and economic processes through the use of ABM. However, their use in the field of state formation and legal regulation as a mandatory stage of lawmaking and law enforcement is a new and promising area. So far, apart from Ramazanov (2018), few scientists have studied this area. The purpose of this study is to clarify the essence of agent-based models (ABM) simulation methods to substantiate the thesis on the feasibility and scientific usefulness of this method in lawmaking and law enforcement in Ukraine and research in the legal field.

Methods

The research process involved theoretical methods, including analysis, synthesis, concretization, generalization, methods of analogies, and comparative methods. The empirical method included the review of scientific articles on studies using ABM concerning social and economic processes and the regulatory framework in lawmaking. The research on the problem was carried out in three stages:

- In the first stage, a theoretical analysis was made of the essence and features of the ABM agent as one of the prospective methods of simulation modeling. The advantages of this method, in comparison with other methods of simulation, were determined, and the problem, purpose, and research methods were identified.
- In the second stage, the theoretical and practical results of the application of ABM in scientific and practical works by other scientists in the economy, ecology, social problems, and strategic planning were investigated. Finally, the results obtained from the conclusions of the examined experimental and theoretical scientific and research work were analyzed, verified, and concretized.
- In the third stage, the theoretical and practical conclusions were codified; the obtained results were summarized and systematized. Then, concrete proposals were presented concerning the use of ABM as an effective method for forecasting sociological, political, economic, and ecological processes in society to provide effective and timely forecasting and adjustment of state formation and legal regulation in Ukraine.

Results and Discussion

ABM, as a special type of simulation

Today, the social sciences, including law, have approached the comprehensive and effective use of new means of acquiring knowledge. The state and society's most acute social,

economic, political, legal, and environmental issues can often be predicted at their inception using modern methods of analysis and prediction of complex systems. Analysis and forecasting, including social phenomena, can be carried out through modeling, which, according to Lychkina (2012), is one of the main methods of cognition. It is a form of reflection of a reality that clarifies or reproduces certain properties of real objects, reflecting objects and phenomena and other objects, processes, phenomena, or with an abstract description such as images, plans, maps, sets of equations, algorithms, and programs. Thus, in modeling, there is always an original (object) and a model that reproduces (models, describes, simulates) some features of the object. The model is an abstract description of a system (object, process, problem, concept) in some form different from its real existence.

One of these methods is simulation modeling, an experimental method of studying a real system based on its computer model. In this type of modeling, the logical-mathematical model of the studied system is an operating algorithm, software implemented on a computer. The methodological basis of simulation is system analysis. Today, there are three types of simulation: system dynamics, discrete-event modeling, and agent-oriented modeling. In a broad sense, simulation in science means the process of construction, analysis, and application of simulation models. In a narrow sense, simulation is interpreted only as a process of constructing a simulation model (Chekmareva, 2016). Agent-based models are the earliest type of simulation. A prototype of the first agent-oriented model was developed in the late 1940s; however, these models became widespread only in the early 1990s due to the advent of microcomputers and the ability to conduct computer simulations (Makarov & Bakhtizin, 2013).

According to Sushko (2012), an agent-oriented (multi-agent) model is an artificial society consisting of interacting independent agents, each of which has a given set of personal characteristics ('resources'), an objective function ('interests'), and obeys the rules of conduct that determine his reaction in various situations that affect the sphere of his interests. To Lychkina (2012), a simulation model is a computer program or software package using a sequence of calculations and graphical display of their results to simulate (reproduce) the social processes of an object or a set of objects under the influence of others, including random factors.

Thus, it is evident that the description of the concept of simulation models varies. Our study maintains that a simulation model is not a computer program. According to Article 2 on the distribution of copies of audio-visual works, phonograms, videograms, computer programs, databases (Law of Ukraine No. 1587-III, 2000), a computer program is a set of instructions in the form of words, numbers, codes, diagrams, symbols, or in any other form, expressed in a computer-readable form that actuates it to achieve a specific goal or result (this concept covers both the operating system and the application, expressed in source or object codes). Therefore, a computer program is not a simulation model itself but a technical tool to create this simulation model.

According to Makarov (2006), an artificial society consisting of interacting agents and computer models, where atoms are agents, is called an agent-oriented model. Thus, agent-oriented computer models, or agent-based models –abbreviated ABM– are artificial societies consisting of agents interacting with each other. The term "agents" is conditional. It has been widely used in the English-language literature, which gave impetus to this area of research, and has taken root and dominates. In different agent-oriented models, the term can represent a person, legal entity, government agency, or a combination of them, among others. Their relationship determines the agent-oriented model's properties noted in science. According to (Epstein, 2006), they include:

- Heterogeneity: agents differ from each other;
- Autonomy: agents act independently of each other;
- Given space parameters in which the agents are located and operate.
- Local interactions take place;
- Agents are characterized by limited rationality;
- Dynamics of events can have any vector of development and is not in equilibrium.

An artificial society is not just one agent; it is a model of society. Thus, there must be at least two agents; they must interact with each other as in society. Most importantly, agents must be similar in interactions to perceive them as similar. It is then that social behavior appears (Makarov, 2006). Compared with other means of simulation modeling, agent-based models allow modeling the system as close as possible to reality. They have the property of emergence (from the English, emergent: arises, suddenly appears), the emergence of special properties in the system that are not inherent in its elements, system effect. Moreover, they enable building models in the absence of knowledge about global dependencies in the relevant subject area, providing a flexible tool to easily add agents to the model and remove them and change the parameters and rules of their behavior (Makarov & Bakhtizin, 2013).

The essence of computer modeling is to obtain quantitative and qualitative results on the existing model. The qualitative analysis results reveal previously unknown properties of a complex system, its structure, development dynamics, stability, and integrity. Quantitative conclusions mainly involve the analysis of an existing complex system or forecasting future values of some variables. The ability to obtain both qualitative and quantitative results is the significant difference between simulation and structural-functional (Lychkina, 2012).

The well-known researcher in the field of ABM, Bakhtizin (2015), defined agents as follows: an autonomous entity, usually assigned a graphical representation, with a specific purpose and a certain level of possibility of learning in the process of existence, determined by the developers of the model. Examples of agents are:

1. People (and other living organisms), cars, and other moving objects;
2. Immovable objects; as well as;
3. A set of similar objects.

Generally speaking, agents in ABM can be any objects observed in real life; however, the main task of their accounting within the model is their correct specification. ABM are usually used in cases where:

- The relationship between the model's variables is difficult or impossible to build;
- The model contains stochastic components;
- To better understand the operation of objects within the system requires visualization of all processes occurring in it.

There are various software tools, including NetLogo, Repast, SWARM, and AnyLogic, that enable ABM development (Bakhtizin, 2015). The most voluminous projects solved with this technology must consider the mechanism of ABM and the application of its results. For instance, under the leadership of Joshua Epstein and John Parker at the Brookings Center on Social Dynamics and Policy, agent-based models were built to include the entire US population, about 300 million agents moving across a map of the country according to the matrix of correspondence of 4000 × 4000. A computational experiment was conducted, simulating the 300-day spread of a disease featuring a 96-hour incubation period and a 48-hour infection period. One of the study's results was a decline in the spread of the disease after 65% of people had recovered and acquired immunity. This model has been used repeatedly at Johns Hopkins University and the US Department of Homeland Security for rapid response to epidemics (Epstein, 2006).

It was used to simulate the effects of the spread of the Influenza A virus (H1N1/09). The model was extended to the Global-Scale Agent Model (GSAM), which included 6.5 billion agents interacting and moving according to the statistics available to developers. John Parker headed this project, which is currently the largest agent-oriented model, representing the planet's entire population. The results of the calculations were displayed on a global map using dynamic color markings according to the status of the agents living in a particular area (Khovpun et al., 2019). For example, black indicated disease-susceptible agents, red was used to isolate the infected, and blue indicated agents who had recovered or died. The figure showed the condition of agents living on the planet 4.5 months after the start of the H1N1 pandemic in Tokyo (Bakhtizin, 2015).

This example and many others included in the scientific literature (Ramazanov, 2018; Ramazanov, 2019; Ageeva, 2018; Ageeva, 2019; Akopov et al., 2020) allow us to conclude that the world economic leaders have access to advanced computer technology to address today's socio-economic, political, environmental, legal, and other challenges. Domestic scientists are beginning to immerse themselves in the topic of agent-oriented

modulation of socio-economic processes; however, such attention is insufficient and is not being used in many suitable areas of life.

Justification of the effectiveness of the use of ABM

With the help of computer simulation –namely ABM– in certain spheres of public life, it is possible to predict specific directions of their development and use this data for timely, effective, purposeful, adequate, and balanced legal decisions. Three basic conditions justify the objectivity of such decisions:

1. The objectivity of the data to be entered into a computer program to create an agent-oriented model (artificial society);
2. Mathematical - technical compliance of the computer program developed for this purpose;
3. Clear formulation of the goal to be achieved through simulation.
4. Clear formulation of the planned goal to be achieved through simulation.

We can conclude from this statement that there is a need for a collective team effort by legal scholars and specialists in mathematics and programming to create ABM. To increase these teams' (associations) efficiency and professionalism, they should not merely be enthusiastic scientists who, for the sake of diversity, have decided to "try their hand" and use ABM technology to predict a social phenomenon. These specialists must become experts and work with higher state body strategic legal decision-makers, such as the Verkhovna Rada of Ukraine, the Cabinet of Ministers of Ukraine, and the National Bank of Ukraine. In the future, forecast teams (centers) may exist in each ministry department. Strategic legal decisions should be made for a period of 5 to 20 years (in some more predictable sectors, up to 50 years), given the development of the economy and Ukraine's social sphere. In addition, they should consider international trends of globalization, cooperation, competition, and political stability of potential partners.

Currently, systemic challenges threaten Ukraine's status as an industrial state. The numerous months of voluntaristic decisions between cabinet ministers and ministers, the steady decline in the country's economic potential, living standards, devaluation of its currency, and increasing external loans undermine Ukraine's independence and threaten it to relegation as an agrarian state and a raw material appendage of the "Western partners." Thus, there is a need for fateful legal decisions on objective grounds. Strategic planning of ways out of the crisis and further state development must be a state priority and strictly abided. To normatively consolidate this development, adopting the law "On strategic planning in Ukraine" is vital to accomplish the following:

1. Regulate the need and procedure for long-term state planning, defining key economic and social indicators in various sectors of the economy;

2. Distribute the powers and responsibilities of state bodies and local governments at different stages of the plan's implementation;
3. Determine the procedure for adopting the "Strategic Program for State Development." One of its elements is to provide for the need to create and agree, within the Verkhovna Rada of Ukraine profile committees, on the ABM's specific areas.

Strategic planning and its organization with the help of ABM

According to Gorbulin and Kaczynski (2010), strategic planning is not the same as strategic thinking and action. Strategic thinking is of the utmost importance here, whereas strategic planning is useful only if it improves strategic thinking and action, but it does not replace them. The creation of strategic documents of different levels has different origins, including the state's top political leadership's vision, National Security and Defense Council's top managers' intuition, and subjects' collective experience. Strategic planning is one of them. All these sources must be considered to optimize strategic thinking and action. Thus, perhaps the most apparent benefit potentially provided by strategic planning is that it stimulates strategic thinking and action.

One can agree with the position of these authors on the primacy of strategic thinking, which is provided by strategic planning, and not vice versa. Therefore, strategic planning is not an end in itself and not a panacea for social unrest. It is a tool of interested leaders who have genuinely set the goal of achieving profound changes in all spheres of public relations and life, which will not give any benefits in the results of such planning (Radzivill et al., 2018). The use of ABM in legal decision-making is possible only if the government has clearly defined the goals of public administration and chosen a suitable vector for the development of society.

Science argues that specific and clear goals can help determine the direction of state national security policy, its individual components, and related programs. Goals in management are presented as an ideal image (logical model) of the vision of the state or object of management, formed based on the understanding and consideration of its objective laws and organizational norms, needs, and interests. Goals are a product of consciousness; thus, each goal can have quite a different relationship between real and ideal (Gorbulin & Kaczynski, 2010).

Most developed countries have laws on strategic planning that allow these countries to achieve economic and social development because they have specific strategic goals and defined ways to achieve them, well-established development vectors, and clear political preferences. For example, the UK's Planning and Compulsory Purchase Bill (RSV), adopted by Parliament in April 2004, provides the legal basis for the system's functioning and the implementation of the strategic planning process at the national level (Ivashchenko & Verbytsky, 2006).

The US legislative act defining strategic planning procedures at the national level is the 1993 Government Performance and Results Act (GPRA). In contrast to the United Kingdom, this document defines the hierarchy of strategic planning of the executive branch and the specific time frame for the preparation of planning documents. It consists of 11 sections: Summary, Data and Objectives Obtained, Implementation of Strategic Planning, Annual Performance Planning and Reporting Mechanism, Management Accountability and Flexibility, Pilot Projects, US Postal Service, Legislative support and supervision of the Congress, Preparation, Implementation of the law, and Technical and Harmonization Annexes (Ivashchenko & Verbytsky, 2006).

In 2014, the Federal Law on Strategic Planning in the Russian Federation (2014) was adopted. It establishes the legal framework for strategic planning in the Russian Federation, coordination of state and municipal strategic management and budget policy, the powers of federal authorities, public authorities of the Russian Federation, local governments, and the procedure for their interaction with the public and scientific and other organizations involved in strategic planning. The existence of normative support for strategic planning in Ukraine and the use of a mechanism for forecasting its consequences through their immediate objectification (in the form of ABM) should provide Ukraine with the necessary impetus for further development. However, the reluctance or inability of the government to provide a transparent, clear, and objective answer to the directions and ways of state development can hinder this stride.

Numerous works by Western scholars evidence a worldwide void in the development of this area of research in the legal field. State support to Ukrainian scientists concerning the development of this vector of scientific research depends on the interested authorities' ability to use the results of this research, which is not limited to providing a step forward but an instant look into decades in the future.

Using agent-oriented models will enable law enforcement agencies to determine the development directions of negative and positive phenomena in society in advance. For example, they can help determine trends in specific offenses and crimes, the best types and amounts of tax rates and tax sanctions, forecast demand for certain goods, and calculate the spread rate of serious diseases to effectively and opportunely take appropriate measures to overcome or support the studied phenomena.

The International Data Corporation (IDC) predicts that the total amount of data will reach 35,000 exabytes by 2020. Compared to 1,200 exabytes in 2010, this almost a 30-fold growth in ten years (blogs, social networks, analytical materials, photos, maps, etc.). The need to process such a large amount requires a new generation of analytical systems, including advanced calculation methods, pattern recognition, data warehouse organization, and statistics collection to extract meaning from the data and obtain information context. This wager includes agent models (Bakhtizin, 2015).

An ordinary personal computer with good performance can perform calculations with a satisfactory speed over the number of agents of about 20 thousand (the behavior of each is given by about 20 functions), and the average conversion time of one unit of model time (one year) is about a minute. With more agents (for example, 100 thousand), the computer simply "idles." However, using 1000 supercomputer processors and executing an optimized code allows the number of agents to reach 100 million agents and run a 50-year model. This enormous array of calculations is performed over a period of approximately 1 minute 30 seconds, depending on the type of processors used (Bakhtizin, 2015).

Conclusions

As shown in this study, the use of ABM to address a state's pressing social, environmental, and economic issues and strategic planning in favor of its development has been studied by many scientists worldwide. Stimulating, complex, and effective studies have been carried out. The real results obtained have had practical significance in forecasting social, ecological, and economic phenomena and, on these bases, state strategic planning. All these scientists unanimously recognize the effectiveness of ABM and agree on the need for its improvement and use in all spheres of society and the state. Similarly, some units of scientific work have been devoted to the possibility of using this type of simulation in forecasting and adjusting state formation and legal regulation.

Based on a well-defined explanation of the features and benefits of ABM, this study aimed to prove the need for their use in strategic state planning, law-making, and law enforcement. The article also formulated and substantiated specific proposals on the need to adopt a law on strategic planning in Ukraine and proposed its content. Furthermore, it justified the need to adopt a strategic state development program to create and coordinate ABM implementation programs within the relevant committees of the Council of Ukraine for specific areas.

We can conclude that the development of digital simulation technologies has provided new opportunities for humanity in recent years. ABM contribute to countries that have mastered their creation, allowing them to predict the emergence and development of socio-economic processes in society. There is no doubt about the effectiveness of ABM both in the field of legal research and law-making and law enforcement activities. The success of Western and some post-Soviet countries using these technologies indicates that, in the future, in conditions of total resource scarcity, civilizational competitiveness will be given to countries that prioritize strategic planning using simulation technologies, applying them to all spheres of life.

ABM technologies can provide answers in state strategic planning. However, they can also contribute significantly to scientific and legal research concerning quantitative and qualitative data on the economy, social reality, and political vectors of develop-

ment, aimed at obtaining objective indicators and their trends and activities using ABM. Unfortunately, as evidenced by the numerous works of Western scholars, there is a worldwide deficiency in the development of this area concerning the legal field. State support for Ukrainian scientists developing this vector of scientific research depends on the interested authorities' ability to use the results of such research.

Ukraine is moving towards Euro-Atlantic integration, so the experience of Great Britain and other European countries, the United States of America, and post-Soviet countries should inspire it to make more active use of ABM technologies. The success of these technologies and knowledge obtained through their use is evidenced in this article, which is clearly in favor of their use.

To ensure the possibility of using ABM to forecast socio-economic, environmental, and political problems in Ukraine, based on this knowledge of timely adjustment of legal decisions in the direction of national development, it is necessary to:

- Adopt the Law of Ukraine "On Strategic Planning," which provides for the sections formulated in the article;
- Based on this law, adopt a strategic state development program, which must be developed with the help of ABM;
- Organize the activities of state bodies that should be engaged in strategic planning (primarily the Verkhovna Rada of Ukraine, Cabinet of Ministers of Ukraine, and later, other state bodies and local governments), supported by a team of experts in economics, law, mathematics, programming, and other areas of knowledge required in specific cases to create ABM of relevant social phenomena and processes;
- Determine the issues concerning ABM development in specialized state educational institutions, and introduce new specialties related to these activities;
- Make strategic legal state decisions based on objective data and calculated for 10-50 years and grant priority and legal supremacy to other (regional, local) legal decisions and development programs.

Recommendations

The conclusions and justifications presented in this article were formulated primarily for use by government agencies and their officials, who analyze the state and forecast its development as a whole and individual areas or territories. Based on these findings, the state can take concrete steps to help strategic planning of its development and improve approaches to strategic legal decisions. The study results can also be useful for the legal community of Ukraine and other countries that seek to overcome global challenges with the help of new technologies and ensure sustainable development of society and the state. Finally, the proposals of this article can be used by large and medium-sized businesses trying to predict the development of the global or sectoral market in which it operates.

Disclaimer

The authors declare no potential conflict of interest related to the article.

Funding

The authors do not report sources of funding for this article.

About the authors

Oleksandr A. Lyubchik is a Ph.D. and professor in Legal Science. He graduated and specialized in Law from the Donetsk Law Institute and has authored nearly 80 scientific and scientific-methodical works. He is currently a professor in the Department of State and Legal Disciplines.

https://orcid.org/0000-0002-4906-959X - Contact: lyubchik8123@neu.com.de

Olha S. Yadlovska graduated in History and Jurisprudence from the Bogdan Khmelnytsky Melitopol State Pedagogical University. She is an associate professor of Social Sciences and Humanities at the Dnipropetrovsk State University of Internal Affairs' faculty of Educational and Scientific Institute of Law and Innovative Education.

https://orcid.org/0000-0001-8579-9023 - Contact: yadlovska8123@acu-edu.cc

Sergii Y. Vavzhenchuk is a Ph.D. in Legal Science. He has authored and co-authored over 240 scientific and educational works. By decision of the Certification Board of the Ministry of Education and Science of Ukraine, he was awarded the title of academic professor.

https://orcid.org/0000-0001-5061-6215 - Contact: vavzhenchuk8123@edu-knu.com

Olena Korolchuk has a Ph.D. in Public Administration. She is a graduate student of the Department of Health Management of the National Academy of Public Administration under the President of Ukraine. She is an associate professor of Health Sciences at the Uzhhorod National University and has authored over 60 scientific and educational works.

https://orcid.org/0000-0002-5083-3225 - Contact: korolchuk8123@sci-univ.com

Oleksandr O. Stakhiv obtained a Master's degree with honors in Jurisprudence from the Dnipro National University, named after Oles Honchar.

https://orcid.org/0000-0002-9240-0890 - Contact: stakhiv8123@edu.cn.ua

References

Ageeva, A.F. (2018). Socio-Natural and Socio-Ecological-Economic Models Created Using the Method of Agent-Based Modeling. *Bulletin of the Plekhanov Russian University of Economics*, *4*, 100-115. https://doi.org/10.18254/S207751800007439-1

Ageeva, A.F. (2019). Agent Modeling of Socio-Political Systems and Processes: History of Development and Prospects for Practical Application. *Modeling, Optimization and Information Technology*, *7*(4). https://doi.org/10.26102/2310-6018/2019.27.4.005.

Akopov, A. S., Beklaryan, L.A., Belyaeva, O., Sahakyan, L., Saghatelyan, A.K., & Tepanosyan, G. (2020). Agent-based modelling of mutual influence between horizontal-vertical greenery systems and air pollut-

ants with the use of the city of Yerevan, Armenia as a case study. *Artificial Societies*, *15*(1). https://doi.org/10.18254/S207751800008317-7

Bakhtizin, A.R. (2015). Agent-based models. Simulation. http://simulation.su/uploads/files/default/prez-bahtizin.pdf

Chekmareva, E.A. (2016). Reproduction of Labor Potential as an Object of Simulation. *Territory Development Problems*, *6*(86), 166-172. http://simulation.su/uploads/files/default/2016-chekmareva-1.pdf

Chyzhmar, Y., Rezvorovich, K., Orlovskyi, R., Kysylova, K., & Buhaichuk, K. (2019). State employment service: European approaches to providing electronic services. *Journal of Legal, Ethical and Regulatory Issues, 22*(6), 1-7. https://www.abacademies.org/articles/State-employment-service-European-approaches-to-providing-electronic-services-1544-0044-22-6-444.pdf

Epstein, J. M. (2006). Chapter 34 Remarks on the Foundations of Agent-Based Generative Social Science. *Handbook of Computational Economics*, *2*, 1585-1604. http://doi.org/10.1016/S1574-0021(05)02034-4

Gorbulin, V. P. & Kaczynski, A.B. (2010). *Strategic planning: solving national security problems.* NISS.

Istratov, V.A. (2006). The basic computer model of human behavior. *Artificial Societies*, *1*(1), 46-49. https://artsoc.jes.su/s207751800000094-2-1/

Ivashchenko, A. & Verbytsky, S. (2006). Regulatory Support of Strategic Planning from the Experience of Great Britain and the USA. *Political Management*, *1*, 140-150. Dspace.Nbuv. http://dspace.nbuv.gov.ua/bitstream/handle/123456789/8714/15-Ivaschenko.pdf?sequence=1

Khovpun, O.S., Zavydniak, V.I., Zavydniak, I.O., Kovtun, V.M., & Zhuravel, Y.V. (2019). International legal norms as a source of criminal procedural law. *Journal of Advanced Research in Law and Economics, 10*(5), 1466–1476. https://journals.aserspublishing.eu/jarle/article/view/4832

Lamperti, F., Dosi, G., Napoletano, M., Roventini, A. & Sapio, A. (2018). Faraway, So Close: Coupled Climate and Economic Dynamics in an Agent-Based Integrated Assessment Model. *Ecological Economics*, *150*, 315-339. http://dx.doi.org/10.1016/j.ecolecon.2018.03.023

Law of Ukraine No. 1587-III (2000). *On the distribution of copies of audio-visual works, phonograms, videograms, computer programs, databases.* March 23. The Verkhovna Rada of Ukraine. https://zakon.rada.gov.ua/laws/show/1587-14#Text.

Law on Strategic Planning in the Russian Federation (2014). *Federal Law. No. 172-FZ*, 28 June 2014. Base. Garant. http://base.garant.ru/70684666/.

Lychkina, N.N. (2012). *Simulation modeling of economic processes: Textbook*. INFRA-M.

Makarov V.L., & Bakhtizin A. H. (2013). *Social modeling is a new computer breakthrough (agent-based models)*. Ekonomika.

Makarov, V.L. (2006). Artificial Societies. *Artificial Societies*, *1*(1), 10-24. http://www.cemi.rssi.ru/publication/e-publishing/makarov/text.pdf

Radzivill, O., Pyvovar, Y., Sopilko, I., & Pyvovar, I. (2018). Coordination of fragmentation within the international air law. *International Journal of Engineering and Technology(UAE), 7*(3.30 Special Issue 30), 280-283. https://doi.org/10.14419/ijet.v7i3.2.14420

Ramazanov, R.R. (2018). The Problem of Delimiting the Powers of Government Levels to Provide Public Services. *USPTU Bulletin. Science, Education, Economics. Series: Economics*, *4*(26), 93-99. https://doi.org/10.17122/2541-8904-2019-4-30-50-60

Ramazanov, R.R. (2019). Agent-based modeling the distribution of authorities between the levels of the state. *Artificial Societies*, *14*(3). https://doi.org/10.18254/S207751800006877-3

Sushko, E.D. (2012). *Multiagent model of the region: the concept, design and implementation*. CEMI Russian Academy of Science. http://simulation.su/uploads/files/default/2012-sushko-1.pdf

Vakulyk, O., Petrenko, P., Kuzmenko, I., Pochtovyi, M., & Orlovskyi, R. (2020). Cybersecurity as a component of the national security of the state. *Journal of Security and Sustainability Issues, 9*(3), 775-784. https://doi.org/10.9770/JSSI.2020.9.3(4)

Esta página queda intencionalmente en blanco

Revista Científica General José María Córdova
(Colombian Journal of Military and Strategic Studies)
Bogotá D.C., Colombia

Volume 20, Number 38, April-June 2022, pp. 355-370
https://dx.doi.org/10.21830/19006586.905

From self-affirmation to national security threat: analyzing the Ukraine's foreign experience in countering cyberattacks

De la autoafirmación a la amenaza a la seguridad nacional: la experiencia ucraniana y extranjera contra los ciberataques

Yuriy Yu. Nizovtsev and Andrii M. Lyseiuk
Ukrainian Scientific and Research Institute of Special Equipment and Forensic Expertise of the Security Service of Ukraine, Ukraine

Mykhailo Kelman
National University, Ukraine

Abstract. This paper aims to study the main stages of cyberattacks' evolution in terms of the danger they pose, from the first hooligan cyberattacks to modern cyberwars. The authors use empirical qualitative and quantitative research methods to assess the stages of cyberattack development, considering their increasing numbers, diversity, and the creation of the malware employed. The paper provides a better understanding of the causes, conditions, and consequences of the emerging types of cyberattacks. The article concludes by pointing out the three stages in the evolution of cyberattacks and draws upon the main characteristic features of the current state of the cyber environment.

Keywords: critical infrastructure; cybercrime; cyber espionage; cyber terrorism; hacker groups; malware

Resumen. Este trabajo tiene como objetivo estudiar las principales etapas de la evolución de los ciberataques en cuanto a su peligrosidad, desde los primeros ciberataques gamberros hasta las ciberguerras modernas. Los autores utilizan métodos empíricos de investigación cualitativa y cuantitativa para evaluar las etapas del desarrollo de los ciberataques, teniendo en cuenta su incremento, su diversidad y la creación del malware empleado. El artículo permite comprender mejor las causas, las condiciones y las consecuencias de los nuevos tipos de ciberataques. El artículo concluye señalando las tres etapas de la evolución de los ciberataques y extrae los principales rasgos característicos del estado actual del ciberentorno.

Palabras clave: ciberdelincuencia; ciberespionaje; ciberterrorismo; grupos de hackers; infraestructuras críticas; malware

Section: Dossier • Scientific and technological research article

Received: November 30, 2021 • Accepted: March 6, 2022

Contact: Yuriy Yu. Nizovtsev ✉ nizovtsev8218@sci-univ.com

Introduction

Over the last few decades, information technologies have become especially developed and deeply integrated into almost all spheres of life, including entertainment, day-to-day life, production, finance, security, and defense. Naturally, criminals have not been oblivious to this progress in digital technologies, interfering in the work of automated information systems (cyberattacks) using various methods, including malicious software. The evolution of cyberattacks has advanced progressively, and the danger of these attacks has increased. The current scale of criminal acts in cyberspace has acquired the characteristics of real wars, providing a basis for considering these actions cyberwars by criminal hacker groups.

Scholars like Henley and Solon (2017), Denyer (2021), Von Neumann (1966), Hold (2010), Holovko (2017), Eaton and Volz (2021), Bakhur (2017), Parfylo (2016), and Woods and Weckler (2017), among others, have dedicated their works to the issues of countering cybercrime, including the investigation of crimes related to the use of malicious software. Nonetheless, the issues of cyberattacks' evolution still lack research. The increasing degree of their danger is a marked concern in modern studies.

There are several views on the origin of cyberattacks and how they have developed, including the use of malicious software. For example, some scholars consider that the first key stage began in December 1949, when John von Neumann (1966) gave a series of lectures at the University of Illinois on the *Theory and Organization of Complex Automata*. The materials of these and other lectures between 1948 and 1952 would form the basis of the theory of self-reproduction of automata and self-reproduction of certain classes of malicious programs. It was mainly students of North American universities who created the first malicious software, primarily distributing it through infected floppy disks (floppy disk drives). As a rule, these programs were created for research purposes or self-affirmation (hooligan motives). The best-known malware at the time included Brain, created in 1986; Lehigh, Stoned, and Jerusalem in 1987; the Morris Worm in 1988; and Michelangelo in 1991.

With time, cyberattacks began to acquire a commercial character, an illegal activity whose main purpose was for profit. Thus, a malware market emerged, where malware was sold or rented through specialized closed Internet resources. At the same time, the following types of malware were becoming increasingly widespread: extortionware, spyware, denial of service attacks software, adware, and spamware, among others. Recently, malware has begun to be used as a weapon (*cyber weapons*) in so-called cyberwars (Nuklearlord, 2012a), involving operations commonly referred to as cyberattacks or cyber diversions. The use of the malicious software, Stuxnet, is considered the first known case of cyber diversion (Nuklearlord, 2012b). Other software tools that appeared later, which accord-

ing to experts, can be attributed to *cyber weapons*, included Duqu, Wiper, Flame, Gauss, MiniFlame, Madi, Shamoon, and Narilam.

However, cyberattacks are no longer aimed at merely obtaining illegal material gains. Instead, they now aim to discredit specific firms or even country governments by exposing their alleged incompetence and weakness. The example here can be the cyberattack carried out by a Russian hacker group known as "Sandworm." This attack caused the world's first confirmed case of a power grid failure when the whole region was left without electricity (80 thousand households in total) (Inshyn et al., 2021).

New opportunities for criminal activity in the cyber environment, the increased intensity of cyberattacks, and the threats they pose to businesses and individual states' national security contribute to the relevance of the issue under research. This paper aims to analyze the main stages in the evolution of cyberattacks in terms of the danger they pose and better understand the causes, conditions, and consequences of the emerging types of cyberattacks.

Evolution of a cyberattack: analyzing the first and second stages

The first epidemic was caused by the Brain virus (also known as the Pakistani virus) in 1987. Its developers were the brothers, Amdjat and Basit Farooq Alvi. According to McAfee data, the virus has infected more than 18 thousand computers in the United States (The first article.., 1988). However, it did not perform destructive actions (Yefymenko, 2007); the program was written to determine the level of piracy in Pakistan. The virus infects the boot sectors, changes the disk label to *(c) Brain*, and leaves messages with the names, addresses, and telephone numbers of the authors. Its distinctive feature is the substitution of the infected sector with an uninfected original at the time of contact. Thus, the Brain can be called the first known stealth (invisible) virus. Within a few months, the program spread beyond Pakistan, and the epidemic reached global proportions by the summer of 1987.

The Lehigh virus was among the first destructive viruses. In 1987, it caused a mass infection of computers at Lehigh University (USA). Later, such phenomena would be called epidemics by analogy with biological viral diseases. The virus only infects the COMMAND.COM system files and is programmed to delete all the information on the current disk. The contents of hundreds of diskettes from the University library and students' personal diskettes were destroyed within a few days. All in all, about 4,000 computers were infected during the epidemic. However, Lehigh did not spread beyond the University (Novikovas et al., 2017).

The Suriv family of memory-resident file viruses, detected in 1987, was created by an unknown Israeli programmer. The most famous modification, Jerusalem, gave rise to

a global viral epidemic, the first real pandemic caused by an MS-DOS virus. Suriv viruses download code to a computer's memory, intercepting file operations and infecting COM and EXE files initiated by a user. This feature ensures the almost instantaneous spread of the virus on mobile data storage devices, at that time, floppy disks. Jerusalem differs from its predecessors by an additional destructive feature –the destruction of all running programs on Friday, the 13th. On the black date of May 13, 1988, the computers of many commercial firms, government agencies, and educational institutions, primarily in the United States, Europe, and the Middle East, became inoperable simultaneously.

On November 2, 1988, Robert Morris, a post-graduate student in the Department of Computer Science at Cornell University, released his worm. In less than a day, the worm spread to 6,000 machines –10% of the Internet at the time. It disabled many servers and users' computers connected to the network (Zobnin, 2015). This was the first case of mass infection via the Internet in history. The Morris Worm applied the following techniques simultaneously to penetrate 4BSD and Sun 3 systems: the Remote Shell Protocol (RSH), the sendmail email transfer agent, and the finger network protocol. The first one came into play when one of the users' passwords was cracked on the already infected machine; the worm would then try to use the same login and password on a remote machine. Infection via sendmail occurred by exploiting a vulnerability in the debug code. Simply connected to the server via SMTP, the worm would give the DEBUG command, pass the source code to its *head,* and the command to run and compile instead of the filling command in the FROM and DATA fields. The worm gained access to the system via finger due to a vulnerability in the gets function of the libc library, which was used by the daemon to read a request from a remote machine. The worm passed 536 bytes to the daemon, provoking a stack failure and transferring the shell code control.

In all three cases, the worm ran the netstat command, read the /etc/hosts file, and searched for neighboring machines on the network in other ways. It would then read the /etc/passwd file and its extracted password hashes and try to find passwords using an internal 432-word database, the /usr/dict/words file, and its own high-performance DES algorithm implementation. Then, the operation was repeated for other hosts. The total damage caused by the Morris Worm was estimated at $96.5 million. After confessing, Morris was sentenced to three years' probation, a fine of $10,000, and 400 hours of community service.

Launched in June 1994, OneHalf is a very complex resident file-loading polymorphic virus that caused a global epidemic, including in Ukraine. Depending on the modification, the OneHalf infects boot sectors of disks and COM/EXE files, increasing their size by 3544, 3577, or 3518 bytes. The last two unencrypted hard disk cylinders are encrypted each time the infected computer is restarted. This process continues until the entire drive is encrypted. The built-in stealth procedure allows the virus to decrypt on the

fly while requesting encrypted information. Consequently, the user will not notice anything suspicious for a long time. The only visual manifestation of the virus is the message, "Dis is one half. Press any key to continue..." This message is displayed on the screen when the number of encrypted disc cylinders reaches half their total number. However, when attempting to treat or after healing the disk's boot sectors, all the information on the disk becomes inaccessible and unrecoverable.

In June 1998, the Win95.CIH virus of Taiwanese origin was detected. It contains a logic bomb to destroy all information on hard drives and damage the BIOS contents on some motherboards. Because the program activation date (April 26) coincided with the date of the accident at the Chernobyl nuclear power plant, the virus received a second name, Chernobyl. The scale of the epidemic came to light on April 26, 1999, when according to various estimates, half a million computers worldwide were affected. The total damage was hundreds of millions of dollars. The epidemic center was South Korea, where more than 300,000 computers were infected.

After these first cyberattacks, this area of illegal activity was commercialized and used for profit. This change was followed by the emergence of a market for malware sold or rented, usually through specialized closed Internet resources. New centrally managed infected computers (so-called botnets) networks are also being sold or leased (Kozlovskyi et al., 2019). Moreover, extortionware, spyware, denial of service attacks software, adware, and spamware, among others, are becoming increasingly widespread.

Ransomware, on the other hand, blocks or significantly complicates the user's ability to work on the computer, requiring a ransom to unlock the computer. Currently, there are several radically different approaches to the work of extortionware, which involves file encryption in the system, blocking or interfering with the system's operation, and blocking or interfering with the Internet browser's work. Spyware is secretly installed on a user's computer, secretly transmitting certain types of information to its server. Spyware can serve a variety of purposes, both harmless and very dangerous (Antoniuk et al., 2018). An example of the former can be collecting particular programs' statistics to transmit them to developers to improve these programs. The authors' example of very dangerous ones includes receiving payment card details and client bank login credentials and transmitting them to the server.

A Denial-of-Service attack (DoS attack) involves interfering with the work of automated information systems; a successful implementation leads to the complete or partial inability of the mentioned systems to perform their functions (provide declared services). If such an attack is implemented from several sources simultaneously, it is called a distributed attack (DDoS attack, Distributed Denial-of-Service). DoS attacks are usually carried out to make the attacked system's resources inaccessible to legitimate users. The predicted consequences of these attacks include the inability to make payments via the Internet, loss

of the attacked resource owner's image of the attacked hosting's owner, and replacing the blocked resource with a *fake* one. Business competitors often commit such actions to gain market advantage, or criminals to demand ransom to stop the attack.

Programs for remote DoS attacks can have a graphical interface and operate with the user's knowledge. The best-known program of this kind is LOIC, an acronym for Low Orbit Ion Cannon or low-orbit ion gun. However, the software secretly installed on an infected computer, becoming part of a botnet, is used more often. A botnet (robot and network) is a computer network consisting of several hosts with running bots –standalone software. Most often, a bot in a botnet is a malicious program secretly installed on the victim's computer, allowing an attacker to perform specific actions using an infected computer's resources (Levchenko & Britchenko, 2021). An infected computer itself is often called a bot. Bots are usually used for illegal activities such as sending spam, retrieving passwords on a remote system, DoS attacks, obtaining users' personal information, and stealing credit card numbers and passwords. Among the largest known botnets is BredoLab, created in 2009 with about 30,000,000 bots, and Mariposa, created in 2008 with 12,000,000 bots.

Adware (from ad or *advertisement*) operation displays advertising. In some cases, this advertising can be useful. For example, when the developer inserts an ad to the program for advertiser discounts, and the user receives the program for free. However, the advertising program is often installed on the computer without the user's permission, most often even without the user's knowledge. Sometimes, the advertising displayed is so intrusive that it interferes with the work on the computer. Spam is the mass distribution of advertising or other correspondence to people who have not expressed a desire to receive it. The term *spam primarily* refers to promotional emails. Specialized programs designed for mass email sending are usually used for spam mass mailing. However, it is impossible to separate the legal program intended for sending mail and the malicious program intended for sending spam, as the harmfulness of distribution is determined by the recipients' authorization of this distribution.

Recently, malware has begun to be used as a weapon (*cyber weapons*) in so-called cyberwars (Nuklearlord, 2012a), some of its operations commonly referred to as cyberattacks or cyber diversions. These publications' format does not provide the specific actions' exact criminal and legal qualifications; their designations (cyber-terrorist attack or cyber sabotage) are approximated. The use of Stuxnet malicious software is considered the first known case of cyber diversion (Nuklearlord, 2012b). In late September 2010, it was discovered that the Stuxnet virus had caused serious damage to Iran's nuclear program. Exploiting operating system vulnerabilities and the infamous *human factor*, Stuxnet successfully affected 1,368 out of 5,000 centrifuges at the Natanga uranium enrichment plant and disrupted the Bushehr nuclear power plant launch. The client is still unknown.

However, many experts consider the United States and Israel as the developers and implementers of this cyber diversion (Nuklearlord, 2012b; Khlapkovskyi, 2016; Holovko, 2017; Stuxnet virus delivers…, 2010). The perpetrator was a negligent Siemens employee who installed an infected flash drive in the workstation. The damage to Iran's nuclear facilities could be compared to an attack by the Israeli Air Force (Hold, 2010).

After accessing the control system of the uranium enrichment centrifuges, the Stuxnet malware changed the centrifuges' normal mode of operation. As a result, they were either accelerated to a critical speed or suddenly decelerated. However, the reading on the screen showed the operator a normal mode of centrifuge operation. Continuous work in these extreme conditions led to the rapid failure of several centrifuges. It should be objectively noted that some sources deny the effectiveness of Stuxnet's harmful effects (Stuxnet and Iran…, 2010).

In terms of applied technologies, Stuxnet is an extremely high-tech and original solution in which the human factor is minimized in its application. Its characteristic feature is a thorough check of the affected automated information system. If the system found is not the targeted, the malicious program self-destructs without causing any harm to the affected system. This feature is not typical of *common* malware, one of the reasons why intelligence agencies have considered developing Stuxnet. Several other software tools subsequently appeared, which, according to experts, can be considered *cyber weapons*, including Duqu, Wiper, Flame, Gauss, MiniFlame, Madi, Shamoon, and Narilam.

Cyberattacks, a threat to a state's national security: third-stage qualitative and quantitative study

According to the authors, greater attention was given to the world's first confirmed case of power grid failure resulting from a cyberattack in Ukraine in December, when the Ivano-Frankivsk region was left without electricity (80 thousand households) due to outside interference in the operation of power grid facilities (Hubenko, 2016). The Security Service of Ukraine reported the detection of malicious software in the computer networks of some oblenergos (Prykarpattiaoblenergo, Kyivoblenergo, and Chernivtsioblenergo), accusing Russian criminal hacker groups of its distribution (SBU Press Service, 2015). Experts from US government agencies (State Department, Department of Energy, Department of Homeland Security, and the FBI) later joined the investigation, confirming the involvement of Russian hackers in the information attack (Perez, 2016). It was found that BlackEnergy malware was used in the attack carried out by a Russian hacker group known as *Sandworm*. Altogether, the cyberattack consisted of five elements: infecting networks with fake emails; obtaining control of the automated control system by disabling substations; decommissioning uninterruptible power supplies, modems, switchboards, and oth-

er IT infrastructure; destroying information on servers and workstations (using KillDisk utility); and attacking through call center telephone numbers (from Russian numbers) to deny energy services to subscribers (Interfax Ukraine, 2016).

On June 27, 2017, an unknown malware attacked many private and public companies in Ukraine, including banks (Cyberattack in Ukraine…, 2017). On that day, the National Bank of Ukraine warned other banks and financial sector industries about an external hacker attack by an unknown virus on several Ukrainian banks and some enterprises of the commercial and public sectors (National Bank of Ukraine, 2017). According to Microsoft, a total of 12.5 thousand computers in the country were affected by the virus (Microsoft Defender Security Research Team, 2017). Among the affected organizations were the Ukrzaliznytsia, Boryspil International Airport, Kyiv International Airport (Zhuliany), Epicenter, Nova Poshta, DTEK, Ukrenergo, Kyivenergo, Kyivvodokanal, Kyiv Metro, Antonov state enterprise, Document state enterprise, all national GSM mobile operators (Lifecell, Kyivstar, and Vodafone Ukraine), banks (Oschadbank, Ukrsotsbank, Ukrgasbank), and many others. State bodies also suffered an attack, particularly the Ukrainian Cabinet of Ministers and Ministry of Finance, and the website of the Lviv City Council, among others (Zakharov, 2017).

On the evening of May 27, 2017, the Cyber Police Department of the National Police of Ukraine published that *M.E.doc.* software (for reporting and document management) updates were used to spread the NotPetya malware (Parfylo, 2016; Cyberpolice…, 2017). This information was later confirmed by experts from the ESET anti-virus laboratory (Bakhur, 2017), Cisco Talos (Chiu, 2017), and Microsoft (Microsoft Defender Security Research Team, 2017). It should be noted that a month before the described events, the Cyberpolice Department warned the *M.E.doc.* program developers about their system's existing vulnerabilities, but the latter did not respond (Channel 24, 2017). *M.E.doc.* Software is widely used for document circulation and reporting in Ukraine. This explains the extremely fast and massive spread of NotPetya malware on the computers of Ukrainian organizations. According to ESET, almost 80% of all NotPetya virus infections occur in Ukraine (Bakhur, 2017). It should be noted that the update server of the *M.E.doc.* Program was hosted by the WNet Internet provider (Medium.com, 2017), whose unreliability in terms of information security was reported by the SSU shortly before the described events (Security Service of Ukraine, 2017; Kapustynska, 2017).

Specialists from the Kaspersky Lab (Ivanov & Mamedov, 2017) and Comae Technologies researcher Matt Suiche (2017) have concluded that it is generally incorrect to call NotPetya a cryptographer. The fact is that this malware is essentially designed to destroy information. It is almost impossible to restore the affected data. This is not a mistake; it is the malware's authors' intention. Therefore, NotPetya should be called a Wiper.

In general, the cyberattack was conducted as follows. Having accessed the hosting of the *M.E.doc.* program update server, the attackers introduced the NotPetya malicious software into the next update package. During the M.E.doc. Program's automatic update, NotPetya malware was downloaded to the computers being updated. NotPetya encrypted the media (hard drives) on the affected computers blocking access to them.

At first glance, the NotPetya malware cyberattack looked like an attack by *ordinary* cybercriminals with selfish motives to make money by extortion. It was only during a thorough investigation involving both domestic and foreign experts that it was established that this cyberattack was, in fact, large-scale cyber sabotage or cyberattack planned and carried out by a criminal hacker group (or association of such groups). It is important to consider the algorithm of operation of this malicious software in more detail.

Once on the computer, the NotPetya malware determines whether Kaspersky, Norton, or Symantec antivirus is running, disabling the antivirus when detected. After identifying and disabling the antivirus, NotPetya encrypts the data on the disk (files with the extension 3ds, 7z, accdb, ai, Asp, Aspx, avhd, back, bak, c, cfg, conf, cpp, cs, ctl, dbf, Disk, djvu, doc, docx, dwg, eml, fdb, gz, h, hdd, kdbx, mail, mdb, msg, nrg, ora, ost, ova, ovf, pdf, php, pmf, ppt, pptx, pst, pvi, py, pyc, rar, rtf, sln, sql, tar, vbox, vbs, vcb, vdi, vfd, and vmc). Then, it deletes the MBR (the original MBR is stored in the 0x22 disk sector and is encrypted using the XOR bitwise operation encoding *with* key *0x7*) and cleans the logs to hide traces of its actions as much as possible (Nesterenko, 2017). If the process has administrative privileges in the operating system, then, before replacing the MBR, the encryptor checks for the file called perfc (or another empty file with a different name) without extension in the directory C:\Windows\ (the directory is specified in the code). This file has the same name as the dll library of this encryptor, without the extension. The presence of such a file in the specified directory can be one of the indicators of compromise. If the file is present in this directory, then the malware execution process is completed (thus, creating a file with the correct name can prevent MBR substitution and further encryption). If the encryptor does not detect such a file during the check, the file is created, and the process of executing malicious software is started. This action is probably to prevent the MBR replacement process from restarting. On the other hand, if the process does not have administrative privileges from the very beginning, the encryptor will not be able to check for an empty file in the C:\Windows\ directory, and the file encryption process will still start without replacing the MBR and restarting the computer.

After starting the malicious file, a task to restart the computer with a 1 to 2-hour delay is created. Thus, there is time to run the bootrec / fixMbr command to restore the MBR and the operating system. Accordingly, it is possible to start the system even after it has been compromised, but it will not be possible to decode the files. A unique

AES key is generated for each disk, which remains in the memory until encryption is complete. Then, it is encrypted on the RSA public key and deleted. Recovering content after completion requires knowledge of the private key, without which it is impossible to recover data. The malware likely encrypts files to a maximum depth of 15 directories; files at greater depths are secure. If the disks were successfully encrypted after the reboot, a window with a message asking to pay a ransom of $ 300 (as of June 27, 2017, approximately 0.123 bitcoins) to obtain the key to unlock the files is displayed. Bitcoin wallet 1Mz7153HMuxXTuR2R1t78mGSdzaAtNbBWX is specified for money transfer.

NotPetya uses TCP ports 135, 139, and 445 (using SMB and WMI services) to spread. Spreading to other hosts on a network occurs in several ways. They include Windows Management Instrumentation (WMI), PsExec, and the MS17-010 (EternalBlue) vulnerability exploit. WMI is a technology to manage and monitor different parts of the Windows-based infrastructure centrally. PsExec is widely used for Windows administration and allows running processes on remote systems. However, running these utilities on the victim's computer requires local administrator privileges, which means that NotPetya can spread only from computers on which users have maximum operating system privileges. The EternalBlue exploit enables maximum privileges on an affected system. The encryptor also uses the publicly available Mimikatz utility to obtain credentials of all Windows users in plaintext, including local administrators and domain users. This toolkit allows NotPetya to spread even in infrastructures where the lessons of WannaCry were considered. This feature makes the encryptor very effective (Everything that you…, 2017).

NotPetya possesses functionality that allows it to spread to other computers in an avalanche-like process. It enables the encryptor to compromise the domain controller and attain control over all domain nodes, which fully compromises infrastructure. It should be noted that the NotPetya attack was not limited to Ukraine. Other countries also suffered huge losses. The malware has been used in Germany (9.06% of attacks), Poland (5.81%), Serbia (2.87%), Greece (1.39%), and Romania (1.02%). In Russia and the Czech Republic, it has accounted for less than one percent of all virus attacks (Stogniy, 2017). In the Russian Federation, the computers of Rosneft (NTV, 2017) and Bashneft (Russia was attacked…, 2017) stopped working almost simultaneously with Ukraine, resulting in the cessation of oil production at several sites.

Following Ukraine and Russia, attacks on networks began to be carried out in Spain, India (Griffin, 2017), Ireland, Great Britain (Woods & Weckler, 2017), and other countries and cities of the EU and the USA (Henley & Solon, 2017). According to Mcafee, more infected computers were recorded in the United States than in Ukraine. However, ESET (2017) antivirus statistics show that the highest number of recorded infections occurred in Ukraine.

On December 13, 2020, the information about a large-scale cyberattack against thousands of governmental and non-governmental institutions in the United States was released. The cyberattack began no later than March of that year. The attackers exploited software vulnerabilities of at least three software developers in the United States, including Microsoft, SolarWinds, and Vmware (Menn, 2020; Krebs, 2020). A supply chain attack on Microsoft cloud service provided attackers with a way to hack victims, depending on whether the services were purchased from an intermediary. The supply chain attack also struck the users of Orion *SolarWinds* IT *monitoring* and *management* tools, widely used by the U.S. Government and industry. Microsoft software vulnerabilities and VMWare allowed attackers to access emails and other documents to perform federated authentication of victims' resources using *Single Sign*-On (*SSO*) technology (Cimpanu, 2020).

The attackers embedded their own module (FireEye experts called it "Sunburst") in the Orion system, which opened a *backdoor* to the victims' computer networks (Goodin, 2020). Up to 200 organizations around the world were attacked. Most of them were US Government agencies and American companies; however, NATO, the UK Parliament, and the European Parliament were also affected (Gallagher & Donaldson, 2020).

On May 7, 2021, Colonial Pipeline, an American oil pipeline system, suffered a cyberattack, which shut down all its pipelines (Bing & Kelly, 2021). Given the scale of the cyberattack, the *President* of the *United States,* Joe Biden, declared a state of emergency (Suderman & Tucker, 2021). The Colonial Pipeline system delivers gasoline, diesel, and avgas from Texas to New York. This pipeline network supplies ~ 45% of the fuel consumed on the east coast of the United States. The attack came amid growing concerns about the infrastructure's vulnerability to cyberattacks, revealed after several high-profile attacks, including the hacking of SolarWinds in 2020, which affected several government agencies, including the Pentagon, the *Department of the* Treasury, the *Department* of *State,* and the Department of Homeland Security.

On May 6, within hours of the attack, the company paid hackers five million in cryptocurrency to restore operations. After the payment, the hackers gave the operator a data decoder. However, it was very slow, and the company had to use its own backups. A state of emergency was declared on May 9, 2021, due to a pipeline shutdown. The fuel tanks' supply was arranged, but their capacity was insufficient. A regional emergency was declared for 17 states and Washington, D.C. Moreover, the Federal Government lightened traffic of motorized transportation on highways to stabilize fuel supplies from Texas. By May 12, the Colonial Pipeline website was down. On May 13, the pipeline resumed operations; however, it took several days for the company to return to standard operation. On May 19, company representatives confirmed the payment to hackers. According to the CEO, Joseph Blount, the company paid them $ 4.4 million (Eaton &

Volz, 2021). The U.S. Department of Justice eventually recovered most of the ransom (Mallin & Barr, 2021).

Cyberattacks should also be considered against the backdrop of the COVID-19 global pandemic. For example, according to South Korean intelligence services, in 2021, hackers from the Democratic People's Republic of Korea (DPRK) attacked the Pfizer pharmaceutical company to steal confidential information concerning vaccines. They also stated that the number of cybercrimes from Pyongyang had increased by 32% over the past year. North Korea has not yet reported a single case of coronavirus in the country. In 2020 alone, North Korean criminals tried to reach at least nine medical organizations, including Johnson & Johnson, Novavax Inc., and AstraZeneca (Denyer, 2021).

Hackers from China also demonstrate considerable activity. The main area of their activity remains cyber espionage. Accordingly, in 2021, Chinese hackers *hacked* the Microsoft email service. It was established that the target included the data of research centers for the study of infectious diseases, law firms, universities, and companies. In addition, small businesses, municipal governments in several cities, and local governments were also affected, with a total of more than 20,000 organizations in the United States and tens of thousands worldwide. Microsoft claims that the cyberattack was probably carried out by attackers from China (BBC News, 2021).

Conclusion

The authors conclude that the danger of cyberattacks increases over time due to the anticipated attack results, the intensive integration of information technology into various spheres of life, and the possibility of influencing these areas through information technology.

The evolution of cyberattacks can be divided into three stages. In the first stage, cyberattacks were not directed against something or someone specific. They either did not have destructive functions, or these functions were insignificant and usually limited to data deletion. The purpose of those first cyberattacks was usually research or the desire for self-affirmation (hooligan motives). The emergence of specific cyberattack targets (Internet banking client apps and bank card payment data, among others) characterized the second stage. The very purpose of cyberattacks acquired clear selfish motives, resulting in significant financial losses. Cyberattacks were actually becoming a kind of criminal business.

The third stage is considered the most dangerous. The current state of global implementation of computer technology creates new opportunities for criminal activity in the cyber environment. As a result, the intensity of cyberattacks has increased significantly. Five to 10 years ago, casual hacker attacks for illegal enrichment were common.

Nowadays, the subject of discussion is true cyberwars by criminal hacker groups. The purpose of cyberattacks is no longer limited to simply obtaining direct illegal material benefits.

Often the purpose of a cyberattack is to discredit specific firms or entire countries (their governments) by revealing their alleged incompetence and weakness. The objects of cyberattacks can be critical infrastructure enterprises, whose shutdown would be critical on a national scale. On a regional or even global scale, the incident can potentially lead to man-made environmental disasters whose consequences can be compared with the Chernobyl disaster (with numerous casualties and significant material losses).

Thus, the danger of modern cyberwars of criminal hacker groups poses a threat not only to small, medium, and large businesses but also to the national security of individual states or even the security of the international community as a whole. It should be noted that cybercrime has no borders, and it is possible to combat it only by joining the efforts of law enforcement agencies and special services of all developed countries.

Disclaimer

The authors declare no potential conflict of interest related to the article.

Funding

The authors do not report sources of funding for this article.

About the authors

Yuriy Yu. Nizovtsev has a Ph.D. in Law. He is a Leading Researcher at the Research Laboratory of the Center for Forensic and Special Expertise Ukrainian Scientific and Research Institute of Special Equipment and Forensic Expertise of the Security Service of Ukraine. He researches cyber wars, cyber security, and the cyber environment.

https://orcid.org/0000-0001-7398-0327 - Contact: nizovtsev8218@sci-univ.com

Andrii M. Lyseiuk has a Ph.D. in Law. He is an Associate Professor at the Ukrainian Scientific and Research Institute of Special Equipment and Forensic Expertise of the Security Service of Ukraine. He has authored approximately 50 scientific works. His research interests include cyberattacks, national security, and forensic expertise.

https://orcid.org/0000-0002-1010-9566 - Contact: lyseiuk8218@edu.cn.ua

Mykhailo Kelman has a Ph.D. in Legal Science. He is a Professor at the Department of Educational and Scientific Institute of Law and Psychology Lviv Polytechnic National University, Ukraine. His research interests include countering cybercrime, international security, and human law.

https://orcid.org/0000-0002-7414-984X - Contact: kelman8218@neu.com.de

References

Antoniuk, L., Britchenko, I., Polishchuk, Y., Rudyk, N., Sybirianska, Y., & Machashchik, P. (2018). Code of ethics for SMEs: Substantiating the necessity and willingness to implement in Ukraine. *Problems and Perspectives in Management, 16*(3), 150-162. https://doi.org/10.21511/ppm.16(3).2018.12

Bakhur, V. (2017, June 28). *ESET: the source of the Petya.C outbreak was the compromised M.E.Doc*. C-News. https://safe.cnews.ru/news/line/2017-06-28_eset_istochnikom_epidemii_shifratora_petyac_stalo

BBC News. (2021, March 6). *Chinese Hackers Hacked Microsoft's Email Service. White House says Thousands of Organizations Remain at risk*. https://www.bbc.com/russian/news-56309038

Bing, C., & Kelly, S. (2021, May 27). *Cyber attack shuts down U.S. fuel pipeline 'jugular,' Biden briefed*. Reuters. https://www.reuters.com/technology/colonial-pipeline-halts-all-pipeline-operations-after-cybersecurity-attack-2021-05-08/

Channel 24. (2017, July 5). *The police explained why the Petya.A virus was spread through M.E.Doc*. 24tv. https://24tv.ua/ru/v_policii_objasnili_pochemu_virus_petyaa_rasprostranili_imenno_cherez_medoc_n837954

Chiu, A. (2017, June 27). New ransomware variant "Nyetya" compromises systems worldwide. *Cisco Talos Intelligence*. https://blog.talosintelligence.com/2017/06/worldwide-ransomware-variant.html

Cimpanu, C. (2020, December 18). *NSA warns of federated login abuse for local-to-cloud attacks*. ZDNet. https://www.zdnet.com/article/nsa-warns-of-federated-login-abuse-for-local-to-cloud-attacks/

Cyberattack in Ukraine. Chronicle is completed. (2017, June 29). Ligue.Business. http://biz.liga.net/all/it/novosti/3696331-v-ukraine-proiskhodit-globalnaya-kiberataka.htm

Cyberpolice: Infection with Petya is due to M.E.Doc. Electronic Document Management System. (2017, June 27). Gordonua.com. http://gordonua.com/ukr/news/localnews/-kiberpolitsija-zarazhennja-virusom-petya-stalosja-cherez-sistemu-elektronnogo-dokumentoobigu-m-e-doc-194997.html

Denyer, S. (2021, February 16). *North Korea tried to steal Pfizer Coronavirus Vaccine Information, South says*. Washington Post. https://www.washingtonpost.com/world/asia_pacific/north-korea-pfizer-coronavirus-vaccine-hack/2021/02/16/c09ec7fc-702e-11eb-8651-6d3091eac63f_story.html

Eaton, C., & Volz, D. (2021, May 19). *Colonial Pipeline CEO tells why he paid hackers a $4.4 million ransom*. The Wall Street Journal. https://www.wsj.com/articles/colonial-pipeline-ceo-tells-why-he-paid-hackers-a-4-4-million-ransom-11621435636

ESET. (2017, June 28). "Petya" Ransomware: What we know now. *ESET North America.* https://www.eset.com/us/about/newsroom/corporate-blog/petya-ransomware-what-we-know-now/

Everything that you Wanted to know about NotPetya but were Afraid to ask. (2017, June 28). Positive Technologies. https://www.ptsecurity.com/ru-ru/about/news/283092/

Gallagher, R., & Donaldson, K. (2020, December 14). *U.K. Government, NATO join U.S. in monitoring risk from hack*. BNN Bloomberg. https://ampvideo.bnnbloomberg.ca/u-k-government-nato-join-u-s-in-monitoring-risk-from-hack-1.1536398

Goodin, D. (2020, December 17). *SolarWinds hack that breached gov networks poses a "grave risk" to the nation*. arsTECHNICA. https://arstechnica.com/information-technology/2020/12/feds-warn-that-solarwinds-hackers-likely-used-other-ways-to-breach-networks/

Griffin, A. (2017, June 27). *Huge 'Petya' cyber attack spreading across the world in potential repeat of 'Wannacry' hack.* Independent. https://www.independent.co.uk/life-style/gadgets-and-tech/news/hack-cyber-attack-ukraine-russia-wannacry-petya-security-internet-broken-computer-not-working-a7810626.html

Henley, J., & Solon, O. (2017, June 27). *'Petya' ransomware attack strikes companies across Europe and US*. The Guardian. https://www.theguardian.com/world/2017/jun/27/petya-ransomware-attack-strikes-companies-across-europe

Hold, R. (2010, October 11). *The virus that attacked Iran's nuclear facilities marked the beginning of the era of cyber warfare. Is the world on the brink of an IT military revolution?* Stuxnet: War 2.0. https://habr.com/ru/post/105964/

Holovko, V. (2017). Cyberattacks: Stuxnet Saboteur Virus in Nuclear Power Program of Iran. *Science and Technology, 128*(2), 33-41. https://naukatehnika.com/kiberataki-virus-diversant-stuxnet-v-yadernoj-energeticheskoj-programme-irana-chast1.html

Hubenko, D. (2016). *After the cyberattack on "Prykarpattiaoblenergo," the US Revises the Protection of Energy Grids*. Deutsche Welle. https://p.dw.com/p/1HZXJ

Inshyn, M., Khutoryan, N., Cherneha, R., Bontlab, V., & Tkachenko, D. (2021). Correlation of labor and civil contracts related to the performance of work: Preventing the substitution of concepts. *Employee Responsibilities and Rights Journal, 33*(4), 265-279. https://doi.org/10.1007/s10672-021-09373-3

Interfax Ukraine. (2016, February 12). *The Ministry of Energy Told the Details of the Cyberattack of the Russian Federation*. InfoResist. https://inforesist.org/v-minenergo-rasskazali-podrobnosti-kiberataki-rf/

Ivanov, A., & Mamedov, O. (2017, June 28). *ExPetr/Petya/NotPetya is a Wiper, Not Ransomware*. Securelist by Kaspersky. https://securelist.com/expetrpetyanotpetya-is-a-wiper-not-ransomware/78902/

Kapustynska, K. (2017, June 1). *SBU summed up the searches in Wnet: The Provider Cooperated with the Russian Special Services*. Ukraine Segodnya. https://ukraine.segodnya.ua/ukraine/sbu-podytozhila-obyski-v-wnet-provayder-sotrudnichal-s-rossiyskimi-specsluzhbami-1026305.html

Khlapkovskyi, V. (2016, February 18). *Hack an entire country. Stuxnet virus was part of the US Plan to attack Iran*. rus.DELVI.lv. https://rus.delfi.lv/techlife/detali/vzlomat-celuyu-stranu-virus-stuxnet-okazalsya-chastyu-plana-ssha-po-kibernapadeniyu-na-iran.d?id=47076733

Kozlovskyi, S., Butyrskyi, A., Poliakov, B., Bobkova, A., Lavrov, R., & Ivanyuta, N. (2019). Management and comprehensive assessment of the probability of bankruptcy of Ukrainian enterprises based on the methods of fuzzy sets theory. *Problems and Perspectives in Management, 17*(3), 370-381. https://doi.org/10.21511/ppm.17(3).2019.30

Krebs, B. (2020, December 18). VMware Flaw a Vector in Solarwinds Breach? *Krebs on Security*. https://krebsonsecurity.com/2020/12/vmware-flaw-a-vector-in-solarwinds-breach/

Levchenko, I., & Britchenko, I. (2021). Estimation of state financial support for non-priority territorial units using the example of bridge construction. *Eastern-European Journal of Enterprise Technologies, 1*, 26-34. https://doi.org/10.15587/1729-4061.2021.225524

Mallin, A., & Barr, L. (2021, June 7). *DOJ Seizes millions in ransom paid by Colonial Pipeline*. ABCnews. https://abcnews.go.com/Politics/doj-seizes-millions-ransom-paid-colonial-pipeline/story?id=78135821

Medium.com. (2017, June 29). *M.E.Doc. Update Servers were Hosted by WNet*. Internetua. http://internetua.com/serveri-obnovlenii-M-E-Doc-okazalis-na-hostinge-WNet

Menn, J. (2020, December 17). *Microsoft Says it Found Malicious Software in its Systems*. Reuters. https://www.reuters.com/article/uk-usa-cyber-breach-idUKKBN28R3B7

Microsoft Defender Security Research Team. (2017, June 27). New Ransomware, old Techniques: Petya adds worm capabilities. *Microsoft Security*. https://blogs.technet.microsoft.com/mmpc/2017/06/27/new-ransomware-old-techniques-petya-adds-worm-capabilities/

National Bank of Ukraine. (2017, 27 June). NBU warned banks and other financial sector participants about external hacker attack. https://bank.gov.ua/ua/news/all/nbu-poperediv-banki-ta-inshih-uchasnikiv-finansovogo-sektoru-pro-zovnishnyu-hakersku-ataku

Nesterenko, S. (2017). *The secret of the Petya A virus has been revealed: it is a cyber weapon*. Code analysis. Personal website of Sergii NESTERENKO. https://sergnesterenko.com.ua/ru/tajna-virusa-petya-raskryta-eto-kiberoruzhie-analiz-koda/

Novikovas, A., Novikoviene, L., Shapoval, R., & Solntseva, K. (2017). The peculiarities of motivation and organization of civil defence service in Lithuania and Ukraine. *Journal of Security and Sustainability Issues, 7*(2), 369-380. https://doi.org/10.9770/jssi.2017.7.2(16)

NTV [@ntv.ru]. (2017, June 27) *Powerful attack: A Clone of the WannaCry Virus Spread on Rosneft's Servers* [video]. NTV. https://www.ntv.ru/novosti/1827659/

Nuklearlord (2012a, December 1). *Cyberwar – Stuxnet, Duqu, Flame, Gauss, and all, all, all...* [Online forum post] The Habr. https://habrahabr.ru/post/160973/

Nuklearlord. (2012b, November 17). *Again, about Stuxnet* [Online forum post]. The Habr. https://habrahabr.ru/post/159053/

Parfylo, O.A. (2016). Current Issues of Forensic and Expert Examination of Malicious Software Devices Within the Framework of the Fight Against Cyberterrorism. *Forensic Bulletin, 1*(25), 78-84. http://irbis-nbuv.gov.ua/cgi-bin/irbis_nbuv/cgiirbis_64.exe?C21COM=2&I21DBN=UJRN&P21DBN=UJRN&IMAGE_FILE_DOWNLOAD=1&Image_file_name=PDF/krvis_2016_1_15.pdf

Perez, E. (2016, February 12). *U.S. official blames Russia for power grid attack in Ukraine*. CNN politics. https://edition.cnn.com/2016/02/11/politics/ukraine-power-grid-attack-russia-us/index.html

Russia was attacked by the same computer virus as Ukraine. (2017, June 27). iPress.ua. https://ipress.ua/news/rosiyu_atakuvav_takyy_zhe_kompyuternyy_virus_yak_i_ukrainu_216370.html

SBU Press Service. (2015, 28 December). *Security Service of Ukraine prevented an attempt by Russian Special Services to disable energy facilities in Ukraine*. Economical Truth. https://www.epravda.com.ua/news/2015/12/28/574276/

Security Service of Ukraine. (2017). SBU Exposed the Ukrainian Internet Provider on Illegal Traffic Routing to Crimea in the Interests of Russian Special Services. https://www.sbu.gov.ua/ru/news/134/category/78/view/3451#.zxQtepPG.dpbs

Stogniy, K. (2017, June 30). *Files cannot be retrieved after a Petya virus attack – experts*. Nnovosti.info. https://nnovosti.info/news/vidnoviti_fajli_pislja_ataki_virusu_petya_nemozhlivo_eksperti-18483.html

Stuxnet and Iran: The Mystery of the A26 module. (2010, December 30). Atomic Energy. https://www.atomic-energy.ru/articles/2015/05/06/17237

Stuxnet Virus Delivers Devastating Blow to Iran's Nuclear Program. (2010, December 16). SecurityLab.ru. http://www.securitylab.ru/news/402905.php

Suderman, A., & Tucker, E. (2021, May 8). *Major US pipeline halts operations after ransomware attack*. AP News. https://apnews.com/article/ga-state-wire-business-c6ef4314af911fb58b8445d2b121e82d

Suiche, M. (2017, June 28). *Petya.2017 is a wiper not a ransomware*. Comae Technologies. https://medium.com/comae/petya-2017-is-a-wiper-not-a-ransomware-9ea1d8961d3b

The First Article about Viruses in Russian. (1988, July 26). SecurityLab.ru. http://www.securitylab.ru/former/240714.php

Von Neumann, J. (1966). *Theory of self-reproducing automata.* Completed by Burks, A. W. (Ed.). Urbana and London: University of Illinois Press.

Woods, B., & Weckler, A. (2017, June 27). *Global cyber attack hits IT systems in Ireland and the UK*. Independent.ie. https://www.independent.ie/business/technology/global-cyber-attack-hits-it-systems-in-ireland-and-the-uk-35871179.html

Yefymenko, V. (2007). *Information security management: Viruses and countermeasures.* Saint Petersburg: National Open University "INTUIT."

Zakharov, D. (2017, June 27). Banks and companies that suffered from the cyberattack: A list. ZN.UA. https://zn.ua/ukr/UKRAINE/banki-ta-kompaniyi-scho-postrazhdali-vid-kiberataki-perelik-246826_.html

Zobnin, Ye. (2015). Infectious penguins. The history of program virus writing for *nix systems in numbers. https://xakep.ru/2015/10/20/nix-viruses-history/

Revista Científica General José María Córdova
(Colombian Journal of Military and Strategic Studies)
Bogotá D.C., Colombia

Volume 20, Number 38, April-June 2022, pp. 371-385
https://dx.doi.org/10.21830/19006586.907

Countering the sexual solicitation of children using computer technology: Ukrainian and foreign experience

La tecnología informática contra la captación sexual de menores: La experiencia ucraniana y extranjera

Natalia Semchuk and Sofiia Lykhova
National Aviation University, Ukraine

Neghdana Udalova
Donetsk State University of Internal Affairs, Ukraine

Andrii Lyseiuk
The Ukrainian Scientific and Research Institute of Special Equipment and Forensic Expertise of the Security Service of Ukraine, Ukraine

Olesia Cheban
National Transport University, Ukraine

Abstract. This article assesses the current state of criminal counteraction to the solicitation of children for sexual purposes using digital technologies in Ukraine and the foreign experience in this area. To this end, it uses the traditional legal research method as a basis for research, partially applying other methods such as comparative, historical, and international law. The article analyzes the composition of a criminal offense under Art. 156-1 of the Criminal Code of Ukraine and compares it to the texts of international acts and foreign legislation. The article concludes that the text of the adopted amendments is generally in line with Ukraine's commitments and foreign experience.

Keywords: children; criminalization; digital safety; Lanzarote Convention; online; sexual exploitation; solicitation

Resumen. Este artículo evalúa el estado actual de la lucha penal contra la captación de niños con fines sexuales mediante el uso de tecnologías digitales en Ucrania y la experiencia extranjera en este ámbito. Para ello, utiliza el método de investigación jurídica tradicional como base de la investigación, aplicando otros métodos como el derecho comparado, histórico e internacional de forma parcial. El artículo analiza la estructura de un delito penal según el Art. 156-1 del Código Penal de Ucrania y lo compara con los textos de los actos internacionales y la legislación extranjera. El artículo concluye que el texto de las enmiendas adoptadas se ajusta en general a los compromisos de Ucrania y a la experiencia extranjera.

Palabras clave: captación sexual; Convenio de Lanzarote; criminalización; explotación en línea; niños; seguridad digital

Section: Dossier • Scientific and technological research article

Received: December 1, 2021 • Accepted: March 10, 2022

Contact: Natalia Semchuk ✉ semchuk8094@edu.cn.ua

Introduction

The rapid development of information technology and the benefits of the modern digital world have led to the emergence of new threats in the information sphere. One such threat is the spread of child sexual exploitation on the Internet, where the number of materials containing sexual exploitation of children continues to grow. At present, the world community has to face new challenges with the development of society and modern technologies (Sopilko, 2013). It is also about protecting children in the digital environment. An analysis of current legislation and the state of combating sexual violence against children in Ukraine using electronic devices and systems shows that our society is not ready to confront this negative phenomenon of the modern world comprehensively. Thus, national legislation needs to be closer to the best practices of other countries.

At the end of 2020, the Parliament of Ukraine adopted the bill, *On Amendments to Certain Legislative Acts of Ukraine Concerning the Implementation of the Council of Europe Convention for the Protection of Children against Sexual Exploitation and Sexual Abuse* (Lanzarote Convention). Three hundred and twenty-two deputies out of 450 voted for this decision. The law supplemented the Criminal Code of Ukraine with new articles concerning the *solicitation of children for sexual purposes* and the *conscious access, acquisition, possession, production, or distribution of child pornography* (The Council has implemented..., 2021).

Ukraine has been a party to the Lanzarote Convention since 2012. As noted by Leonov et al. (2020), the imperfection of the legal framework of Ukraine in the field of protection of children from sexual exploitation was identified by the Lanzarote Committee in its first report on December 4, 2015, on the implementation by the states of the Lanzarote Convention. However, the results of a study conducted in 2019 as part of a project to end online sexual exploitation and violence against children in Europe, supported by the Department for the Protection of the Rights of the Child of the Directorate for Combating Discrimination of the Council of Europe, could generate changes in the laws of Ukraine. Their adoption could bring Ukrainian legislation closer to European standards.

Until recently, the digital safety of children in Ukraine had not been given due attention. The State had largely shifted responsibility for children's digital safety to their parents. In fact, the State would merely give the parents recommendations and consider its mission complete. Even now, the State Information Security Strategy does not even mention issues like child pornography, grooming, or sexting. However, at the local level, various organizations have been offering some practical recommendations to combat the sexual solicitation of children for sexual purposes. Resources include the *INSPIRE*

Handbook: Action for implementing the seven strategies for ending violence against children, which has been translated into Ukrainian (WHO, 2019), and The International Telecommunication Union's (ITU) Online Guidelines on Child Online Protection (The International Telecommunication Union, 2020)

This approach is generally appropriate. Research on the prevention of sexual violence against children on the Internet suggests that prioritizing intervention and prevention in this area should be based on a multidisciplinary approach considering medical aspects where all stakeholders involved standardize their activities with clear and consistent goals and objectives (EU Child Online Safety Project, 2020). Given the above, this article aims to assess the current state of criminal counteraction to the solicitation of children for sexual purposes using digital technologies in Ukraine and the foreign experience in this area.

Methodological Framework

Scientific analysis of the problems of criminal law, and Criminal Law in general, were carried out primarily using a dialectical method of cognition, which involves thinking from the concrete to the abstract with a subsequent transition in the other direction, from abstract to concrete. This method was used to select specific legal norms for comparison and the formulation of comparison results. This method was also fundamental in formulating the conclusions. Semchuk et al. (2019) indicate that Legal Science is currently actively searching for new solutions in matters of methodology. Tyler (2017) states that scientific works are often not theoretical but empirical. Theoretical research is better suited to address how certain legal phenomena may function in different conditions at the present stage in Law.

Nolasco et al. (2010) maintain that the most prestigious scientific journals in the field of criminal law focus on articles produced using empirical methods borrowed from other social sciences. According to these authors, legal research, based on the inductive comparison of legal precedents and laws in different conditions, is also a promising area of research that cannot be neglected. Langbroek et al. (2017) contend that court cases and authoritative works of scholars are used in classic legal research to understand the content of formal rules. At the same time, the influence of certain cases is different, and the authority of the scientists involved in the work is not identical. Therefore, the main task of scientific work in jurisprudence is to analyze the available information and formulate it in such a way as to convince other experts in the field of law (Radzivill et al., 2018).

Today in Ukraine, classifying legal methods has its own approach, mainly used in works to expand the theoretical base. Among such methods, the formal-logical one is primarily used. The formal-logical method is a means of research and study of the state and

legal phenomena using the basic laws of formal logic. Induction and deduction form the philosophical basis of this method. Because this study is theoretical and the analyzed subject is the novelty of the legislation whose application is currently non-existent, this was chosen as this work's main method. With its help, we were able to define the conformity of the construction of criminal law norms with formal logic laws and rules. This method was used throughout the work to formulate the study and the conclusions.

The formal-logical method is otherwise called formal-dogmatic or legal. Methodologically, this label is not entirely correct; however, from a practical point of view, it accurately reflects this method's essence. After all, strict observance of the laws of logic is of great importance in constructing legal constructions and revealing legal concepts. The dialectical method is used at all stages of scientific research. The use of this method allows for making scientifically significant conclusions by comparing different points of view on the issue to investigate the phenomenon in its continuous development.

The historical method is used to study the development of the analyzed legal phenomena. It is based on studying the origin, formation, and development of the studied phenomenon in a chronological sequence and in specific historical contexts. The comparative legal method involves comparing similar legal phenomena in different countries and formulating relevant conclusions to provide practical recommendations. This method is used to compare the current rules of law –which may be almost the same at the present stage of widespread international norm application– and the application of these rules by courts with scientific research by scientists from different countries.

The comparative method is used to study the legal phenomena of the Special Part of criminal law, compare the same objects, and establish similarities and differences. Comparing these objects from the point of view of the decision of legal regulation in various legal systems of the criminal legislation revealed the general and the special, both positive and negative. This method allows using the established positive legal regulation on the specified problems to formulate suggestions on improving the current criminal legislation and practice of its application.

Given the above, this article used the traditional legal research method as a basis for research. Other methods, such as comparative, historical, and international law, were also partially applied. However, given that the article, as a whole, is a classic legal study in the field of Ukrainian criminal law, the traditional national tools for analyzing the components of criminal offenses, called *the composition of a criminal offense*, were used. Chorniy (2019) indicates that the elements of the composition of a criminal offense are the crime's object and its objective side; together, they are the objective features of the composition. Together, its subject and subjective side are the subjective features of the composition. Jointly, these objective and subjective features form the composition of the crime.

Results

The Criminal Code of Ukraine (hereinafter - the Criminal Code) adopted by the Ukrainian parliament (Criminal Code of Ukraine, 2001) includes a norm aimed primarily at fulfilling the international obligations undertaken by Ukraine in the framework of the Council of Europe Convention on the Protection of Children against Sexual Exploitation and Sexual Abuse (Lanzarote Convention). This Convention is the first international legal instrument covering preventive measures; criminal offenses, including several entirely new offenses, such as *child grooming*; protective measures and assistance to child victims and their families; *child-friendly* investigation and prosecution procedures adapted to children's specific needs; intervention programs or measures for child sex offenders; data recording and storing on convicted sex offenders; international cooperation; and a monitoring mechanism. According to Articles 18, 20, and 23 of The Lanzarote Convention, each Party shall take the necessary legislative or other measures to criminalize the intentional proposal of an adult, through information and communication technologies, to meet a child who has not reached the age *for sexual activities*, for the purpose of committing *sexual abuse* or *child pornography*, against him or her, where this proposal has been followed by material acts leading to such a meeting (Council of Europe, 2007). Many Ukrainian scholars, including Lykhova et al. (2021), Lasechko et al. (2020), and Akimova et al. (2020), are now pointing to the growing importance of international treaties in amending criminal law.

It should be noted that the parliament adopted this article a few months before it was written. However, given the peculiarities of criminal investigations and criminal trial specifics in Ukraine, no one has been convicted under this article. Thus, it was impossible to interview convicts or victims to analyze this rule's effectiveness. Given this crime's international nature, this work used surveys from foreign research. It also analyzed the foreign experience of more than ten countries on this issue to better understand the essence of such criminal offenses. No works exist by Ukrainian researchers on understanding these criminal offenses in the Ukrainian context. Therefore, a proper theoretical inductive study of this issue was conducted (Orlovskyi et al., 2018). After all, a thorough study of the theory of moldy law enforcement was the basis for improving this article. The absence of the practical aspect in the Ukrainian context does not make the article impractical. On the contrary, this theory is the basis to further law enforcement practice. After all, the traditional way to develop criminal law involves finding the formula according to which practice follows a properly formulated theory. Moreover, the relevant practice formulated will be analyzed in a separate study.

To fulfill the obligation to criminalize such acts, the Ukrainian legislator adopted Article 156-1 CC. This article, entitled *Solicitation of children for sexual purposes*, refers to

criminal offenses against a person's sexual freedom and the sexual inviolability of minors. This article would criminalize an act involving "an offer of a meeting made by an adult, including using information and telecommunication systems or technologies, to a person under the age of sixteen, for the purpose of committing any acts of a sexual nature or lewd acts against him or her, if such an offer was made after such an offer at least one action aimed at making such a meeting take place" (Criminal Code of Ukraine, 2001). In practice, the terms *grooming* and *sexting* are also used for the actions indicated in this article.

The *object of crime* is among the legally protected goods of man and society. In this case, the object of this crime is the sexual inviolability of minors under the age of sexual consent by adult encroachment. Thus, the victim is an obligatory indication of this crime. The victim may be an individual under sixteen; however, the liability for this crime is increased if the victim is under 14 years of age. The objective side of a criminal offense is a set of features that determine the external aspects of the crime. They characterize a socially dangerous act (action or inaction), its negative consequences, the causal link between the act and the consequences that caused the latter, and the place, time, situation, method, tools, and means to commit the crime. From the objective point of view, a crime can be committed only through active action (impossible through inaction). A criminal offense is considered completed from the moment of committing at least one action aimed at achieving a criminal result. The consequences, in this case, are not binding on the offense, so it has a formal composition (Vakulyk et al., 2020).

The legislator also draws attention to one of the types of instruments for committing this criminal offense, computer equipment, information, and telecommunications systems or technologies. However, the construction of the offense does not preclude the commission of this crime using other tools and means (for example, by personal paper correspondence). In this case, a literal citation of Article 23 of the Convention is appropriate because it is the use of information technology that characterizes the vast majority of such encroachments. From the objective point of view, the crime is committed through a meeting proposal, which should be accompanied by at least one action directed at making such a meeting take place. In this case, the meeting, even the conversation, should be understood to involve the use of information and telecommunications systems or technologies.

Communication with a child using information and communication technologies does not necessarily lead to a personal meeting; they can remain merely online encounters. However, even these can cause serious harm to the child. For example, crimes of a sexual nature intentionally committed during online encounters using communication technologies are often associated with the manufacture, possession, and transfer of child pornography. Such actions are provided in part 2 of Art. 156-1 of the Criminal Code and qualified as corpus delicti. However, according to Pollack & MacIver (2015), generally,

the behavior of an offender in one type of crime is not specific at the initial stage, and it is often difficult to distinguish it from the usual behavior of an adult.

De Hart et al. (2016) point out that online chats, bulletin boards, and social networks are the means most often used to commit such offenses. Scientists note that, on average, it takes four days from online acquaintance with a child to a meeting. In this case, communication often includes stages in which the offender asks for photos of the child, talks about sex, requests meetings, and offers to use additional means of communication. De Santisteban et al. (2017) indicate that aggressors study the age characteristics of children for years, understanding their weaknesses and studying social ties in detail. To do this, they use different methods and develop individual strategies. These strategies can be divided into four main groups: aggression, bribery, involvement, and deception. Deception is one of the most common strategies; it involves concealing true intentions and creating an entirely fictional personality to interact with the child. Bribery usually involves offering certain goods and gifts to children. Involvement is based on building emotionally engaged and trusting relationships with the child. Lastly, the perpetrators use aggressive actions to intimidate children after the threat of exposure (Petrov & Serdyuk, 2008).

Thus, we can see that the methods of cyber grooming can be divided into two types: contact (provided for in Part 1 of Article 156-1 of the Criminal Code) and contactless (provided for under Part 2 Article 156-1 of the Criminal Code), aimed at a personal meeting with a child to obtain obscene images of a child. In this case, the subject of this crime, in other words, the criminal, can only be an adult. After all, Article 20 of the Lanzarote Convention does not provide for the interference of sexual interaction between minors by mutual consent. In Ukrainian criminal law, this is called a special subject. The subjective side of the crime is the inner aspect of the crime, that is, the individual's mental activity that reflects the attitude of consciousness and will to the socially dangerous act committed and its consequences. The subjective side of the crime is formed by an individual's following features: guilt, motive, purpose, and emotional state. Under Art. 156-1 of the Criminal Code, the subjective side of the crime is characterized by direct intent. In case of a person's conscientious mistake regarding the victim's age, liability is excluded under Art. 156-1. At the same time, the corpus delicti is available when the offender communicates with a police officer pretending to be a minor.

The purpose is also an obligatory sign of this crime. Part 1 of Article 156-1 of the Criminal Code defines the purpose of committing any acts of a sexual nature or lewd acts against a minor. Part 2 describes the involvement of a minor in the production of child pornography. It should be noted that in the case of cyber grooming, there is a very close relationship between the objective and subjective signs of crime. The nature of this crime can be considered the reason for this. At the beginning of the interaction between an adult

offender and a child, the perpetrator's actions may seem so familiar that they cannot be distinguished from ordinary attention (de Santisteban et al., 2018). However, already at this stage, there is a clear sexual intention to such interaction, not yet obvious to others.

Discussion

The question analyzed in this article has interested scientists from different fields of knowledge and countries for over 20 years. Although the sexual grooming of minors was criminalized in Ukraine just a few months before this article was written, Ukrainian scholars have already produced publications on the subject.

Trifu and Dragoi (2019) analyzed the psychological causes of crimes committed by persons accused at the time of the study of sexual abuse of minors. In their opinion, today's communication conditions significantly enable the communication of sex offenders and children in different countries. Winters and Jeglic (2016) state that pedophiles choose strategies that are initially very difficult to distinguish from ordinary interests. The researchers point out that the behavior of grooming goes largely unrecognized by the participants in the experiment, even at the stages of the process where grooming was easiest to determine.

Nebytov (2015) points out that on November 20, 1989, the United Nations Convention on the Rights of the Child was adopted at the 44th session of the UN General Assembly. Furthermore, according to Article 34 of the Convention, state parties must protect the child from all forms of sexual exploitation and sexual abuse. In addition, the *Optional Protocol to the Convention on the Rights of the Child on the sale of children, child prostitution and child pornography* was adopted on January 18, 2000, in which state parties prohibit child trafficking, prostitution, and pornography. According to Article 3, each state party shall ensure that its criminal or criminal law fully covers such acts and types of activities, regardless of whether they are committed nationally or transnationally, individually or in an organized manner, within the context of trafficking, including the offer, transfer, or receipt of a child by any means for the purpose of sexual exploitation (Yaroshenko et al., 2018).

Leonov et al. (2020) draw attention to the fact that sexual crimes against children using the Internet have ceased to be a national issue of states and are subject to interstate regulation. Europol and Child Sexual Exploitation European Multidisciplinary Platform Against Criminal Threats (EMPACT-Cyber-CSE) play a particularly active role in this process.

Rutai (2020) indicates the measures needed to monitor the implementation of the Lanzarote Convention of Europe. This convention, which protects the rights of the child, is now considered the most comprehensive international instrument dedicated to protect-

ing children from sexual violence in all conditions and spheres of life. It aims to prevent and combat sexual violence against children, protect the rights of child victims, and promote international cooperation between states. Although the Convention does not allow the state parties to narrow the territorial application after the signature, in 2015, Ukraine informed the Secretary-General that the application of all Council of Europe treaties, including the Lanzarote Convention, is limited or not guaranteed in the Autonomous Republic of Crimea and the City of Sevastopol, as well as certain districts of the Donetsk and Luhansk oblasts.

Klimek (2012) stated that most European countries criminalized online grooming in national law by 2012. However, it was only in 2012 that the problem of double European obligations to criminalize the solicitation of children for sexual purposes arose. On the one hand, since 2007, all EU countries have been members of the Council of Europe and have had corresponding obligations according to the Convention on the Protection of Children against Sexual Exploitation and Sexual Abuse. On the other hand, in 2011, the EU adopted the Directive 2011/92/EU on combating the sexual abuse and sexual exploitation of children and child pornography.

As Klimek (2012) indicated, Directive 2011/92/EU contains a list of actions for which the parties should be punished. Among such punishable acts, Article 6 primarily provides for the solicitation of children for sexual purposes. These actions are especially dangerous in the Internet age, which provides users with anonymity and the ability, among others, to hide their age, gender, and place of residence. States are encouraged to criminalize preparing a meeting with a child in the attempt of a crime or preparation for one as a separate criminal offense or a separate form of sexual abuse. States shall take measures to ensure that an adult's offer to meet a child under the age of sexual consent using information technology is punishable if the purpose of the meeting was child pornography or sexual intercourse and if concrete actions accompany the proposal. According to the Directive, a child is a person under 18 years of age. The age of consent in the Directive is interpreted as the age before which, according to the country's national legislation, it is prohibited to have sexual intercourse with adults. The most common age of consent is 16. Thus, it can be considered that the main factor in adopting Article 156-1 of the Criminal Code is the implementation of Ukraine's international obligations. Given that international instruments impose obligations on many countries, we must pay attention to the practice of other states on this issue.

Atabekova and Filippov (2018) indicate that almost all European countries have rules on the solicitation of children for sexual purposes and child pornography. In particular, states establish responsibility for compulsion and sexual abuse of children (Albania, Greece); pornography, solicitation, and compulsion (Croatia, Hungary); prostitution and pornography (Denmark); violence and blackmail (Germany, France); pornography and

solicitation (Latvia); violence, solicitation, child pornography production, and blackmail (Spain); pornography, blackmail/violence, calumny, violation of the secret domain or private domain using a camera, and confinement (Switzerland); and rape, sexual coercion, sexual abuse, solicitation, pornography, and seducement to sexual intercourse (Czech Republic). The Criminal Code of the Republic of Moldova also contains a wide range of punishable acts concerning the sexual integrity of minors.

The first European country to adopt strict legislation on combating the sexual abuse of children was the United Kingdom. Sexual grooming of minors has been a criminal offense in Britain since 2003. Norway and the Netherlands were the first to support the UK's initiative to criminalize the sexual grooming of minors. In Norway, the relevant legislation was adopted in 2007, and in the Netherlands in 2010. Outside of Europe, Australia and the United States were the first to criminalize grooming. In countries without a specific criminal ban on non-online grooming, law enforcement agencies apply general rules on crimes against sexual freedom and inviolability to such actions (Klimek, 2012).

Pollack and MacIver (2015) indicate that in the United States, section 2422 of the Criminal Code criminalizes the use of interstate trade to unlawfully influence persons under the age of 18 to involve them in prostitution or other sexual conduct that may be considered a crime. Karthi and Ramu (2020) studied India's fight against child pornography. Section 67B of its Law on Information Technology of 2008 states that child pornography is recognized as an information crime. This section penalizes images of children performing sexual acts, creating digital images or text containing child pornography, or advertising materials of this nature, promoting violence against children online, encouraging children to have an online relationship with one or more children, and so on. For the purposes of this section, persons under the age of 18 are considered children. Given the above, Ukraine has currently fulfilled its international obligations to comply with the Lanzarote Convention. Therefore, the quality of such regulation is also appropriate.

Conclusions

Ukraine has been a party to the Council of Europe Convention on the Protection of Children against Sexual Exploitation and Sexual Abuse (Lanzarote Convention) since 2012. However, until recently, the digital safety of children in Ukraine had not been given due attention. The state has largely shifted children's digital safety responsibility to their parents. In fact, the state only gave the parents recommendations and considered its mission complete.

At the end of 2020, the Parliament of Ukraine adopted the bill, *On Amendments to Certain Legislative Acts of Ukraine Concerning the Implementation of the Council of Europe*

Convention for the Protection of Children against Sexual Exploitation and Sexual Abuse (Lanzarote Convention). Article 156-1 of the Criminal Code of Ukraine provides criminal liability for the solicitation of children for sexual purposes. This article is entitled, *Solicitation of children for sexual purposes*. It refers to criminal offenses against an individual's sexual freedom and the sexual inviolability of minors. The article criminalizes acts that involve

> (…) an offer of a meeting made by an adult, including using information and telecommunication systems or technologies, to a person under the age of sixteen, for the purpose of committing any acts of a sexual nature or lewd acts against him or her, if such an offer was made after such an offer at least one action aimed at making such a meeting take place (Criminal Code of Ukraine, 2022; Article 156-1).

However, communication with a child through information and communication technologies does not necessarily lead to a personal meeting. It can remain an online encounter but cause serious harm to the child. Crimes of a sexual nature that are intentionally committed during an online encounter are often associated with the manufacture, possession, and transfer of child pornography. Such actions in part 2 of Art. 156-1 of the Criminal Code are qualified as corpus delicti.

The object of this crime is the sexual inviolability of minors under the age of sexual consent by the encroachment of adults. The victim is an obligatory sign of this crime. The victim may be an individual under the age of sixteen. If the victim is under 14, these acts are qualified as crimes with increased liability. From the objective point of view, a crime can be committed only through active action (inaction is impossible). A criminal offense is considered completed from the moment of committing at least one action aimed at achieving a criminal result. The consequences, in this case, are not binding on the offense, so it has a formal composition.

The legislator draws attention to the types of instruments for committing this criminal offense, computer equipment, and information and telecommunications systems or technologies. The construction of the offense does not preclude the commission of this crime using other tools and means (for example, by personal paper correspondence). However, in this case, a literal citation of Article 23 of the Convention is appropriate because the use of information technology characterizes the vast majority of such encroachments. From the objective point of view, the crime is committed by proposing a meeting. At the same time, at least one action to make such a meeting take place must accompany the proposal. In this case, the meeting should be understood as involving information and telecommunications systems or technologies.

In this case, the subject of this crime (the criminal) can only be an adult. After all, Article 20 of the Lanzarote Convention does not provide for the interference of sexual

interaction between minors by mutual consent. In Ukrainian criminal law, this is called a special subject. The subjective side of the crime is the inner aspect of the crime; it is the mental activity of a person that reflects the attitude of his or her consciousness and will to the socially dangerous act committed and its consequences. The subjective aspect of the crime is formed by the following features of the person: guilt, motive, purpose, and emotional state. Under Article 156-1 of the Criminal Code, in the criminal offense, the subjective aspect of the crime is characterized by direct intent. In case of a person's conscious mistake regarding the victim's age, liability is excluded under Article 156-1. At the same time, the corpus delicti is available when the offender communicates with a police officer pretending to be a minor. The purpose is also the obligatory sign of this crime. Part 1 of Article 156-1 of the Criminal Code defines the purpose of committing any acts of a sexual nature or lewd acts against a minor. Part 2 defines the involvement of a minor in the production of child pornography.

In fact, the text of Article 156-1 of the Criminal Code is a translation of the Lanzarote Convention. Therefore, the adoption of this article is a fulfillment of Ukraine's international obligations more than an act of national lawmaking. At the same time, the adopted text is of sufficient quality and meets similar standards to other European countries. At present, it is not necessary to talk about judicial practice in this category of cases because less than six months have passed from the moment of its entry into force to the moment of completion of this article. At the same time, the simultaneous translation into Ukrainian and distribution of literature on the practical implementation of the provisions of the Lanzarote Convention gives hope that the adopted norm will be actively applied in practice.

Disclaimer

The authors declare no potential conflict of interest related to the article.

Funding

The authors do not report sources of funding for this article.

About the authors

Natalia Semchuk is a Ph.D. and an Attorney-at-law. She is an Assistant Professor in the Department of Criminal Law and Prosses, National Aviation University. She was a legal consultant for the book "Women's Rights in Childbirth and Their Implementation in Ukraine."

https://orcid.org/0000-0002-0267-8996 - Contact: semchuk8094@edu.cn.ua

Sofiia Lykhova graduated with honors from the Kiev Order of Lenin State University T.G. Shevchenko, majoring in jurisprudence. She was awarded the academic title of

Professor in Criminal Law and Procedure. She is Head of the Department of Criminal Law and Procedure of the Faculty of Law of the National Aviation University.

https://orcid.org/0000-0003-2861-519X - Contact: lykhova8094@edu-knu.com

Neghdana Udalova has a Master's degree in Law from the Dnipropetrovsk State University of Internal Affairs. She is currently a lecturer at the Department of Law Enforcement and Police of the Donetsk State University of Internal Affairs.

https://orcid.org/0000-0001-5889-2126 - Contact: udalova8094@acu-edu.cc

Andrii Lyseiuk has a Ph.D. in Law and is a leading specialist at the Ukrainian Scientific and Research Institute of Special Equipment and Forensic Expertise of the Security Service of Ukraine. She is an Associate Professor at the Department of Investigative activities of the University of the State Fiscal Service of Ukraine.

https://orcid.org/0000-0002-0598-7532 - Contact: lyseiuk8094@neu.com.de

Olesia Cheban has a Ph.D. in Law and is an Associate Professor at the Department of Constitutional and Administrative Law of the National Transport University. She obtained a Master's degree in Law from the Academy of Municipal Administration.

https://orcid.org/0000-0003-0448-5968 - Contact: cheban8094@sci-univ.com

References

Akimova, L. M., Litvinova, I. F., Ilchenko, H.O., Pomaza-Ponomarenko, A.L., & Yemets, O.I. (2020). The negative impact of corruption on the economic security of states. International Journal of Management, *11*(5), 1058-1071. https://iaeme.com/MasterAdmin/Journal_uploads/IJM/VOLUME_11_ISSUE_5/IJM_11_05_097.pdf

Atabekova, A., & Filippov, V. (2018). Legislation response to use of minors' self-generated sexual content for their ICT-facilitated sexual coercion. European Research Studies Journal, *21*(4), 763-772. https://doi.org/10.35808/ersj/1244

Chorniy, R. (2019). Problem issues of objectives and motives in composition of crimes against the basis of national security of Ukraine. Herald of Criminal Justice, 4, 89-103. https://doi.org/10.17721/2413-5372.2019.4/89-103

Council of Europe (2007). Convention du Conseil de l'Europe sur la protection des enfants contre l'exploitation et les abus sexuels. *Série des Traités du Conseil de l'Europe – No. 201Conseil de l'Europe*. October 25, 2007. Lanzarote. https://rm.coe.int/1680084833

Criminal Code of Ukraine. (2001). *Law No. 2341-III*. Verkhovna Rada of Ukraine. https://zakon.rada.gov.ua/laws/show/2341-14#Text

Criminal Code of Ukraine. (2022). *Article 156-1 Harassment of a child for sexual purposes*. https://urst.com.ua/kku/st-156-1

De Hart, D., Dwyer, G., Seto, M. C., Moran, R., Letourneau, E., & Schwarz-Watts, D. (2016). Internet sexual solicitation of children: a proposed typology of offenders based on their chats, e-mails, and social network posts. Journal of Sexual Aggression, *23*(1), 77-89. https://doi.org/10.1080/13552600.2016.1241309

De Santisteban, P., del Hoyo, J., Alcazar-Corcoles, M. A., & Gamez-Guadix, M. (2018). Progression, maintenance, and feedback of online child sexual grooming: a qualitative analysis of online predators. Child Abuse & Neglect, 80, 203-215. https://doi.org/10.1016/j.chiabu.2018.03.026

EU Child Online Safety Project. (2020). *Enhancing police and industry practice*. Mdx. https://www.mdx.ac.uk/__data/assets/pdf_file/0017/250163/ISEC-report-FINAL.pdf

Iasechko, S., Skomorovskyi, V., Andronov, I., Oleksii Zaitsev, O., Bortnik O. (2020). The investigation of peculiarities of the occurrence of subjective civil rights in registration of a patent. Journal of Advanced Research in Law and Economics, *11*(3), 844-849. https://doi.org/10.14505/jarle.v11.3(49).17

International Telecommunications Union. [ITU] (2020). *Child protection in digital environment: recommendations for industries*. Mediacenter. https://www.itu.int/en/mediacentre/Pages/pr10-2020-Guidelines-Child-Online-Protecion.aspx

Karthi, N., & Ramu, M. (2020). A study on cyber child pornography. Psychology and Education Journal, *58*(2), 6519-6528. https://doi.org/10.17762/pae.v58i2.3185

Klimek, L. (2012). Solicitation of children for sexual purposes: The new offence in the EU Under the directive 2011/92/EU). International and Comparative Law Review, 12(1), 141-151. https://doi.org/10.1515/iclr-2016-0083

Langbroek, P., Van den Bos, K., Simon Thomas, M., Milo, M., & Van Rossum, W. (2017). Editorial methodology of legal research: challenges and opportunities. Utrecht Law Review, *13*(3), 1-8. https://doi.org/10.18352/ulr.411

Leonov, B.D., Chumak, L.A., Hrynenko, S.V. (2020). The problems of combating the sexual exploitation of children on the internet: analysis of the EU Experience. Information and Law, *2*(33), 32-39. https://doi.org/10.37750/2616-6798.2020.2(33).208080

Lykhova, S. Y., Leonov, B. D., Lysko, T. D., Shaptala, N. K., & Maksymov, S. I. (2021). Criminal-legal ensuring of freedom of religion in modern conditions: a comparative analysis. Cuestiones Políticas, *39*(68), 620-649. https://doi.org/10.46398/cuestpol.3968.40

Nebytov, A. (2015). Legislative support to combat sexual exploitation in Ukraine. Scientific Bulletin of the National Academy of Internal Affairs, *2*, 52-60. https://ojs.naiau.kiev.ua/index.php/scientbul/article/view/287

Nolasco, C. A., Vaughn, M. S., & del Carmen, R. V. (2010). Toward a new methodology for legal research in criminal justice. Journal of Criminal Justice Education, *21*(1), 1-23. https://doi.org/10.1080/10511250903518944

Orlovskyi, R., Shapoval, R., & Demenko, O. (2018). Possibilities of adapting the typologies of the international standards for establishing criminal liability for corruption-related crimes in Ukraine. *Journal of Eastern European and Central Asian Research, 5*(2), 12. https://doi.org/10.15549/jeecar.v5i2.230.

Petrov, R., & Serdyuk, O. (2008). Ukraine: The quest for democratization between Europe and Russia. In: *International Actors, Democratization and the Rule of Law: Anchoring Democracy?* (pp. 189-223). London: Routledge. https://doi.org/10.4324/9780203894699.

Pollack, D., & MacIver, A. (2015). Understanding sexual grooming in child abuse cases. CLP ABA Child Law Practice, *34*(11), 165-168. https://www.americanbar.org/groups/public_interest/child_law/resources/child_law_practiceonline/child_law_practice/vol-34/november-2015/understanding-sexual-grooming-in-child-abuse-cases/

Radzivill, O., Pyvovar, Y., Sopilko, I., & Pyvovar, I. (2018). Coordination of fragmentation within the international air law. *International Journal of Engineering and Technology(UAE), 7*(3.30 Special Issue 30), 280-283. https://doi.org/10.14419/ijet.v7i3.2.14420.

Rutai, Z. (2020). The Lanzarote Committee: Protecting children from sexual violence in Europe and beyond. Pécs Journal of International and European Law, 1, *24*-42. https://www.researchgate.net/publication/342170798_The_Lanzarote_Committee_protecting_children_from_sexual_violence_in_Europe_and_beyond

Semchuk, N., Lykhova, S., & Demianenko, U. (2019). Using English as a foreign language when teaching subjects of the criminal law cycle. *Life Sciences:* The Asian International Journal of Life Science, *21*(2), 517-534. https://doi.org/10.5281/zenodo.3605130

Sopilko, I. N. (2013). Formation of cybersafety policy (Ukrainian experience). *World Applied Sciences Journal, 27*(13 A), 371-374. https://doi.org/10.5829/idosi.wasj.2013.27.elelc.75.

The Council has implemented the provisions of the Council of Europe Convention on the Protection of Children against Sexual Abuse. (2021). *Radiosvoboda*. https://www.radiosvoboda.org/a/news-rada-zahyst-ditey-seksualne-nasylstvo/31110019.html

Trifu, S., & Dragoi, A. M. (2019). From sexting to child pornography. Journal of Health and Medical Sciences, *2*(4). https://doi.org/10.31014/aior.1994.02.04.80

Tyler, T.R. (2017). Methodology in legal research. Utrecht Law Review, *13*(3), 130. https://doi.org/10.18352/ulr.410

Vakulyk, O., Petrenko, P., Kuzmenko, I., Pochtovyi, M., & Orlovskyi, R. (2020). Cybersecurity as a component of the national security of the state. *Journal of Security and Sustainability Issues, 9*(3), 775-784. https://doi.org/10.9770/JSSI.2020.9.3(4).

WHO. (2019). INSPIRE Handbook: Action for implementing the seven strategies for ending violence against children. (Translation Shliakh do domu). https://apps.who.int/iris/bitstream/handle/10665/272996/9789241514095-ukr.pdf?ua=1

Winters, G.M., & Jeglic, E.L. (2016). Stages of sexual grooming: Recognizing potentially predatory behaviors of child molesters. Deviant Behavior, *38*(6), 724-733. https://doi.org/10.1080/01639625.2016.1197656

Yaroshenko, O. M., Moskalenko, O. V., Sliusar, A. M., & Vapnyarchuk, N. M. (2018). Commercial secret as an object of labour relations: Foreign and international experience. *Journal of Legal, Ethical and Regulatory Issues, 21*(Special Issue 1). https://www.abacademies.org/articles/commercial-secret-as-an-object-of-labour-relations-foreign-and-international-experience-7853.html

Esta página queda intencionalmente en blanco

Revista Científica General José María Córdova
(Colombian Journal of Military and Strategic Studies)
Bogotá D.C., Colombia

Volume 20, Number 38, April-June 2022, pp. 387-406
https://dx.doi.org/10.21830/19006586.902

Ukraine's constitutional doctrine of national security

Doctrina constitucional de la seguridad nacional de Ucrania

Hryhorii V. Novytskyi and Olha Ye. Kartamysheva
Berdyansk University of Management and Business, Ukraine

Leonid I. Shcherbyna
National Academy of Security Service of Ukraine, Ukraine

Volodymyr V. Pyvovarov and Oleksandr V. Lysodyed
Yaroslav Mudryi National Law University, Ukraine

Abstract. This article aims to set the foundations for a comprehensive legal system ensuring national security through establishing the scientific principles and framework legislation and developing a constitutional Ukrainian national security doctrine. The empirical basis for this research consists of published documents and materials concerning national security in the USA, particularly the US National Security Strategy. The drafting of the mentioned doctrine as a main scientific result is of national significance for Ukraine. Furthermore, the scientific results presented in the article, including principles, general scientific, system-structural, and legislative models, can be used for the democratic development of constitutional models in Eastern European countries to ensure national and collective security in the world.

Keywords: constitutional doctrine; national interests; national security; public administration; threats; Ukraine

Resumen. El artículo tiene como objetivo sentar las bases de un sistema jurídico integral que garantice la seguridad nacional mediante el establecimiento de los principios científicos y la legislación marco y la elaboración de una doctrina constitucional de seguridad nacional de Ucrania. La base empírica de esta investigación consiste en documentos y materiales publicados sobre la seguridad nacional de los Estados Unidos, en particular, su Estrategia de Seguridad Nacional. El diseño de dicha doctrina, como principal resultado científico, tiene una importancia nacional para Ucrania. Junto con los demás resultados científicos presentados en este artículo, los principios, los modelos científicos generales, sistémico-estructurales y legislativos, pueden utilizarse para el desarrollo democrático de los modelos constitucionales de los países de Europa del Este, garantizando la seguridad nacional y colectiva en el mundo.

Palabras clave: administración pública; amenazas; doctrina constitucional; intereses nacionales; seguridad nacional; Ucrania

Section: Dossier • Scientific and technological research article

Received: November 30, 2021 • Accepted: March 4, 2022

Contact: Hryhorii V. Novytskyi ✉ novytskyi8157@acu-edu.cc

Introduction

The development of Ukrainian statehood, globalization processes, geopolitical changes, and radical reforms in all spheres of public life have caused diverse, large-scale issues in the field of national security. Their solution required nontraditional measures and reconsideration of many established approaches and stereotypes. Unfortunately, Ukraine was unprepared to face the challenges and threats to national security effectively. These potential threats were easily activated in Ukraine due to typecast-thinking, misinterpretation of the core of problems and mechanisms to resolve them, an attitude towards national security as a secondary issue, and an unclear understanding of the legal regulation system in this area (Novytskyi, 2004). As a result, we have lost a significant part of the territory, population, and national wealth. Moreover, there is a war happening in Ukraine.

Even under such conditions, the Ukrainian State still disregards the problems of national security legal regulation. Chaotic, random legislative initiatives do not contribute to the proper solution of national security problems; they significantly complicate them and block the activities of state institutions (Alguliyev et al., 2020; Mykola et al., 2019).

The development of the latest legislation in national security seems particularly relevant in this context. However, it should be noted that the search for a scientific solution to the problems of this study and the development of an appropriate legal framework is only at its initial stage (Mukhammadsidiqov & Turaev, 2020). All research in this area addresses mainly national security as a public phenomenon and excludes studies on domestic legislation or the experience of foreign countries.

Analysis of regulatory legal acts related to national security issues shows their fragmentary character. The matter is that many legislative acts are separate from each other, regulate different aspects of this issue, and even belong to different branches of law. Nevertheless, because national security is one of the most important objects of state and legal protection, it is enshrined in almost all branches of domestic law (Kopeychikov, 1995).

The current state of affairs can be explained by the fact that Ukraine has no generally accepted notion of national security in jurisprudence and legal science. Therefore, when developing a legal framework and a national security law itself, the issue of systematization is challenging due to the disorder in this field. The lack of system character and methodological basis for national security generates problematic aspects in developing a legal framework in this field.

The establishment of the social, legal, and democratic state governed by the rule of law has led to a change in the legal space in Ukraine (Isakovich, 1993; Gnatenko et al., 2020). Along with the reforms in the state system and geopolitical situation, this leads to the domination of national security as a democratic, social, and legal state (Mykiyevych, 1993).

The State has no common principles and values; this hinders its activities aimed at establishing and ensuring security and integrity and developing a systematic legal framework in this field. Ensuring the State's integrity and security is a set of public relations. Thus, national security legal regulation is subject to the same principles as all public relations in general. Therefore, this study aims to set the foundations for a comprehensive legal system in the field of ensuring national security by determining the scientific principles and framework legislation and developing the constitutional doctrine of the national security of Ukraine.

Methodological Framework

A complex of philosophical (particularly dialectical), general scientific (synthesis, analysis, induction, deduction, and generalization), and specific scientific methods formed the basis for methodological analysis. Given the aim of the research, specific methods of legal science were used. The logical and semantic method allowed explaining the content of concepts and legal notions of national security. The formal and legal (dogmatic) method provided a formal and logical interpretation of relevant legislative acts and revealed common trends in legislative processes and legal principles used by the legislator.

We used historical and legal comparative methods to comprehensively analyze the statutory regulations of different hierarchies and periods to reveal the features of the Ukrainian legislation on ensuring national security from the XX to the XXI century. These methods allowed us to observe and scientifically describe the development patterns of the National Security Institute of Ukraine's legal framework.

We used the system-structural method to study the relationship between the systematization of legislation and the achievements in ensuring national security in the XXI century. Furthermore, the same method allowed the formulation of the scientific conceptual foundations of legislation, notions, and the role of framework legislation to develop the draft of the constitutional doctrine of the national security of Ukraine.

The theoretical basis of the article consists of the works of the Ukrainian and foreign researchers in the fields of constitutional, administrative, and international law, the norms of Ukraine's international treaties, and domestic legislation on issues of national security, as well as other authors' research materials. The empirical basis for the research consisted of published documents and materials related to US national security issues, particularly the US National Security Strategy. Moreover, this article analyzes the regulatory legal acts of Japan, Britain, and the Russian Federation. Finally, the article also includes the results of individual authors' unpublished research, conducted in general accordance with the above methods.

Results

Features of public relations in the field of ensuring national security

Legislation is a set of laws and other regulatory legal acts that regulate one sphere or another of public relations and are the source of a particular branch of law (Korelskiy & Perevalov, 1997). In turn, the legislative system is an ordered and approved complex of legislative mandates, enshrined in laws and divided by a subject and method of legal regulation into institutes and branches of the legislation. These two concepts can be linked through the coordination of various factors, such as the desire of the legislature to develop a systematic and integrated legal system and the subject of legal regulation.

The development of a comprehensive legal framework influences the emergence of independent branches of law, which constitute part of the entirety of national law and the independent branches of law. The separation of branches of law is due to the features of content and essence of legal regulation in a particular sphere of public relations. The state's government system creates the difference between the system of law and the system of legislation in this sphere of public relations. After all, the system of regulatory legal acts depends not only on the principles and logic of the system of law but on various subjective and objective reasons.

In turn, the method and subject of legal regulation affect the division of the legal system's structure into branches and, subsequently, institutions. Therefore, legal rules are characterized by the high homogeneity of the content and structure. The legislative branch is less homogeneous; it influences public relations and differs according to the subject of legal regulation, sharing no common methods. The previous can be explained because the concept of branches of law does not include social reality as a category, unlike the complex branches of legislation. It should be noted that the same rule of law cannot regulate public relations of contrary legal nature. Therefore, it is impossible to say that such a set of legal rules forms a single branch of law. The matter is that the presence of other branches in the branch of rules excludes such a possibility.

We should highlight that the branches of law and legislation, even sub-branches, sometimes coincide, for example, legislation and copyright. Their structure can be divided into horizontal (branches of legislation) and vertical (a set of current regulatory legal acts and the hierarchy among the public authorities of the body that adopted this legal act). For the legislative body, the system of regulatory legal acts should represent the objective law. When developing new legislative acts, the legislator should analyze whether new independent branches, sub-branches, and institutions are required. Moreover, the characteristic aspects of special branches of legislation, the correlation, and uniqueness between them must be regarded. Namely, legal science must provide for the improvement of a legal framework. Therefore, new scientific proposals must be developed.

Legislative and law enforcement bodies must approach public relations that arise in ensuring the state's national security in a systematic, careful, and responsible way (Ibrayeva et al., 2018). The allocation of the necessary system of legislation, which will coordinate the various branches of legislation and the legislative system of national security, is due to the importance of ensuring the legal regulation of national security.

The given system forms the legal framework for regulating the protection of Ukraine's national security, which is combined into an inter-branch complex with its branches, sub-branches, and institutions. Examples of such legislation can be financial, civil and criminal. The high number of branches, sub-branches, and institutions in this field is due to the variety of public relations that arise in connection with ensuring national security. However, we should not overlook the systematization of legislation in the field of national security, which requires a single configuration and system when coordinating different branches of legislation. This is essential to eliminate the difference in rule-making subjects, their time of adoption, and the availability of legislation during its enforcement.

Systematization of legislation in the field of ensuring national security: formal and logical principles

The authors of this article believe that systematizing and reordering the legal basis in national security is essential for effective rule-making and identifying and eliminating contradictions existing in legislation. It will positively affect the increase in legal awareness and the legal culture of the population as a whole. Without improving the legislation in this field, it will be very difficult, almost impossible, to increase the role and importance of national security law. This is perhaps the most important instrument and way to achieve secure and contractual principles of functioning and development in modern society (Novikovas et al., 2017).

If we characterize national security as a legal category, it is possible to achieve coherence and order in all existing public relations in the systematization of legislation; this reflects public values and aims at their protection. Here, the question of the method of systematization arises. Today, incorporation is the only possible method to systematize the current legislation ensuring national security. It provides for the compilation of legislative acts while preserving their content in specific collections and books, where each document retains its independent meaning. Moreover, choosing a thematic principle of incorporation is suggested to allow the division of the national security legislation into specific pieces. Then, depending on the result obtained, they can be further codified. National security issues are codified within the relevant traditional branches of law in most states of both the continental and Anglo-Saxon legal systems. For example, a separate chapter (No. 15) within the US Code regards national security issues under Title 50, *War and National Defense* (Beskow & Carley, 2019).

This incorporation method is used to compile most of the generalized collections of regulatory legal acts aimed at unifying the national security issues. For example, the USA's legal system includes the following in the issues of ensuring national security: rules of international law related to the treaty obligations of the United States, arm control standards, internal laws, and bylaws on ensuring national security in its various directions. In addition, procedural issues of interdepartmental interaction, distribution of powers, and subjects of state bodies in internal and external threats, primarily military, receive considerable attention.

We must note that carrying out the comprehensive thematic incorporation of the entire legislation in national security within this research framework would have been impossible. However, it was possible to work out the foundations of such incorporation to the last detail and define the types and features of the above legislation. This compilation will provide the foundation for future work on specific (thematic) systematization of legislation to ensure national security.

The systematization of legislation or regulatory legal acts involves the organization and improvement of legislation, bringing it into an internally coherent system using primarily formal logic. As known, it belongs to methodological sciences. Therefore, its achievement will help build the system of legislation ensuring national security and avoid scholastic theories on the feasibility of particular components of the inter-branch complex (Sybirianska et al., 2018).

Let us briefly describe particular formal and logical rules of division of system-structural phenomena (authors' approach). First, the division must be sum. This approach determines that the sum (volume) of individual formations in the national security ensuring legislative structure should equal the volume of the above inter-branch complex. If we fail this rule, there will be either incomplete division or division with superfluous formations. The division should have one basis. The feature taken as the basis for division should not be replaced by another. Thus, the legislation division ensuring national security should be carried out according to one criterion, which cannot be automatically applied at the subsequent levels of system formation.

Given that the branches of legislation are divided only by the subject of legal regulation, we suggest taking it as a basis for special classification of legislation ensuring national security. This subject is homogeneous public relations in the sphere of ensuring national security. Therefore, new formations should exclude each other. Regarding the system of legislation ensuring national security, this rule can be formulated as follows: if we include a regulatory legal act in one of the types of legislation that form an inter-branch complex, then it cannot be included in another type.

The division must be continuous. The system of legislation should be divided into separate branches, from generic (general) formations to specific (special) ones. Given

that the national security ensuring legislation is a generic phenomenon in Ukraine's legal system, it should be divided into special formations. If we fail the rule, the so-called jump in the division will occur (Preston, 2021). Therefore, the criterion taken as a basis for the division of the said legislation should be clear to exclude the variety of interpretations. Otherwise, each researcher will use this criterion to substantiate a *required* type of legislation.

Namely, the violation of this rule (ambiguous interpretation of a category such as the subject of legal regulation) caused contradictions in many discussions on the legal system related to the features of Civil Law involving the presence of certain branches of law. As a result, different textbooks on the theory of law list branches of law that do not always coincide in name and number. Recently, this list has expanded rapidly. Having analyzed basic formal-logical formations of the legislation in ensuring national security briefly, we can examine the structure of the inter-branch complex –legislation in national security.

Framework legislation: theory and practice of application

In the system of national security legislation, legislation occupies a special place that establishes a system of values, goals, objectives, and measures in this field and identifies existing and potential threats. In the field of ensuring national security, this legislation is called a framework *guide*. It consists of regulatory legal acts, including the national security doctrine and national security ensuring subjects' strategy under defined conditions and periods. A single system with common principles, ideas, tasks, and goals can cover the activities of the subjects of ensuring national security. Therefore, we propose calling the above type of legislation framework one.

Here, we need to note the historical significance of the Law of Ukraine, *On Fundamentals of National Security of Ukraine*. It was essentially the first regulatory legal act of framework legislation to ensure national security. Part 2 of Art. 2 of this law defined the general features of framework legislation. It provided for the development of the National Security Strategy of Ukraine. Moreover, it provided for the Military Doctrine of Ukraine's doctrines, concepts, strategies, and programs for fulfilling its goals and principles in the development of military capabilities and functions of public authorities to rapidly identify and neutralize existing and potential threats to Ukrainian national interests (Verkhovna Rada of Ukraine, 2003).

This rule established that Ukraine's National Security Strategy and Military Doctrine were compulsory for forming and functioning programs and measures of public policy in national security. This situation has slightly changed since adopting the Law of Ukraine, *On National Security of Ukraine*. The legislator decided that forming a system of values, goals, objectives, and measures and identifying existing and potential threats in the field of national security requires nothing more than planning in the said field. According to

the Part 1 of Art. 25 of the Law, planning in the field of national security and defense aims at ensuring public policy in these fields through the development of strategies, concepts, programs, road maps for the security and defense sector, resource management, and efficient allocation of resources (Verkhovna Rada of Ukraine, 2018).

The given rule sets forward several questions. Where can a person view the *public policy on national security*? Is it not necessary to clearly understand the ultimate purpose before planning or managing something? First, let us consider the legal definition of the *National Security Strategy of Ukraine*. This document defines the current threats to Ukraine's national security and relevant purposes, objectives, and mechanisms to protect its national interests. It forms the basis for planning and developing public policy in national security.

What is the public policy of national security, in any case? The legislator set out to *build a national security establishment* but neglected to specify the parameters of its foundation. Meanwhile, the national security doctrine is the foundation of legal regulation of national security. Therefore, this document should include the ideas on public policy concerning national security. With this in mind, another question arises regarding the correlation between the notions of the *National Security Strategy of Ukraine*, the *Military Doctrine of Ukraine*, and their *doctrine*, *concept*, *strategy*, *program*, *purpose*, and *content*. First, determining these notions' content is essential to structure their hierarchy as a system of regulatory legal acts, each with its purpose and performing certain tasks.

The *doctrine* is a common term for rule-making only in International Law. In the legal systems of individual countries, this term is used cautiously. However, this does not apply to Ukraine. At present, there are ample *doctrines* in Ukraine, including the Military Doctrine of Ukraine, the National Strategy of Development of Education in Ukraine, the Maritime Doctrine of Ukraine to 2035, the Information Security Doctrine of Ukraine, and the Military Medical Doctrine of Ukraine. An analysis of the definition of the notion of doctrine in International Law, the Monroe, Toba, and Estrada doctrines allows us to conclude that a doctrine is a set of basic provisions or guidelines that influence the solution of problematic aspects and issues of states and international relations' functioning and development. These provisions are usually contained in the rules of written law or documents of a political nature, but not always. It is worth highlighting the following features of a doctrine: its constructive and regulatory role to other regulations, consistency over a relatively long period, conciseness, clarity, and, of course, social significance. For example, President James Monroe's 1823 message to Congress contained the Monroe Doctrine. Its content defined three main principles of US foreign policy in relations with Europe. They were the US non-interference in the internal affairs of European states, the non-interference of European states in the internal affairs of the United States, and the determination to thwart any attempt by European states to encroach on US independence.

In Ukraine, the *relativity* of understanding the notion of doctrine in rule-making becomes noticeable when comparing legal systems of individual countries and regulatory legal acts of international law, known and recognized by lawyers as doctrine, with Ukrainian regulatory legal acts, the content of which is of doctrinal character. This mentioned *doctrine* has little in common with the notion of doctrine in its fullest sense. The content of the Military Doctrine of Ukraine is similar to its Military Security Strategy. The above is true because the Military Doctrine of Ukraine (President of Ukraine, 2021) will be in force until the adoption of the Military Security Strategy under the Law of Ukraine, *On National Security of Ukraine*.

Thus, there is no distinction between notions of doctrine and strategy in the current Ukrainian system for ensuring national security. However, there are rules of doctrinal character that regulate the sphere of ensuring national security in the Ukrainian laws. For example, Paragraph 5 of Section IX of the Declaration of Ukrainian State Sovereignty states that the Ukrainian Soviet Socialist Republic (SSR) declares its intention to remain a permanently neutral state, rejecting its participation in military blocs and producing or purchasing nuclear weapons. The doctrinal character of this rule is incontestable. We should note that the Declaration does not use the notion of *national security*; it considers only the issues of external and internal security. Scientists believe this negatively affects the Declaration's content (Isakovich, 1993).

Another example is the Resolution of the Verkhovna Rada of Ukraine No. 3360-XII, *On the Main Directions of Ukraine's Foreign Policy*, of July 7, 1993, which is no longer in effect. Nevertheless, the authors believe Section II (Principles of Ukraine's Foreign Policy) of this document contained the following doctrinal provisions on national security:

1. Ukraine seeks to pursue an open foreign policy and establish cooperation with states without the intervention of other regions or groups.
2. Ukraine declares no territorial encroachments on neighboring countries and does not allow such encroachments on its territory.
3. Ukraine has a right to use its Armed Forces in cases of armed aggression against it or other encroachments on territorial integrity and sovereignty or the implementation of international obligations.
4. Ukraine shall not allow the presence of foreign troops on the territory of its country or other countries without their consent, except for the case of the imposition of sanctions under the UN Charter.
5. Ukraine respects the principle of international security and the inviolability of peace. It agrees that a threat to the national security of one country means a threat to world security as a whole. Ukraine adheres to the principle that *security for oneself is the security of all*.

The Resolution of the Verkhovna Rada of Ukraine No. 3360-XII of July 7, 1993, was repealed by the Law of Ukraine, *On Foundations of Foreign and Domestic Policy* (Verkhovna Rada of Ukraine, 2010). In this context, we must highlight recent amendments to the Constitution of Ukraine (Verkhovna Rada of Ukraine, 1996). According to the legislator, these amendments had to enshrine the inviolability of the country's commitment to join the EU and NATO. Further analysis of Ukrainian regulatory legal acts is superfluous to argue with a high degree of probability that many other legal acts contain doctrinal rules on national security. Given this context, the need to systematize these rules using some systematization method is clear, as well as the need to create a level of legislative consolidation of the results.

Regarding the method of systematization, it should be noted that it refers to individual rules rather than all regulatory legal acts. It is problematic to place certain rules on national security, including doctrinal, in regulatory legal acts of various branches of law. At the same time, it is quite logical and fitting that the main content of these regulatory legal acts consists of the rules governing public relations in these branches of law. In turn, the rules of ensuring national security are included in these regulatory legal acts, given that the sphere of national security touches upon all aspects of society and can be enshrined in each branch of national law.

In this case, employing the incorporation method would be advantageous because it would produce a list of regulatory legal acts from various branches of law, containing rules on ensuring national security of a doctrinal nature. However, given its importance, the doctrinal level of legal regulation of ensuring national security should be in the form of an individual regulatory legal act or its part. Therefore, the next step would be to codify the relevant rules from previously incorporated regulatory legal acts and register them as a single legal act or its part. But, again, we highlight that this coding involves individual rules rather than regulatory legal acts.

We are referring to forming a regulatory legal act containing the so-called rules/principles (Kopeychikov, 1995). These rules/principles enshrine the foundations for ensuring national security. This regulatory legal act should become the basis for developing conduct standards, constituent rules, and rules/principles in the field of national security. It is well-acknowledged that the level of consolidation of a rule in the vertical structure of legislation depends on its importance for the state and society as a whole. Therefore, let us discuss rather than provide a political assessment of some of the above rules that the authors believe to be doctrinal, given the recent events in the world and Ukraine.

The mentioned Resolution of the Verkhovna Rada of Ukraine No. 3360-XII *On the Main Directions of Ukraine's Foreign Policy* of July 7, 1993, states that Ukraine is against encroachments and the presence of foreign troops on the territory of its country or other countries without their clear consent (Verkhovna Rada of Ukraine, 1993). The exception

is the imposition of sanctions under the UN Charter. Article 11 of the Law of Ukraine, *On Foundations of Foreign and Domestic Policy*, defines the principles of external policy. They include the following:

- Affirm Ukraine's security and interests in the international arena through peaceful and mutually beneficial cooperation with foreign countries under the rules and principles of international law;
- Ensure the protection of the country's territorial integrity and sovereignty, its interests in the fields of politics, economy, and energy by diplomatic means and methods according to international law;
- Use the international potential to establish and develop the country as an independent, sovereign, democratic legal, and social state and economic development;
- Establish appropriate political conditions for Ukraine's development in the international arena and Ukrainian national dignity, citizen identity, historical consciousness, economic potential, and the cultural, ethnic, religious, and linguistic identity of Ukrainians;
- Take Ukraine's necessary place in the system of international relations, strengthening its authority in the international arena;
- Achieve international peace and security in the world, participate in a comprehensive political dialogue to enhance mutual trust between states, and avoid traditional and new security threats;
- Establish cooperation with the North Atlantic Treaty Organization with the prospect of becoming a member;
- Increase the role of international law in international relations, ensuring compliance and implementation of existing ones, developing new ideas, principles, and rules of international law;
- Eliminate and prevent conflict situations in the regions bordering Ukraine and resolution of existing conflicts;
- Protect Ukrainian citizens and legal entities' rights and interests abroad;
- Search for favorable conditions to meet the national, cultural, and linguistic needs of Ukrainians living abroad, organize and maintain permanent ties with them;
- Integrate Ukraine into the European political, economic, and legal space to obtain membership in the European Union;
- Develop commercial and economic, scientific and technical, and investment cooperation between Ukraine and international organizations and countries through mutual benefit;
- Increase Ukraine's welfare and assertion in the world economic system for full economic development;

- Establish international cooperation to attract foreign investment, new technologies, and management experience to the national economy for its reformation, modernization, and innovative development;
- Assert State integration into the world information space. (Verkhovna Rada of Ukraine, 2010)

We cite the entire rule intentionally and raise the question: What is Ukraine's official position on stationing troops on foreign state territories? Analysis of the Laws mentioned above does not answer this question. Meanwhile, this is rather a matter of national security than slogans or declarations. Let us remember the events of 2008 in Abkhazia and South Ossetia. Obviously, Ukraine's official position, given the use of the Russian Black Sea Fleet forces in the conflict, was not the least to make certain decisions both in favor of resolving the war and a peaceful settlement of the conflict. The Russian Federation took all necessary measures to make this decision with the utmost loyalty. Why is it so? The events' direction was so because the discussed rule had been at the level of the legislative hierarchy, which meant its near absence. This situation created conditions for various political forces both in Ukraine and abroad to manipulate Ukraine's position.

A fundamentally different scenario would have been possible provided that the Constitution of Ukraine had enshrined this rule. In this case, the potential aggressor would have been aware of the unambiguity, specificity, and invariability of Ukraine's position despite the circumstances that the aggressor could have created. Furthermore, the complexity and duration of certain measures toward Ukraine to change its official position would be obvious. Therefore, the authors believe that the existence of the above rule in the Constitution of Ukraine can be an important factor in ensuring national security under political instability.

However, an even more realistic example of the problem is the mentioned provision of the Declaration of Ukrainian State Sovereignty on Ukraine's intention to become a permanently neutral state in the future. It is acknowledged that when adopting the current Constitution of Ukraine, the legislator was guided by the Act of Independence of Ukraine, which was confirmed by an all-Ukrainian referendum. Furthermore, the Act itself was issued to implement the Declaration of State Sovereignty. Thus, the current foundations of the constitutional legislation of Ukraine are aimed at implementing a policy of permanent neutrality, which provides for the non-alignment of Ukraine.

Here, the question arises of Ukraine's current orientation towards NATO. Does it comply with the Constitution of Ukraine? The matter is that the non-aligned status proclaimed in the Declaration of Ukrainian State Sovereignty is in clear conflict with the intentions to join the Alliance, enshrined in the Law of Ukraine, *On National Security of Ukraine*, and amendments to the Constitution. The Parliament of Ukraine approved

draft law No. 9037 on Amendments to the Law on European Integration and Accession to NATO. Approval of these changes should strengthen the course of the State to join the EU and NATO. However, the issue is that the Parliament of Ukraine has no right to amend particular articles of the Constitution. They require a special procedure for approval by referendum. This refers to Chapter I *General principles*, Chapter III *Elections. Referendum*, and Chapter XIII *Amendments to the Constitution of Ukraine*. Therefore, this question is included in Articles 85 and 116 of the Constitution of Ukraine.

Now, the powers of the Verkhovna Rada include the implementation of EU and NATO membership, and the powers of the Cabinet of Ministers include ensuring this implementation. According to Art. 102 of the Constitution of Ukraine, the President of Ukraine shall be the guarantor of the above. However, it is unclear by whom and where this course of integration is defined. The problem is that expanding the President's powers has led to additional rules of conduct for the Parliament and the Government, which are not the principles intended to consolidate the State's strategic course. Instead, they act as the basis for rules/principles and constituents.

Discussion

To study the issue more objectively, we offer additional analysis of the doctrinal studies, particularly concerning foreign approaches to determining their national security doctrines. Studying doctrinal approaches to the definition of US national security, M. Mukhammadsidiqov and A. Turaev (2020) point out its neoconservative nature, which emphasizes the State's military power without rejecting the instruments of international legal relations. It also emphasizes the strict regulation of aspects of the State's domestic and foreign policy on national security at the legislative level. The scientists' position is confirmed by the fact that the United States also developed a US National Security Strategy in 2017, in addition to a relevant section in the US Code, which deals mainly with national security issues (Spoehr & Handy, 2018).

It reflects the versatility, multifacetedness, and comprehensiveness of this issue's regulation. This Strategy consists of the following pillars: *Protect the American People, the Homeland, and the American Way of Life*, *Promote American Prosperity*, and *The Strategy in a Regional Context* (The White House, 2017). In the US national security doctrine, the so-called *traditional* means of ensuring it plays a significant role (particularly obtaining intelligence on various related issues) (Mandel & Tetlock, 2018). The same applies to *new* ones that occur in continuous scientific and technological progress (particularly in cybersecurity) (George, 2019). Artificial intelligence is used to ensure national security and counteract artificial intelligence in occurrences using the latter to harm US national security (Congressional Research Service, 2020; Sayler, 2020; Aldrich & Moran, 2018).

The British approach is similar to the American. It has been purposefully been aligned with the American one since the beginning of the Cold War. Strict legal regulation of the British national security doctrine is expressed, among other things, in the adoption of a permanent national security strategy of the United Kingdom. In addition to this, it is characterized by institutional, systematic, and specific nature, which is expressed, particularly in the functioning of the National Security Council of the UK, organizing and conducting regular five-year Strategic Defense and Security Reviews (Thomson & Blagden, 2018; Mattsson & Saljo, 2017).

We also find the American approach to defining national security in Japan's national security system. In his work, Yamakage (1997) characterizes Asian defense policy, including Japanese, as relying firstly on the *power of the weapon*. The similarity with the American one is that this requires both a clear institutional and legal regulation of doctrinal approaches to defining national security, set in the National Security Strategy of Japan. In Japan, such institutional regulation exists, represented by the National Security Council, headed by the Prime Minister, and the National Security Secretariat within the Cabinet of Ministers (Liff, 2018).

A similar approach to defining the national security policy also takes place in India (Pant & Bommakanti, 2019). Even in the Russian Federation –in ongoing armed conflict with Ukraine– systematic approaches to defining the national security doctrine have been updated and brought into line since 2014. However, being concentrated primarily on the regulatory aspect, we should note that the following acts have been updated and re-adopted: the Military Doctrine of 2014, the National Security Strategy of 2015, the Scientific and Technical Development Strategies of 2016, the Information Security Doctrine of 2016, and the Concept of Foreign Policy of 2016 (Pynnoniemi, 2018).

As for the domestic approach to the defining national security doctrine, and given the above foreign approaches, we propose to focus primarily on the regulatory level, namely the Basic Law –the Constitution of Ukraine. It establishes key, fundamental approaches, including determining the State's national security. In the Constitution of Ukraine, the rules/principles are included in Chapter 1; therefore, it is impossible to amend it. Chapter 1 includes Article 18, which states that Ukraine's foreign political activity shall be aimed at ensuring its national interests and security by maintaining peaceful and mutually beneficial cooperation with members of the international community in compliance with the principles and rules of international law.

It is necessary to amend this article by chapter, indicating the need for Ukraine to adhere to the principles of collective security –*security for oneself means security for all*. Ukraine aims to enter into the EU and NATO, the organizations based on democratic principles and values. If such amendments are made to the Constitution of Ukraine,

the Ukrainian Parliament, Government, and President's rules/principles of conduct will change.

In such a case, the Verkhovna Rada of Ukraine does not adopt the Constitution; it only approves particular amendments and changes. Using the old principles and rules enshrined in the 1996 Constitution is challenging enough. There must be a new Constitution with new values, motives, and principles. However, even 300 votes of parliamentarians cannot guarantee anything. Only a referendum can bring about changes and guarantee a new stage of development, as the deputies' votes have not been convincing enough for a long time.

Thus, we support the NATO representatives who believe the referendum should be held before Ukraine can enter this organization. This is not only to clarify the will of the Ukrainian people. The referendum results should become the legal basis for bringing the current foundations of Ukraine's constitutional legislation in line with its foreign policy intentions (Sanclemente, 2021). On the other hand, in the long-term, the uncertainty enables the manipulation of the Ukrainian position by various political forces both inside the country and abroad. This factor in no way affects the end of the armed conflict and the resolution of the political situation in eastern Ukraine and may even lead to its expansion. The matter is that any uncertainty creates new opportunities for the aggressor, pushing the aggressor to take action in pursuit of its interests, contrary to the Ukrainian.

Thus, in today's Ukraine, several regulatory legal acts include the rules on issues of national security that are of doctrinal nature. Some of them contradict each other, creating conditions for political manipulations. The authors agree with Mykiyevych (1993), who points out that guiding principles and rules of the State in the international arena will be enshrined without legal regulation, despite their progress. Because their role is significant, they shall be enshrined in the Basic Law –the Constitution of Ukraine.

The above gives grounds to conclude that it is necessary to amend the Constitution of Ukraine with the chapter of *National Security* or *Doctrine of National Security*. In the Constitution, this chapter shall include so-called rules/principles enshrining the foundations of national security and, therefore, perform the function of the doctrine of national security of Ukraine. Meanwhile, one draft of the Constitution of Ukraine of 1993 provided a chapter on national security. It defined the strategic directions for state security and the functions and powers of the National Security and Defense Council (Isakovich, 1993). Studying the constitutional practice of foreign countries, experts noted the expediency of the rule on establishing the National Security and Defense Council. However, they offered to enshrine the main features of the concept for ensuring national security in the special law that could be changed where needed.

Conclusion and Recommendations

In this study, we analyzed both domestic and foreign approaches to defining national security doctrine and policy. As a result, the authors propose that the constitutional doctrine of national security of Ukraine today could read as follows:

Doctrine (fundamentals) of National Security of Ukraine:

Article 1. Fundamentals of Ukraine's foreign policy.

Ukraine shall pursue an open foreign policy and seek equal cooperation with all States abiding by the fundamental rules of international law concerning peace, good neighborliness, and non-interference in the internal affairs of other States.

The principle of collective security shall be enshrined in the legislation of Ukraine. It can be characterized as "security of oneself through the security for all." Ukraine aims to become a member of the EU and NATO, which adhere to collective security and defense and democratic principles and values. Ukraine also respects the borders and sovereignty of other countries, shares no territorial encroachments on neighboring countries, and does not allow territorial encroachments on its borders.

Article 2. The Use of the Armed Forces of Ukraine and the Territorial Defense Forces of Ukraine.

Ukraine shall use its Armed Forces in cases of armed aggression against it and any other armed encroachments on its territorial integrity and inviolability of borders or the fulfillment of international obligations. The Territorial Defense Forces of Ukraine organized by the state shall be in force in Ukraine. Territorial Defense Forces shall be used exclusively on the territory of Ukraine and only in cases of acts of armed aggression of foreign states against Ukraine. In any other case, the use of the Armed Forces of Ukraine and the Territorial Defense Forces shall be prohibited and punished by law.

Article 3. Armed Forces of Other States on the Territory of Ukraine.

The presence of armed forces of other states on the territory of Ukraine shall be allowed only under Ukraine's participation in European and Euro-Atlantic structures of collective security and defense and fulfillment of its international obligations, approved by the Verkhovna Rada of Ukraine. Furthermore, Ukraine shall not support the invasion and deployment of foreign troops on the territory of other countries without their consent, except for the case of the imposition of sanctions under the UN Charter.

Article 4. Nuclear Status of Ukraine.

Until the acquisition of membership in European and Euro-Atlantic structures of collective security and defense, or until the restoration of Ukraine's sovereignty within its

borders as of January 1, 2013, Ukraine shall reserve the right to deploy and manufacture nuclear weapons.

Article 5. Objects of National Security of Ukraine.

Ukraine shall be responsible to the citizens of Ukraine for its population, the integrity of the territory, the inviolability of its borders, the preservation and increase of the national wealth of Ukraine, and the preservation and development of the national identity of the Ukrainian people.

Article 6. The Main Objectives of the State in the Field of National Security and Defense.

1. To create economic and social conditions to increase the population of Ukraine to 60 million.
2. To restore the sovereignty of Ukraine within its borders as of January 1, 2013.
3. To increase the national wealth of Ukraine to the level of 500 trillion UAH.
4. To preserve and develop the national self-consciousness of the Ukrainian people.

Article 7. Restriction of Human and Civil Rights and Freedoms in the Interests of National Security and Defense of Ukraine.

The rights and fundamental freedoms of humans shall not be restricted in the interests of the national security and defense of Ukraine. The rights and freedoms of a citizen of Ukraine may be restricted in the interests of national security and defense of Ukraine only in cases established by law and a court decision.

Disclaimer

The authors declare no potential conflict of interest related to the article.

Funding

The authors do not report sources of funding for this article.

About the authors

Hryhorii V. Novytskyi has a Ph.D. in Legal Science. He is a Professor and Head of the Department of Sectoral Legal Disciplines at the Berdyansk University of Management and Business, Ukraine. His research interests are Criminal Law and matters ensuring Ukraine's national security.

https://orcid.org/0000-0002-3543-308X - Contact: novytskyi8157@acu-edu.cc

Leonid I. Shcherbyna has a Ph.D. in Law. He is a Senior Researcher, Chief Researcher of the Scientific and Organizational Center of the National Academy of the Security Service

of Ukraine in Kyiv. He researches Criminal Procedure and matters ensuring Ukraine's national and state security.

https://orcid.org/0000-0003-3119-9684 - Contact: shcherbyna8157@neu.com.de

Volodymyr V. Pyvovarov has a Ph.D. in Law. He is a Lawyer and Associate Professor of Criminology and Criminal Enforcement Law at the Yaroslav Mudryi National Law University in Kharkiv, Ukraine. His research interests include Corporate Crime, Economic Crime, Cybercrime, Psychology, Criminology, and National Security Policy.

https://orcid.org/0000-0002-3239-7036 - Contact: pyvovarov8157@edu-knu.com

Olha Ye. Kartamysheva has a Ph.D. in Law. She is an Associate Professor in the Department of Sectoral Legal Disciplines of Berdyansk University of Management and Business, Ukraine. She boasts more than 18 years of scientific and pedagogical activity experience.

https://orcid.org/0000-0002-1040-2703 - Contact: kartamysheva8157@sci-univ.com

Oleksandr V. Lysodyed has a Ph.D. in Law and is an Associate Professor in the Department of Criminology and Criminal Enforcement Law at Yaroslav the Wise National University of Law in Kharkiv, Ukraine. His research subjects include Crime Prevention, convicts' legal status, and criminal punishment execution.

https://orcid.org/0000-0003-0648-829X - Contact: lysodyed8157@edu.cn.ua

References

Aldrich, R.J., & Moran, C.R. (2018). "Delayed Disclosure": National Security, Whistle-Blowers, and Nature of Secrecy. *Political Studies*, *67*(2), 291-306. https://doi.org/10.1177/0032321718764990

Alguliyev, R.M., Imamverdiyev, Y.N., Mahmudov, R.S., & Aliguliyev, R.M. (2020). Information security as a national security component. *Information Security Journal*, *30*(1), 1-18. https://doi.org/10.1080/19393555.2020.1795323

Beskow, D., & Carley, K.M. (2019). *Social cybersecurity: An Emerging National Security Requirement*. Apps. Dtic. Mil. https://apps.dtic.mil/sti/pdfs/AD1108494.pdf

Congressional Research Service. (2020). *Artificial Intelligence and National Security.* https://sgp.fas.org/crs/natsec/R45178.pdf

George, A.M. (2019). The National Security Implications of Cyberbiosecurity. Frontiers in Bioengineering and Biotechnology, *7*. https://doi.org/10.3389/fbioe.2019.00051

Gnatenko, K. V., Yaroshenko, O. M., Inshyn, M. I., Vapnyarchuk, N. M., & Sereda, O. H. (2020). Targeted and effective use of state and non-state social funds. *International Journal of Criminology and Sociology, 9*, 2861-2869. https://doi.org/10.6000/1929-4409.2020.09.350

Ibrayeva, A., Sannikov, D. V., Kadyrov, M. A., Zapevalov, V. N., Hasanov, E. L., & Zuev, V. N. (2018). Importance of the Caspian countries for the European union energy security. *International Journal of Energy Economics and Policy, 8*(3), 150-159. https://www.econjournals.com/index.php/ijeep/article/view/6263

Isakovich, S.V. (1993). *International legal aspects of national security of Ukraine*. Kyiv: Printing House of the Ministry of Internal Affairs of Ukraine.

Kopeychikov, V.V. (Ed.) (1995). *Theory of state and law: textbook*. Kyiv: Yurinform.

Korelskiy, V.M. & Perevalov, V.D. (1997). *Theory of state and law*. Moscow: NORMA-INFRA-M.

Liff, A.P. (2018). Japan's National Security Council: Policy Coordination and Political Power. *Japanese Studies*, *38*(2), 253-279. https://doi.org/10.1080/10371397.2018.1503926

Mandel, D.R., & Tetlock, P.E. (2018). Correcting Judgment Correctives in National Security Intelligence. Frontiers in Psychology, *9*. https://doi.org/10.3389/fpsyg.2018.02640

Mattsson, C., & Saljo, R. (2017). Violent Extremism, National Security and Prevention. Institutional Discourses and Their Implications for Schooling. *British Journal of Educational Studies*, *66*(1), 109-125. https://doi.org/10.1080/00071005.2017.1337870

Mukhammadsidiqov, M., & Turaev, A. (2020). Influence of US Neoconservatism on Formation of National Security Paradigm. *The Light of Islam*, *3*(3), 113-120. https://www.researchgate.net/publication/349151434_INFLUENCE_OF_US_NEOCONSERVATISM_ON_FORMATION_OF_NATIONAL_SECURITY_PARADIGM

Mykiyevych, M.M. (1993). *Constitutional consolidation of Ukraine's foreign policy*. Kyiv: Printing House of the Ministry of Internal Affairs of Ukraine.

Mykola, I., Tetiana, K., Ruslan, K., Ihor, D., & Volodymyr, P. (2019). European standards for the protection of social rights of labor migrants. *Journal of Legal, Ethical and Regulatory Issues, 22*(6), 1-8. https://www.abacademies.org/articles/European-standards-for-the-protection-of-social-rights-of-labor-migrants-1544-0044-22-6-439.pdf

Novikovas, A., Novikoviene, L., Shapoval, R., & Solntseva, K. (2017). The peculiarities of motivation and organization of civil defence service in Lithuania and Ukraine. *Journal of Security and Sustainability Issues, 7*(2), 369-380. https://doi.org/10.9770/jssi.2017.7.2(16)

Novytskyi, H.V. (2004). National Security of Ukraine: Creation of a System of Legal Regulation. *State Security of Ukraine*, *2*, 13-17.

Pant, H.V., & Bommakanti, K. (2019). India's national security: challenges and dilemmas. *International Affairs*, *95*(4), 835-857. https://doi.org/10.1093/ia/iiz053

President of Ukraine. (2021). Military doctrine of Ukraine. Verkhovna Rada of Ukraine (Parliament of Ukraine). https://zakon.rada.gov.ua/laws/show/121/2021#Text

Preston, A. (2021). National security as grand strategy: Edward Mead Earle and the Burdens of World Power. In Borgwardt, E., McKnight Nichols, C., & Preston, A, (Eds.) *Rethinking American Grand Strategy*, 238-253. https://doi.org/10.1093/oso/9780190695668.003.0012

Pynnoniemi, K. (2018). Russia's National Security Strategy: Analysis of Conceptual Evolution. *The Journal of Slavic Military Studies*, *31*(2), 240-256. https://doi.org/10.1080/13518046.2018.1451091

Sanclemente, G.L. (2021). Reliability: Understanding cognitive human bias in artificial intelligence for national security and intelligence analysis. *Security Journal*. https://doi.org/10.1057/s41284-021-00321-2

Sayler, K.M. (2020). *Artificial Intelligence and National Security*. Congressional Research Service. R45178. Version 7. Updated Novemeber 10, 2020. https://sgp.fas.org/crs/natsec/R45178.pdf

Spoehr, T., & Handy, B. (2018). The Looming National Security Crisis: Young Americans Unable to Serve in the Military. February 13, 2018. The Heritage Foundation. https://www.heritage.org/defense/report/the-looming-national-security-crisis-young-americans-unable-serve-the-military

Sybirianska, Y., Dyba, M., Britchenko, I., Ivashchenko, A., Vasylyshen, Y., & Polishchuk, Y. (2018). Fintech platforms in SME'S financing: EU experience and ways of their application in Ukraine. *Investment Management and Financial Innovations, 15*(3), 83-96. https://doi.org/10.21511/imfi.15(3).2018.07

The White House. (2017). *National Security Strategy of the United States of America*. Trumpwhitehouse. Archives. December 2017. https://trumpwhitehouse.archives.gov/wp-content/uploads/2017/12/NSS-Final-12-18-2017-0905.pdf

Thomson, C., & Blagden, D. (2018). A Very British National Security State: Formal and Informal Institutions in the Design of UK Security Policy. *The British Journal of Politics and International Relations*, *20*(3), 573-593. https://doi.org/10.1177/1369148118784722

Verkhovna Rada of Ukraine. (1993). Resolution of the Verkhovna Rada of Ukraine. *On the Main Directions of Ukraine's Foreign Policy*. Verkhovna Rada of Ukraine (Parliament of Ukraine). https://zakon.rada.gov.ua/laws/show/3360-12#Text

Verkhovna Rada of Ukraine. (1996). *Constitution of Ukraine*. Verkhovna Rada of Ukraine (Parliament of Ukraine). https://zakon.rada.gov.ua/laws/show/254%D0%BA/96-%D0%B2%D1%80#Text

Verkhovna Rada of Ukraine. (2003). Law of Ukraine. *On Fundamentals of National Security of Ukraine*. Verkhovna Rada of Ukraine (Parliament of Ukraine). https://zakon.rada.gov.ua/laws/show/964-15#Text

Verkhovna Rada of Ukraine. (2010). Law of Ukraine. *On the Principles of Domestic and Foreign Policy*. Verkhovna Rada of Ukraine (Parliament of Ukraine). https://zakon.rada.gov.ua/laws/show/2411-17#Text

Verkhovna Rada of Ukraine. (2018). Law of Ukraine. *On National Security of Ukraine*. Verkhovna Rada of Ukraine (Parliament of Ukraine). https://zakon.rada.gov.ua/laws/show/2469-19#Text

Yamakage, S. (1997). Japan's National Security and Asia-Pacific's Regional Institutions in the Post-Cold War Era. In Katzenstein, P. J., & Shiraishi, T. (Eds.) *Network Power*, 275-305. New York: Cornell University Press.

Revista Científica General José María Córdova
(Colombian Journal of Military and Strategic Studies)
Bogotá D.C., Colombia

Volume 20, Number 38, April-June 2022, pp. 407-423
https://dx.doi.org/10.21830/19006586.901

Forensic and technical criminalistics support in cybercrime investigation: countering cyber threats in Ukraine

Apoyo criminalístico forense y técnico en la investigación de la ciberdelincuencia: la lucha contra las ciberamenazas en Ucrania

Andrii Padalka
Ukrainian Scientific and Research Institute of Special Equipment and Forensic Expertise of the Security Service of Ukraine, Ukraine

Abstract. The issue of cyber security has become a key State objective in Ukraine. Cyber espionage and cyber-attacks by intelligence agencies (predominantly non-democratic countries) have become the most significant modern threat to automated systems, surpassing ordinary crimes seeking profit. Besides effective protection and immediate responses to counter cyber threats, cyber incident investigations are an important element that must be conducted by authorized law enforcement agencies and intelligence agencies when necessary. This article considers key aspects and issues to suggest practical recommendations to prepare and appoint forensic expertise in cybercrime investigations. Furthermore, it addresses the objects under examination, their removal's particularities, and the questions to ask telecommunications and technical computer experts.

Keywords: criminalistics; cyber-attack; cybercrime; cyber incident; cyber threat; forensic expertise; investigation; Ukraine

Resumen. La ciberseguridad se ha convertido en un objetivo clave del Estado en Ucrania. El ciberespionaje y los ciberataques de las agencias de inteligencia (predominantemente de países no democráticos) se han convertido en la amenaza moderna más importante para los sistemas automatizados, superando los delitos ordinarios con fines de lucro. Además de la protección efectiva y respuesta inmediata a las ciberamenazas, la investigación de los ciberincidentes es un elemento clave llevado a cabo por organismos policiales y de inteligencia autorizados cuando sea necesario. Este artículo considera aspectos y cuestiones clave para sugerir recomendaciones prácticas para la preparación y contratación de expertos forenses en estas investigaciones. Además, aborda los objetos examinados, las particularidades de su eliminación y las preguntas que deben formularse a los expertos en telecomunicaciones e informática.

Palabras clave: ciberamenaza; ciberataque; ciberdelincuencia; ciberincidente; criminalística; investigación; peritaje forense; Ucrania

Section: Dossier • Scientific and technological research article

Received: November 30, 2021 • Accepted: March 2, 2022

Contact: Andrii Padalka ✉ andrii_padalka@edu.cn.ua

Introduction

Appointing forensic expertise is an important stage in investigating nearly every criminal offense. In *science-intensive*, *highly intelligent*, and *high-tech* crimes, appointing forensic expertise is crucial.

Legal knowledge alone will not enable an investigator to identify the traces of these crimes and their settings or perform further investigations that require reproducing the stages of these illegal acts; specialized knowledge must be involved. This requirement is fully applicable to the investigation of cybercrime. It requires a deep knowledge of modern information technology. Thus, the investigation of cybercrime without the appointment of computer or telecommunications expertise is inconceivable. The investigator must also be able to formulate the correct questions for the expert to obtain answers that can be effectively used in the process of evidencing the crime. Often, the initiator poses incorrect questions when appointing an examination. These may be issues that cannot legally be resolved by experts (Criminal Procedure Code of Ukraine, 2012c). Furthermore, replicating all the questions from the reference books, manuals, or departmental instructions on the appointment of forensic examinations (Ministry of Justice of Ukraine, 1998) would complicate and slow down an expert's work.

Thus, the preparation and appointment of forensic examinations during cybercrime investigations remain relevant objects of scientific research to develop scientifically substantiated recommendations for their implementation. According to the Criminal Procedure Code of Ukraine (2012c), an expert in criminal proceedings is a person with scientific, technical, or other specialized knowledge; the right to conduct an expert study, according to the Law of Ukraine (1994) *On Forensic Examination*; and the training to examine objects, phenomena, and processes concerning circumstantial information on the criminal offense and offer an opinion on issues that arise during the criminal proceedings according to the individual's scope of knowledge. An expert study is conducted by a professional expert organization or experts engaged by the parties to the criminal proceedings. In the cases provided in Article 244 of this Code, the investigating judge will seek expert support at the defense's request if specialized knowledge is required to clarify the circumstances relevant to the criminal proceedings. However, this expertise cannot be used to clarify legal issues (Security Service of Ukraine, 2015).

While some criminal offenses can be successfully investigated without the appointment of forensic expertise, others may require specific knowledge. A forensic expert possesses specialized knowledge in fields including science, technology, art, and craft that other participants of the criminal proceeding do not. For example, forensic expertise is essential in *high-tech* crimes, given the intense development of computer technologies

that require new technical solutions almost on a daily basis. Fittingly, criminals *hack* these technologies or methods to commit illegal acts. Although legal knowledge is fundamental for the investigator, prosecutor, and judge, they usually lack technical knowledge in information technology, making cybercrime investigation without expert help impossible (Yaroshenko et al., 2018).

The expertise typically required in criminal investigations can be referred to as *general*. However, we will refer to the expertise required in the crimes addressed here as *specialized*. In the investigation of cybercrime, the first group of *specialized* expertise includes those necessary to study the mechanisms and means of conducting cyberattacks. Specialized knowledge in information technology, namely computer technology and telecommunications, is vital in these crimes.

It should be noted that depending on the subject under study, certain computer and technical examinations can be attributed to *general* expertise categories. These include examining a suspect's signature in documents and examining photos or video surveillance camera recordings to identify a suspect's laptop or establish its brand and model. For example, the examination of email history can be considered *general* expertise, as it does not presuppose studying the mechanisms and means of cyberattacks. The need to investigate correspondence may arise in investigating many crimes, including theft and corruption. However, if this correspondence contains a description of a cyberattack, this description should be provided to the expert to meticulously examine the attack's mechanism, making it *specialized* expertise.

Specialized expertise implies a more detailed examination of items containing information on a cyberattack. These include:

- Items containing information regarding a possible a cyberattack;
- Items evidencing a consummated cyberattack (or its individual stages) or information on the consequences.

It should be noted that large-scale cyberattacks, especially Advanced Persistent Threat (APT), which are complex cyberattacks to gain unauthorized access to the victim's information systems for control or future use (Daly, 2009), are usually implemented in several stages. Each stage, including the preparation stage, can be a separate cyberattack. Traces of these stages can be considered a plan for a cyberattack, whose final stage is the actual attack. These individual stages –considered cyberattacks in themselves– are a chain of attacks, components of a large-scale cyberattack.

Usually, before appointing an expert, investigative actions are carried out to seize material evidence, which is subsequently submitted for expert examination. For example, when inspecting the attacked system, the following items are seized and submitted for expert examination:

- Media, their clones, or bitmaps;
- RAM dumps;
- Log files of services and applications;
- Login settings;
- Diagnostic report files;
- Diagnostic utility setups;
- Schemes for building automated systems and their integration into clusters and networks;
- Schemes of internal networks (LAN, Local Area Network) and connection to the global network (WAN, Wide Area Network);
- Network equipment setups;
- Software configuration (system, server, and user) of the automated system, particularly remote access configurations; and
- Email correspondence, primarily emails containing attachments (potential malware) or external links (potential sources of malware downloads).

Each cyberattack has its own characteristics; therefore, an exhaustive list of recommendations to extract each specific item is impossible. To find and extract the evidence correctly, the investigator must involve a knowledgeable person in the investigative action and a technical and forensic support unit specialist in the investigation actions. This specialist's knowledge should be in the middle ground between the investigator and the forensic expert (Kozlovskyi et al., 2019).

Prior to the 2016 internal affairs bodies reform, the expert service of the Ministry of Internal Affairs was part of the police. The experts were police officers that, in addition to performing forensic examinations, also provided technical and forensic support for investigative actions. After the reform, the Ministry of Internal Affairs' expert service was no longer part of the Ukrainian National Police's structure; forensic examinations remained the core function of external experts. However, the National Police introduced positions for technical and forensic support of investigative actions for forensic inspectors.

The experience, however, revealed that the quality of site inspections by forensic inspectors was much worse than by forensic experts (Guliyeva et al., 2018). The outcome was not surprising. Unlike the forensic inspectors, the experts are not only knowledgeable in finding and collecting material evidence, but they also know how to analyze this evidence further during the expert examination. Moreover, an expert can assess the identified material evidence better in terms of its further suitability for examination, including recording, extracting, and storing the evidence better, ensuring its proper preservation.

Literature Review

Expert units in the Security Service of Ukraine simultaneously perform the functions of forensic support of justice and technical and forensic support of investigative actions, counterintelligence, and operational and investigative measures. Therefore, forensic activity in Ukraine is considered here in more detail.

The Law of Ukraine (1994), *On forensic examination*, regulates the basic principles of forensic activity in Ukraine. It defines a forensic examination as a study of objects, phenomena, and processes based on specialized knowledge in science, technology, art, and craft, among others, to provide an opinion on issues that are or will be the subject of litigation. Therefore, persons can be forensic experts if they possess the necessary knowledge to provide an opinion on the issues under investigation.

The legal procedure for appointing an expert and using the expert's opinion as a source of evidence is regulated by the relevant procedural codes. These are the Criminal Procedural Code of Ukraine (2012a), Civil Procedural Code of Ukraine (2004), Commercial Procedure Code of Ukraine (1991), and the Code of Administrative Procedure of Ukraine (2005).

Article 7 of the Law of Ukraine (1994), *On forensic examination*, defines the system of forensic institutions in Ukraine. These specialized agencies operate within the systems of the Ministry of Justice, Ministry of Internal Affairs, Ministry of Health, Ministry of Defense, the Security Service of Ukraine, and the State Border Guard Service of Ukraine.

It should be noted that expert profiling (computer-technical and telecommunication) in cyber-attack-related cybercrime investigations is not performed in all the forensic institutions listed above. It is only performed in expert institutions of the Ministry of Justice, Ministry of Internal Affairs, and the Security Service of Ukraine.

The Ministry of Justice's system of forensic institutions consists of the Scientific Research Institutes of Forensic Expertise (NDISE) and the Research Center for Forensic Examination on Intellectual Property. Currently, there are six NDISE in Ukraine located in Dnipro, Donetsk (temporarily moved to Slovyansk due to the partial occupation of some territories of the Donetsk region), Kyiv, Lviv, Odesa, and Kharkiv, with regional offices in other regions.

The Ministry of Justice's Department of Expert Support of Justice directs and controls the activities of forensic science and research institutions belonging to this Ministry and forensic experts that are not employees of state specialized institutions. The Ministry of Justice has established and operates an interdepartmental Coordination Council for Forensic Problems and a Central Expert Qualification Commission, as well as the Scientific Advisory and Methodological Council on the Issues of Forensic Examination.

Analysis of Expert Services

Expert services in Ukraine

The forensic institutions of Ukraine's Ministry of Justice annually conduct more than 100 thousand examinations (about 83 thousand are in criminal proceedings) and support the activities of the courts of all levels. They also support the National Anti-Corruption Bureau of Ukraine (NABU), the Specialized Anti-Corruption Prosecutor's Office (SAPO), the investigative bodies of the Ministry of Internal Affairs, Ukraine's Security Service (SSU), prosecutor's offices, customs service, and other institutions (Ministry of Justice of Ukraine, 2021).

In addition to providing a wide range of forensic expertise, these institutions also provide expertise in scientific forensic theoretical and practical principles, new methods of expert research, and forensic expert training and certification in these areas of research. The Kyiv NDISE (KNDISE) is the Ministry of Justice's largest forensic institution in Ukraine. It has five multidisciplinary laboratories and two departments that are directly involved in forensic science. The KNDISE has seven additional regional departments in Vinnytsia, Zhytomyr, Kropyvnytskyi, Ternopil, Khmelnytsky, Cherkasy, and Chernihiv.

The National Scientific Center, "Hon. Prof. M. S. Bokarius Forensic Science Institute" (NSCFSI), is one of the Ministry of Justice's leading scientific and research institutions. The Institute offers more than thirty types of expertise, including criminalistic, chemical forensic, biologic, physical, automotive forensic, construction, technical and commodity, and forensic accounting. The NSCFSI has a forensic theory department with an information and computing center that develops automated data banks and information retrieval systems. The NSCFSI also includes the Poltava and Sumy regional branches. It offers a postgraduate and doctoral program in specialty 081, Law, and forensic profiling to train highly qualified scientific and scientific-pedagogical staff.

In terms of its number and its tasks, the Expert Service of the Ministry of Internal Affairs of Ukraine is the largest. It includes the State Scientific Research Forensic Center (SSRFC) and the Ministry of Internal Affairs of Ukraine, the main institution of the service. It provides the service's organizational, managerial, and scientific-methodological management, with territorial research forensic centers (SRFC) located in the regions of Ukraine.

The main tasks of this expert service include forensic activities, involving employees in pre-trial investigation and trial, certification and other tests, property assessment, ensuring the functioning of accounting for instruments of criminal offenses, information retrieval systems, training, retraining, and advanced training of employees as forensic experts.

The Security Service of Ukraine's system of expert institutions includes the Ukrainian Research Institute of Special Equipment and Forensic Expertise of the Security Service of Ukraine (ISSEE SSU) and separate expert units in the regional bodies of the SSU. Some of the main forensic expertise classes conducted by divisions include criminalistic, special technical means of information interception, forensic biological, explosive technical, and computer and telecommunications. Its functions are entrusted to the ISSEE SSU.

The ISSEE SSU consists of five centers, three separate departments, and six separate sectors. The Center for Forensic and Special Expertise (CFSE) performs the functions of forensic support of justice, forensic support of investigative actions, and operational search activities carried out by the SSU's investigative and operational units and other law enforcement agencies. The CFSE is the ISEE SSU's only structural unit with a proper name in addition to a number (other units have only numbers), indicating the extreme importance of its responsibilities.

The ISEE SSU also has 15 separate expert units in SSU Departments in Donetsk, Luhansk, Odesa, Lviv, Kharkiv, Dnipropetrovsk, Chernihiv, Rivne, Volyn, Zakarpattia, Ivano-Frankivsk, Ternopil, Chernivtsi, Kirovohrad, Poltava, and the Zhytomyr region. Some of these separate units are zonal; they provide services to several regions (Ukraine Security Service, 2020). The responsibilities of the ISEE SSU include:

- Development of the latest forensic tools, technologies, forensic expertise methods, and the preparation of practice manuals and their implementation in practical activity;
- Scientific, methodological, and informational support of expert activity, analysis of expert practice, development of practice manuals, and other methodological support of the forensic activity.

In this regard, the Institute develops forensic examination methods and organizes their certification and state registration according to the procedure prescribed by the Cabinet of Ministers of Ukraine.

The ISSEE SSU has a Scientific and Methodological Council for Forensic Expertise (SMC), whose main task is to review the Institute's forensic expertise staff's scientific works. The SMC's chairman is the Institute's director. Its first deputy chairman is the deputy director supervising the activities of the CFSE and the head of the center. The other members of the Council are elected by CFSE staff by secret ballot.

It should be noted that forensic institutions must have ISO / IEC 17025 accreditation to guarantee their compliance with the international standard requirements recognized worldwide, ensuring the quality of their forensic activities. Similarly, certain issues related to forensic expertise also require ISO / IEC accreditation regulating international sectoral standards. The ISSEE SSU, for example, is currently developing the

Ukrainian Scientific Research and Training Center for Standardization, Certification, and Quality Problems (DSTU) using a direct translation of the ISO / IEC 27042: 2015 Information technology –Security techniques– Guidelines for the analysis and interpretation of digital evidence. The introduction of international standards in expert institutions not only ensures the use of best practices in forensic activities; it standardizes approaches to these activities. Regardless of whether the examination is conducted in Germany, France, or Ukraine, the basic principles of the examination will be the same (Parfilo & Nizovtsev, 2020).

The ISSEE SSU is the only state forensic institution in Ukraine. Besides being an expert institution, it has research and development units and certain production facilities. As part of improving forensic activities, it develops and implements specialized forensic equipment (specialized software and hardware, means for search and retrieval of forensic evidence, among others) and improves existing ones in close cooperation with experts.

According to part two of Article 8 of the Law of Ukraine, *On the basic principles of cybersecurity in Ukraine*, the main subjects of the national cyber security system are the State Service for Special Communications and Information Protection of Ukraine, the National Police of Ukraine, the Security Service of Ukraine, the Ministry of Defense of Ukraine and General Headquarters of the Armed Forces of Ukraine, intelligence agencies, and the National Bank of Ukraine (Law of Ukraine, 2017). The task of ensuring the implementation of the Cybersecurity Strategy Implementation Plan of Ukraine is entrusted to Ukraine's Security Service, its cabinet of Ministers, and the Foreign Intelligence Service (President of Ukraine, 2021).

Each agency forms and develops its expert institutions according to its needs. Among them, only the Security Service of Ukraine has forensic units in its structure. Out of all the expert institutions (Ministry of Justice, Ministry of Internal Affairs, and the Security Service of Ukraine [SSU]), only the SSU's forensic experts are servicemen; in fact, more than half of its experts are service members, some with access to secret State information in the prescribed form (Abrhám et al., 2018).

Because of the peculiarities of the special services' operational and service activities, experts must often conduct forensic examinations and expert studies on materials considered State secrets. In addition, because some SSU experts are servicemen, their involvement effectively supports technical and forensic investigative and operational actions (counterintelligence and operational search), including covert operations or those conducted in combat areas (Joint Forces Operation). Finally, when required, the experts can also perform urgent expertise or expert analyses around the clock; this is especially relevant, for example, when investigating the preparation of a terrorist act to prevent it.

Types of expertise

The types of expert investigations conducted by the Institute are also influenced by the profile of the Service's activity. For example, only SSU experts can conduct expert inquiries regarding special technical information interception because the responsibility of its investigative units includes crimes related to these specific technical means, including illicit trafficking and espionage. Considerable attention is also focused on computer-technical and telecommunication expertise, particularly the relevant expert unit's proper technical equipment. In this case, special attention is paid to the technical means of obtaining forensic information while preserving the original condition of the objects, avoiding their destruction or damage.

Thus, hardware write blockers are used to avoid making changes to the information content of the examined storage media. These include the EPOS WriteProtector (2021c), a hardware protector designed to prevent accidental or intentional changes to the data on the Hard Drive Disk (HDD) when investigating computer incidents and crimes; the EPOS BadDrive Adapter, a specialized recording blocker used in the recovery process of hard disks with defective and unstable sectors (EPOS, 2021a); the EPOS BadDrive Adapter USB, a specialized hardware recording blocker for removing and recovering information on USB-drives with defective sectors (EPOS, 2021b); the Tableau T6es-B, a compact write-blocker for hard drives with SAS interface (Guidance Software, 2020a); the Tableau T3458is, which is a universal hardware recording blocker that supports several interfaces, including IDE, SATA, SCSI, and USB (Guidance Software, 2021b); the CRU WiebeTech Forensic UltraDock Fudv5.5 Drive Write Blocker, a universal hardware write-blocker that supports several interfaces, including eSATA, USB 3.0, PATA/IDE/EIDE, FireWire 800, SATA II, USB 2.0, SATA III, SATA I, and FireWire 400 (WiebeTech, 2021a); and the CRU WiebeTech USB 3.0 WriteBlocker compact hardware (WiebeTech, 2021b).

In addition, modern forensic software provides the direction of computer and technical expertise in expert units. X-Ways Forensics software, for example, provides support for file systems of various types (FAT12, FAT16, FAT32, exFAT, TFAT, NTFS, Ext2, Ext3, Ext4, Next3 ®, CDFS / ISO9660 / Joliet, and UDF). It detects and accesses alternative NTFS (ADS) data streams, providing the built-in interpretation of JBOD, RAID 0, RAID 5, RAID 5EE, and RAID 6 systems; software RAID implementations in Linux and Windows operating systems and LVM2 dynamic disks; and the ability to read partitions and file system structures from RAW images (.dd), as well as ISO, VHD, and VMDK, among others (X-Ways, 2021). Running X-Ways Forensics without installation allows running it on third-party computers during investigations. Although X-Ways Forensics has effective capabilities for detecting and recovering deleted files, the powerful R-STUDIO Network Technician tool is also used to recover deleted information.

Another powerful software package is the Magnet AXIOM, developed by Magnet Forensics, which is used to examine different media (Magnet Forensics, 2021). This software package enables automated and manual searches for digital evidence in media images and mobile devices running on iOS, Android, Windows Phone, Blackberry, and Windows Mobile. It allows extracting, decrypting, and decoding the structure of mobile file systems devices manufactured by Apple, Blackberry, and Android-based devices. It also allows processing images in E01, DD, and DMG formats, virtual hard disks and virtual machine disks, memory dumps, and physical and logical copies of mobile devices supporting file systems such as NTFS, FAT / ExFAT / TFAT, Ext2-Ext4, ReiserFS, UFS / UFS2, HFS / HFS +, Next3, CDFS, ISO9660, Joliet, and UDF. The Magnet AXIOM complex can also be used to examine (analyze and recover) data in RAM dumps.

Cellebrite UFED Touch 2 software and hardware are used to examine mobile devices, such as mobile phones, smartphones, tablets, and GPS navigators, providing full access to physical, logical, and file system data. Software functions include extracting, decoding, analyzing the information obtained, and compiling a practical report for other participants in the criminal process. The complex's compact format and convenient, intuitive interface help create information content dumps of mobile devices outside the forensic institution (Cellebrite, 2021).

The Center for Forensic and Special Expertise experts use the XRY software and hardware complex to examine mobile devices. Although XRY is usually sold as a software product, the developers produced a unique software and hardware complex based on a moisture-resistant tablet at the request of experts. This technical solution has enabled the effective use of XRY in investigative (search) activities outside the expert unit (MSAB, 2021).

The examination of mobile devices, including outside the unit, is conducted using a software and hardware complex based on the specialized forensic software, MOBILedit Forensic Express PRO (MOBILedit, 2021), and a compact and powerful ultrabook-transformer.

In 2018, the ISSEE SSU received accreditation according to the ISO / IEC 17025 international standard in computer and technical examinations. The Institute is also actively involved in implementing international standards for the investigation of cyber incidents within the Ukrainian regulatory framework, particularly the international ISO-IEC 27042-2016 standard. However, despite the significant efforts in managing expert institutions to successfully provide forensic support in investigating cybercrimes and countering cyber threats in Ukraine, several problematic issues remain unresolved. They are discussed in more detail below.

One of these problematic points is the insufficient scientific and methodological base. According to Russetskiy (2018), the analysis of scientific developments in recent

years shows that the difficulty in generalizing empirical material is that methods for detecting cyberattacks using malicious software (malware) are sealed and mainly carried out by the relevant units of the SSU.

Given its prevalence in cyberattacks and the potential destructive power of malware –a software specially designed or modified for these purposes– performing high-quality investigations of cyber incidents involving the illegal use of such software is becoming increasingly important. However, although approved by the Ministry of Justice of Ukraine, the document, *Methods of computer and technical research in cases related to the establishment of facts of interference in the work of automated systems*[1], did not provide clear answers on how to investigate potential malware nor on the general criteria for deeming a program malicious.

With this in mind, between 2014 and 2018, the ISSEE SSU developed a guideline called the "Forensic examination of malicious software" (Nizovtsev, 2018). It consists of six sections. The first one discusses the subject of malicious software, defining the concept and the task of forensic expertise in this regard. The other sections include the classification of malicious software, some examples of malicious software, the requirements for materials provided for examination, the methods of malicious software examination, and the stages of expert examination. In addition, it provides a list of abbreviations and references. In 2020, these guidelines were completed, and the techniques for malware detection were expanded (Nizovtsev, 2018). Earlier, in 2016, the ISSEE SSU developed guidelines for forensic examination of signs of remote Denial-of-Service attacks, which constitute a significant share of the cyberattacks (Nizovtsev, 2016).

Another significant problem is the lack of highly qualified experts, especially those specialized in telecommunications systems (equipment) examinations and tools. As most cyberattacks are carried out via the Internet or local area networks, experts must have in-depth knowledge of network technologies, including network types, data transmission protocols, and network addressing methods, to conduct examinations. Unfortunately, as of October 2021, only 34 out of 61 forensic experts certified in this specialty nationwide were authorized, a critically low number. The main reason is not the quality of education, as many higher education institutions in Ukraine train highly qualified IT specialists. However, government agencies and even expert institutions cannot offer these specialists competitive wages. Therefore, graduates prefer private companies that can offer much higher salaries.

Expanding on the issue of the definition of malicious software (malware) according to Ukrainian legislation, Article 361-1 of the Criminal Code of Ukraine (2001) defines it as malicious software intended for unauthorized interference involving electronic com-

1 Method registration number 10.9.12, registered on January 29, 2016.

puters, automated systems, computer networks, or telecommunications networks Article 361 provides for liability for unauthorized interference involving electronic computers, automated systems, computer networks, or telecommunications networks leading to leakage, loss, forgery, and blocking of information, distortion of the processing of information, or violating the established procedure for its routing (Criminal Code of Ukraine, 2001). Thus, Ukrainian legislation provides a concordant definition and liability for the mentioned actions.

However, investigators typically appoint forensic expertise during malicious software crime investigations to obtain an expert opinion on whether the program is, in fact, malicious software, and establishing the program's *harmfulness* is beyond the expert's competence. Several technical and legal factors hinder the expert's right to determine whether the program is malicious software, negating the expert's opportunity to do so. The following are among the legal factors.

First, classifying the program as malicious software implies deeming it *unauthorized*. This feature is a legal concept, and the solution of legal issues through expertise is prohibited by Art. 242 of the Criminal Procedure Code of Ukraine (Criminal Procedural Code of Ukraine, 2012b). Secondly, an investigation must take place to determine the designed program's exact purpose and the program developer's (or customer's) intent behind its creation (including unauthorized interventions). In this regard, several problem issues arise, which are discussed below.

Intention is a form of guilt, which is an element of the crime. Establishing the corpus delicti –or *legal qualification of the corpus delicti*– is the main object of proof. However, under Ukrainian law, the burden of proof lies with the investigator and prosecutor, not the expert. *Proof* involves the collection of evidence, but the law prohibits an expert from gathering evidence on his or her own. Lastly, the intent is not reflected in the program code (although it may be reflected in some way in the technical documentation); thus, the gathering of evidence is unavoidable.

The following should be noted regarding the technical factors preventing forensic experts from classifying the program as malicious software.

1. There are no purely malicious functionalities. Any function can be inherent in useful programs (for example, deleting a file can be both useful and malicious).
2. There is no one-size-fits-all link between a program's functionality and its purpose; the same function can be used for different purposes.
3. Programs with the same purpose can have significant differences in functionality and the basic principles of operation. Conversely, programs with different uses may have similar functionality.
4. A useful program can be used for harmful purposes and vice versa, depending on the user's intention.

5. Technical failures, like *bugs* or vulnerabilities, in a useful program can perform malicious actions. However, this does not imply that the program is malicious.
6. A useful program can perform malicious actions when run with the wrong settings (the user makes a mistake).

Discussion

Thus, an expert cannot classify a particular program as harmful upon examination. Instead, the expert can examine the program's functionality to determine whether it can, for example, be used to perform certain (harmful) actions, function in a specific automated information system, and copy itself to removable media (flash carrier). Therefore, when appointing forensic expertise, the correct wording of the questions to the expert is essential. The *Scientific and methodological recommendations for the preparation and appointment of forensic expertise and expert examinations* by the Ministry of Justice of Ukraine (1998) provide a significant amount of information on the functions of certain types of expertise. Similarly, common questions that may be posed to the expert can be found in the Security Service of Ukraine's (2015) document, *On the approval of the Instruction on appointment and conduct of forensic examinations and expert research in the system of the Security Service of Ukraine*, and directories. In addition, examples of questions concerning scientific and methodological materials, specifically, are provided in the sources mentioned above.

The following are general exemplary issues that can be raised for forensic expertise in investigating cybercrime and countering cyber threats.

1. Are there any signs of interference in the telecommunications system?
2. Do the log files submitted for examination (indicate which ones) or the diagnostic utilities report files (indicate which ones) contain evidence of a cyberattack? If so, what cyberattack evidence do the log files or diagnostic utilities report files provided for examination contain?

It should be explained why this last question concerns evidence of a cyberattack and not establishing the fact. Firstly, a cyber incident may be caused by a technical failure, and it is not always possible to positively establish that a technical failure has occurred, especially if the failure occurred outside the affected system. For example, if a computer user visited a web page on the affected system and the computer's browser began to refresh the page indefinitely due to an F5 sticky key, in effect, performing a remote denial-of-service attack. Of course, this can also result from conscious user actions; it is enough to simply press the "F5" key with an object. Technically, the identical thing happened in both cases (Inshyn et al., 2021). However, in the first case, it is a technical failure without any user intention; meanwhile, the second one involves intentional illegal actions by the user. The

log files of the affected automated system will not show the reason for pressing the "F5" key on the user's computer; only information regarding numerous requests of a specific Internet page from a specific computer is recorded. Thus, we are referring only to the signs of a cyberattack. Initial data may not be enough to establish the fact of a cyberattack.

3. Was there evidence of access to the telecommunication system; how was it done?

This question concerns obtaining remote control of the affected automated system. This control is possible with the help of regular operating system tools, usually if the attackers know the relevant authorization data. Also, third-party applications are often used for remote administration, including TeamViewer, Radmin, and Ammyy Admin, again, provided that the attackers have authorization data. However, attackers often use specially designed malicious software to penetrate automated systems –the so-called backdoors.

4. Was there evidence of information transmission (receipt) in the telecommunication system; in what way?

Cybercriminals often download additional files to the affected system (usually specific additional modules of malicious software) or download specific files from this system (for example, keylogger logs).

5. In which operating system is the program provided for examination able to function? (Specify which one is the file name, folders, etc.)
6. Can the program submitted for examination (specify which one) function in the following conditions: (specify the architecture and composition of the computer, the name and version of the operating system, and the presence or absence of certain libraries.)?
7. Is it possible to perform certain actions (specify which ones) with the help of the examined program (specify which one)?

These last questions concern the potential malware's functionality.

Only the most common questions that can be posed to a forensic expert in the investigation of cybercrime and countering cyber threats in Ukraine have been listed. Consideration of all issues and disclosure of their essence is beyond the scope of this publication.

Conclusion

There are several departmental expert services and institutions in Ukraine. The largest is the expert service of the Ministry of Internal Affairs of Ukraine and expert institutions subordinated to the Ministry of Justice of Ukraine. Although the smallest in employee

numbers, the expert service of the Security Service of Ukraine plays a significant role in supporting forensic, technical, and criminalistic cybercrime investigation and countering cyber threats in Ukraine, given its tasks. The institution is accredited in computer and technical expertise under the ISO / IEC 17025 international standard. It actively participates in the implementation of international standards for cyber incident investigations in the Ukrainian regulatory framework and develops scientific and methodological materials for expert assessments in cybercrime investigations.

The most effective measures directly aimed at combating cybercrime include:

- Increasing the number of scheduled and unscheduled inspections.
- Establishing strict control over the circulation of technical means prohibited or restricted in free civil circulation.
- Adopting the experiences in this area of law enforcement agencies abroad.
- Cooperating with relevant authorities in other countries on detecting, investigating, and preventing crimes in the analyzed area.
- Exchanging experiences in law enforcement; and
- Identifying persons prone to committing crimes in the analyzed area.

However, these measures require further research developments to create effective tools to counter the modern challenges of cybercrime.

Despite considerable efforts to increase the capacity of expert institutions in performing computer and telecommunications expert investigations in cybercrime, there are still significant challenges in this area. They include insufficient scientific and methodological base, lack of highly qualified personnel, and inadequate legislation.

Disclaimer

The authors declare no potential conflict of interest related to the article.

Funding

The authors do not report sources of funding for this article.

About the authors

Andrii Padalka is a Ph.D. in Legal Science, Deputy Director of the Ukrainian Scientific and Research Institute of Special Equipment and Forensic Expertise of the Security Service of Ukraine, and Associate Professor at the Department of Financial Investigations of the University of the State Fiscal Service of Ukraine.

https://orcid.org/0000-0003-1433-1030 - Contact: andrii_padalka@edu.cn.ua

References

Abrhám, J., Britchenko, I., Jankovic, M., & Garškaite-Milvydiene, K. (2018). Energy security issues in contemporary Europe. *Journal of Security and Sustainability Issues, 7*(3), 387-398. https://doi.org/10.9770/jssi.2018.7.3(1)

Cellebrite. (2021). *UFED Touch 2*. https://www.cellebrite.com/en/ufed/

Civil Procedural Code of Ukraine. (2004). Law No. 1618-IV. Base "Legislation of Ukraine." March 18, 2004. https://zakon.rada.gov.ua/laws/show/1618-15#Text

Code of Administrative Procedure of Ukraine. (2005). Law No. 2747-IV. Base "Legislation of Ukraine." July 6, 2005. https://zakon.rada.gov.ua/laws/show/2747-15#Text

Commercial Procedural Code of Ukraine. (1991). Law No. 1798-XII. Base "Legislation of Ukraine." November 6, 1991. https://zakon.rada.gov.ua/laws/show/1798-12#Text

Criminal Code of Ukraine. (2001). Law of Ukraine No. 2341-III. Article 361-1. https://zakon.rada.gov.ua/laws/show/2341-14#Text

Criminal Procedural Code of Ukraine. (2012a) Law of Ukraine No. 4651-VI. Article 4651-VI. https://zakon.rada.gov.ua/laws/show/4651-17#Text

Criminal Procedural Code of Ukraine. (2012b). Law of Ukraine No. 4651-VI. Base "Legislation of Ukraine." April 13, 2012. https://zakon.rada.gov.ua/laws/show/4651-17#Text

Criminal Procedural Code of Ukraine. (2012c). Law of Ukraine No. 4651-VI. Code of Ukraine. May 20, 2012. https://zakon.rada.gov.ua/laws/show/4651-17#Text.

Daly, M.K. (2009). *The Advanced Persistent Threat (or Informationized Force Operations)*. USENIX. https://static.usenix.org/event/lisa09/tech/slides/daly.pdf

EPOS. (2021a). *EPOS BadDrive Adapter* https://www.epos.ua/view.php/ua/products_epos_baddrive_adapter

EPOS. (2021b). *EPOS BadDrive Adapter USB* https://www.epos.ua/view.php/products_epos_baddrive_usb

EPOS. (2021c). *EPOS WriteProtector*. https://www.epos.ua/view.php/en/products_epos_write_protector

Guidance Software (2020a). *Tableau T6es SAS Forensic Bridge.* https://tableau.guidancesoftware.com/pdf/en/Tableau_T6es_Product_Brief.pdf

Guidance Software (2021b). *Tableau Hardware T3458is*. https://tableau.guidancesoftware.com/index.php?pageid=specs&xml=spec_t3458is.xml&model=T3458is

Guliyeva, A., Britchenko, I., & Rzayeva, U. (2018). Global security and economic asymmetry: A comparison of developed and developing countries. *Journal of Security and Sustainability Issues, 7*(4), 707-717. https://doi.org/10.9770/jssi.2018.7.4(8)

Inshyn, M., Vakhonieva, T., Korotkikh, A., Denysenko, A., & Dzhura, K. (2021). Transformation of labor legislation in the digital economy. *InterEULawEast, 8*(1), 39-56. https://doi.org/10.22598/iele.2021.8.1.3

Kozlovskyi, S., Butyrskyi, A., Poliakov, B., Bobkova, A., Lavrov, R., & Ivanyuta, N. (2019). Management and comprehensive assessment of the probability of bankruptcy of Ukrainian enterprises based on the methods of fuzzy sets theory. *Problems and Perspectives in Management, 17*(3), 370-381. https://doi.org/10.21511/ppm.17(3).2019.30

Law of Ukraine (1994). *On forensic examination*. No. 4038-XII. Article 7. February 25, 1994. https://zakon.rada.gov.ua/laws/show/4038-12#Text

Law of Ukraine. (2017) No. 2163-VIII. *On the basic principles of cybersecurity in Ukraine*. Article 8, part 2. https://zakon.rada.gov.ua/laws/show/2163-19#Text

Magnet Forensics. (2021). MAGNET AXIOM. https://www.magnetforensics.com/products/magnet-axiom/

Ministry of Justice of Ukraine. (1998). Instruction No. 53/5. *Scientific and methodological recommendations on the preparation and appointment of forensic examinations and expert studies*. https://zakon.rada.gov.ua/laws/show/z0705-98#Text.

Ministry of Justice of Ukraine. (2021). *Transition Book: Mission and Responsibilities*. https://www.pravojustice.eu/storage/app/uploads/public/5d7/f77/c88/5d7f77c88c23b147881339.pdf

MOBILedit. (2021). *MOBILedit Forensic Express PRO*. https://www.mobiledit.com/online-store/forensic-express

MSAB. (2021). *XRY Mobile Forensics and Data Recovery Software*. https://www.msab.com/product/xry-extract/

Nizovtsev, Yu.Yu. (2016). *Forensic examination of signs of interference in the work of information and telecommunications systems by remote attacks on denial of service: guidelines.* Kyiv: ArTek Publishing House.

Nizovtsev, Yu.Yu. (2018). *Forensic examination of malicious software: guidelines*. Kyiv: ArTek Publishing House.

President of Ukraine. (2021). Presidential Decree No. 447/2021. *On the Cyber Security Strategy of Ukraine*. Decision of the National Security and Defense Council of Ukraine. August 26, 2021. https://www.president.gov.ua/documents/4472021-40013

Russetskiy, A. A. (2018). Place of Forensic Science in the Cyberthreats Prevention System in Field of a Ukrainian Information Security. *Theory and Practice of Forensic Science and Criminalistics*, *18*, 263-271. https://doi.org/10.32353/khrife.2018.29

Security Service of Ukraine. (2015). Request No. 371. *On the Approval of the Instruction on Appointment and Conduct of Court Appraisals and Expert Surveys in the System of the Ukrainian Security Service.* https://zakon.rada.gov.ua/laws/show/z0738-15

Ukraine Security Service, Order of the Central Department. (2020). Request No. 80. *On approval of Amendments to the Regulation on the Security Service of Ukraine Expert-Qualification Commission and Certification of Court Experts*. https://zakon.rada.gov.ua/laws/show/z0310-20#Text

WiebeTech. (2021a). *Forensic UltraDock FUDv5.5 by* CRU. https://www.cru-inc.com/products/wiebetech/forensic-ultradock-v5-5/

WiebeTech. (2021b). *USB 3.0 WriteBlocker by CRU*. https://www.cru-inc.com/products/wiebetech/usb-3-0-writeblocker/

X-Ways. (2021). *X-Ways Forensics: Integrated Computer Forensics Software*. http://www.x-ways.net/forensics/

Yaroshenko, O. M., Vapnyarchuk, N. M., Lozovoi, S. V., Yakovleva, G. O., & Yakovlyev, O. A. (2018). General-compulsory medical insurance: World experience. *Journal of Advanced Research in Law and Economics, 9*(5), 1829-1838. https://doi.org/10.14505//jarle.v9.5(35).38

Esta página queda intencionalmente en blanco

Revista Científica General José María Córdova
(Colombian Journal of Military and Strategic Studies)
Bogotá D.C., Colombia

Volume 20, Number 38, April-June 2022, pp. 425-442
https://dx.doi.org/10.21830/19006586.912

The International Court of Justice and the international humanitarian law rules for armed conflicts

La Corte Internacional de Justicia y las normas de derecho internacional humanitario en conflictos armados

Walter Arévalo-Ramírez
Universidad del Rosario, Bogotá D.C., Colombia

Abstract. This article analyzes the undermined importance of the International Court of Justice's (ICJ) case law in interpreting international humanitarian law (IHL) and its relationship with public international law. It examines how the ICJ has elevated IHL to customary law, declaring it "intransgressible" and equating it with jus cogens, and identified particular obligations for the parties in conflict. The article studies how the Court has clarified the relationships between customary IHL with the law of treaties and has declared which elements of IHL constitute the most basic principles of humanity, applicable whether it is an international or non-international armed conflict. Finally, the text analyzes how the Court has discouraged counterproductive separations between the application of IHL and international human rights law.

Keywords: customary law; International Court of Justice; humanitarian law; peremptory norm; treaties

Resumen. El artículo analiza la importancia socavada de la jurisprudencia de la Corte Internacional de Justicia (CIJ) para establecer la interpretación del derecho internacional humanitario (DIH) y su relación con el derecho internacional público. El artículo estudia cómo la CIJ ha elevado el DIH a derecho consuetudinario y lo ha declarado "intransgressible", equiparándolo con el jus cogens y ha identificado obligaciones particulares para las partes en conflicto. El artículo estudia cómo la Corte ha aclarado las relaciones entre el DIH consuetudinario con el derecho de los tratados y ha declarado qué elementos del DIH constituyen los principios más básicos de humanidad, aplicables tanto si se trata de un conflicto armado internacional como de uno no internacional. Finalmente, el texto analiza cómo la Corte ha desalentado separaciones contraproducentes entre la aplicación del DIH y el derecho internacional de los derechos humanos.

Palabras clave: costumbre; Corte Internacional de Justicia; Derecho internacional humanitario; norma imperativa; tratados

Section: Dossier • Scientific and technological research article

Received: December 6, 2021 • Accepted: March 12, 2022

Contact: Walter Arévalo-Ramírez ✉ walter.arevalo@urosario.edu.co

Introduction and theoretical approach

The contemporary International Humanitarian Law (IHL) scholarship and case-law research is heir to the proliferation of *ad hoc* decisions by international criminal tribunals (Schlütter, 2010) and the recent experience of its Residual Mechanism (Soufi, 2015), the International Criminal Court's ICC current activity, and its jurisprudential development in the matter of judging individual responsibility under armed conflicts (Sánchez, 2018). In general, contemporary IHL teaching focuses on the applications of internal armed conflict-derived rules –as a predominant form of conflict– and its particularities (Olasolo, 2019) and the study of the practice by National Armies and Organized Armed Groups, reflected in national legislations and the "rules of engagement" (Ardila-Castro, 2020). These feed customary international law, duly codified by the International Committee of the Red Cross (ICRC) (Henckaerts, 2005), which has developed an enormous amount of specific and deeply technical international law rules and identified their international criminal consequences. Paradoxically, this scope makes us forget, or at least overlook, the International Court of Justice's fundamental role in establishing the nature, definition, and application of international humanitarian law in selected cases since its first judgment in the *Corfu Channel case*.

This article proposes that it is fundamental to recapitulate the cases in which the International Court of Justice has been confronted with applying and analyzing facts or rules relating to international humanitarian law. As pointed out recently by authors such as Chetail (2003) in "The contribution of the International Court of Justice to international humanitarian law" or Gardam (2003) because of its special institutional characteristics, the International Court of Justice's normative relationship with international humanitarian law has special legal effects on States that cannot be ignored in the due application and development of international humanitarian law in internal armed conflicts or by the relevant actors guided by the most basic humanitarian guarantees.

Starting with the theoretical foundations of this position, first, we must highlight that, as the principal judicial organ of the United Nations, the International Court of Justice has a normative interpretative power and a particular "norm-making" capacity in identifying the rules of law and determining their nature like customary rules, *erga omnes*, and *jus cogens* (Henckaerts, 2005), that exceeds those that national courts, *ad hoc* international criminal courts, or transitional scenarios may have in their jurisprudence.

Thus, by identifying certain characteristics of international humanitarian law in its different aspects through the cases that will be analyzed, we propose that the International Court of Justice's proclamations on the nature and content of international humanitarian law has a broader universal effect on progressive development (Lauterpacht, 1982) and normative consolidation than other tribunals' judgments.

Secondly, its Statute being the most paradigmatic of the criteria for establishing the sources of international law in its Article 38, not only does the ICJ's particular authority and relationship with the sources of international law endow it with special power in establishing the content of international law but also, as an inter-state tribunal, the scope of its jurisprudence and advisory function is broader than the sometimes restricted and extremely casuistic-technical character of international criminal tribunals' jurisprudence, which as their mandate undoubtedly requires, deal with situations particular to the responsibility of individuals and is not easily extended into universal principles.

When analyzing cases of international State responsibility for internationally wrongful acts involving the major treaties of international humanitarian law such as the Geneva Conventions or the Convention on the Prevention and Punishment of Genocide, the International Court of Justice necessarily generates much more universalizable criteria on the nature of IHL rules in terms of its most essential principles (Crawford, 2002).

In turn, in its advisory opinions, the Court's ruling on what "is the law in force" in the matter in question (Verma, 2018) generates a pronouncement of special relevance for international law. This particular progressive development of international law in advisory jurisdictions is increasingly recurrent in international tribunals. It is based both on the strategic questions submitted by legal entities with procedural standing, such as states or international organizations, and the tribunals' initiative to take advantage of the opportunity to answer the questions submitted to them to generate normative developments (Abello-Galvis & Arévalo-Ramírez, 2019).

In this sense, it is the ICJ that, through its decisions and the justifications (dictum) included in them, is called upon to establish the relationship between particular regimes of law, such as the law of the sea or environmental law (Vinuales, 2008), with general public international law (general international law) (Chetail, 2003). The decisions analyzed in this article precisely exemplify this work of unification of international humanitarian law with the precepts of public international law. It analyzes and pronounces the customary nature of its rules and their relationship with classical issues of public international law and the law of treaties, including their temporal application, denunciations or reservations, the hierarchical relationship of IHL rules with concepts such as *ius cogens* or *erga omnes* obligations, and the legal structure of IHL itself concerning its status as a single law derived from basic principles of humanity.

This ICJ task has already occurred with other regimes, such as international human rights law; through its judgments, it has succeeded in establishing the necessary links to interpret it as a formative part of general international law.

The following sections will analyze the decisions of the ICJ's extensive docket (Arévalo-Ramirez & Martínez Vargas, 2018), recognized as directly related to international humanitarian law, and the criteria emanating from these decisions considered funda-

mental contributions of the Court to the understanding of international humanitarian law and its conception and application by the parties to the conflict.

Methodological approach of the case law review

Using all the available cases that relate to IHL since 1947 and a methodology involving a case-law doctrinal analysis with a descriptive-analytic approach to normative sources, this article examines how the ICJ jurisprudence has elevated international humanitarian law to customary law, declared it "intransgressible"–equating it with *jus cogens*–, and identified particular obligations for the parties in conflict, complementing the work of traditional customary IHL sources like the ICRC Customary International Humanitarian Law Handbook.

The article also studies how the Court has clarified the relationships between customary international humanitarian law with the law of treaties on issues such as reservations or denunciations to international humanitarian law treaties by states, establishing the elements of humanitarian law that constitute principles emanating from the most basic principles of humanity, which go beyond considerations relating to whether it is an international or non-international (internal) armed conflict or a case relating to the means of war or the principle of distinction.

Finally, the text analyzes how the Court has effectively avoided counterproductive separations between the scope of application of international humanitarian law and international human rights law (IHRL).

Discussion and analysis of ICJ case-law on international humanitarian law

Advisory Opinion on the legality of the threat or use of nuclear weapons (1996) and the indivisible nature of IHL

In the 1996 Advisory Opinion: *The Legality of the Threat or Use of Nuclear Weapons*, the ICJ had the particular opportunity, because of the tenor of the question, to analyze one of the typical discussions relating to international humanitarian law. Namely, the question of whether it is a unitary and indivisible body of rules (conventional, customary, and others) that applies uniformly or whether the idea remains, as taught, a law divided into sub-issues usually attributed to sets of treaties, as replicated by the concepts of "Hague Law" and "Geneva Law." The latter is usually understood as the set of rules regulating the use and humanitarian prohibitions predicated on the means of war and weapons; the other as the basic protections and guarantees of humanity to be observed over combatants and non-combatants.

This distinction is usually considered a strength of international humanitarian law. It is one of the most widely codified branches of law, with a long tradition of treaties relating to the weapons regulation and a long history of conferences and conventions, from the first humanitarian agreements prior to the Great Conference of 1907 to the current Additional Protocols of 1977 to the Geneva Conventions. However, their application by *ad hoc* criminal tribunals has shown that their separate idealization (the law of weapons on the one hand and the law of humanitarian guarantees on the other) can lead to normative gaps. Moreover, it can lead to debates on which norms apply to a state and which do not, depending on its ratified treaties when the idea that both sets of norms reflect the same unitary principles and customs should prevail.

In this regard, in the advisory opinion on the legality of the threat or use of nuclear weapons (International Court of Justice, 1996), the ICJ took an affirmative position on how this instrument had achieved the absolute consolidation of both parts of IHL as a single system after Protocol I of 1977[1]. It definitively developed the simultaneous application of the two regimes as one, both being expressions of the same customary principles of humanitarian nature. In this regard, the International Court of Justice (1996) stated:

> 75. A large number of customary rules have been developed by the practice of States and are an integral part of the international law relevant to the question posed. The "laws and customs of war" –as they were traditionally called– were the subject of efforts at codification undertaken in The Hague (including the Conventions of 1899 and 1907), and were based partly upon the St. Petersburg Declaration of 1868 as well as the results of the Brussels Conference of 1874. This "Hague Law" and, more particularly, the Regulations Respecting the Laws and Customs of War on Land, fixed the rights and duties of belligerents in their conduct of operations and limited the choice of methods and means of injuring the enemy in an international armed conflict. One should add to this the "Geneva Law" (the Conventions of 1864, 1906, 1929 and 1949), which protects the victims of war and aims to provide safeguards for disabled armed forces personnel and persons not taking part in the hostilities. These two branches of the law applicable in armed conflict have become so closely interrelated that they are considered to have gradually formed one single complex system, known today as international humanitarian law. The provisions of the Additional Protocols of 1977 give expression and attest to the unity and complexity of that law.
>
> 76. Since the turn of the century, the appearance of new means of combat has –without calling into question the longstanding principles and rules of international law– rendered necessary some specific prohibitions of the use of certain weapons, such as explosive projectiles under 400 grammes, dum-dum bullets and asphyxiating gases. Chemical and bacteriological weapons were then prohibited by the 1925 Geneva Protocol. More recently, the use of weapons producing "non-detectable fragments", of other types of "mines, booby traps and other devices", and of "incendiary weapons", was either

1 Protocol Additional to the Geneva Conventions of August 12, 1949, and relating to the Protection of Victims of International Armed Conflicts [Protocol I], 8 June 1977.

> prohibited or limited, depending on the case, by the Convention of 10 October 1980 on Prohibitions or Restrictions on the Use of Certain Conventional Weapons Which May Be Deemed to Be Excessively Injurious or to Have Indiscriminate Effects. The provisions of the Convention on "mines, booby traps and other devices" have just been amended, on 3 May 1996, and now regulate in greater detail, for example, the use of anti-personnel land mines. (p. 34 [sic]).

In terms of the scope of application established by the ICJ in 1996, the unification and indivisibility of IHL rules must be taken into account and fully observed by all State agents, members of the judiciary, members of armed groups, and any actors in conflict to avoid debates regarding one-sided applications. For instance, the false argument that only states shall comply with the usage of certain weapons, depending on the status of their ratification of certain treaties, and that those obligations do not extend to members of organized armed groups opposing the state. It also allows a better understanding of the holistic way in which humanitarian considerations should be applied in the face of new instruments and forms of warfare that simultaneously threaten the restrictions on weapons and the principle of distinction (e.g., cluster munitions, autonomous bomber drones). In turn, in Paragraphs 75 and 76 of the Advisory Opinion, the scenario set by the Court for establishing the applicable law (Savoie, 2005) is of vital importance regarding the sources of IHL. With declarative force, it expresses (Meron, 1987) that the Hague and Geneva codification process is representative (Talmon, 2015) of international customary law and not merely of a conventional regime.

The advisory opinion on the legality of the threat or use of nuclear weapons and the relationship between international humanitarian law and international human rights law

The relationship between IHL and human rights, whether enshrined at the domestic level (Ramelli, 2004) or with international human rights law (IHRL), is a complex relationship with multiple positions reflected in the doctrine (Tomuschat, 2010), the conduct of states, and the possibilities of exception and suspension enshrined in different instruments. It is often said that in armed conflict scenarios, whether internal (von der Groeben, 2011) or international, broad suspensions of human rights are allowed. International humanitarian law is applied, almost as a "replacement"; humanitarian guarantees are applicable in exchange for suspending the usual human rights regime. However, this position is not legally correct. The different nature of human rights instruments compared to those of international humanitarian law does not admit such a simple or immediate derogation due to the mere occurrence of armed conflict.

The ICJ clarified part of this debate by choosing to exemplify the general rule regarding the continuity of obligations under the Covenant on Civil and Political Rights

during armed conflicts that trigger the application of the Geneva Conventions and their protocols. In this regard, the International Court of Justice (1996) stated in its Advisory Opinion:

> 24. Some of the proponents of the illegality of the use of nuclear weapons have argued that such use would violate the right to life as guaranteed in Article 6 of the International Covenant on Civil and Political Rights, as well as in certain regional instruments for the protection of human rights. Article 6, paragraph 1, of the International Covenant provides as follows: "Every human being has the inherent right to life. This right shall be protected by law. No one shall be arbitrarily deprived of his life."
>
> In reply, others contended that the International Covenant on Civil and Political Rights made no mention of war or weapons, and it had never been envisaged that the legality of nuclear weapons was regulated by that instrument. It was suggested that the Covenant was directed to the protection of human rights in peacetime, but that questions relating to unlawful loss of life in hostilities were governed by the law applicable in armed conflict.
>
> 25. The Court observes that the protection of the International Covenant of [sic] Civil and Political Rights does not cease in times of war, except by operation of Article 4 of the Covenant whereby certain provisions may be derogated from in a time of national emergency. Respect for the right to life is not, however, such a provision. In principle, the right not arbitrarily to be deprived of one's life applies also in hostilities. The test of what is an arbitrary deprivation of life, however, then falls to be determined by the applicable lex specialis, namely, the law applicable in armed conflict which is designed to regulate the conduct of hostilities. Thus whether a particular loss of life, through the use of a certain weapon in warfare, is to be considered an arbitrary deprivation of life contrary to Article 6 of the Covenant, can only be decided by reference to the law applicable in armed conflict and not deduced from the terms of the Covenant itself (pp. 239-240 [sic]).

In paragraphs 24 and 25 of the 1996 Advisory Opinion, the Court demonstrates how different situations within the armed conflict can violate both the existing general IHRL norms and specific reinforced protections and guarantees derived from the relevant IHL norms. It also expresses that the latter's applicability due to the existence of the armed conflict does not automatically derogate the general human rights norms. Their suspension requires compliance of one or the other regime with specific norms (Hampson, 2008), including duly activated states of emergency, enactment of legislation publicly declaring the alteration of social order, or the confirmation of situations of loss of humanitarian protection that turns individuals from objects into lawful military objectives.

The advantage of this interpretation, as pointed out by authors such as Chetail (2003) or Milanović (2009), is that the diametrically different nature of universal and regional human rights treaties can complement the war-minded specificity of the norms of international humanitarian law. In addition, the norms of IHRL have monitoring mechanisms with more robust and diverse monitoring, enforcement, and dispute

resolution mechanisms than those usually included in IHL treaties, such as the Geneva Conventions. Their continued and concomitant non-derogation and application during armed conflict can subsequently ensure access to international human rights law justice in regional or universal settings.

Advisory Opinion on the legality of the threat or use of nuclear weapons and the normative hierarchy of international humanitarian law: *Ius Cogens*, customary law, principles, and the Martens Clause

In paragraphs 78 to 79 of the 1996 Advisory Opinion on nuclear weapons, the ICJ establishes a special legal nature of the basic principles of IHL. In these two paragraphs, the Court (1) states the basic guarantees of IHL from which the Geneva Conventions and the well-known "common articles" (De chazournes & Condorelli, 2000) emanate, (2) declares them as customary international law, and (3) seems to classify them in a special legal category of sources similar to that of *ius cogens* (International Court of Justice, 1996).

> 78. The cardinal principles contained in the texts constituting the fabric of humanitarian law are the following. The first is aimed at the protection of the civilian population and civilian objects and establishes the distinction between combatants and non-combatants; States must never make civilians the object of attack and must consequently never use weapons that are incapable of distinguishing between civilian and military targets. According to the second principle, it is prohibited to cause unnecessary suffering to combatants: it is accordingly prohibited to use weapons causing them such harm or uselessly aggravating their suffering. In application of that second principle, States do not have unlimited freedom of choice of means in the weapons they use.
>
> The Court would likewise refer, in relation to these principles, to the Martens Clause, which was first included in the Hague Convention II with Respect the Laws and Customs of War on Land of 1899 and which has proved to be an effective means of addressing the rapid evolution of military technology. A modern version of that clause is to be found in Article 1, paragraph 2, of Additional Protocol 1 of 1977, which reads as follows:
>
> > "In cases not covered by this Protocol or by other international agreements, civilians and combatants remain under the protection and authority of the principles of international law derived from established custom, from the principles of humanity and from the dictates of public conscience."
>
> In conformity with the aforementioned principles, humanitarian law, at a very early stage, prohibited certain types of weapons either because of their indiscriminate effect on combatants and civilians or because of the unnecessary suffering caused to combatants, that is to Say, a harm greater than that unavoidable to achieve legitimate military objectives. If an envisaged use of weapons would not meet the requirements of humanitarian law, a threat to engage in such use would also be contrary to that law.
>
> 79. It is undoubtedly because a great many rules of humanitarian law applicable in armed conflict are so fundamental to the respect of the human person and "elemen-

> tary considerations of humanity" as the Court put it in its Judgment of 9 April 1949 in the *Corfu Channel* case (*I.C.J. Reports 1949*, p. 22), that The Hague and Geneva Conventions have enjoyed a broad accession. Further these fundamental rules are to be observed by all States whether or not they have ratified the conventions that contain them, because they constitute intransgressible principles of international customary law. (p.35 [sic])

In the final sentence of Paragraph 79, the International Court of Justice establishes the universality of such principles independent of the ratifications of treaties because of their customary content. However, it adds that they must also be binding because they are "intransgressible" principles of customary international law. The previous, seemingly, stated to hide the formula of *jus cogens* without mentioning it directly (Shelton, 2006), as the category of "intransgressible" is not common when referring to custom or any other international legal norm referring to its binding nature. The Court's reinforcement of IHL (Chetail, 2003, p. 242), elevating them to the category of "intransgressible," is usually understood as its way of classifying them as norms of peremptory international law (Wood, 2018).

In the paragraphs cited above, the Court also identifies the well-known Martens Clause or Humanity Clause as an effective element and an unequivocal component of the principles of international law that all Parties to a conflict must observe. It deems them an effective mechanism to address the rapid evolution of the means used to conduct hostilities in the face of the slow pace of codifications and the process of treaty negotiation dealing with new issues, which nowadays include autonomous weapons and electronic warfare.

The customary character of IHL in the "Legality of the Threat or Use of Nuclear Weapons" and "Reservations to the Convention on the Prevention and punishment of the crime of Genocide" advisory opinions and in the "Military and Paramilitary Activities" and "Corfu Channel" cases as a shield against reservations and denunciations of IHL treaties

The declaratory and interpretative relationship of the ICJ's judgments and opinions with the sources of IHL (Abello-Galvis & Arévalo-Ramírez, 2020), its role as the principal State-vs-State jurisdiction identifying the content of international custom, and its relationship with treaties have produced two very useful developments, regarding the quality of IHL as custom in the face of reservations and denunciation of treaties. These situations could be considered, from the perspective of general international law, as formal obstacles to compliance with international humanitarian law.

In the Advisory Opinion on the legality of the threat or use of nuclear weapons (International Court of Justice, 1996), the Court stated:

82. The extensive codification of humanitarian law and the extent of the accession to the resultant treaties, as well as the fact that the denunciation clauses that existed in the codification instruments have never been used, have provided the international community with a corpus of treaty rules the great majority of which had already become customary and which reflected the most universally recognized humanitarian principles. These rules indicate the normal conduct and behaviour expected of States. (p. 36)

In the case of military and paramilitary activities the International Court of Justice (1986) states:

217. The Court observes that Nicaragua, which has invoked a number of multilateral treaties, has refrained from making reference to the four Geneva Conventions of 12 August 1949, to which both Nicaragua and the United States are parties. Thus at the time when the Court was seised [sic] of the dispute, that dispute could be considered not to "arise", to use the wording of the United States multilateral treaty reservation, under any of these Geneva Conventions. The Court did not therefore have to consider whether that reservation might be a bar to the Court treating the relevant provisions of these Conventions as applicable. However, if the Court were on its own initiative to find it appropriate to apply these Conventions, as such, for the settlement of the dispute, it could be argued that the Court would be treating it as a dispute "arising" under them; on that basis, it would have to consider whether any State party to those Conventions would be "affected" by the decision. [sic] for the purposes of the United States multilateral treaty reservation.

218. The Court however sees no need to take a position on that matter, since in its view the conduct of the United States may bejudged according to the fundamental general principles of humanitarian law; in its view, the Geneva Conventions are in some respects a development, and in other respects no more than the expression, of such principles. It is significant in this respect that, according to the terms of the Conventions, the denunciation of one of them

> "shall in no way impair the obligations which the Parties to the conflict shall remain bound to fulfil by virtue of the principles of the law of nations, as they result from the usages established among civilized peoples, from the laws of humanity and the dictates of the public conscience" (Convention 1, Art. 63; Convention II, Art. 62; Convention III, Art. 142; Convention IV, Art. 158).

Article 3 which is common to al1 four Geneva Conventions of 12 August 1949 defines certain rules to be applied in the armed conflicts of a noninternational character. There is no doubt that, in the event of international armed conflicts, these rules also constitute a minimum yardstick, in addition to the more elaborate rules which are also to apply to international conflicts; and they are rules which, in the Court's opinion, reflect what the Court in 1949 called "elementary considerations of humanity" (*Corfu Channel, Merits, I. C. J. Reports 1949*, p. 22; paragraph 215 above). The Court may therefore find them applicable to the present dispute, and is thus not required to decide what role the United States multilateral treaty reservation might otherwise play in regard to the treaties in question. (pp. 103-104 [sic])

In the cases of the legality of the threat or use of nuclear weapons and military and paramilitary activities, the Court strengthened IHL compliance by elevating the general

principles that inspire the Geneva Conventions to customary law and not subjecting it to the strict world of conventional international law (the law of treaties). On the one hand, the previous in response to the reservation that the United States had presented in one of the cases against the Geneva Conventions. On the other, it interpreted that the norms of international humanitarian law, being customary, are not to be affected by states' observance, following specific denunciations that could be made to conventional instruments that crystallize them, as long as they continue to be bound by custom.

In turn, the reference to the rules of international law as "elementary considerations of humanity," inherited from the Corfu Channel case (International Court of Justice, 1949) and the nature of common Article 3 as a basic and minimum criterion customarily applicable to armed conflicts, prevents its circumvention through mechanisms such as denunciation or reservation of treaties.

The ICJ also discussed the relationship between customary and conventional law regarding reservations and the preservation of the existence and binding nature of custom in the face of reservations, denunciation, or other treaty mechanisms, in the Advisory Opinion "Reservations to the Convention on the Prevention and Punishment of the Crime of Genocide" (1951). Here, by way of custom, the Court also developed the notion of *erga omnes* obligations derived from such universal prohibitions, such as genocide, which are not limited to the conventional scope of its own Convention and its ratifications. Consequently, they do not admit unilateral limitations contrary to its object and purpose by considering that those obligations, derived from custom, can create obligations owned before the entire international community.

> The solution of these problems must be found in the special characteristics of the Genocide Convention. The origins and character of that Convention, the objects pursued by the General Assembly and the contracting parties, the relations which exist between the provisions of the Convention, inter se, and between those provisions and these objects, furnish elements of interpretation of the will of the General Assembly and the parties. The origins of the Convention show that it was the intention of the United Nations to condemn and punish genocide as "a crime under international law" involving a denial of the right of existence of entire human groups, a denial which shocks the conscience of mankind and results in great losses to humanity, and which is contrary to moral law and to the spirit and aims of the United Nations (Resolution 96 (1) of the General Assembly, December 11th 1946). The first consequence arising from this conception is that the principles underlying the Convention are principles which are recognized by civilized nations as binding on States, even without any conventional obligation. A second consequence is the universal character both of the condemnation of genocide and of the co-operation required "in order to liberate mankind from such an odious scourge" (Preamble to the Convention). The Genocide Convention was therefore intended by the General Assembly and by the contracting parties to be definitely universal in scope. It was in fact approved on December 9th, 1948, by a resolution which was unanimously adopted by fifty-six States.

> The objects of such a convention must also be considered. The Convention was manifestly adopted for a purely humanitarian and civilizing purpose. It is indeed difficult to imagine a convention that might have this dual character to a greater degree, since its object on the one hand is to safeguard the very existence of certain human groups and on the other to confirm and endorse the most elementary principles of morality. In such a convention the contracting States do not have any interests of their own; they merely have, one and au, a common interest, namely, the accomplishment of those high purposes which are the raison d'être of the convention. Consequently, in a convention of this type one cannot speak of individual advantages or disadvantages to States, or of the maintenance of a perfect contractual balance between rights and duties. The high ideals which inspired the Convention provide, by virtue of the common will of the parties, the foundation and measure of al1 its provisions (International Court of Justice, 1951, p. 23 [sic]).

The "Military and Paramilitary Activities" case: The obligations to respect IHL in non-international armed conflicts and the notion of effective control of the state's conducts

The mentioned judgment in the Nicaragua v. United States of the military and paramilitary activities case includes two fundamental contributions to the substantive and procedural reasoning of IHL and its international adjudication in the context of the state's international responsibility for internationally wrongful acts.

In this case, the ICJ establishes that the customary scope of Article 1 of the Geneva Conventions not only imposes the obligation on party or non-party States to respect international humanitarian law, understood as the obligation to take all measures to ensure that their agents do not violate the precepts of international humanitarian law. It also includes the customary obligation to ensure respect, for international humanitarian law, in the context of the case, understood as the obligation to disfavor or allow third-party violations of IHL (International Court of Justice, 1986):

> 219. The conflict between the *contras'* forces and those of the Government of Nicaragua is an armed conflict which is "not of an international character". The acts of the *contras* towards the Nicaraguan Government are therefore governed by the law applicable to conflicts of that character; whereas the actions of the United States in and against Nicaragua fall under the legal rules relating to international conflicts. Because the minimum rules applicable to international and to non-international conflicts are identical, there is no need to address the question whether those actions must be looked at in the context of the rules which operate for the one or for the other category of conflict. The relevant principles are to be looked for in the provisions of Article 3 of each of the four Conventions of 12 August 1949, the text of which, identical in each Convention, expressly refers to conflicts not having an international character.
>
> 220. The Court considers that there is an obligation on the United States Government, in the terms of Article 1 of the Geneva Conventions, to "respect" the Conventions and even "to ensure respect" for them "in al1 circumstances", since such an obligation does

> not derive only from the Conventions themselves, but from the general principles of humanitarian law to which the Conventions merely give specific expression. The United States is thus under an obligation not to encourage persons or groups engaged in the conflict in Nicaragua to act in violation of the provisions of Article 3 common to the four 1949 Geneva Conventions. (p. 104 [sic])

The issue of third parties and the international responsibility of states for internationally wrongful acts (Caflisch, 2017) is of special relevance in this case. It is recognized as one of the most controversial issues in the relationship of the ICJ with the case-law of other tribunals, especially ad hoc tribunals in criminal matters and its developments in the matter of attribution of conduct (Chetail, 2003).

Contrary to the flexible and most recent criteria of general (total) control established by international criminal tribunals, such as the International Criminal Tribunal for the former Yugoslavia (ICTY), one of the first decisions in the judicial activity of the International Court of Justice on this matter occurred in the 1986 case of military and paramilitary activities in Nicaragua. One of the central questions was whether the violations of IHL committed by the irregular forces (*Los contras*), which, according to various sources, were allegedly supported, incited, and even instructed by the United States Government, that confronted the Nicaraguan Government at the time could be attributed to the United States as international law violations of various IHL customary norms.

At the time, the ICJ, identifying the difference between these non-state subjects, grouped as an organized armed group, and the members or agents of State organs of the United States, decided to address this attribution question (Crawford, 2002). It constructed a control criterion with a high and strict threshold, thus avoiding that simpler connections between the State and the *contras* could be considered an attribution link, further requiring the State to have strict and effective control over their conduct, means, and results.

> 114. In this respect, the Court notes that according to Nicaragua, the contras are no more than bands of mercenaries which have been recruited, organized, paid and commanded by the Government of the United States. This would mean that they have no real autonomy in relation to that Government. Consequently, any offences which they have committed would be imputable to the Government of the United States, like those of any other forces placed under the latter's command. In the view of Nicaragua, 'stricto sensu, the military and paramilitary attacks launched by the United States against Nicaragua do not constitute a case of civil strife. They are essentially the acts of the United States.' If such a finding of the imputability of the acts of the contras to the United States were to be made, no question would arise of mere complicity in those acts, or of incitement of the contras to commit them.
>
> 115. The Court has taken the view (paragraph 110 above) that United States participation, even if preponderant or decisive, in the financing, organizing, training, supplying and equipping of the contras, the selection of its military or paramilitary

> targets, and the planning of the whole of its operation, is still insufficient in itself, on the basis of the evidence in the possession of the Court, for the purpose of attributing to the United States the acts committed by the contras in the course of their military or paramilitary operations in Nicaragua. Al1 the forms of United States participation mentioned above, and even the general control by the respondent State over a force with a high degree of dependency on it, would not in themselves mean, without further evidence, that the United States directed or enforced the perpetration of the acts contrary to human rights and humanitarian law alleged by the applicant State. Such acts could well be committed by members of the contras without the control of the United States For this conduct to give rise to legal responsibility of the United States, it would in principle have to be proved that that State had effective control of the military or paramilitary operations in the course of which the alleged violations were committed. (International Court of Justice, 1986; p. 104 [sic])

This position would be decisive for consolidating how the Court attributes third-party conducts to states. It would impact its decisions in the so-called "Genocide Cases" in the context of the armed conflict in the Balkans (Cassese, 2007) and is expected to impact its position in the future merits decision in the current case of Gambia v. Myanmar, in the docket of the Court since 2019.

Advisory Opinion on the construction of a wall in Palestine.

The International Court of Justice faced another issue closely related to international humanitarian law, territory, and sovereignty (Simma, 2013) in responding to the question of the legal consequences deriving from the construction of the Israeli wall in Palestinian territory. In this case, other members of the international community opposed Israel's effective control of East Jerusalem and the surrounding townships, alleging Israel's violation (Sunga, 2006) of the 1949 Geneva Convention on Civilian Persons, the International Covenant on Civil and Political Rights, the International Covenant on Economic, Social and Cultural Rights, and the United Nations Convention on the Rights of the Child.

In its opinion, the Court analyzed the impact of the wall's construction on the daily life and human rights of the inhabitants of the Palestinian territory. It found that the wall's construction was contrary to the provisions of the Hague Convention of 1907 and the Fourth Geneva Convention. Moreover, it involved the violation of the freedom of movement of the territory's inhabitants as guaranteed by the International Covenant on Civil and Political Rights.

In this analysis, the Court, based on its position concomitantly with the application of IHL and IHRL in conflict settings, considered that the construction of the wall also violated the inhabitants' free exercise of the right to work, access to health, education, and an adequate standard of living under the International Covenant on Economic, Social, and Cultural Rights standards and the Convention on the Rights of the Child.

The Court determined that the establishment of settlements related to the wall and the construction and administration of the wall itself would seriously alter the demographic composition of the occupied Palestinian territory. It considered the previous a contravention of the Fourth Geneva Convention and the relevant resolutions of the Council of Security in the context of civil rights amid conflict. In conclusion, this Advisory Opinion becomes a practical guideline for the rights and duties of occupation forces and their duties regarding international human rights (International Court of Justice, 2004).

Conclusion

The cases and Advisory Opinions analyzed above are a clear expression of the decisive role played by the jurisprudence of the International Court of Justice in establishing the nature and interpretation of international humanitarian law, its incorporation, and its relationship with public international law. In a repeated and consistent manner, the International Court of Justice has elevated international humanitarian law principles and practices into customary law of a universal nature, declaring it "intransgressible" and equating it to *jus cogens*. It has also identified several particular obligations for the parties involved in armed conflicts. Likewise, the Court has clarified the relationship between customary and conventional international humanitarian law and established which of its elements constitute fundamental principles emanating from the most basic principles of humanity. Principles that go beyond the considerations of whether an armed conflict is international or non-international, or whether it is a case concerning the means of warfare or the principle of distinction. The Court's sociological factor, as the highest court of the United Nations, and its inter-state nature are fundamental to universalizing these premises on international humanitarian law, overcoming merely local positions of the belligerents who tend to contextualize the scope of humanitarian norms according to their own needs or intentions. The Court has also effectively managed to avoid an unnecessary and counterproductive separation between the scope of application of international humanitarian law and international human rights law.

Acknowledgments

The author thanks Valeria Maldonado, an undergraduate assistant at the Universidad del Rosario (Colombia), for her help reviewing and editing this article.

Disclaimer

The author declares no conflicts of interest or funding (no external funding). The article belongs to the international law research group of the Faculty of Jurisprudence of the Universidad del Rosario. Research: International Law in light of the various international tribunals.

Funding

The author declares no source of external funding for this article.

About the authors

Walter Arévalo-Ramírez holds a Master's in Law from Stetson University College of Law and a postgraduate diploma in Constitutional Law. Lawyer/Ph.D. graduated summa cum laude from the Universidad del Rosario. A senior professor at the university's Faculty of Jurisprudence and Director of the specialization in International Law. Vice-president of the Colombian Academy of International Law.

https://orcid.org/0000-0002-8501-5513 - Contact: walter.arevalo@urosario.edu.co

References

Abello-Galvis, R., & Arévalo-Ramírez, W. (2019). Inter-American Court of Human Rights Advisory Opinion OC-23/17: Jurisdictional, procedural and substantive implications of human rights duties in the context of environmental protection. *Review of European, Comparative and International Enviromental Law, 28*(2), 217-222. https://doi.org/10.1111/reel.12290

Abello-Galvis, R., & Arévalo-Ramírez, W. (2020). La recepción y desarrollo jurisprudencial de la responsabilidad internacional del Estado por la Corte Interamericana de Derechos Humanos en materia de los criterios de atribución de conductas al Estado: el hecho ilìcito en el tiempo y las formas de reparación. In R. Abello, H. Olasolo, A. Varón, & W. Arévalo (Eds.), *Dialogos y casos iberonamericanos sobre derecho internacional penal, derecho internacional humanitario y justicia transicional*. https://doi.org/https://isbn.camlibro.com.co/catalogo.php?mode=resultados_rapidos&palabra=978-958-784-505-1

Ardila-Castro, C. A., Ramírez-Benítez, E., and Cubides-Cárdenas, J. (2020). El derecho internacional humanitario y su significado para las operaciones militares presentes y futuras. *Revista Científica General José María Córdova*, *18*(32), 857-882. https://doi.org/10.21830/19006586.697

Arévalo-Ramirez, W., & Martínez Vargas, J. R. (2018). La actividad judicial de la Corte Internacional de Justicia. In Olasolo, H. (Ed.). *ALCANCE Y LIMITACIONES DE LA JUSTICIA INTERNACIONAL*, *4*, 89 - 120. Tirant Lo Blanch. https://pure.urosario.edu.co/es/publications/la-actividad-judicial-de-la-corte-internacional-de-justicia

Caflisch, L. (2017). Atribución responsabilidad y jurisdicción en el Derecho Internacional de los Derechos Humanos. *ACDI-Anuario Colombiano de Derecho Internacional 10*, 161-203. https://doi.org/10.12804/revistas.urosario.edu.co/acdi/a.5292

Cassese, A. (2007). The Nicaragua and Tadić tests revisited in light of the ICJ judgment on genocide in Bosnia. *European journal of international Law, 18*(4), 649-668. https://doi.org/10.1093/EJIL/CHM034

Chetail, V. (2003). The contribution of the International Court of Justice to international humanitarian law. *International Review of the Red Cross 85*(850), 235-269. https://www.icrc.org/en/doc/assets/files/other/irrc_850_chetail.pdf

Crawford, J. (2002). *The International Law Commission's Articles on State Responsibility: Introduction, Text and Commentaries*. Cambridge University Press.

De Chazournes, L. B., & Condorelli, L. (2000). *Common Article 1 of the Geneva Conventions revisited: Protecting collective interests*. International Committee of the Red Cross 82, 67. https://international-review.icrc.org/sites/default/files/S1560775500075404a.pdf

Gardam, J. (2001). "The contribution of the International Court of Justice to international humanitarian law. *Leiden Journal of International Law, 14*(2), 349. https://doi.org/10.1017/S0922156501000176

Hampson, F. J. (2008). The relationship between international humanitarian law and human rights law from the perspective of a human rights treaty body. *International Review of the Red Cross, 90*(871), 549. https://international-review.icrc.org/sites/default/files/irrc-871-hampson_0.pdf

Henckaerts, J.-M. (2005). *Customary international humanitarian law*, *Volume 1: Rules*. International Committee of the Red Cross - ICRC. https://www.icrc.org/en/doc/assets/files/other/customary-international-humanitarian-law-i-icrc-eng.pdf

International Court of Justice (1949). *Corfu Channel Case (United Kingdom of Great Britain and North Ireland v. Albania)*. ICJ Reports 1949, 4. https://www.icj-cij.org/en/case/1

International Court of Justice (1951). *Reservations to the Convention on the Prevention and Punishment of the Crime of Genocide*. I.C. J. Advisory Opinion 1951, p.23. https://www.law.umich.edu/facultyhome/drwcasebook/Documents/Documents/ICJ%20Advisory%20Opinion%20on%20Reservations%20to%20the%20Genocide%20Convention.pdf

International Court of Justice (1986). *Military and Paramilitary Activities in and against Nicaragua (Nicaragua v. United States of America)*. I.C.J. Reports 1986, 104-105, para. 220. https://www.icj-cij.org/public/files/case-related/70/070-19860627-JUD-01-00-EN.pdf

International Court of Justice (1996). *Legality of the Threat or Use of Nuclear Weapons; Advisory Opinion of 8 July 1996*, (p. 226, paras.75 & 76). https://www.icj-cij.org/public/files/case-related/95/095-19960708-ADV-01-00-EN.pdf

International Court of Justice (2004). *Legal Consequences of the Construction of a Wall in the Occupied Palestinian Territory*. Overview of the Case, 2003. https://www.icj-cij.org/en/case/131

Lauterpacht, H. (1982). *The development of international law by the International Court*. Cambridge University Press.

Meron, T. (1987). The Geneva Conventions as customary law. *The American Journal of International Law, 81*(2), 348-370. https://doi.org/10.2307/2202407

Milanović, M. (2009). A norm conflict perspective on the relationship between international humanitarian law and human rights law. *Journal of Conflict & Security Law, 14*(3), 459-483. https://doi.org/10.1093/jcsl/krp033

Olasolo, H. (2019). "Are the Targets of Aerial Spraying Operations in Colombia Lawful Under International Humanitarian Law? *Yearbook of International Humanitarian Law, 20,* 229-252. https://doi.org/10.1007/978-94-6265-264-4_7

Ramelli, A. (2004). Sistema de fuentes del derecho internacional público y bloque de constitucionalidad en Colombia. *Cuestiones constitucionales,* (11), 157-175. http://dx.doi.org/10.22201/iij.24484881e.2004.11.5711

Sánchez, J. S. (2018). ¿Por qué es importante que la Corte Penal Internacional condene más allá de toda duda razonable? *ACDI-Anuario Colombiano de Derecho Internacional, 11*, 101-130. https://doi.org/10.12804/revistas.urosario.edu.co/acdi/a.5421

Savoie, P. (2005). The ICJ, Advisory Opinions, and the Judicial Function: Between Adjudication and Consultation. *Canadian Yearbook of International Law/Annuaire Canadien de Droit International 42*, 35-90. https://doi:10.1017/S0069005800008493

Schlütter, B. (2010). *Developments in customary international law: theory and the practice of the International Court of Justice and the International ad hoc Criminal Tribunals for Rwanda and Yugoslavia*. Brill.

Shelton, D. (2006). International law and "relative normativity." In Evans, M. (Ed.) *International Law, 2 ed.*, 159-184. Oxford University Press.

Simma, B. (2013). Human Rights Before the International Court of Justice: Community Interest Coming to Life? In Tams, C.J. & Sloan, J. (Eds.), *The Development of International Law by the International Court of Justice*, 301. https://doi.org/10.1093/acprof:oso/9780199653218.003.0013

Soufi, J. S. (2015). Structure, Functions and Initial Achievements of the Mechanism for International Criminal Tribunals (MICT). *International criminal law review, 15*(3), 544-564. https://doi.org/10.1163/15718123-01503007

Sunga, L.S. (2016). *The International Court of Justice's growing contribution to Human Rights and Humanitarian Law*. The Hague: The Hague institute for Global Justice, 18 April 2006

Talmon, S. (2015). Determining customary international law: the ICJ's methodology between induction, deduction and assertion. *European Journal of International Law 26*(2), 417-443. https://doi.org/10.1093/ejil/chv020

Tomuschat, C. (2010). Human Rights and International Humanitarian Law. *European Journal of International Law, 21*(1), 15-23. https://doi.org/10.1093/ejil/chq003

Verma, B. (2018). Advisory Opinion of ICJ–an Alternative Dispute Settlement Mechanism under International Law. *Journal of Constitutional Law and Jurisprudence, 1*(1), 1-5. https://lawjournals.celnet.in/index.php/Jolj/article/view/18

Vinuales, J. E. (2008). The contribution of the international court of justice to the development of international environmental law: a contemporary assessment. *Fordham International Law Journal 32*(1), 232. https://ir.lawnet.fordham.edu/ilj/vol32/iss1/14

von der Groeben, C. (2011). The Conflict in Colombia and the Relationship Between Humanitarian Law and Human Rights Law in Practice: Analysis of the New Operational Law of the Colombian Armed Forces. *Journal of Conflict & Security Law, 16*(1), 141-164. https://doi.org/10.1093/jcsl/krr004

Wood, M. (2018). The Evolution and Identification of the Customary International Law of Armed Conflict. *Vanderbilt Journal of Transnatuinal Law, 51*(3), 727. https://scholarship.law.vanderbilt.edu/vjtl/vol51/iss3/6


ESMIC
SELLO EDITORIAL

Revista Científica

General José María Córdova

(Revista Colombiana de Estudios Militares y Estratégicos)

Rev. Cient. Gen. José María Córdova	Bogotá Colombia	abril-junio 2022	Vol. 20	Núm. 38	pp. 243-442	ISSN 1900-6586

ESCUELA MILITAR DE CADETES
General José María Córdova

ESMIC
SELLO EDITORIAL

ISSN 1900-6586