Review paper
Received: 29 October 2024
Accepted: 17 March 2025
UDC: 343:355.40
DOI: *https://doi.org/10.31299/ksi.33.1.5*

CRIMINAL LAW PROTECTION OF STATE SECRETS IN THE CONTEXT OF HYBRID WARFARE: A COMPARATIVE ANALYSIS OF UKRAINE AND THE EUROPEAN UNION

Ruslan Semenovych Orlovskyi
Yaroslav Mudryi National Law University
Depatment of Criminal Law

Vasyl Mykhailovych Kozak
Central Office of the Security Service of Ukraine

✉ E-mail: *rs.10@ukr.net*

ABSTRACT

In the context of information warfare, the contemporary security environment is evolving quickly. The protection of secrets has emerged as a crucial element of national security, particularly for Ukraine, which has been dealing with a growing number of hybrid threats and overt military activities by the Russian Federation since 2014. Such security issues have highlighted the gaps in Ukrainian legislation and institutional architecture for the preservation of secrets. With an emphasis on legislative frameworks, classification processes, enforcement strategies, and global best practices, this paper compares the criminal law protection of state secrets in Ukraine and a few member states of the European Union (EU). Ukraine has to address many important issues, such as institutional inefficiencies, cyber dangers, and legislative gaps, in order to strengthen its state secret protection system. This article addresses the NotPetya hacking attack in 2017, incidents of spying on high-ranking officials, and the release of military documents during the full-scale invasion in 2022. These incidents highlight the need for changes in cybersecurity and legislation. The study also examines how international treaties and agreements are being implemented, including the military policy of the North Atlantic Treaty Organisation (NATO), EU cybersecurity guidelines, and intelligence-sharing programmes such as European Union Intelligence and Situation Centre (INTCEN) and the Five Eyes Alliance. The study emphasises how important it is to create a comprehensive action plan for Ukraine that includes technological advances in cybersecurity, increased criminal penalties for cyber espionage, enhanced interagency cooperation, and legislative reforms. In addition, the protection of sensitive materials depends on institutional changes, including the creation of an independent national security agency, mandatory cybersecurity training for civil servants, and stricter verification processes. In addition to improving national security, closer adherence to EU and NATO security standards would facilitate Ukraine's integration into the Euro-Atlantic space. The conclusions of this study provide advice to policy makers, lawyers, and Ukrainian security agencies. The proposed changes are expected to modernise Ukraine's state secret protection system, put an end to cyber espionage and hybrid threats, and align their security legislation with international best practices.

Keywords: state secret, armed conflict, information security, criminal law, international law

INTRODUCTION

The events that occurred after February 24, 2022, have dramatically affected the conditions for the functioning of Ukraine as a state, transforming ordinary legal relationships into those that arise and operate under a state of martial law, as stipulated in the Constitution of Ukraine. Accordingly, the issue of preserving national security has taken precedence over other spheres of state governance, as the state faces the greatest risk of losing its independence. Everything from military-political to economic and digital aspects of public life is interconnected in the context of national security. Special attention is being given to economic security as well. The recent political, climatic, and epidemiological challenges have had a negative impact on the economic security of the state (Hacker et al., 2018; Jankovska, 2018; Nicola et al., 2020).

Information protection is an essential component of national security during a period of competition for influence in the global arena, as well as in terms of priorities established in the scientific, technological, socioeconomic, and other domains. Information has become one of the decisive factors affecting the development of the global and regional economy. However, along with new opportunities, information technology has also brought risks and challenges, making data security especially important (Korol, 2015). Many states are seriously concerned about information security issues, including the storage and non-disclosure of information. This has led to the emergence of a new concept of the "economy of secrecy," where secrecy shapes interstate relationships by adjusting the relationship between "knowledge" and "ignorance" (Balzacq & Puybareau, 2018). The economy of secrecy involves cooperation between states in certain areas that affect their international image and constitute a matter of national security such as the fight against terrorism. However, the methods used to address these issues remain undisclosed since they are considered unacceptable in public opinion. This means that perception and representation are related to the economics of secrecy: given that states want to be able to control their image and influence the perceptions of other actors, they are willing to maintain a certain level of secrecy in their relationships with other states (Kaur & Ramkumar, 2022).

When dealing with such trends, it is necessary to accurately assess the risks associated with strategies developed for information protection. This is especially true for countries that are constantly characterised by a complex geopolitical situation and the threat of aggression. In the context of the present study, Ukraine is of particular interest: due to its current political and economic activities, Ukraine is trying to accumulate all available resources as efficiently as possible to successfully counter the large-scale invasion of the Russian Federation. This is especially true against the background of threats such as the destruction of military infrastructure, information sabotage (hacker attacks) related to the dissemination of possible fake information, and the manipulation of personal data. Furthermore, the issue of implementing strategies to counter possible hybrid threats against other EU countries continues to persist. The EU case study holds great importance for Ukraine, as the country has announced its intention to integrate into the European Union. Therefore, it is essential to improve and adapt the strategies for safeguarding state secrets by focusing on the experiences of other nations and utilising their advanced mechanisms and technologies. The experience of protecting state secrets in the countries of Central and Eastern Europe is of particular importance in the context of our study. This is due to the similarity of the regulatory framework of legislation on the protection of state secrets, which was inherited from the countries that were formerly part

of the socialist camp, and successful cases of reforming their own systems of protection of state secrets based on the best practices of other Western countries in Europe and North America.

The significance of the present study can be explained by how relevant data on state secret protection in the context of hybrid warfare has been organised and how this has led to a search for the best answers to problems affecting political and socioeconomic life. Additionally, a system for assessing actions in order to neutralise threats to national security from the information environment and to define a set of protective measures is currently being developed. The purpose of our study is to identify positive experiences related to the legislative regulation of the protection of state secrets based on the practices of EU countries in comparison with the current legislation of Ukraine with the further possibility of implementing best practices. These topics are addressed with the understanding that it is essential for Ukraine's security framework to align with international legal standards.

As part of the study, the following tasks were defined:

1. Systematise the legislative framework for the protection of state secrets, both within the legal framework of the Ukraine and the EU countries;
2. Investigate the need to develop recommendations and legislative initiatives aimed at preventing and minimising the negative impact of threats to the protection of state secrets and national security in general.

LITERATURE REVIEW

International legal instruments are essential in shaping national policies on state secrets. This research is based on the consideration of a scientific discussion on concepts such as information security, hybrid warfare, and the classification of state secrets, in comparison with the current understanding from the point of view of the legislation of foreign countries. If information security is widely considered as a factor that affects many spheres of life, the issue of defining the concept of "hybrid war" remains both controversial and popular at the same time. The reason for this situation is due to the fact that the idea of "hybrid war" has been constantly subjected to conceptual expansion, and therefore, it seems to be a rather vague and ambiguous concept today (Atkinson, 2018; Caliskan, 2022). The widely used term "hybrid warfare" was first mentioned in a speech by General James Mattis at the Defence Forum supported by the Naval Institute and the Marine Corps Association in September 2005, and later along with analyst Hoffman, he published a short article on "hybrid warfare" in November 2005. Mattis & Hoffman (2005) argued that future threats will be a combination of many conflict modes and they called this synthesis "hybrid warfare". Later, new interpretations of hybrid warfare and associated threats emerged. Glenn (2009) defined a "hybrid threat" as follows: "An adversary who simultaneously and adaptively uses a certain combination of (1) political, military, economic, social and information means and (2) conventional, irregular, catastrophic, terrorist and subversive/criminal methods of warfare.". The term "hybrid war" was made public at the official level as a result of the occupation of the Russian Federation of Crimea to denote the so-called "new" form of the current Russian conflict in Ukraine. This choice is per-

haps the most important turning point in the evolution of the concept of "hybrid warfare" in military-political, journalistic, and academic circles (Libiseller, 2023).

During a hybrid war, cyberspace serves as a great influence on the confrontation between states. In the era of cyber warfare, a country's security is exposed through the risk of critical equipment and devices containing data on the protection of information systems in the banking sectors of global economic corporations, the protection of information systems, as well as the regulation of road, rail, water, air transport: in such scenarios, the protection of state secrets is no exception (Lysko, 2022; Petreski & Ago, 2017).

In terms of state secret protection, the majority of the scientific literature in both Ukraine and Europe address the issue primarily from the perspective of information security, with little attention on specific issues with the system of state secret protection. There are two legal concepts in the Ukrainian scientific discourse, where one focuses on understanding and applying information security as part of information relations, while the other appeals to security studies and military science, considering information security as part of the overall security of the state (Melnyk, 2022). Analysing the Ukrainian scientific base, Zadorozhnya (2005) mainly emphasised the relevance of the problem of the legislative settlement of information security issues as a component of the national issue. They are defined in relation to information security. On the one hand, it is the protection of information, and especially the protection of secrets, commercial information, restricted information, personal data, and so on. On the other hand, it is the protection of information systems, which are actually a means of transmitting information. In contrast, Kharchenko et al. (2004) defined information security as "a component of national security, a process of managing threats and dangers by state and non-state institutions, individual citizens, which ensures the information sovereignty of Ukraine.".

According to the identical position of Dovhan and Thachuk (2011), information security of Ukraine also acts as the protection of state interests, which ensures the prevention, detection, and neutralisation of internal and external information threats, the preservation of the information sovereignty of the state, as well as the safe development of international information cooperation.

Other researchers understand the phenomenon of information security through a broader perspective. They consider this sphere of activity not only through the prism of information relations, but also through the system of state administration, which is more relevant to a more detailed consideration of the topic of state secrets as a legal component of national security in general. We are talking about the fact that this system consists of institutions and means of ensuring information security that use a system of administration, legal information, and analytical measures aimed at ensuring the sustainable functioning of the public administration system (Lipkan et al., 2006). This means that the issue of protection of state secrets is the prerogative of state regulation, which covers limited access to its systematisation, transfer, and use, taking into account the criteria for access to state secrets by relevant officials in order to comply with the national interests of Ukraine.

As for the legal analysis of state secrecy policies, the discussion is based on the interpretation of state secrets within the framework of the criminal law doctrine. This concerns the direct object of disclosure of state secrets, an aspect that continues to lack a common consensus. According to

some authors, the direct object of criminal encroachment is social relationships that ensure the preservation of state secrets (Boldyr, 2017).

Studies of European countries over the past 15 years have mostly focused on problems of an economic nature, rather than the state. Despite external political risks from the Russian Federation and China, developed countries in Europe and North America are focused on information security in their economic activities, given the processes of globalisation and the development of information and communication technologies (ICTs). Based on the above-mentioned information and the fact that there is a growing dependence on ICTs, the number of infrastructure facilities that are very important for the national and economic security of the state (energy, transport, communications, financial services, and so on) continues to increase. In addition, after taking big data into account, they have turned into critical information infrastructures (CII), the protection of which is a priority for any state (Newlove-Eriksson et al., 2018). Today, the issue of improving information security is coming to the forefront due to the increased number of cyberattacks on the information systems of financial institutions, government agencies, and industrial and production complexes. Therefore, the issue of protection of state secrets is mostly concentrated in the area of information security. In modern Western literature, many different terms are used to describe information security, including "information systems security", "IT security", "cybersecurity", and "cyber resilience" (Diesch et al., 2018; Vanoni, 2018). The terms "cybersecurity" and "information security" are synonyms (Luiijf et al., 2013).

Nevertheless, some studies of the specific nature of state secrets are characterised by a historical search for the philosophical foundations of the introduction of state secrets as a separate doctrine in legal relationship between the state and the citizen. Wischmeyer (2023) pointed out that despite the experience of political regimes and the openness of society to new knowledge of a rich amount of information through technology, the very essence of secrecy is to create an information asymmetry that allows the state to act strategically in its own interests. For private stakeholders, this is probably the main reason for keeping information secret, namely maintaining a competitive advantage for the interests of private life, such as commerce. The actions of public authorities also need to be planned out carefully. However, the goals of the strategic means of the state are always related to its constitutional mission. The strategic use of information is a common practice, not only in foreign policy towards other states, but also within national borders, where the state acts as an "organised unit for decision-making and execution" that depends on its ability to fight crime, enforce tax and competition laws, and regulate the financial market (Wischmeyer, 2023). Thus, the issue of criminal law protection of state secrets should be discussed in the context of the security block of issues as a special component of the national security of the State, while taking into account the trends in the development of information relations in a modern post-industrialised society.

METHODOLOGICAL FRAMEWORK

This study is based on the systematisation of approaches used to protect state secrets in Ukraine and EU member states. It was essential to analyse the experience of EU member states in order

to find a more acceptable option for the criminal legal protection of information constituting a state secret that may prove useful for Ukrainian realities. At the same time, since the authors of the present study cannot cover each of the 27 countries in the EU, the main focus of this research is based on the following criteria:

— historical (countries with a common socialistic past, which was characterised by a unique practice of protecting state secrets, as well as the subsequent process of reforming the sphere in the implementation of European integration processes after the collapse of the socialist block);

— geopolitical (the presence of risks and hybrid threats in the relevant EU country - associated with the past experience of the influence of the USSR and the current influence of the policy of the Russian Federation on the national interests of the relevant state);

— economic potential (developed countries that have a great influence on decision-making in the EU and NATO and those that serve as an outpost of NATO's interests regarding the risks of hybrid threats to the Russian Federation).

Among the 27 EU countries, the authors selected 5 countries that meet a majority of the above criteria. This list includes Germany, Lithuania, Finland, Romania, and Croatia. For Germany, with its characteristic stable legal tradition, it is important to have a proper historiographical, theoretical, and methodological base that can be helpful in the specified tasks of the study, while taking into account the specifics of the past totalitarian period within the period of the Third Reich and the German Democratic Republic (GDR).

Romania and Lithuania are interested in protecting state secrets due to the following factors: institutional experience in protecting classified information for the government of these countries in different historical periods, starting with the restoration/declaration of state sovereignty after World War I. Additionally, these countries have a long history of market economy development, high per capita incomes, and significant opportunities to influence regional geopolitical processes in the eastern territories of the EU and NATO, not excluding the traditional historical rivalry with Russia.

Finland's experience is particularly interesting because it takes into account the geopolitical context of the Cold War conflict between the Western and "socialist camps", as well as the growing interest in information regulation since the early 1990s. Since then, Finland has emerged a leader in fostering the sustainable and successful digitalisation of the economy, public services, governance, and other areas.

Croatia's experience is important for studying how the country gained independence and became a sovereign democracy in difficult conditions after the breakup of Yugoslavia, and how military operations and reunification of territories with an appropriate legal framework helped restore constitutional order and put the country on the path to European integration, leading to EU membership in 2013.

While systematising the development of legal support for the information security of the above countries and their separate norms for ensuring state secrets (secret information), Ukraine also has an appropriate regulatory framework that largely regulates the issues of information policy and

information security and so on. In this context, the materials of the study became the basis for the systematisation of legislation on the protection of state secrets:

— The Constitution of Ukraine (Verkhovna Rada of Ukraine, 1996);

Laws of Ukraine:

— Criminal Code of Ukraine (Verkhovna Rada of Ukraine, 2001);

— "On State Secrets" (Verkhovna Rada of Ukraine, 1994);

— "On the Security Service of Ukraine" (Verkhovna Rada of Ukraine, 1992);

— "On the State Service for Special Communications and Information Protection of Ukraine" (Verkhovna Rada of Ukraine, 2006).

In addition, the legal framework regulating the issues of state secrets, secrecy regimes, and their criminal legal protection within the law of the EU member states was subject to analysis:

— Germany: Gesetz über die Voraussetzungen und das Verfahren von Sicherheitsüberprüfungen des Bundes und den Schutz von Verschlusssachen (Sicherheitsüberprüfungsgesetz - SÜG) (The Law on Requirements and Procedure for Federal Security Clearances and Protection of Classified Information) (Service of the Federal Ministry of Justice and the Federal Office of Justice of Germany, 1994);

— Lithuania: Lietuvos Respublikos valstybės ir tarnybos paslapčių įstatymas (Law of the Republic of Lithuania on State and Official Secrets) and the Criminal Code of the Republic of Lithuania (Seimas of the Republic of Lithuania, 1999, 2000);

— Finland: Finnish Data Management Act, Finnish Open Government Act, Finnish Criminal Code (Finlex, 1889, 2020; Finnish Ministry of Justice, 1999);

— Romania: Romanian Law on the Protection of Classified Information, Law on the Romanian Intelligence Service, and Romanian Criminal Code (Constitutional Assembly of Romania, 1992, 2002, 2009);

— Croatia: Croatian Data Privacy Act and Croatian Criminal Code (Croatian Parliament, 2007a, 2007b).

Additionally, the Romano-Germanic legal system, which has a long tradition of codification, unites all the nations that are the focus of the present systematic research study. Therefore, another subject of this study is the common ground for legal systems is the existence of criminal legislation, which is formalised in the relevant codes. Given the fact that the real system of state secret protection is closed, the research methodology is focused on the use of data from open sources. The study is based on the content analysis method, since legislative acts and materials related to strategic documents are available in the public domain. After analysing the obtained data, based on a qualitative assessment of the state of normative acts of Ukraine and the above-mentioned EU countries, the authors involved in the study concerning state secrets present their positions based on either norms or strategies that have a characteristic difference based on classifications. After

that, an analysis was conducted to identify the legislative experiences of other EU countries that can be beneficial for the Ukraine, taking into account the peculiarities of the national legal system and the current realities of martial law. In accordance with its systematic approach, this study does not delve into technical issues, but includes a review of legislative acts and concepts, as well as a review of existing state (public) and international legal practice.

RESULTS

Characteristics of criminal law protection of state secrets of Ukraine

First of all, the storage, protection, and transmission of information is the main subject of any state policy on national security, regardless of the nation's legal foundation. Information is the legal basis on which the state and international institutions rely to formulate and implement their policies. Given this, identifying the specifics of the protection of state secrets may relate not only to ensuring national security in general, but also, first and foremost, to information security. The basis for information is provided by data availability, confidentiality, and integrity, as well as accountability and the knowledge that all procedures are followed in compliance with approved rules, regulations, and protocols (White et al., 2019). Information security is ensured through the implementation of a complex set of policies, procedures, and organisational structures that have evolved dynamically over the past decade due to rapid globalisation and the expansion of information technology-based business processes (Cristea, 2020).

The experience of Ukraine has a short legislative tradition in terms of time. However, in terms of intensity of regulation of state secrets, it is extensive and based on Soviet law. Since the proclamation of Ukraine's independence, there has been a need for independent rule-making and identification of current legal positions on the protection of state secrets as a component of ensuring Ukraine's national security. According to the Law of Ukraine "On State Secrets" (1994), state secrets are defined as a type of secret information covering information in the field of defence, economy, science and technology, foreign relations, as well as state security and law enforcement, the disclosure of which may harm the national security of Ukraine. The following information is recognised as a state secret in accordance with the procedure established by the Law of Ukraine "On State Secrets" and is subject to state protection (Verkhovna Rada of Ukraine, 1994). In turn, Article 328 of the Criminal Code provides for liability for disclosure of state secrets. Information constituting a state secret is one of the main elements of the crime, which is the subject of this crime. Liability under Article 328 of the Criminal Code of Ukraine arises regardless of the nature of the information constituting a state secret that was disclosed (except for information in the field of defence, in certain cases). This is relevant only for establishing the severity of the damage caused, i.e., the degree of public danger of the crime. This can be taken into account by the court when settling the issue of assigning a specific punishment to the guilty person, which currently varies between 5 and 8 years of imprisonment (Verkhovna Rada of Ukraine, 2001). A separate provision is made for liability for espionage, which is reflected in Article 114 of the Criminal Code, and this can be imposed on foreigners. Article 114 is the transfer or collection of information that constitutes a

state secret for the purpose of transferring it to a foreign organisation. The sanction for the crime is 10-15 years of imprisonment (Verkhovna Rada of Ukraine, 1992).

Speaking about the peculiarities of criminal law protection of state secrets in Ukraine in comparison to other European counterparts, it is worth noting the fact that the legal nature of the development of legal secrets differs between Ukraine and EU member states, especially those that were not part of the "socialist camp". First of all, the difference is evident in the legal systems of countries that are primarily NATO members. Thus, if the issue of state secrets in Ukraine institutionally originated from the USSR and the transfer of part of its "secrets" to the successor states caused a corresponding impact on the legislation of the newly created states, then, for example, in NATO countries, from the point of view of institutional development, there is no distribution of information with limited access to state secrets and other secrets provided by law. In accordance with their regulatory legal systems, there is a single classification of so-called sensitive information (analogue of restricted information), which is already burdened by the imposition of appropriate access restrictions on it (Dzhus et al., 2023). Nevertheless, according to the methodology, the study covers a number of EU countries that, due to their institutional past and current external security risks, have an appropriate regulatory framework.

Case studies of state secret breaches and cyberattacks in Ukraine

A study of previous breaches and cyberattacks in Ukraine is necessary to understand the serious consequences of a weak system of state secret protection. These cases emphasise the need and complexity of strengthening national security laws and institutions. The NotPetya attack in June 2017, which began as a targeted attack on Ukrainian institutions, but later spread globally, was one of the most devastating cyberattacks against Ukraine (Wired, 2018). Initially posing as wiper malware, NotPetya was actually harmful software that disrupted key infrastructure, including banks, media, energy companies, and government organisations, and permanently erased their data. The hacker attack caused $10 billion in losses worldwide due to interference with government databases and financial activities. The strategy of hybrid warfare against Ukraine was highlighted by attributing the attack to Russian state actors. This demonstrated the vulnerability of state cybersecurity architectures, as well as the need for stronger criminal and legal measures against cyber espionage (Security Outlines, 2024).

Ukrainian intelligence services uncovered an insider computer hacking network containing top-secret military material after Russia invaded Ukraine in 2022. Cyber hacking and human intelligence (HUMINT) activities were used to obtain these records, which included supply chain details and strategic military plans (CBS News, 2025). The data leaks resulted in specific attacks on supply chains and critical defence infrastructure. Ukraine responded by adopting a state of emergency law that tightened restrictions on access to classified material and increased penalties for unauthorised disclosure (Reuters, 2022). These incidents demonstrate the growing danger that the Internet age poses to national secrets. Ukraine's legal framework should be constantly adjusted in accordance with best practices in cybersecurity and counterintelligence due to the intersection of cyberwarfare, cyberespionage, and internal security risks.

State secrets in the context of criminal law: Germany

As we currently know, Germany has extensive institutional experience in maintaining state security. After the unification of Germany in 1990 and the elimination of state and special services of the GDR, there was a need to update the doctrine of national security, and, accordingly, the methodology for ensuring it. Since 1994, a new federal law has been in force - the Law on Access to Classified Information, which regulated the peculiarities of protecting state secrets. This law regulates the requirements and procedures for verifying a person to whom the competent authority entrusts sensitive security-related activities (security clearance) or has already been entrusted (re-verification), as well as the protection of classified information (Service of the Federal Ministry of Justice and the Federal Office of Justice of Germany, 1994). The law is based on factors that contain precise instructions for handling state secrets. The main effect of the law is that it ensures transparency by defining the conditions under which different types of information can be classified and defining what level of secrecy they fall under (Section 4). This Law prevents the creation of information "black holes" within government bodies, which are completely exempt from any control. Additionally, a characteristic feature of this legislation is that it imposes a burden of justification on each act of secrecy of state information, instead of providing such employees with benefits and privileges (Wischmeyer, 2023).

Another normative act that regulates the term of state secrets is the Criminal Code of the Federal Republic of Germany. In contrast to Ukraine, where Section 1 covers aggressive war, high treason, and anti-constitutional actions, Section 2 of the Special Part introduces the idea of state secrets (Federal Ministry of Justice of Germany, 1998).

According to the above-mentioned Criminal Code, these are items or information that are available only to a limited number of persons and must be kept secret from a foreign state in order to prevent damage to Germany's external security (Article 93). At the same time, it was noted that the facts of violation of the free democratic constitutional order, or those that are kept secret in relation to the partners of the Federal Republic of Germany under agreements on state-agreed restrictions in the field of armaments were not considered to be state secrets. Thus, the norms of the German Criminal Code contain a general concept of state secrets and do not refer to the norms of another normative legal acts. Violation of the state secrets regime in Germany constitutes a direct form of treason, which is punishable by imprisonment for a term of 1 to 10 years, and in special cases, even life imprisonment, according to Article 94 (Seimas of the Republic of Lithuania, 1999).

State secrets in the context of criminal law: Lithuania

The period of restoration of independence was characterised by the process of "De-Sovietization" of the regulatory framework and the strategy of early accession to the Euro-Atlantic political and economic unions. Similar to other countries of the post-socialist camp, the young Republic of Lithuania considers its strategic stability to be crucial to its membership in Euro-Atlantic political, military, and economic associations, as well as to respond to current challenges such as international terrorism, illegal migration, and hybrid threats from the Russian Federation as a result of aggressive actions on the territories of sovereign states.

The legal basis of national security is relevant legislation on the preservation of state secrets. The Law of the Republic of Lithuania "On State and Official Secrets" (1999) and its accompanying amendments defines state secrets as information in the military, political, economic, law enforcement, science and technology fields, the unlawful disclosure or loss of which may violate the sovereignty, defence capability, or economic power of the state, harm its constitutional order and political interests, as well as endanger human life, health, and constitutional rights (Seimas of the Republic of Lithuania, 1999). Classified information is categorised into "Top Secret", "Secret", "Confidential", depending on the importance, severity of damage that may be caused to the state, its bodies or persons as a result of its disclosure, as well as the level of protection necessary to preserve it.

Article 7 of the above-mentioned law describes in great detail (30 items in paragraph 1) the categories of information that fall under the category of "State Secret". It should be noted that these are materials related to defence, science and technology, international relations, and cryptography. However, some items are more specific, including issues of ensuring special communication, protection of critical infrastructure facilities, issues of declaring officials. The protection of classified information falls under the authority of the Commission of the Republic of Lithuania for the Coordination of the Protection of Secrets, a collegial body with seven members, six of whom are appointed by the President and the Prime Minister of Lithuania, as well as the Chairman of the Seimas. This is in accordance with the law regarding institutional order in the Lithuanian legal system.

The chairman of this commission is the Director General of the State Security Department, who also appoints one official as the secretary of the commission, whose duties include the preparation and submission of documents for consideration. With regard to criminal law protection of state secrets, Lithuanian legislation has retained the traditional approach to criminal liability for disclosure of state secrets that existed in Soviet criminal law, which is reflected in the Criminal Code of the Republic of Lithuania, namely Article 125. Here the penalty for disclosure of state secrets without signs of espionage is up to 3 years of imprisonment. Punishment for loss, destruction, damage to state secrets, which is provided for in Article 126, involves up to 2 years of imprisonment. The most severe penalty is provided for in Article 119 for espionage, i.e., for stealing, buying, collecting information constituting a state secret or other information of interest in order to aid the intelligence of a foreign state: this involves between 3 to 15 years of imprisonment (Seimas of the Republic of Lithuania, 2000).

State secrets in the context of criminal law: Finland

During the Cold War, this country occupied a significant place in the political confrontation between NATO countries and the countries that were part of the Warsaw Pact under the leadership of the USSR. Nevertheless, the country was able to rebuild constructive relations with both blocs, given its strategic geographical position and economic potential: this was marked by rapid economic growth since the second half of the twentieth century. Today, Finland has changed its policy as a result of growing hybrid challenges from its eastern neighbour, the Russian Federation. As a culmination of recent shifts in the political landscape, since the beginning of February, Finland has abandoned the policy of balance and neutrality and joined NATO in response to the challenges associated with the full-scale war in Ukraine. The current legal system regarding the protection of

classified information of the Republic of Finland will cover the following regulations outlined in the "Finnish Data Management" Act. The unification of information security, information management, and the digitalisation of official operations are encouraged by this act, which was set up in 2020. It contains provisions for the entire public administration regarding the organisation and description of information management, the interaction of information reserves, the implementation of the interaction of information systems, the implementation of technical interfaces and viewing connections, as well as the implementation of information security.

In accordance with the law, a Public Administration Information Management Council was established under the Ministry of Finance to assess and guide the information management process of state and municipal authorities (Finlex, 2020). Another piece of legislation that mentions secrecy provisions is the "Finnish Open Government" Act 621 (1999). It focuses on the concept of secrecy of a document (Article 22), the provision of non-disclosure obligations (Article 23), the list of documents containing secrecy (Article 24), such as documents of the Government, the Ministry of Foreign Affairs, foreign diplomatic missions, reports of law enforcement agencies on criminal investigations, documents on the activities of the army, intelligence, data on the situation in the economic and social spheres, and so on (Finnish Ministry of Justice, 1999).

However, with regard to documents containing state secrets, there are some regulatory differences from the legislation of other European countries. The main provisions of the law on the protection of classified data are explained by the resolutions of the executive bodies (Government Decree on the secrecy of documents in the state administration 1101/2019), the activities of the information management board (Government Decree on the information management board in the state administration 1338/2019), and the procedure for managing information about state bodies (Government Decree on the procedure for applying for changes in information management) on issues related to 1301/2019. The Criminal Code of Finland, which was created in 1889 when Finland was still a part of the Russian Empire, governs the criminal security function of secrecy. Taking into account the changes, this Code contains provisions on crimes related to national security and disclosure of classified information. Thus, paragraphs 5-6 (Espionage), 7 (Disclosure of State Secrets) of Chapter 12 (21.4.1995/578) on crimes relating to high treason of the Code cover the issue of disclosure of state secrets.

According to the above-mentioned criminal code, any person who unlawfully publishes or transmits to another person, or for this purpose unlawfully obtains information about a matter regulated by or ordered to be kept secret for the purpose of Finland's external security, or a matter which is of such a nature that its disclosure could cause serious damage to Finland's national defence and security, foreign relations, or national economy, shall be punished by imprisonment for a term of 4 months to 4 years for disclosure of a secret constituting a state secret. According to Chapter 12 of the Code on Crimes of High Treason, the harsher sanction applies only to espionage, which ranges from 1 to 10 years in prison, and grave espionage, which ranges from 4 years in prison to life imprisonment. Additionally, Chapter 38 (21.4.1995/578) of this code covers crimes in the field of information and communication, such as crimes of secrecy, violation of confidentiality, interference with telecommunications, communications, data leaks, and so on (Finlex, 1889).

State secrets in the context of criminal law: Romania

The experience of this country in ensuring national security is considerable. Since the royal and socialist periods, local intelligence services have proven effective in defending the interests of the ruling circles and external challenges during the geopolitical turbulence both in the interwar period (1918-1939) and the Cold War (1949-1990). Romania's modern legal system in the field of national security is regulated by both the Constitution and the relevant legislation. This includes the Law of Romania "On the Protection of Classified Information". According to Article 4, the main tasks of protecting classified information are as follows:

a) protection of classified information from espionage, compromised or unauthorised access, modification or modification of its content, as well as from sabotage or unauthorised destruction;

b) achieving the security of computer systems and the transfer of classified information.

In accordance with Article 5, the measures taken to apply the law are aimed at:

a) preventing unauthorised access to classified information;

b) identifying the circumstances and the circle of persons who may jeopardise the security of classified information through their actions;

c) guaranteeing the dissemination of classified information exclusively among persons who have the right to use it in accordance with the law;

d) ensuring physical protection of information, as well as appropriate personnel necessary to protect classified information.

According to Article 6, from the point of view of institutional support for the protection of classified information, standards for the protection of classified information are mandatory and have been established by the Romanian Intelligence Service with the consent of the national security body. In the case of Romania, such a body is the Intelligence Service (Constitutional Assembly of Romania, 1992). The law's explicit acknowledgment of NATO's role, of which Romania is a member, is one of its defining characteristics. According to Article 6, in the event of a conflict between internal rules for the protection of classified information and NATO rules, NATO rules will prevail in this matter (Constitutional Assembly of Romania, 2002). As a result, the Romanian lawmakers recognise the superiority of international law over domestic law, namely NATO's norms as a military and political bloc (Constitutional Assembly of Romania, 1992). The rules governing liability for crimes committed in relation to the protection of state secrets are the Romanian Criminal Code, separately in Articles 178, 303-305, 395 and 409.

For example, Article 303 establishes a punishment of 2 to 7 years of imprisonment and the use of certain rights for unlawful disclosure of state secrets by a person who has access to these secrets through their official duties, especially if this affects the interests of public administration bodies. There is liability for any negligence that results in the destruction, alteration, loss or theft of a document containing information constituting a state secret, as well as negligence that allows another person to learn about this information, punishable by imprisonment for a term of three months to one year. According to Article 395, the highest penalty is for treason. A Romanian citizen who

transfers secret state information to a foreign state, organisation, or their agents, or who receives or possesses documents or data that constitute a state secret with the intent to transfer it to a foreign authority, organisation, or its agents, faces a term of 10 to 20 years in prison. (Constitutional Assembly of Romania, 2009).

State secrets in the context of criminal law: Croatia

This country went through a difficult state-building process as a result of the devastating Yugoslav wars, which were the main challenge for the new Republic. After the war, there was the path of recovery. Accordingly, in order for the young state to develop and consolidate its activities through the development of the national security system, it also required appropriate legislative support. The legal basis of national legislation on the protection and storage of classified information is set out in the Criminal Code, the Law on Data Confidentiality, which defines the concept of classified and unclassified data, the degree of secrecy, the procedure for classification and declassification, access to classified and unclassified data, as well as their protection and control over the implementation of this law. In addition, the above-mentioned law applies to state bodies, local and regional self-government bodies, legal entities with public powers, as well as legal entities and individuals who have access to or deal with classified and unclassified data in accordance with this law (Croatian Parliament, 2007).

The law also covers the degree of secrecy (Section 2), the classification and declassification of data (Section 3), access to data (Section 4), their protection (Section 5) and supervision of the implementation of the law (Section 6). Criminal law protection of official secrecy is ensured by the Croatian Criminal Code. Article 300 of the Code provides information on liability for the transfer of state secrets and for attempts to make them public, amounting to up to 3 years in prison. The highest punishment is provided for espionage (Article 348 of the Criminal Code) - from 1 to 10 years of imprisonment in times of peace and up to 15 years in times of war (Croatian Parliament, 1997). The Criminal Code also defines the concept of classified information, which duplicates the provisions of the above law.

Regarding the institutional aspect of safeguarding classified information, the Bureau, the National Public Information Authority of the Republic of Croatia, and the Office of the National Security Council of Croatia are responsible for Croatia's security information protection (Vijeće za nacionalnu sigurnost) (Tkachuk, 2017). Croatia supplements its legal framework for regulating national security issues, while providing a legislative opportunity to harmonise its national legislation in accordance with the norms of the EU and NATO, of which Croatia is a member. The Croatian National Security Council provides relevant recommendations to the competent state authorities on harmonising national procedures and rules with NATO and EU crisis response procedures. This is a continuation of European integration processes, taking into account current trends in international information security and digitalisation (Bondarenko, 2021).

Compared to other EU countries, the legal nature of state secrets is generally the same in the Ukrainian legal framework. It sometimes has a synonymous meaning with the concept of secret information in the laws of countries such as Germany and Finland, but the legal framework was not similar in legal structure to the criminal laws of the countries of the "socialist camp", which in-

cluded Romania and Lithuania (as part of the USSR), and Croatia (as part of the Socialist Republic of Yugoslavia). At the same time, given the factor of following the integration into Euro-Atlantic institutions, there is a need to improve the system of state secret protection further, with special attention on the constant improvement of organisational and technical capabilities to defeat the system of state secret protection, taking into account current military-political, hybrid, and cyber threats.

DISCUSSION

It is hard to say under what circumstances incorporating foreign expertise in the fundamentals of maintaining state and national security may be important. Namely, this is due to the factor of a full-scale war between Ukraine and the Russian Federation. When studying the results, especially those related to the analysis of the legal systems of the EU countries analysed, it is extremely important to emphasise that the national security system of Ukraine has never had to function under a state of martial law, which was introduced on the first day of the full-scale invasion of the Russian Federation (Verkhovna Rada of Ukraine, 2022). The martial law regime allows the transition of the state to another level of regulation of steam relations, which are related to ensuring state sovereignty, defence, and national security (Stefanchuk et al., 2022). Except for Croatia, none of the EU countries under review had explicit legal provisions addressing responsibility for transmitting or preserving state secrets during periods of war. In the case of Croatia, there are provisions in the criminal law that provide for such a state of war, where the sanction for committing these types of crimes increase, and it is not regulated by separate special laws, as in the cases of other EU and NATO countries. Accordingly, none of the EU countries, except Croatia, has a similar experience of being in the "hot" phase of recovery from military aggression. Although it may be considered inappropriate, one could potentially reference Poland's experience during the communist era: this is because Wojciech Jaruzelski's earlier leadership led to the enforcement martial law for various reasons, including internal politics (Zhaboklichka & Stankowski, 2022).

Ukraine, as part of its legally enshrined strategic course of Euro-Atlantic integration, will have to strengthen, in practice, the principle of international law taking precedence over national legislation by continuing the process of harmonising its legal norms with those of the EU and its individual provisions, including those on security and defence.

Integration of international legal instruments for state secret protection

Bringing national legislation in line with international security treaties and best practices is a key step in improving Ukraine's legislation on the protection of state secrets. Although Ukraine has made significant progress in adopting NATO and EU norms, further integration with international systems is needed to improve operational efficiency and legal coherence in the area of state secret protection.

EU cybersecurity directives and data protection regulations are crucial for strengthening the protection of sensitive data. The NIS 2 Directive (European Parliament, 2022) is important for increas-

ing cybersecurity requirements for key infrastructure, especially for state institutions that manage state secrets. Ukraine should establish cross-border cooperation structures and risk-based cybersecurity policies to meet these criteria. Furthermore, while the General Data Protection Regulation (GDPR) focuses on the protection of personal data, its principles of good data governance, encryption, and notification are extremely valuable for improving the handling of state secrets in Ukraine (North Atlantic Council, 2002).

The guidelines necessary to protect sensitive data are also contained in the NATO Security Policy and the Classified Information Framework. The NATO Security Policy (C-M(2002)49) defines how sensitive material is classified and handled by the governments of NATO member and partner countries. In order to maintain consistency in access restrictions, classification levels, and declassification processes, Ukraine should align its legal system with these standards. In addition, to further strengthen legal and operational integration, further cooperation between Ukraine and NATO in the areas of cybersecurity and counterintelligence should be authorised through legislative changes that bring national security laws in alignment with NATO's Classified Information Agreements (CIA) (United Nations General Assembly, 1994).

The Budapest Memorandum and other security agreements emphasise the need for further robust protection of state secrets in terms of security guarantees. The 1994 Budapest Memorandum is an example of an international commitment to Ukraine's security, despite the fact that it failed to stop the aggression against Ukraine. To prevent foreign intelligence services from exploiting legal loopholes, all future agreements should contain legally binding provisions that explicitly protect state secrets. To facilitate real-time threat assessments and national security measures, Ukraine should also strengthen intelligence sharing arrangements with its major international partners, including the EU's Intelligence and Situation Centre (INTCEN) and the Five Eyes Alliance (FVEY) (European Parliament, 2016). Ukraine will be able to improve cooperation with its allies, strengthen its resilience to hybrid threats, and modernise its system of state secret protection by incorporating these international legal instruments into its national legislation.

The results of the comparative analysis in the present study demonstrate that, in order to harmonise laws with contemporary national security and defence realities, each individual topic needs to be examined further and discussed with the involvement of an expert network, taking into account the lessons learned from past hostilities and martial law. International experience outside the EU, such as in Israel, Syria, and the Philippines, indicates that martial law can be applied to all or some aspects of state policy, including internal issues. Considering foreign experience, there is a need to investigate successful practices regarding the functioning of the state and its legal system, especially during a period of crisis.

Another issue related to the protection of state secrets is the challenge of preserving secret data: not only state secrets, but also commercial secrets and confidential business correspondence. The right to confidentiality of correspondence and its transportation is unconditionally guaranteed, and some European laws establish effective rules for its protection (Dovha & Luhina, 2021). However, this does not preclude greater involvement of the world's population in the digital sector, which has become an integral part of everyday life. The level of public discussion on protecting human rights in the digital sphere and not restricting these rights in correspondence with the cur-

rent challenges of hybrid threats has increased as a result of current trends in the harmonisation of legislation and the simplification of obtaining any information through ICTs. There are still no answers regarding the question of how to combine innovations in the field of digital security with universal constitutional principles related to human rights. These innovations will be correlated with life, health, privacy, security of human life, and so on, especially in times of war (Murtishcheva, 2022). Additionally, the state may be the target of fiduciary secrecy due to the tendencies toward accountability and openness at the level of citizen-state relationships. This situation occurs, for instance, when someone makes a request to a state agency and reveals information that the applicant believes has to be kept confidential. Furthermore, government organisations are permitted to gather personal data, whether in an open or hidden way. This data must then be kept private and not shared with third parties. Here the state becomes the guardian of secrecy and is, thus, responsible for protecting the integrity and confidentiality of information (Wischmeyer, 2023). Therefore, there is a need to update legislative support, regulate social relations, and review law enforcement and crime prevention through effective reform of national legislation.

CONCLUSION

The study covered the issue of criminal law protection of state secrets based on the comparative characteristics of the legal norms of Ukraine and five EU countries, some of which were singled out in accordance with the approved methodology. In the process of studying the legislation in the field of state secrets of Ukraine and the EU countries, namely Germany, Lithuania, Finland, Romania and Croatia, the authors of the present study focused on several aspects, in particular: types of information that fall or do not fall under state secrets, degrees of classification, authorised institutions, scientific search for the legal nature of the concepts of state secrets and/or secret data, and peculiarities of legal liability for violations in the field of state secrets. The authors came to the conclusion that there is strong criminal law protection for state secrets in each country they reviewed. This is particularly true when adjusting to the new realities of digitalisation, which can be complicated when it comes to information security in Finland, the relatively advanced experience of post-conflict reconstruction and reintegration in Croatia, and the rapid harmonisation of laws in Lithuania and Romania concerning national security in accordance with EU law and NATO Euro-Atlantic doctrines. The legislation in these states not only clearly defines what constitutes a state secret and how classified information is classified, but it also confirms the consistency of institutional support and the synchronisation of policies regarding the protection of state secrets. Furthermore, most of the time, these laws avoid issues with qualifying such acts, particularly when it comes to criminal liability for the transfer or destruction of this kind of information. Each of these countries, similar to Ukraine, does not tolerate espionage and imposes the most severe sanction for committing this crime.

To enhance Ukraine's legislative and institutional framework for state secret protection, a structured action plan is necessary. Based on the comparative analysis of EU legal frameworks and Ukraine's national security challenges, a step-by-step roadmap is proposed. The first priority is strengthening legal frameworks through legislative reforms. Existing laws, such as the Law of Ukraine "On State Secrets" (1994), should be amended to align with NATO security protocols and EU cybersecurity

directives. Criminal penalties for cyber espionage and unauthorised access to classified information must be enhanced, following the stricter legal provisions applied in Germany and Romania. Additionally, classification procedures should be streamlined by establishing clearer guidelines for classifying, declassifying, and handling state secrets, as well as reducing bureaucratic inefficiencies and preventing unnecessary overclassification.

Institutional reforms are also necessary for more effective oversight. Ukraine should establish an independent regulatory agency dedicated to monitoring and enforcing compliance with state secret protection laws. Furthermore, interagency coordination must be strengthened, particularly among the Security Service of Ukraine (SBU), the Ministry of Defence, and cybersecurity agencies, to ensure a unified national security approach.

Technological and cybersecurity upgrades are another essential component of reform. End-to-end encryption and multi-factor authentication should be mandated for classified government communications. Regular cybersecurity audits must be conducted, including periodic security assessments and penetration testing to identify vulnerabilities in government networks. Additionally, a national cyber incident response plan should be developed to create a rapid response mechanism for addressing cyber intrusions targeting classified information.

Capacity building and human resource development are also critical to improving state secret protection. Mandatory cybersecurity and counterintelligence training should be introduced for all government officials handling classified information. At the same time, vetting and background checks for personnel with access to state secrets must be enhanced to prevent insider threats.

Public awareness and international cooperation should also be prioritised. To counter disinformation, awareness campaigns must be launched to educate citizens about state security risks, including cyber threats and foreign intelligence activities. Strengthening partnerships with international allies, particularly through increased collaboration with EU and NATO intelligence-sharing mechanisms, will further improve Ukraine's resilience against hybrid threats. By implementing these strategic reforms, Ukraine can significantly enhance the protection of state secrets, align with international best practices, and mitigate the risks posed by hybrid warfare and cyber espionage.

REFERENCES

Atkinson, C. (2018). Hybrid warfare and societal resilience implications for democratic governance. *Information & Security*, *39*(1), 63-76. *https://doi.org/10.11610/isij.3906*

Balzacq, T., & Puybareau, B. (2018). The economy of secrecy: security, information control, and EU-US relations. *West European Politics*, *41*(4), 890-913. *https://doi.org/10.1080/01402382.2018.1431490*

Boldyr, S. V. (2017). Prospects for reforming the system of protection of state secrets and proprietary information. *Information and Law*, *(4),* 79-85. *https://ippi.org.ua/sites/default/files/10_6.pdf*

Caliskan, M. (2019). Hybrid warfare through the lens of strategic theory. *Defense & Security analysis*, *35*(1), 40-58. *https://doi.org/10.1080/14751798.2019.1565364*

CBS News. (2025). *Ukraine detains top intelligence official, accuses "the rat" of working for Russia*. https://www.cbsnews.com/news/ukraine-sbu-intelligence-official-the-rat-accused-working-for-russia

Constitutional Assembly of Romania. (1992). *Law No. 14 "On the Organization and Functioning of the Romanian Intelligence Service"*. https://legislatie.just.ro/Public/DetaliiDocumentAfis/2144

Constitutional Assembly of Romania. (2002). *Law No. 182 "On Protection of Restricted Information"*. https://legislatie.just.ro/Public/DetaliiDocument/35209

Constitutional Assembly of Romania. (2009). *Law No. 286/2009 Criminal Code*. https://legislatie.just.ro/Public/DetaliiDocumentAfis/223635

Cristea, L. M. (2020). Current security threats in the national and international context. *Journal of Accounting and Management Information Systems, 19*(2), 351-378.

Croatian Parliament. (2007a). *No. 114/23, 86/12. "Criminal law"*. https://www.zakon.hr/z/98/Kazneni-zakon

Croatian Parliament. (2007b). *No. 79/07, 86/12. "Data Protection Act"*. https://www.zakon.hr/z/217/Zakon-o-tajnosti-podataka

Diesch, R., Pfaff, M., & Krcmar, H. (2018). Prerequisite to measure information security. *Information Management and Computer Security*, *99*(7), 7. https://doi.org/10.5220/0006545602070215

Dovha, M. O., & Luhina, N. A. (2021). Criminal law protection of the secrecy of correspondence of foreign states: a comparative analysis. *Kyiv Journal of Law*, *(4)*, 258-264. https://doi.org/10.32782/klj/2021.4.39

Dzhus, O. A., Zolotareva, M. K., Kopotun, I. M., Makarova, T. P., Mykytyuk, M. A., Pavlyuk, O. O., Pasika S. P., Petkov S. V., Skrynkovskyi R. M., Sopilnyk L. I., Chubenko A. G., & Shevchenko, A. M. (2023). *State secret as a component of national security of Ukraine: protection and access to state secrets; legislative provision of state secrets; responsibility for disclosure of state secrets; peculiarities of observance of state secrets during the administration of justice; peculiarities of regulation in a special period and during martial law*. PROFESSIONAL.

European Parliament. (2016). Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation). *Official Journal of the European Union, L*(119), 1-88. https://eur-lex.europa.eu/eli/reg/2016/679/oj

European Parliament. (2022). Directive (EU) 2022/2555 "of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS 2 Directive)". *Official Journal of the European Union, L*(333), 80-152. https://eur-lex.europa.eu/eli/dir/2022/2555/oj/eng

Federal Ministry of Justice of Germany. (1998). *Criminal Code*. https://www.gesetze-im-internet.de/stgb/BJNR001270871.html

Finlex. (1889). *Criminal Code*. https://www.finlex.fi/fi/laki/ajantasa/1889/18890039001

Finlex. (2020). *Data Management Law*. https://www.finlex.fi/fi/laki/alkup/2019/20190906

Finnish Ministry of Justice. (1999). *Act on the Openness of Government Activities*. *https://www.finlex.fi/en/laki/kaannokset/1999/en19990621_20150907.pdf*

Glenn, R. W. (2009). Thoughts on hybrid conflict. *Small Wars Journal*, *2*(1), 1-8.

Dovhan, O. D., & Tkachuk, T. Y. (2011). Information security system of Ukraine: Ontological dimensions. Information and Law, 1(24), 89-103. *https://doi.org/10.37750/2616-6798.2018.1(24).270748*

Hacker, J. S., Stiglitz, J. E., Fitoussi, J. P., & Durand, M. (2018). *Economic Security. In For good measure: Advancing research on well-being metrics beyond GDP*. OECD.

Jankovska, L., Tylchyk, V., & Khomyshyn, I. (2018). National economic security: an economic and legal framework for ensuring in the conditions of the European integration. *Baltic Journal of Economic Studies*, *4*(1), 350-357. *https://doi.org/10.30525/2256-0742/2018-4-1-350-357*

Kaur, J., & Ramkumar, K. R. (2022). The recent trends in cyber security: A review. *Journal of King Saud University-Computer and Information Sciences, 34*(8), 5766-5781. *https://doi.org/10.1016/j.jksuci.2021.01.018*

Kharchenko, L. S., Lipkan, V. A., & Loginov, O. V. (2004). *Information Security of Ukraine: glossary.* Tekst.

Korol, A. (2015). Information technologies in the system of international relations: the problem of implementation. *Multiverse. Philosophical Almanac*, (3-4), 59-67.

Libiseller, C. (2023). Hybrid warfare 'as an academic fashion. *Journal of Strategic Studies, 46*(4), 858-880. *https://doi.org/10.1080/01402390.2023.2177987*

Lipkan, V. A., Maksymenko, Y. Y., & Zhelikhovskyi, V. M. (2006). *Information security of Ukraine in the context of European integration*. KNT.

Luiijf, E., Besseling, K., & De Graaf, P. (2013). Nineteen national cyber security strategies. *International Journal of Critical Infrastructures, 9*(1-2), 3-31. *https://doi.org/10.1504/IJCIS.2013.051608*

Lysko, T. (2022). Bot farms and other cyber threats during martial law: issues of criminal liability. *Legal Scientific Electronic Journal*, *11*, 570-572. *https://doi.org/10.32782/2524-0374/2022-11/138*

Mattis, J. N., & Hoffman, F. G. (2005). Future Warfare: The Rise of Hybrid Wars. *Proceedings Magazine, 132*(11), 18-19.

Melnyk, O. (2022). *Criminal liability for crimes against peace, security of mankind and international law and order under martial law in Ukraine*. International Science Group.

Murtishcheva, A. O. (2022). *Certain aspects of the functioning of local self-government bodies under martial law.* H.S. Skovoroda Kharkiv National Pedagogical University.

Newlove-Eriksson, L., Giacomello, G., & Eriksson, J. (2018). The invisible hand? Critical information infrastructures, commercialization and national security. *The International Spectator, 53*(2), 124-140. *https://doi.org/10.1080/03932729.2018.1458445*

Nicola, M., Alsafi, Z., Sohrabi, C., Kerwan, A., Al-Jabir, A., Iosifidis, C., Agha, M., & Agha, R. (2020). The socio-economic implications of the coronavirus pandemic (COVID-19): A Review. *International Journal of Surgery, 78*, 185-193. *https://doi.org/10.1016/j.ijsu.2020.04.018*

North Atlantic Council. (2002). Security within the North Atlantic Treaty Organization (NATO) (C-M(2002)49). *https://www.freedominfo.org/documents/C-M(2002)49.pdf*

Petreski, D. S., & Ago, A. (2017). *Hybrid warfare through the prism of Ukrainian crisis. International scientific conference security concepts and policies - new generation of risks and threats*. Netherlands. *https://eprints.uklo.edu.mk/id/eprint/6809/1/2017-tom-2.pdf#page=121*

Reuters. (2022). *Ukraine detains senior public figures suspected of spying for Russia*. *https://www.reuters.com/world/europe/ukraine-detains-senior-public-figures-suspected-spying-russia-2022-06-21*

Security Outlines. (2024). NotPetya: understanding the destructiveness of cyberattacks. *https://www.securityoutlines.cz/notpetya-understanding-the-destructiveness-of-cyberattacks*

Seimas of the Republic of Lithuania. (1999). Law of the Republic of Lithuania "On State and Official Secrets". *https://e-seimas.lrs.lt/portal/legalAct/lt/TAD/TAIS.91654/BnLuwmQrpO*

Seimas of the Republic of Lithuania. (2000). Criminal Code of the Republic of Lithuania No. VIII-1968. *https://e-seimas.lrs.lt/portal/legalAct/lt/TAD/TAIS.111555*

Service of the Federal Ministry of Justice and the Federal Office of Justice of Germany. (1994). Law on Requirements and Procedures for Conducting Federal Audits of Security and Protection of Classified Information. *https://www.gesetze-im-internet.de/s_g/S%C3%9CG.pdf*

Stefanchuk, R. O., Myshchak, I. M., & Savchenko, L. A. (2022). *Legislative support for the formation and implementation of state policy of Ukraine under martial law*. Lyudmila.

Tkachuk, T. Y. (2017). Ensuring information security in the countries of Central Europe. *Legal Scientific Journal*, *5,* 104-110. *http://lsej.org.ua/5_2017/30.pdf*

United Nations General Assembly. (1994). Memorandum on Security Assurances in Connection with Ukraine's Accession to the Treaty on the Non-Proliferation of Nuclear Weapons. *https://treaties.un.org/doc/Publication/UNTS/Volume%203007/Part/volume-3007-I-52241.pdf*

Vanoni, L. P. (2018). Balancing privacy and national security in the global digital era: a comparative perspective of EU and US constitutional systems. In L. Violini & A. Baraggia (Eds.), *The Fragmented Landscape of Fundamental Rights Protection in Europe* (pp. 114-137). Edward Elgar Publishing.

Verkhovna Rada of Ukraine. (2022). Law of Ukraine No. 64/2022. "On the introduction of martial law in Ukraine". *https://zakon.rada.gov.ua/laws/show/64/2022#n2*

Verkhovna Rada of Ukraine. (1992). Law of Ukraine No. 2229-XII. "On the Security Service of Ukraine". *https://zakon.rada.gov.ua/laws/show/2229-12*

Verkhovna Rada of Ukraine. (1994). Law of Ukraine No. 3855-XII. "On State Secrets". *https://zakon.rada.gov.ua/laws/show/3855-12#Text*

Verkhovna Rada of Ukraine. (1996). Constitution of Ukraine. *https://www.president.gov.ua/documents/constitution*

Verkhovna Rada of Ukraine. (2001). Criminal Code of Ukraine. *https://zakon.rada.gov.ua/laws/show/2341-14#Text*

Verkhovna Rada of Ukraine. (2006). Law of Ukraine No. 3475-IV. "On the State Service of Special Communications and Information Protection of Ukraine". *https://zakon.rada.gov.ua/laws/show/3475-15#Text*

White, G. L., Hewitt, B., & Kruck, S. E. (2019). Incorporating global information security and assurance in IS education. *Journal of Information Systems Education, 24*(1), 11-16. *https://aisel.aisnet.org/jise/vol24/iss1/1/*

Wired. (2018). The untold story of NotPetya, the most devastating cyberattack in history. *https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world*

Wischmeyer, T. (2023). Why do States Keep Secrets? *In Transparency or Opacity*. Nomos Publishing Company mbH & Co.

Zadorozhnya, L. M. (2005). *Issues of improving the legislation of Ukraine in the field of information and informatization.* Academy of Legal Sciences.

Zhaboklichka, E., & Stankowski, D. (2022). Time of war and martial law, relations, mutual dependencies and legal, organisational and functional dillema. *Defense Science Review, 7*(13), 115-126. *https://doi.org/10.37055/pno/155529*

Međunarodna licenca / International License:
Creative Commons Attribution-NonCommercial-NoDerivatives 4.0.