JOURNAL OF SECURITY AND SUSTAINABILITY ISSUES
ISSN 2029-7017 print/ISSN 2029-7025 online
2020 March Volume 9 Number 3
https://doi.org/10.9770/jssi.2020.9.3(22)

Scopus®

CYBERSECURITY: LEGAL AND ORGANIZATIONAL SUPPORT IN LEADING COUNTRIES, NATO AND EU STANDARDS

Iryna Shopina[1], Dmytro Khomiakov[2], Nadiia Khrystynchenko[3], Serhii Zhukov[4*], Dmytro Shpenov[5]

[1]Lviv State University of Internal Affairs, Gorodotska Street, 26, Lviv, 79000, Ukraine;
[2,4]Military Institute of Taras Shevchenko National University of Kyiv,*
81 Mikhail Lomonosov Street, Kyiv, 03680, Ukraine
[3]Ternopil National Economic University, 11, Lvivska Street, Ternopil, 46000, Ukraine
[5]Verkhovna Rada of Ukraine, 5 Mikhail Hrushevsky Street, Kyiv, 01008, Ukraine

E-mail: [4]koaduep@gmail.com (Corresponding author)*

Received 16 March 2019; accepted 15 December 2019; published 30 March 2020

Abstract. The authors have investigated the features of legal support for cybersecurity in some of the leading countries of the world, have established the organizational basis for its support, as well as the main aspects of NATO and the EU's activities and standards in this area. In particular, the essence of the concept of cybersecurity is determined by referring to the views of both foreign scientists and Ukrainian scientists, and fixing this definition in normative documents of international importance (international standard ISO/IEC 27032:2012). Actual strategic goals in the direction of ensuring cybersecurity in countries such as France, the UK, the United States, as well as the settlement of these issues at the legislative level in Ukraine are highlighted. It has been established which state bodies operate in the indicated countries, whose powers include ensuring cybersecurity. Attention is paid to the settlement of cybersecurity and cyber protection issues at the international level, in particular at the EU and NATO levels. Particular attention is paid to NATO standards - TEMPEST. The content of the norms of the current legislation of Ukraine in the field of ensuring cybersecurity and the nature of the priority tasks of the National Cyber Security Coordination Center under the National Security and Defense Council of Ukraine are disclosed, which are normatively enshrined in the relevant Regulation. The features of the regulatory and organizational support of cybersecurity in some leading countries of the world and in Ukraine are structured.

Keywords: cyberspace; cybersecurity; cyber defense; TEMPEST.

Reference to this paper should be made as follows: 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)

JEL Classifications: F35, F42

1. Introduction

In recent years, the use of computer and telecommunication technologies has become widespread in various areas of human life, which is marked not only by positive changes in the transformation of social relations but also has led to new threats. The latter in the modern world is called "cyberthreats", the existence of which causes significant damage to both the national security of individual countries and has reached a global scale.

The existence of new negative challenges of the information age suggests the need to neutralize them and therefore led to the emergence of the concept of cybersecurity. To date, ensuring cybersecurity is no longer limited to the creation of the information security system at a separate facility. Solving this issue requires the formation of a unified system of protection of potential threats to the country's national security in cyberspace.

The development of strategic goals and the adoption of measures to ensure cybersecurity require the existence of an appropriate regulatory framework because they must be regulated at the legislative level. To this end, many countries of the world developed cybersecurity strategies that reflect not only the state's priority goals in this direction but also possible ways of implementing such measures and expected results. Given the above, it seems relevant to study the features of the legal and organizational support of cybersecurity in individual countries, as well as NATO and EU standards in this area.

2. Literature Survey

The essence of the concept of cybersecurity is the object of study by both many foreign scientists and Ukrainian scientists. Thus, Kumar & Somani (2018) focuses on the fact that the cybersecurity points to both the uncertainty in this new space and the practice or procedures to make it (progressively) safe. This, in turn, points to a multitude of exercises and activities, both specialized and non-specialized, which, as it is expected, should provide the bioelectric state and the information that it contains and transport from all possible threats (Tvaronavičienė, 2018a; Korauš et al., 2019; Ključnikov et al., 2019; Vlasov et al., 2019).

Panchanatham (2015) notes that advanced technologies such as cloud services, mobile phones, e-commerce, that participate in these transactions contain the most sensitive and important information about users. Therefore, providing them with the necessary security is very important. Improving cybersecurity and protecting sensitive data and infrastructure are important to all countries, which is a first and foremost security (Tvaronavičienė 2018b; Lialina, 2019; Vigliarolo, 2020; Chehabeddine, Tvaronavičienė, 2020; Petrenko et al., 2019; Markopouloua et al., 2019).

Weiss et al. (2013) define cybersecurity as the management, development, management, and use of information security, and the protection of operational technologies (IT) and IT security means to achieve regulatory compliance, protect assets and compromise the assets of opponents.

Samuel & Osman (2014) point out the crucial role of cybersecurity in the field of data transfer technologies, the protection of which is the most difficult today. The main essence of cybersecurity, on which an important emphasis is placed, is associated with cybercrime, which is characterized by a rapid growth day by day.

According to Rus (2017), under a systemic approach, cybersecurity covers: (1) protection of electronic equipment; (2) data and information processing software. In terms of the concept, cybersecurity includes information security, it is extended to mobile devices and intelligent equipment, structured and unstructured information that it controls.

The enough interesting idea is expressed by the team of authors Galinec et al. (2017), who point out that cybersecurity is not:

(1) simply synonymous with information security, OT security, or IT security;

(2) the use of information security to protect the enterprise from crime.

(3) Cyberwar - although the definition of this term is still controversial. The consensus is that "cyberwar" means taking advantage of cybersecurity in the conditions of the war. This is a complex area and should not be confused with physical attacks on infrastructure (for example, destruction of property and equipment) and information war (for example, with the use of psychological operations using propaganda and disinformation).

(4) Cyberterrorism - like cyberwar, "cyberterrorism" refers to the use of cybersecurity techniques as part of the terrorist campaign or activity.

(5) Cybercrime is only an injured or pretentious term for criminal attacks using IT infrastructure. This is not related to cybersecurity.

Authors Panteleeva et al. (2019) believe that the concept of "cybersecurity" is complex, which in its essence combines the subject basis of cyberspace and the process functionality of the defense mechanism, relies on

systemic and institutional approaches, principles of efficiency, reliability, and optimality.

It is also necessary to focus on the fact that the concept of "cybersecurity" is not only researched and defined in the scientific refinements of scientists but also is enshrined in regulatory documents of international importance. In particular, in clause 4.20 of the international standard ISO/IEC 27032:2012 "Information technology - Security techniques - Cybersecurity guidelines", the concept of "cybersecurity" is interpreted through the category "cyberspace security", which refers to the confidentiality, integrity, and accessibility of information in cyberspace. The definition of cyberspace is contained in clause 4.21, which refers to a complex environment arising from the interaction of people, software and the Internet using technological devices and networks connected to it, which does not exist in any physical form (ISO/IEC 27032:2012 Information technology - Security techniques - Cybersecurity guidelines, 2012). In order to harmonize national Ukrainian legislation with international and European regulatory documents, DSTU ISO/IEC 27032:2016 "Information Technologies. Methods of protection. Cybersecurity guidelines", which came into force on January 1, 2018.

3. Methods

The study of the concept of cybersecurity, the features of its legal support in some leading countries of the world, the definition of the organizational framework for ensuring cybersecurity, as well as the coverage of the main aspects of NATO and the EU's activities in this area, were carried out using dialectic, comparative-legal, formal-legal, and system structural methods.

Using the dialectical method, the essence of the concept of "cybersecurity" was revealed by referring to the views of both foreign scientists and Ukrainian scientists.

The comparative-legal method made it possible to determine the legal framework on the specifics of ensuring cybersecurity in the leading countries of the world. In addition, the current strategic goals in this direction (for example, France, Great Britain, the USA), as well as resolving these issues at the legislative level in Ukraine, are highlighted.

Using the formal-legal method, the contents of the current legislation of Ukraine in the field of cybersecurity and the nature of the priority tasks of the National Cyber Security Coordination Center under the National Security and Defense Council of Ukraine are disclosed, which are normatively enshrined in the relevant Regulation.

Using the system-structural method, the analysis is carried out and the features of the regulatory and organizational support of cybersecurity in some leading countries of the world and in Ukraine are determined.

4. Results

Within the framework of the subject under study, it is necessary to determine what regulatory documents of the leading countries of the world have settled the issue of cybersecurity and what organizations operate in this area.

In France, for example, the 2011 French National Cyber Security Strategy is the founding document. The Strategy defines cybersecurity as the desired state of an information system in which it can withstand events from cyberspace that may compromise the availability, integrity or confidentiality of the data which are stored, processed or transmitted, and the related services that these systems offer or make available. Cybersecurity uses the methods of protecting information systems and is based on the fight against cybercrime and the establishment of cyber defense. In turn, cyberspace is defined as a communication space created through the worldwide interconnection of automated digital data processing equipment (Information systems defense and security - France's strategy, 2011).

On October 16, 2015, the French National Digital Security Strategy, based on five strategic priorities, was announced by French Prime Minister Manuel Valls:

(1) the main interests, defense, and security of state information systems and critical infrastructure, the most important operators of the economy and society, the big cybersecurity crisis;

(2) digital trust, confidentiality, personal data, cyber identity;

(3) raising awareness, primary education, continuing education;

(4) digital business environment, industrial policy, export, and internationalization;

(5) Europe, digital strategic autonomy, stability in cyberspace (The French national digital security strategy, 2015).

In France, the Agence nationale de la sécurité des systèmes d'information (ANSSI) is the government agency in the field of cyber defense and network and information security. To carry out its missions, ANSSI has launched a wide range of regulatory and operational activities, ranging from issuing regulations and verifying their application to monitoring, alerting and rapid response, especially in government networks. ANSSI maintains bilateral relations with numerous foreign agencies on every continent.

Following a multilateral approach, ANSSI works closely with the Ministry of Foreign Affairs and International Development (Ministère des Affaires étrangères et du Développement international (MAEDI) and the Ministry of Defense to define and promote French positions on political cybersecurity priorities (for example, the application of international law in cyberspace, the role of regional cybersecurity organizations, etc.). At the European Union (EU) and NATO level, ANSSI plays an important role through the National Communication Security Authority (NCSA) and the National Cyber defense Authority (NCDA). ANSSI is involved in providing communications to these organizations, ensuring that the EU and NATO have the necessary structures and resources to provide their own cybersecurity and support these organizations in their efforts to achieve this goal. ANSSI also represents France in the European Network and Information Security Agency (ENISA) and the National Liaison Officers (NLO) (The official website of ANSSI).

In 2013, many years of experience and cooperation with critical operators led ANSSI to propose to adopt a regulatory framework "Critical Information Infrastructure Protection (CIIP) Law", which was promulgated on December 18, 2013. The law was proposed with the goal of establishing a common minimum cybersecurity level for all critical operators and enhancing ANSSI to support them in the event of a cyberattack. The law applies to more than 200 public and private operators from 12 sectors that are already recognized as critical in France. Security requirements will apply only to the most "critical information systems" of operators responsible for identification. The law provides for 4 main activities:

(1) Incidents Notification - ANSSI directly informs operators of cases that occur in their critical information systems, protecting the confidentiality of operators;

(2) Security Rules - ANSSI should establish technical and organizational rules, mainly basic cyber hygiene measures and common ones to all sectors;

(3) Inspection - ANSSI may run security audits conducted by its services, another government agency, or a trusted service provider regularly or after an incident;

(4) Major Crisis - ANSSI may introduce measures in the event of a major crisis announced by the Prime Minister. He establishes the legal basis for action under the crisis management plans (The French CCIP framework).

In April 2019, the French Military Cyber Strategy, consisting of two separate documents: the Public Elements for the Military Cyber Warfare Doctrine (hereafter the Public Elements) and the Ministerial Policy for Defensive Cyber Warfare (hereafter the Ministerial Policy), was introduced by the Minister of Armed Forces Florence Parly in France. The first of two documents containing the strategy of France is the Public Elements, which makes it possible to act on both the defense and offensive levels using cyber capabilities. The second document is the Ministerial Policy. Based on the recognition that cyber defense is a shared responsibility, the ministerial policy aims to better define the distribution of powers between the Ministry of Defense, its various structures,

and their industrial partners outside the government. The Chief of Defense Staff is responsible for defending the French Ministry of Defense against cyberthreats, and COMCYBER is responsible for its implementation. Together, these documents define the doctrine of the French Ministry of Defense (Ministère des Armées) on informative defense and offensive action, or on defense and offensive cyber warfare. The military cyber strategy, both its offensive and defense components, demonstrates a comprehensive approach to cyber defense, involving the entire French military industrial complex, including the Ministry of Defense (Delerue et al., 2019; Sitdikova & Starodumova, (2019).

Thus, in France, the Head of ANSSI is generally responsible in the field of the state's cybersecurity, while the cyber defense commander (COMCYBER) is exclusively responsible for the cyber defense of the Ministry of Defense.

In the UK, the main regulatory document, the provisions of which are aimed at ensuring cybersecurity, is the National Cyber Security Strategy for 2016-2021. Clause 2.11 of Section 2 of the Strategy provides a definition of cybersecurity as protection of the information systems (hardware, software and related infrastructure), data about them and the services they provide against unauthorized access, damage, or misuse. Cyber security also includes damage caused by the system operator intentionally or accidentally due to non-compliance with security procedures (National Cyber Security Strategy 2016-2021, 2016).

The National Cyber Security Strategy is designed to shape government policies and offer a coherent and credible vision for sharing with the public and private sectors, civil society, academia, and the public. The strategy determines the proposed or recommended actions for all sectors of the economy and society, from the central government to the leaders of various industries and individuals.

It is also important to note that the National Cyber Security Strategy addresses cybercrime in the context of two interrelated forms of criminal activity:

(1) cyber-dependent crimes - crimes that can only be committed with the help of information and communication technology (ICT) devices, where the devices are both a tool for committing a crime and a goal of a crime (for example, the development and distribution of bogusware for the purpose of financial profit, hacking to steal, damage, distortion or destruction of data and/or network or activity);

(2) cyber-enabled crimes - traditional crimes that can be scaled up or expanded through the use of computers, computer networks, or other forms of ICT (for example, data theft) (National Cyber Security Strategy 2016-2021, 2016).

According to the National Cyber Security Strategy, the future vision until 2021 is that the UK is reliable and resilient to cyber threats, prosperous and confident in cyberspace. Such a vision involves the achievement of relevant goals in three directions, namely:

(1) Protection - the availability of funds to protect the United Kingdom from developing cyber threats, an effective response to incidents and assurance of the protection and resilience of the UK networks, data, and systems.

(2) Deterrence - The UK must be a difficult target for all forms of aggression in cyberspace, which is ensured by the identification, investigation, and deterrence of hostile actions taken against the country.

(3) Development - the presence of an innovative, growing cybersecurity industry, supported by the world leading research and development (National Cyber Security Strategy 2016-2021, 2016).

In the UK, the Government Communications Headquarters (GCHQ) is active in cybersecurity and cyber defense. GCHQ provides intelligence, protects information, and informs relevant UK policy to keep society safe in the Internet age. GCHQ's cybersecurity policy is to create an environment, in which the UK is considered a safe place to live and do business on the Internet. GCHQ activities are directed in three areas, namely:

(1) collection - with strict observance of the current legislation, a number of methods are used to collect messages and data that are important;

(2) analysis - communications and data are analyzed to create intelligence reports;

(3) effects - the use of various Internet opportunities that can lead to a real world result (The official website of GCHQ).

The National Cyber Security Center (NCSC) was created in the GCHQ structure, which is aimed at establishing cooperation between the industry and the government by providing advice, guidance, and support on cybersecurity issues, including the management of cybersecurity cases. NCSC provides support to key UK organizations, the public sector, industry, and the general public. The NCSC is designed to respond effectively to the emergence of various cyber incidents in order to minimize damage to the UK. The NCSC's cyber defense activities include cooperation with law enforcement, national defense, intelligence and security services in the UK and international partners (The official website of NCSC).

In order to strengthen cybersecurity in the country, the Cyber-Attacks (Asset-Freezing) Regulations were adopted on May 20, 2019, which provide for measures to freeze the funds and economic resources of all individuals and organizations listed in Appendix I of the Regulation, and to ensure that it is impossible to provide funds and economic resources to them or to their benefit (The Cyber-Attacks (Asset-Freezing) Regulations, 2019).

At a NATO Cyber Defense Conference held on May 23, 2019, Ciaran Martin (Head of the NCSC) noted in his report that the NCSC has already developed world-class methods to track the most threatening attack groups, tools, and techniques to counter them. At the same time, there are a number of activities that help make the Internet vulnerable automatically safe. It is important to focus attention on Ciaran Martin's comments that the NCSC is a part of the GCHQ, and that is why success in the NCSC activities is achieved at the national level. As part of the international community, a cybersecurity alliance with NATO is very important. The NCSC strongly supports the full implementation of Cyber Defense Pledge 2016 (Ciaran Martin's speech at the NATO Cyber Defense Pledge Conference, 2019).

In the United States, the legal cybersecurity principles are concentrated in the 2018 National Cyber Defense Strategy. The priorities of the National Cyber Defense Strategy include:

(1) protection of the homeland by protecting networks, systems, functions, and data;

(2) fostering America's prosperity by developing a secure, prosperous digital economy and fostering strong domestic innovation;

(3) maintaining peace and security by enhancing the ability of the United States in collaboration with allies and partners to deter and, if necessary, punish those who use cyber tools for malicious purposes;

(4) expanding American influence abroad to expand the basic principles of an open, collaborative, reliable, and secure Internet (National cyber strategy of the United States of America, 2018).

Based on the analysis of the provisions of the National Cyber Defense Strategy, it is important to pay attention to the fact that, unlike the similar strategies in the field of cybersecurity in France and the United Kingdom, there is no definition of cybersecurity in it.

The Privacy and Civil Liberties Final Guidelines: Cybersecurity Information Sharing Act (2015) defines that the goal of cybersecurity is to protect an information system or information that is stored, processed, or transmitted through information systems against cybersecurity threats or security vulnerability. Cybersecurity threats are identified as actions that can lead to unauthorized efforts to adversely affect the security, accessibility, privacy, or integrity of the computer system (Privacy and Civil Liberties Final Guidelines: Cybersecurity Information Sharing Act (2015).

As for the state body vested with authority in the field of cybersecurity in the United States, it is the Cybersecurity and Infrastructure Security Agency (CISA), which operates in compliance with the provisions of the Law on the Agency for Cybersecurity and Infrastructure adopted in 2018. The CISA coordinates security and resilience efforts using strong partnerships in the private and public sectors and provides technical assistance and evaluation to federal stakeholders, critical infrastructure owners and operators across the country. To ensure

cybersecurity among the main areas of CISA activities, it is necessary to highlight the following:

(1) the provision of free tools and resources for public and private partners;

(2) facilitating the assessment of the critical infrastructure vulnerability;

(3) enhancing safety and sustainability in the chemical sector;

(4) providing training, encouraging the exchange of information, and promoting industry partnerships and international engagement (Cybersecurity and Infrastructure Security Agency Act, 2018).

The CISA works with businesses, communities, and governments at all levels to make the country's critical infrastructure more resilient to cyber threats (The official website of CISA).

The issue of cybersecurity is relevant not only at the national level of individual states but also at the international level. In particular, NATO and its allies rely on strong and sustainable cyber defense to fulfill the Alliance's core tasks of collective defense, crisis management, and shared security. The Alliance must be prepared to defend its networks and operations against the growing complexity of cyberthreats and attacks it faces (The official website of NATO). Among the main events in the field of cybersecurity, it is important to highlight the following ones:

(1) cyber defense is part of the key mission of NATO's collective defense.

(2) NATO has confirmed that international law applies in cyberspace.

(3) NATO's focus on cyber defense is to protect its own networks (including operations and missions) and increase resilience in the Alliance.

(4) In July 2016, the allies reaffirmed NATO's defensive mandate and recognized cyberspace as a field of operations, in which NATO must defend itself as effectively as it does in the air, on land, and at sea.

(5) In July 2016, the allies also committed themselves to cyber defense in order to improve their cyber defense as a priority. Since then, all allies have improved their cyber defense.

(6) NATO reinforces its opportunities in the field of cyber-learning.

(7) Allies should strengthen the exchange of information and mutual assistance in preventing, mitigating, and recovering from cyberattacks.

(8) NATO cyber defense rapid response teams are ready to help allies 24 hours a day, if required and approved.

(9) At the Brussels summit in 2018, the allies agreed to create a new Cyberspace Operations Center as part of NATO's strengthened team structure. They also agreed that NATO could use national cyber retaliation for its missions and operations.

(10) In February 2019, the allies approved NATO's leadership, which contains a number of tools to further strengthen NATO's ability to respond to significant harmful cyber activities.

(11) NATO and the European Union (EU) collaborate thanks to the cyber defense technical agreement, which was signed in February 2016. In light of the common challenges, NATO and the EU strengthen cooperation in the field of cyber defense, especially in the areas of information exchange, training, research, and exercises.

(12) NATO is stepping up cooperation with industry through a partnership in NATO's cyber industry.

(13) NATO recognizes that its allies can take advantage of standards-based, predictable, and secure cyberspace (Cyber defense, 2019).

Responsibility for planning and conducting all cybersecurity lifecycle management activities is vested in the authority of the NATO Communications and Information Agency (NCI Agency) Cyber Security (CS) Service Line (SL). The cybersecurity service line provides specialized cybersecurity services covering a range of scientific, technical, and operational support throughout the life cycle of NATO's information communications and technologies, and allows the Alliance to operate safely and securely. Cybersecurity provides for the provision of a wide range of services in such specialized areas of security: CIS security, cyber protection, information security, computer security, and communications security. When carrying out its duties, CS SL supports the development and implementation of the cybersecurity policy and strategy and provides lifecycle security risk management services for all NATO ICTs (The official website of NCI Agency).

In 2016, Cyber Defense Pledge was signed by NATO member countries. In accordance with this document, the heads of states and governments of the member countries of the Alliance assumed the obligation to ensure the security of the Alliance against cyber threats, as well as the possibility of their own protection in cyberspace. The work of the allies and the EU on enhancing cybersecurity, which helps to strengthen resilience in the Euro-Atlantic region, and further cooperation between NATO and the EU in the field of cyber defense are recognized as one of the priority areas. In addition, the member states affirmed the applicability of international law in cyberspace in the Cyber Defense Pledge. The role of NATO in promoting cooperation in the field of cyber defense, including through multinational projects, education, training, and the exchange of information to support national cyber defense efforts, is noted. Among the obligations of NATO member states, the following ones are enshrined in Cyber Defense Pledge:

(1) To develop the fullest range of capabilities to protect national infrastructure and networks;

(2) To allocate adequate resources at the national level to strengthen cyber defense capabilities;

(3)To strengthen the synergy between relevant cyber defense stakeholders in order to deepen collaboration and share best practices;

(4) To improve understanding of cyber threats, including the exchange of information and assessments;

(5) To enhance the skills and knowledge of all defense stakeholders at the national level on fundamental cyber hygiene through sophisticated and reliable cyber defense;

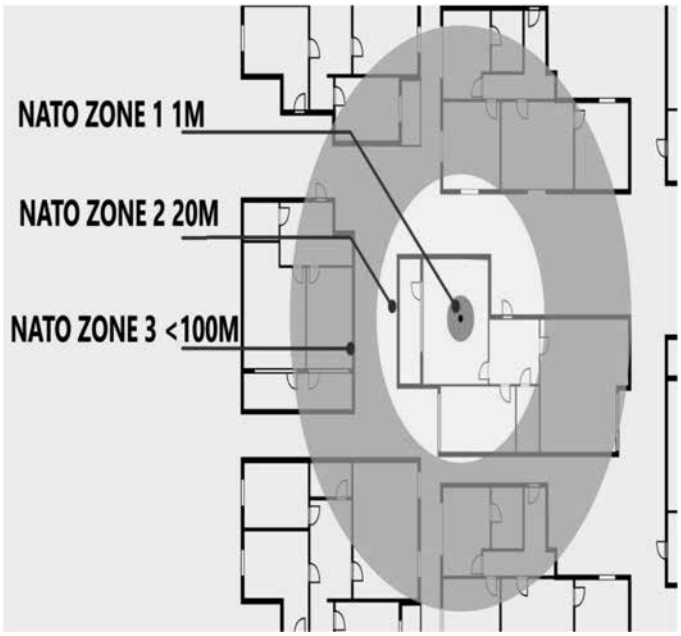
(6) To promote cyber education, training, and the fulfillment of forces, as well as strengthening educational institutions, building trust and knowledge in the Alliance;

(7) To speed up the implementation of agreed cyber defense obligations, including for the national systems, on which NATO depends (Cyber Defense Pledge, 2016).

So, in 2018, NATO member states agreed on how to integrate the sovereign cyber effects, voluntarily provided by the allies, into the operations and missions of the Alliance, as well as create a Cyberspace Operations Center (CyOC). CyOC is responsible for information on cyberspace, centralized planning for cyberspace aspects of Alliance operations and missions, and coordination of cyberspace operational issues (Brent, 2019).

Today, NATO TEMPEST standards are world-famous in the field of cyber defense. TEMPEST deals with radiated electromagnetic waves of equipment (both radiated and conducted) and assesses the risk of eavesdropping. All electrical and electronic equipment generates electromagnetic radiation. In EMC, radiation from data processing equipment such as laptops or mobile phones contains sensitive information that is easy to intercept. In accordance with NATO TEMPEST standard, the so-called zones are defined - Zone 0, Zone 1, Zone 2 or Zone 3, and for which a standard for equipment test is required, which processes sensitive data in these rooms (Figure 1).

The European Union Agency for Cybersecurity (ENISA) has been operating in the European Union since 2004. ENISA works closely with member states and other stakeholders to provide advice and solutions, as well as improve their cybersecurity capabilities. It also supports the development of a joint response to large-scale cross-border incidents in the field of cybersecurity or crisis and has been developing cybersecurity certification schemes since 2019. The Regulation (EU) 2019/881 (Cybersecurity Act) establishes a European cybersecurity certification system for ICT products, services, and processes. ENISA is participating in this new structure, preparing candidate certification schemes at the request of the European Commission or the European Cybersecurity Coordination Group (member state delegation) (Regulation (EU) 2019/881).



LEVEL A – NATO SDIP-27

High level A is NATO's most stringent standard, and therefore it is sometimes called "FULL". Level A is applied to environments and equipment where immediate eavesdropping from an adjacent room (approximately 1 meter) can occur. Therefore, this standard applies to the equipment operating in the NATO zone 0.

LEVEL B – NATO SDIP-27

High level B is NATO's next highest standard, also known as "IMMEDIATE". This standard is applied to equipment, which is not heard at a distance of more than 20 meters. This "IMMEDIATE" standard is applied to equipment that operates in NATO Zone 1 and protects equipment both at 20 meters of unobstructed distance and at a comparative distance through walls and obstacles.

Level C - NATO SDIP-27

Temperature level C is also called "TACTICAL". This standard is applied to environments and equipment in NATO Zone 2 (where eavesdropping can be possible at least 100 meters away). This standard protects equipment at 100 meters of unobstructed distance or comparable distance through walls and obstacles (What is the US NATO TEMPEST).

Figure 1. NATO ZONING (https://www.interelectronix.com/en/tempest.html)

The important role of standardization is caused by the following factors:

- there is a need for closer international cooperation to improve cybersecurity standards, including the need to define common standards of behavior, adopt codes of conduct, use international standards and exchange information, fostering faster international cooperation in response to the network and information security problems and promoting a joint global approach to such issues;

- European cybersecurity certification schemes should be non-discriminatory and based on European or international standards, if only these standards are ineffective or inappropriate to fulfill the Union's legitimate goals in this regard;

- The EU certificate or declaration of conformity must contain technical specifications, standards. and procedures (Cybersecurity Standards and Certification, the official website of ENISA)

The ENISA strategy for 2016 - 2020 includes the following priority areas:

(1) to foresee and support Europe in solving new problems related to network and information security;

(2) to promote the network and information security as a priority of EU policies,

(3) to support Europe in supporting the advanced capabilities of the Network Information Service (NIS)

(4) to contribute to the formation of the European Community of the CIS;

(5) to enhance the effect of ENISA (Markopouloua et al., 2019).

In Ukraine, the concept of «cybersecurity» is defined by the legislator in the Law of Ukraine «On the basic principles of ensuring cybersecurity of Ukraine» dated October 5, 2017. In accordance with the clause 5 part 1 article 1 of the Law, cybersecurity means the protection of the vital interests of a person and citizen, society and the state when using cyberspace, which ensures the sustainable development of the information society and digital communication environment, timely identification, prevention, and neutralization of real and potential threats to the national security of Ukraine in cyberspace. Clause 7 part 1 Article 1 of the Law contains a definition of the concept of cyber protection as a combination of organizational, legal, engineering and technical measures, as well as measures of cryptographic and technical information protection aimed at preventing cyber incidents, identifying and protecting against cyberattacks, eliminating their consequences, and restoring the stability and reliability of communication and technological systems (Law of Ukraine on the basic principles of ensuring cybersecurity of Ukraine, 2017).

The Cyber Security Strategy of Ukraine, approved by the presidential decree of March 15, 2016 is currently in force. The priority areas of the Strategy include:

(1) elaboration and operational adaptation of state cybersecurity policies aimed at developing cyberspace, achieving compatibility with relevant EU and NATO standards,

(2) creation of a domestic regulatory and terminological base in this area, harmonization of regulatory documents in the field of electronic communications, information protection, information and cybersecurity in accordance with international and EU and NATO standards,

(3) formation of a competitive environment in the field of electronic communications, the provision of services for the protection of information and cyber defense;

(4) development of cybersecurity technologies for mobile communications, ensuring hardware, content security, and application and communication services security;

(5) attracting the expert potential of scientific institutions, professional and public associations to prepare projects of conceptual documents in the field of cybersecurity;

(6) improvment of the digital literacy of citizens and a culture of safe behavior in cyberspace, integrated knowledge, skills, and abilities necessary to maintain the goals of cybersecurity, implementing state and public projects to increase public awareness of cyber threats and cyber protection;

(7) conducting exercises on cyberspace emergencies and incidents;

(8) development and improvement of the system of state control over the state of information security, as well as the system of independent audit of information security, the implementation of international best practices and international standards on cybersecurity and cyber protection;

(9) development of electronic communications infrastructure, including broadband Internet access, digital and interactive television;

(10) development of a network of computer emergency response teams;

(11) creation of a system for the timely detection, prevention, and neutralization of cyber threats, including with the involvement of volunteer organizations;

(12) development and improvement of the technical and cryptographic information protection system;

(13) development of international cooperation in the field of cybersecurity, support of international initiatives in the field of cybersecurity that are in line with the national interests of Ukraine, deepening cooperation between Ukraine and the EU and NATO to strengthen Ukraine's capabilities in the field of cybersecurity, participation in OSCE-sponsored cyberspace confidence-building activities;

(14) creation of the conditions for the introduction of modern cyber defense technologies in Ukraine (Cyber Security Strategy Of Ukraine, 2016).

It is important to note that the working body of the National Security and Defense Council of Ukraine in the field of cyber defense is the National Cyber Security Coordination Center, which operates in accordance with the Regulation. The priority tasks of the National Cyber Security Coordination Center include:

(1) analysis: cybersecurity status; results of a review of the National Cyber Security system; the state of readiness of cybersecurity entities to fulfill the tasks of countering cyber threats, implementing measures to prevent and combat cybercrime;

(2) participation in the development of industry cybersecurity indicators;

(3) forecasting and identifying potential and real threats in the field of cybersecurity of Ukraine;

(4) development of conceptual principles and proposals for ensuring state cybersecurity;

(5) synthesis of international experience in the field of cybersecurity;

(6) participation in ensuring the development and implementation by cybersecurity entities of information exchange mechanisms necessary for organizing a response to cyber attacks and cyber incidents, eliminating their causes and consequences;

(7) operational, informational, and analytical support of the National Security and Defense Council of Ukraine on cybersecurity issues;

(8) developing and submitting proposals to the National Security and Defense Council of Ukraine, its Chairperson, in accordance with the established procedure, on defining Ukraine's national interests in the field of cybersecurity;

(9) monitoring the development and implementation of national standards and technical regulations for the use of information and communication technologies, harmonized with EU and NATO standards;

(10) the elaboration of issues to determine the ways, mechanisms, and methods for resolving problematic issues that arise during the implementation of state policy in the field of ensuring cybersecurity;

(11) participation in ensuring the monitoring of the implementation of decisions of the National Security and Defense Council of Ukraine on cybersecurity of the state, enforced by decrees of the President of Ukraine;

(12) study of international experience in the creation and functioning of National Cyber Security systems, its distribution among organizations and institutions in accordance with its competence, monitoring of its implementation in Ukraine;

(13) participation in the organization and conduct of interethnic and interdepartmental cyber-learning and training in the field of cybersecurity, the development of relevant methodological documents and recommendations (Regulations on the National Cyber Security Coordination Center, 2016).

Thus, on the basis of the study conducted, it is possible to formulate regulatory and organizational support in the leading countries of the world and Ukraine in the corresponding table (Table 1).

Table 1. Regulatory and organizational support of cybersecurity in some leading countries of the world and in Ukraine

Country	Regulatory support (basic regulatory documents)	Organizational support (state authorities)	Strategic goals
France	1. The French national digital security strategy (2015) 2. French Military Cyber Strategy (2019): the Public Elements for the Military Cyber Warfare Doctrine (the Public Elements) and the Ministerial Policy for Defensive Cyber Warfare (the Ministerial Policy) 3. Critical Information Infrastructure Protection (CIIP) Law (2013) 4. French Data Protection Act (2018)	Agence nationale de la sécurité des systèmes d'information (ANSSI)	(1) the main interests, defense, and security of state information systems and critical infrastructure, the most important operators of the economy and society, the big cybersecurity crisis; (2) digital trust, confidentiality, personal data, cyber identity; (3) raising awareness, primary education, continuing education; (4) digital business environment, industrial policy, export, and internationalization; (5) Europe, digital strategic autonomy, stability in cyberspace
United Kingdom	1. National Cyber Security Strategy 2016-2021 2. The Cyber-Attacks (Asset-Freezing) Regulations (2019)	Government Communications Headquarters (GCHQ)	(1) Protection - the availability of funds to protect the United Kingdom against developing cyber threats, the effective response to incidents and assurance of the protection and resilience of the UK networks, data, and systems. (2) Deterrence - The UK must be a difficult target for all forms of aggression in cyberspace, which is ensured by the identification, investigation, and deterrence of hostile actions taken against the country. (3) Development - the presence of an innovative, growing cybersecurity industry, supported by world-leading research and development.

United States	1. National cyber strategy of the United States of America (2018) 2. Cybersecurity and Infrastructure Security Agency Act (2018) 3. Privacy and Civil Liberties Final Guidelines: Cybersecurity Information Sharing Act (2015)	Cybersecurity and Infrastructure Security Agency (CISA)	(1) protection of the homeland by protecting networks, systems, functions, and data; (2) fostering America's prosperity by developing a secure, prosperous digital economy and fostering strong domestic innovation; (3) maintaining peace and security by enhancing the ability of the United States in collaboration with allies and partners to deter and, if necessary, punish those who use cyber tools for malicious purposes; (4) expanding American influence abroad to expand the basic principles of an open, collaborative, reliable, and secure Internet.
Ukraine	1. Ukraine's Cyber Security Strategy (2016) 2. The Law of Ukraine "On the Fundamental Principles of Cybersecurity of Ukraine" (2017) 3. Regulations on the National Cyber Security Coordination Center (2016)	The National Cyber Security Coordination Center is a working body of the National Security and Defense Council of Ukraine	(1) elaboration and operational adaptation of state cybersecurity policies aimed at developing cyberspace, achieving compatibility with relevant EU and NATO standards, (2) creation of a domestic regulatory and terminological base in this area, harmonization of regulatory documents in the field of electronic communications, information protection, information, and cybersecurity in accordance with international and EU and NATO standards, (3) formation of a competitive environment in the field of electronic communications, the provision of services for the protection of information and cyber defense; (4) development of cybersecurity technologies for mobile communications, ensuring hardware, content security, and application and communication services security; (5) attracting the expert potential of scientific institutions, professional and public associations to prepare projects of conceptual documents in the field of cybersecurity; (6) improvement of the digital literacy of citizens and a culture of safe behavior in cyberspace, integrated knowledge, skills, and abilities necessary to maintain the goals of cybersecurity, implementing state and public projects to increase public awareness of cyber threats and cyber protection; (7) conducting exercises on cyberspace emergencies and incidents; (8) development and improvement of the system of state control over the state of information security, as well as the system of the independent audit of information security, the implementation of international best practices and international standards on cybersecurity and cyber protection; (9) development of electronic communications infrastructure, including broadband Internet access, digital and interactive television; (10) development of a network of computer emergency response teams; (11) creation of a system for the timely detection, prevention, and neutralization of cyber threats, including with the involvement of volunteer organizations; (12) development and improvement of the technical and cryptographic information protection system; (13) development of international cooperation in the field of cybersecurity, support of international initiatives in the field of cybersecurity that are in line with the national interests of Ukraine, deepening cooperation between Ukraine and the EU and NATO to strengthen Ukraine's capabilities in the field of cybersecurity, participation in OSCE-sponsored cyberspace confidence-building activities; (14) creation of the conditions for the introduction of modern cyber defense technologies in Ukraine

5. Discussion

In the modern world, one of the priorities in ensuring the national security of the state is the formation of the cybersecurity policy. This is explained by the fact that with the development of information and communication technologies, the emergence of new threats in cyberspace, called cyber threats, became inevitable.

That is why the effectiveness of the normative and organizational support of cybersecurity in any country is an indicator of its ability to withstand the cyber threats that exist in cyberspace and take various forms every day.

Achievement of the desired cybersecurity level in a given country is seen to be effective, provided that there is both coordination between national government bodies that are vested with the relevant authority in this area and at the level of interstate ties. In particular, in the context of European integration for Ukraine, the urgent strategic goal of ensuring cybersecurity is the harmonization of regulatory documents with international and EU and NATO standards.

Conclusions

According to the results of the study, it should be noted that in many leading countries of the world, cybersecurity systems of national importance have already been formed and are functioning.

So, in France, the Agence nationale de la sécurité des systèmes d'information (ANSSI) acts as the state body in the field of cyber defense and network and information security. To carry out its missions, ANSSI has launched a wide range of regulatory and operational activities, ranging from issuing regulations and verifying their application to monitoring, alerting, and rapid response, especially in government networks.

In the UK, the Government Communications Headquarters (GCHQ) actively operates in the area of cybersecurity and cyber defense, which provides intelligence, protects information, and informs relevant UK policies to keep society safe in the Internet age. Moreover, the National Cyber Security Center (NCSC) was created in the GCHQ structure, which is aimed at establishing cooperation between industry and the government by providing advice, guidance, and support on cybersecurity issues, including the management of cybersecurity cases.

In the United States, the legal framework for cybersecurity is concentrated in the 2018 National Cyber Security Strategy, and the Sybersecurity and Infrastructure Security Agency (CISA) acts as the government agency with powers in cybersecurity, which operates in compliance with the relevant laws of the agency.

The issue of cybersecurity is relevant not only at the national level of individual states but also at the international level. In particular, NATO and its allies rely on strong and sustainable cyber defense to fulfill the Alliance's core tasks of collective defense, crisis management, and shared security.

Responsibility for planning and conducting all cybersecurity lifecycle management activities is vested in the authority of the NATO Communications and Information Agency (NCI Agency) Cyber Security (CS) Service Line (SL). Today, NATO TEMPEST international standards are world-famous in the field of cyber defense. The European Union Agency for Cybersecurity (ENISA) has been operating in the European Union since 2004, which works closely with member states and other interested parties to provide advice and solutions, as well as improve their cybersecurity capabilities.

References

Brent, L. (2019). NATO's role in cyberspace. URL: https://www.nato.int/docu/review/articles/2019/02/12/natos-role-in-cyberspace/index.html

Ciaran Martin's speech at the NATO Cyber Defence Pledge Conference (2019). *The official website of National Cyber Security Centre (NCSC)*. URL: https://www.ncsc.gov.uk/speech/ciaran-martin-speech-nato-cyber-defence-pledge-conference

Cyber defence (2019). *The official website of NATO*. URL: https://www.nato.int/cps/en/natohq/topics_78170.htm

Cyber Defence Pledge (2016). *The official website of NATO*. URL: https://www.nato.int/cps/en/natohq/official_texts_133177.htm

Cybersecurity and Infrastructure Security Agency Act (2018). URL: https://www.congress.gov/bill/115th-congress/house-bill/3359

Cybersecurity Standards and Certification. *The official website of ENISA*. URL: https://www.enisa.europa.eu/topics/standards?tab=details

Cybersecurity Strategy Of Ukraine (2016). URL: https://zakon5.rada.gov.ua/laws/show/96/2016

Delerue, F., Desforges, A., & Géry, A. (2019). A close look at France's new Military Cyber Strategy. URL: https://warontherocks.com/2019/04/a-close-look-at-frances-new-military-cyber-strategy

Galinec, D., Možnik, D., & Guberina, B. (2017). Cybersecurity and cyber defence: national level strategic approach. *Automatika: Journal for Control, Measurement, Electronics, Computing and Communications, 3*(58), 273-286. https://doi.org/10.1080/00051144.2017.1407022

Information systems defence and security – France's strategy (2011). URL: https://www.enisa.europa.eu/media/news-items/Information_system_security_France_strategy.pdf/view

ISO/IEC 27032:2012 Information technology – Security techniques – Guidelines for cybersecurity (2012). URL: https://www.iso.org/obp/ui/#iso:std:iso-iec:27032:ed-1:v1:en

Ključnikov, A., Mura, L., Sklenár, D. (2019). Information security management in SMEs: factors of success. *Entrepreneurship and Sustainability Issues,* 6(4), 2081-2094. http://doi.org/10.9770/jesi.2019.6.4(37)

Korauš, A., Gombár, M., Kelemen, P., Polák, J. **(**2019). Analysis of respondents' opinions and attitudes toward the security of payment systems. *Entrepreneurship and Sustainability Issues,* 6(4), 1987-2002. http://doi.org/10.9770/jesi.2019.6.4(31)

Kumar, D., & Panchanatham, Dr.N. (2015). A case study on Cyber Security in E-Governance. *International Research Journal of Engineering and Technology, 2*(8), 272-275.

Kumar, S., & Somani, V. (2018). Social Media Security Risks, Cyber Threats and Risks Prevention and Mitigation Techniques. *International Journal of Advance Research in Computer Science and Management, 4*(4), 125-129.

Law of Ukraine on the basic principles of ensuring cyber security of Ukraine (2017). *As amended up to Act of July 08, 2018*. URL: https://zakon.rada.gov.ua/laws/show/2163-19

Lialina, A. (2019). Labor market security in the light of external labor migration: new theoretical findings, *Entrepreneurship and Sustainability Issues* 6(3): 1105-1125. http://doi.org/10.9770/jesi.2019.6.3(11)

Markopouloua, D., Papakonstantinoua, V., & Hert, P. (2019). The new EU cybersecurity framework: The NIS Directive, ENISA's role and the General Data Protection Regulation. *Computer Law & Security Review, 4*(35). https://doi.org/10.1016/j.clsr.2019.06.007

National cyber security strategy 2016-2021 (2016). URL: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/567242/national_cyber_security_strategy_2016.pdf

National cyber strategy of the United States of America (2018). URL: https://www.whitehouse.gov/wp-content/uploads/2018/09/National-Cyber-Strategy.pdf

Panteleeva, N.N., Romanovska, L., & Romanovska, M. (2019). Cyber threats in the digital economy. *Finansovyi prostir, 1*(33), 130-139. https://doi.org/10.18371/fp.1(33).2019.177107

Privacy and Civil Liberties Final Guidelines: Cybersecurity Information Sharing Act (2015). *As amended up to Act of June 15, 2018*. URL: https://www.us-cert.gov/sites/default/files/ais_files/Privacy_and_Civil_Liberties_Guidelines.pdf

Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act). URL: https://eur-lex.europa.eu/eli/reg/2019/881/oj

Regulations on the National Cybersecurity Coordination Center (2016). *As amended up to Act of June 20, 2019*. URL: https://zakon.rada.gov.ua/laws/show/242/2016

Rus, I. (2017). Study of cybersecurity issues. *Studia universitatis petru maior series oeconomica, 1*, 1-16.

Samuel, K.O., & Osman, W.R. (2014). Cyber Terrorism Attack of the Contemporary Information Technology Age: Issues, Consequences and Panacea. *International Journal of Computer Science and Mobile Computing, 3*(5), 1082-1090.

Sitdikova, L.B., Starodumova, S.J. (2019). Corporate agreement as a means of providing security in the course of entrepreneurship development. *Entrepreneurship and Sustainability Issues,* 7(1), 324-335. http://doi.org/10.9770/jesi.2019.7.1(24)

The Cyber-Attacks (Asset-Freezing) Regulations (2019). URL: https://www.legislation.gov.uk/uksi/2019/956/contents/made

The French CCIP framework. *The official website of ANSSI*. URL: https://www.ssi.gouv.fr/en/cybersecurity-in-france/ciip-in-france/#anchor0

The French national digital security strategy (2015). *The official website of ANSSI*. URL: https://www.ssi.gouv.fr/uploads/2015/10/strategie_nationale_securite_numerique_en.pdf

The official website of Agence nationale de la sécurité des systèmes d'information (ANSSI). URL: https://www.ssi.gouv.fr/

The official website of Cybersecurity and Infrastructure Security Agency (CISA). Retrieved from https://www.cisa.gov/about-cisa

The official website of Government Communications Headquarters (GCHQ). URL: https://www.gchq.gov.uk

The official website of National Cyber Security Centre (NCSC). URL: https://www.ncsc.gov.uk

The official website of NATO Communications and Information Agency (NCI Agency). URL: https://www.ncia.nato.int

The official website of North Atlantic Treaty Organization (NATO). URL: https://www.nato.int

Tvaronavičienė M. (2018a). Towards internationally tuned approach towards critical infrastructure protection. *Journal of Security and Sustainability Issues,* 8(2), 143-150. https://doi.org/10.9770/jssi.2018.8.2(2)

Tvaronavičienė, M. (2018b). Toward efficient policy making: forecasts of vulnerability to external global threats. *Journal of Security and Sustainability Issues*, 7(3), 591-600. https://doi.org/10.9770/jssi.2018.7.3(18)

Vlasov, A.I., Shakhnov, V.A., Filin, S.S., Krivoshein, A.I. (2019). Sustainable energy systems in the digital economy: concept of smart machines. *Entrepreneurship and Sustainability Issues,* 6(4), 1975-1986. http://doi.org/10.9770/jesi.2019.6.4(30)

Weiss, J., Perkins, E., & Walls, A. (2013). Definition: Cybersecurity. *Gartner*. URL: https://www.gartner.com/en/documents/2510116/definition-cybersecurity

What is the US NATO TEMPEST. URL: https://www.interelectronix.com/en/tempest.html

Vigliarolo, F. 2020. Economic phenomenology: fundamentals, principles and definition. *Insights into Regional Development*, 2(1), 418-429. http://doi.org/10.9770/IRD.2020.2.1(2)

Chehabeddine, M., Tvaronavičienė, M. (2020.) Securing regional development. *Insights into Regional Development*, 2(1), 430-442. http://doi.org/10.9770/IRD.2020.2.1(3)

Petrenko, Y., Vechkinzova, E., Antonov, V. (2019). Transition from the industrial clusters to the smart specialization of the regions in Kazakhstan. *Insights into Regional Development,* 1(2), 118-128. https://doi.org/10.9770/ird.2019.1.2(3)

Short biographical note about the contributors at the end of the article:

Iryna SHOPINA, Doctor of Science of Law, Professor, Lviv State University of Internal Affairs
ORCID ID: orcid.org/0000-0003-3334-7548

Dmytro KHOMIAKOV, Candidate of Juridical Sciences, Military Institute of Taras Shevchenko National University of Kyiv
ORCID ID: orcid.org/0000-0002-1246-0266

Nadiia KHRYSTYNCHENKO, Doctor of Science of Law, Professor, Ternopil National Economic University
ORCID ID: orcid.org/0000-0001-7473-7193

Serhii ZHUKOV, Doctor of Science of Law, Assotiate Professor, Military Institute of Taras Shevchenko National University of Kyiv
ORCID ID: orcid.org/0000-0001-6511-2482

Dmytro SHPENOV, Doctor of Science of Law, Verkhovna Rada of Ukraine
ORCID ID: orcid.org/0000-0003-2661-0245