https://doi.org/10.15407/scine17.03.003

YERINA, A. M. (https://orcid.org/0000-0002-3765-4441),
HONCHAR, I. A. (https://orcid.org/0000-0002-3167-1240),
and ZAIETS, S. V. (https://orcid.org/0000-0002-6133-1087)
Taras Shevchenko National University of Kyiv,
90 A, Vasylkivska St., Kyiv, 03022, Ukraine,
+380 44 521 3505, kaf_stat@ukr.net

STATISTICAL INDICATORS OF CYBERSECURITY DEVELOPMENT IN THE CONTEXT OF DIGITAL TRANSFORMATION OF ECONOMY AND SOCIETY

Introduction. *The scale and destructive consequences of the unlawful impact on cyberspace is a key problem of modern geopolitics, and cyber reliability is recognized as one of the most important security priorities by the subjects of international relations.*

Problem Statement. *Monitoring of cyber incidents and anomalies in information and communication systems and prompt response to risks determined by cyber threats require the development of a system of indicators and criteria for cybersecurity assessment.*

Purpose. *Summarize the international experience of assessing the cybersecurity, to position countries by their level of development in the global space, to identify strengths and weaknesses in cybersecurity management, and to ensure effective protection of cyberspace at the national level.*

Materials and Methods. *Used the component indices of the international rankings characterizing the potential of the digital economy (ICT IDI, NRI, EGDI) and the participation of countries in the field of cybersecurity (GCI and NCSI).*

Results. *It has been argued that cybersecurity ratings play the role of a kind of identifier of the relative advantages and vulnerabilities of the national cyber strategies, and indicate the need for their review in order to strengthen protection against cyber-attacks and improve the cyber risk management system.*

In countries with a high level of economic development, which is largely based on the contribution of IT technologies to the national production, the cybersecurity potential is significantly higher, regardless of geolocation. The discovered correlation between GCI, information society development indices (IDI, NRI, EGDI) and GDP per capita confirms that the digital transformation of the economy and society acts as a key driver of economic development if the information- and cyber-security are assured only. The best practices are highlighted, and critically weak segments of the national cybersecurity are identified.

Conclusions. *Using the NCSI indicators, the preparedness of Georgia and Ukraine to prevent the implementation of fundamental cyber threats and to manage cyber incidents and large-scale cyber crises is assessed.*

Keywords: cybersecurity, cyber threats, cybercrime, global cybersecurity index, national cybersecurity index, and security management.

Citation: Yerina, A. M., Honchar, I. A., and Zaiets, S. V. Statistical Indicators of Cybersecurity Development in the Context of Digital Transformation of Economy and Society. *Sci. innov.* 2021. V. 17, no. 3. P. 3—13. https://doi.org/10.15407/scine17.03.003

Information and communication technologies (ICT), having become an integral component of the modern world, contribute to the emergence and intensive dissemination of fundamentally new models of communication, social integration, lifestyle, education, etc. However, the technological advances in informatization of society have created not only progressive opportunities, but also new challenges and threats in the field of cyber security: (i) unauthorized access to information and telecommunication systems and networks; (ii) targeted cyber-attacks on infrastructure facilities that ensure the life of society; (iii) breach of confidentiality of information stored, transmitted and processed in the information and telecommunication systems (state, commercial, banking secrets, personal data, intellectual property objects). The illegal actions of subjects of informational legal relations that create a danger to the vital interests of a person, society and the state as a whole, are defined by the term "cyber threats" [1, 2]. The sources or initiators of cyber threats can be international criminal groups of hackers, certain specialized groups trained in the field of information technology that operate in the interests of foreign states, terrorist and extremist groups, transnational corporations and financial and industrial groups.

The current global landscape of cyber threats is rather complicated, as evidenced by Cisco and Cybersecurity Ventures' researches [3]. Cyberthreats have various forms, scales and are constantly evolving. From the point of view of legal regulation of the problems of protecting the cyberspace, the whole range of illegal cybernetic influences can conditionally be combined into the following blocks: "classic" crimes; crimes specific to geopolitical struggle and cyber-attacks as components of military operations [4].

"Classic" cybercrimes are types of fraudulent activities aimed at unlawful access to confidential user information and automated databases: *fishing*, carding, hacking, malware and piracy. The object of cybercrime is personal data, bank accounts, logins and passwords, other personal information of both individuals and business and the public sector. A type of cybercrime is content cyberthreats (child pornography, Internet violence, drug trafficking, the dissemination of information of extremist content, etc.).

Cyber espionage. This is a criminal activity aimed at unauthorized access to information containing the state secrets in the field of defense, science and technology, economics, finance, foreign relations. Cyber espionage is most often an element of special information operations of special services of foreign states and an instrument of influence on the geopolitical environment.

Cyber diversions and cyber terrorism are politically motivated hacker attacks on critical infrastructure or any technological processes through a computer network, in particular, the Internet. Cyber diversions are mainly aimed at the destruction of industrial equipment, automated control systems, and military infrastructure facilities.

During unlawful interference in the work of information and telecommunication systems and networks, several interrelated threats can be realized at the same time, and radically different subjects of information legal relations, say, hacker groups and private IT companies controlled by special services, can be involved in their implementation. This indicates a rather complex nature of modern cyber incidents. In the political confrontation of countries, in order to achieve certain military and political goals, cyberspace is used as an arena of military operations — cyber warfare [5].

The steady increase in the number and power of cyber-attacks, motivated by the interests of individual states, groups and individuals, is one of the modern global trends [3; 6]. From year to year, cybercrimes are becoming more organized, technically advanced and psychologically elegant, and the consequences of using cyberspace for illegal purposes are becoming ever more widespread and destructive. According to the *Allianz* Risk Barometer yearbook, global losses from cybercrimes reach USD 600 billion per year, which is almost three times the average annual loss from natural disasters [7].

Large-scale targeted cyber-attacks and the associated risks to the national security have become a key problem of modern geopolitics, and the protection of the cyber environment is increasingly seen by the subjects of international relations as one of the most important security priorities. Under these circumstances, the development of effective nationwide cybersecurity systems that can timely identify real and potential threats, adequately respond to them and eliminate the consequences with minimal losses is of utmost importance.

Nowadays, almost all the leading countries experience cyber-attacks and form and constantly modernize the national cyber security systems to protect the national cyberspace. However, given the high technical capabilities of cybercriminals, the latent and transnational nature of cyber-attacks, no country is able to fight them on its own. Expert claims are true that cybersecurity should therefore become a collective responsibility [8]. It is possible to prevent and counteract all sorts of crimes with the use of information and communication technologies, subject to coordinated international cooperation in the field of cybersecurity. At the same time, it is important to combine the efforts and experience of various countries in the fight against cybercrime both at the state level and at the level of the commercial, public and private sectors. The creation of such a holistic international system of cooperation allows for the rapid exchange of the necessary information and to consolidate the efforts of countries to prevent the latest cyber threats.

1. INTERNATIONAL CYBERSECURITY RESEARCH EXPERIENCE

The Global Cybersecurity Agenda (GCA ITU) has become the basis for international cooperation and coordination of countries' confidence-building and security activities in the information society. According to GCA requirements, every ITU partner country must have a Computer Emergency Response Team (CERT), which is responsible for protecting state information resources and information and telecommunication systems from unauthorized access and misuse, as well as breaches of their privacy, integrity and accessibility.

At the global level, cybersecurity is the subject of consideration by the UN General Assembly, as well as a number of international organizations: G7 Group, Council of Europe, the European Union (EU), North Atlantic Treaty Organization (NATO), Organizations for Economic Cooperation and Development (OECD), Asia-Pacific Economic Cooperation (APEC), World Economic Forum (WEF), etc. They work in the following areas: creating a single database on cyberthreats and a system for the constant exchange of information, improvement of technical standards and rules, attention is paid to security issues on the Internet.

A single cybersecurity certification for IT products, services and processes is being introduced in the EU, which will undoubtedly enhance the security of online services and consumer devices and will facilitate the smooth functioning of the Digital Single Market. A key role in cybersecurity certification rests with the European Network and Information Security Agency (ENISA) [9].

NATO plays an important role in developing a unified approach to cybersecurity as a component of the national security. Within the organization, there are several specialized units that focus on the development of strategies and mechanisms for cyber-threat detection and counteraction to cyber-attacks, as well as offering a wide range of educational, training and training opportunities. The EU-NATO interaction is the cornerstone of Euro-Atlantic cybersecurity in the military field, and cyber defense is one of NATO's priorities [10; 11]. The role of NATO in providing cybersecurity not only to Allies but also to Partner countries is increasing.

Cybersecurity is not just a set of strategies and principles for protecting cyberspace from threats. It is an ongoing process, the active component of which is monitoring incidents and anomalies in network systems and responding promptly to the risks caused by cyber threats. The balanced use of

forces and means of ensuring cybersecurity requires appropriate methodological tools, first of all, the formation of a system of indicators and criteria for assessing the development of cybersecurity at the global and local levels.

At present, the main developers of theoretical and methodological foundations and applied aspects of statistical assessment of cybersecurity are mainly information and analytical teams of experts in international organizations specializing in information- and cyber-security: International Telecommunication Union (ITU), Centre for European Policy Studies (CEPS), e-Governance Academy (eGA) of Estonia, Potomac Institute for Policy Studies, EY Global Information Security Survey (GISS), world leaders in the field of network technologies and the cybersecurity industry Cisco Security and Cybersecurity Ventures, etc. Analytical reviews and reports from these organizations have been published by, among others, Kerry Nelson, Lorenzo Pupillo, Raul Rikk, Melissa Hathaway, Paul van Kessel, Andra Zaharia, Steve Morgan, Martin Lee and others. Among domestic scientists, V. Buryachok, A. Voytsikhovkyy, I. Voronenko, Yu. Danyk, I. Diorditsa, D. Dubov, V. Lipkan, R. Lukianchuk, G. Piskorska, V. Petrov and others devoted their scientific works to the issue of cybersecurity.

2. METHODOLOGY FOR ASSESSING THE CYBERSECURITY AS A COMPLEX MULTIDIMENSIONAL PHENOMENON

The purpose of this research is to summarize the international experience of assessing the cybersecurity, to position countries by their level of development in the global space, to identify strengths and weaknesses in cybersecurity management, and to ensure effective protection of cyberspace at the national level.

The subject of research is the current state of the global cybersecurity and specifics of cybersecurity in the NATO Member States and Aspirant countries Ukraine and Georgia.

In accordance with the ISO/IEC 27032 — SIS international standard, cybersecurity integrates network security, security of critical information infrastructure and Internet security [12]. Like any complex phenomenon, cybersecurity cannot be directly measured as it turns out to be a certain set of various signs and symptoms. Therefore, it is possible to measure/evaluate such phenomena only indirectly by aggregating the sets of these signs into one integral assessment. It is the integrated estimates (composite indices), formed on the basis of a unique data set, that are the basis for positioning countries in the world coordinate system.

The study uses international rating systems that characterize the level of the digital economy development and the country's involvement in cybersecurity: ICT Development index (IDI), Networked Readiness Index (NRI) [13[, the UN Global E-Government Development Index (EGDI), Global Cybersecurity Index (GCI), National Cyber Security Index (NCSI). Each rating, in addition to the function of a comparative analysis of the potential of individual countries in the field of digital transformations or cybersecurity, serves as a kind of identifier of the relative advantages and vulnerabilities of national cyber strategies, indicates the need for their review in order to strengthen protection against cyber-attacks and improve the cyber crisis management system.

3. INDICATORS OF DIGITAL ECONOMY DEVELOPMENT

The ICT Development Index is used to measure the level of development and to monitor changes in information and communication technologies. Its calculation is based on 11 indicators, which are combined into three sub-indices: access to ICT, ICT usage intensity and ICT level of practical skills [14].

The Network Readiness Index NRI measures the propensity of countries to leverage ICT capabilities. The index aggregates 53 indicators combined into four basic sub-indices. Three of them characterize the role of government, business and society in shaping the prerequisites for the development of ICT, and the fourth one describes the socio-economic effects of using the ICT: availabi-

lity of conditions for the development of ICT (regulatory, business and innovation environment); readiness of citizens, business and government to use ICT (infrastructure and digital content, accessibility of ICTs, population skills); the level of use of ICT at public, business and private levels; the impact of ICT on the economy and society [15]. The NRI is considered to be the most comprehensive source for assessing the quality of the internal environment of ICT development and the ability of society and its institutions to make effective use of existing and new knowledge. The index identifies drivers and barriers to network readiness and widespread adoption of ICT in the country. This assumes the equal role and responsibility of all the "players" of the society: government, business, and citizens.

The rapid spread of the Internet and the global network has become the basis for the transformation of public administration in the direction of its adaptation to the requirements of the information society. The level of willingness and ability of the national government agencies to provide online government services using the ICT is indicated by the rating of countries based on the Electronic Government Development Index (EGDI). The index aggregates 13 indicators, which, from the point of view of international experts, embody the country's ability to participate in the information society [16]. These indicators are combined into three sub-indices: the Online Service Index (OSI), the Telecommunication Infrastructure Index (TII), and the Human Capital Index (HCI).

4. CYBERSECURITY INDICATORS

4.1. Global Cybersecurity Index (GCI)

The monitoring of the status of the global network space of the UN member countries is carried out by ITU. To assess the countries' involvement in cybersecurity, ITU experts annually determine the Global Cybersecurity Index (GCI), which relies on the country's legal, technical, managerial institutions, their educational and research capabilities, the availability of cooperation mechanisms and information exchange systems in networks. Accordingly, the level of development of cybersecurity at the national level is analyzed by five pillars: legislative framework, technical implementation, organizational measures, capacity building, national and international cooperation. Each pillar is represented by a certain number of indicators based on binary answer options that confirm the presence or absence of certain, predefined solutions for cybersecurity (24 indicators in total). The structure of the GCI by pillars is illustrated in Fig. 1, the number of indicators is indicated in parentheses.

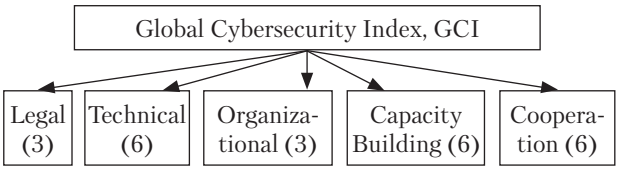

Fig. 1. The pillars of the Global Cybersecurity Index

According to GCI data, in 2018, 9 out of 10 countries had cybersecurity legislation: the vast majority of countries had a national cybersecurity strategy (58%) and an active national CERT (56%) that helped detect attacks on government computer systems and databases, as well as critical infrastructure facilities [17].

The purpose of the GCI is to enable the UN member states to identify potential ways to strengthen the protection of the global network space against cyber threats. The results of the 2018 global cybersecurity survey at a planetary level indicate a significant digital divide between countries in the context of awareness of cyber threats and their ability to prevent them. Based on the GCI, countries are divided into three classes by their level of commitment: the high class has the highest level of global cybersecurity commitments ($GCI \geq 0.670$); the medium one has developed complex commitments and is involved in cybersecurity programs and initiatives ($0.340 \leq \leq GCI \leq 0.669$); and the low one has initiated a cybersecurity commitment ($GCI \leq 0.339$). 53 countries are assigned to the high class, 54 ones to the medium class, and 87 ones to the low class. The shares of these classes by the world regions are

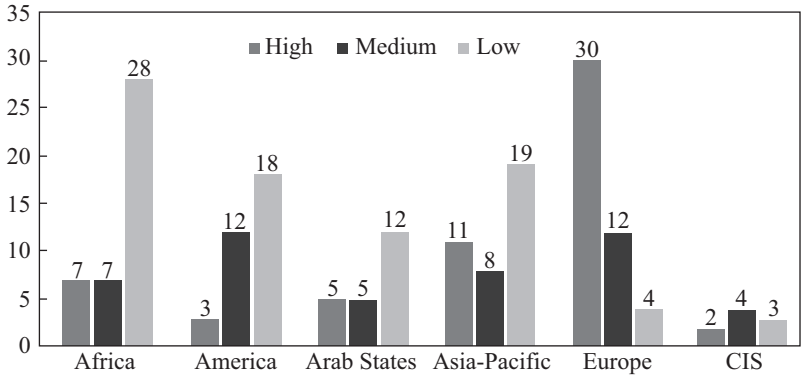

Fig. 2. Regional groupings of countries of the world by GCI in 2018, place
Source: created by the authors on the basis of [17].

shown in Fig. 2. The largest number of countries with a high cybersecurity development is concentrated in Europe (30): 20 countries are NATO members; their GCI ranges from 0.931 (the United Kingdom) to 0.527 (Greece). Georgia takes the 18th place (GCI = 0.857, high class), and Ukraine is ranked 54th (GCI = 0.661, medium class).

Most often, cyberattacks are experienced by countries with high levels of economic development, which are largely based on the contribution of IT technologies to national production (mainly OECD member countries, which account for more than two-thirds of global GDP). In terms of the volume and scale of IT technology, the level of cybersecurity in all highly developed countries, regardless of geolocation, is much higher. Table 1 shows the ratings for all five pillars of cybersecurity among the leading countries of the world's regions: the United Kingdom, in Europe; the USA, in the American continent; Singapore, in the Asia-Pacific region; Saudi Arabia, in the Middle East; Mauritius, in Africa; and Russia, in the Central Eurasia.

Almost all of the leading countries have reached peak values (0.200) in the Legal, Technical and Organization areas. Much lower values in the Cooperation area (interagency and international cooperation, public-private partnership). In Russia, the GCI values are the lowest in all cybersecurity areas compared to other regional leaders.

The sample of NATO member countries in terms of cybersecurity development should be recognized as statistically homogeneous, which with probability of 0.95 confirms the Grubbs' test ($G = 2.26 < G1-0.05 = 2.73$). In this sample, one can also trace the relationship between the Global Cybersecurity Index (GCI), the information society development indexes (IDI, NRI, EGDI) and the indicator of economic development of countries (GDP per capita). All coefficients of the cor-

Table 1. **Global Cybersecurity Index (GCI) of the Regional Leaders in Terms of the GCI Pillars in 2018**

Index pillars	United Kingdom	USA	Singapore	Saudi Arabia	Mauritius	Russia
Legal	0.200	0.200	0.200	0.187	0.182	0.197
Technical	0.191	0.184	0.186	0.179	0.168	0.162
Organizational	0.200	0.200	0.192	0.158	0.200	0.177
Capacity building	0.189	0.191	0.195	0.198	0.186	0.166
Cooperation	0.151	0.151	0.125	0.160	0.144	0.135
Global Index	**0.931**	**0.926**	**0.898**	**0.881**	**0.880**	**0.836**

Source: created by the authors on the basis of [17].

relation matrix (Table 2) are significant with a probability of 0.95: that is, the digital transformation of the economy and society depends on the economic development of the country and, in turn, plays the role of a key driver of economic development only if information- and cyber security are ensured.

Thus, GCI is a unique and easy-to-use tool for assessing the countries' preparedness for a particular type of cyber threats, forcing them to identify areas where cybersecurity can be strengthened and protect the economic interests of the country: by improving legislation, standards, market leverage or other initiatives.

4.2. National Cyber Security Index (NCSI)

The preparedness of countries to prevent the realization of fundamental cyber threats, manage cyber incidents and large-scale cyber crises is measured by the National Cyber Security Index (NCSI). Considering the principles of cybersecurity developed by the European Union, this index includes the most important aspects of network and information security, electronic identification, trust services, protection of personal data and many other aspects [18]. By statistical nature, the NCSI is a relative value that, as a percentage, indicates the degree to which a country meets cybersecurity criteria.

Table 2. **Relationship of the Global Cybersecurity Index (GCI) with the Information Society Development Indices (IDI, NRI, EGDI) and the Level of Economic Development (GDP per capita) of NATO Members**

Variable	Correlation matrix Number of observations N = 28 (Casewise deletion of missing data)				
	GCI	IDI	NRI	EGDI	GDP per capita
GCI	1.000	0.583	0.691	0.598	0.564
IDI	0.583	1.000	0.878	0.814	0.847
NRI	0.691	0.878	1.000	0.815	0.877
EGDI	0.598	0.814	0.815	1.000	0.787
GDP per capita	0.564	0.847	0.877	0.787	1.000

Source: created by the authors on the basis of [17].

In recent years, **Estonia** has become one of the world centers in the field of protecting the national information cyberspace and preparedness to confront online threats (the NATO Cyber Defense Center operates in the capital of Estonia). In 2019, Estonia met 91% of the cybersecurity criteria and was in the TOP-3 of the NCSI rating [18]. Fig. 3 shows the positions of Estonia, Georgia, and Ukraine in the NCSI's international digital development and national cybersecurity rankings. In Georgia, the share of fulfilled criteria is 65%, in Ukraine, it accounts for 64%. At the same time, in each of these countries, the development of the national cybersecurity and information and communication technologies is approximately at the same level, that is, the development of cybersecurity to a certain extent corresponds to the digital development of society.

The NCSI structure includes 3 components, 12 segments and 46 indicators. When drawing up the scale, the NCSI project analysts considered the existence of a national strategy in the field of ensuring measures to protect systems, networks and applications from digital attacks, their practical implementation, as well as legal responsibility. The value of each indicator depends on its weight in the structure of the index: for the presence of a legal act that regulates a particular area, experts score one point; 2—3 points for specialized unit; 2 points for official format of cooperation; 1—3 points for result/product. The total number of points for a certain segment ranges from 5 to 9 points, the maximum possible score (points) for all segments is 77. The NCSI index is determined by comparing the amount of points scored by the j-th country with the maximum possible score (points):

$$NCSI = \frac{Country\ Points \times 100}{Maximum\ Points}. \qquad (1)$$

In Estonia in 2019, the total number of points scored was 70, hence NCSI = 70 : 77 = 0.9091.

Similarly, the level of fulfillment of cybersecurity criteria for any NCSI segment is evaluated by comparing the score provided by experts with

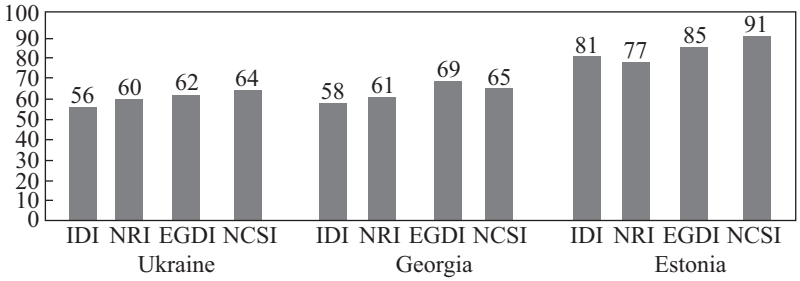

Fig. 3. The level of development of information and communication technologies and cybersecurity (NCSI version) in Estonia, Georgia, and Ukraine in 2019, point

Source: created by the authors on the basis of [18].

the maximum possible one. The shares of the criteria met by the national cybersecurity segments of Ukraine, Georgia, and Estonia are presented in Table 3. Their values give grounds to identify the strengths and weaknesses of national cyberstrategies, in particular, regarding the country's ability to manage cyber incidents and large-scale cyber crisis.

When analyzing the development of national cybersecurity, NCSI values are also compared with the Digital Development Level indicator (DDL). The latter is calculated as the arithmetic average percentage the country received from the maximum value of the ICT Development Index (IDI) and the Networked Readiness Index (NRI):

$$\text{DDL} = \frac{\text{IDI\%} + \text{NRI\%}}{2}. \qquad (2)$$

The difference (NCSI — DDL) indicates the coherence (inconsistency) of the development of the national cybersecurity and digital technology. A positive result shows that the development of cybersecurity in the country is in line with digital development or is ahead of it; a negative one gives grounds to conclude that the digital society in the country is more developed than the scope of national cybersecurity.

In Ukraine, IDI = 56%, NRI = 60%, hence DDL = = 0.5 (56 + 60) = 58%, so NCSI > DDL. In Estonia and Georgia, the development of national cybersecurity is also in line with the digital development of the information society.

The analysis of compliance with the criteria of individual segments of the national cybersecurity of Ukraine and Georgia gives grounds to draw the following conclusions.

Ukraine. In Ukraine, the positive segments of the cybersecurity sphere include: development of a cybersecurity concept; education and professional development in the field of cybersecurity; protection of personal data and the fight against cybercrime. In these segments, Ukraine received 80—100% of the maximum level. Less developed segments of cybersecurity are: protection of basic e-services; electronic identification and trust services; reaction to computer incidents. The most problematic cybersecurity segments in Ukraine should be recognized as an analysis of cyber threats, international cooperation in the field of cybersecurity; protection of digital services; ability to manage large-scale cyber crisis and military cyber operations.

Georgia. In Georgia, the level of cybersecurity is slightly higher. Georgia received maximum NCSI ratings (100%) in five segments of cybersecurity: developing a cybersecurity policy and analysis of cyber threats; protection of basic e-services; protection of personal data and the fight against cybercrime. The following cybersecurity segments require attention: the ability to manage cyber incidents and large-scale cyber crisis, especially education and professional development in the field of cybersecurity; protection of digital services and military cyber operations.

Thus, the cyberspace of both NATO aspirant countries remains a weak component of the national security and retains a high degree of vulnerability to cyber threats. Cyber security issues common to Ukraine and Georgia are the low level of development of the segment of the national defense operations (military cyber operations). Another equally important issue is the protection of digital services and the unpreparedness to respond to cyber incidents. The mechanism of public-private partnership in the field of cybersecurity with the owners and operators of private critical infrastructure facilities also requires adjustment.

International cooperation significantly enhances the ability of these countries to counteract all kinds of cyber influences. For example, the CERT-UA team works with other CERT teams in the Member States, as well as with the Cisco Talos Intelligence Team, to address the impact of cyberattacks on critical information infrastructure and identify the causes and circumstances of cyber incidents. Within the framework of Ukraine-NATO cooperation, the Cybersecurity Trust Fund has been set up to strengthen cyber potential, assist Ukraine in developing the defense capabilities for responding to cybersecurity incidents and eliminating their consequences [19]. Such cooperation will help to ensure that countries are prepared to prevent the realization of fundamental cyber threats and manage cyber incidents and large-scale cyber crises.

A necessary condition for the successful digital transformation of the economy and society is counteracting cyber threats and the fight against cybercrime. Among the main obstacles to the promotion of the basic principles of cyber defense, information security experts point out: lack of

Table 3. **Indicators of Cybersecurity Development in Some Countries as of 2019**

Segment #	NCSI components & segments	Max score	Ukraine, version as of Jul 14, 2018	Georgia, version as of Nov 21, 2017	Estonia, version as of Feb 18, 2019
	GENERAL CYBER SECURITY INDICATORS				
1	Cyber security policy development	7	100	100	57
2	Cyber threat analysis and information	5	20	100	80
3	Education and professional development	9	89	22	67
4	Contribution to global cyber security	6	33	50	50
	BASELINE CYBER SECURITY INDICATORS				
5	Protection of digital services	5	20	0	20
6	Protection of essential services	6	83	100	17
7	E-identification and trust services	9	78	78	67
8	Protection of personal data	4	100	100	100
	INCIDENT AND CRISIS MANAGEMENT INDICATORS				
9	Cyber incidents response	6	67	50	67
10	Cyber crisis management	5	0	60	60
11	Fight against cybercrime	9	100	100	100
12	Military cyber operations	6	17	17	83
Score (points) obtained		77	49	50	70
NCSI, %		x	63.6	64.9	90.9
DDL		x	58.1	59.6	79.3
Difference		x	5.5	5.3	11.6

Source: created by the authors on the basis of [18].

resources, incompatibility of information security systems, and a shortage of qualified cybersecurity specialists. Nowadays, the staffing challenge for the cybersecurity industry has become global and is showing a tendency to deepen.

International cybersecurity ratings (GCI and NCSI) are useful to make sound decisions about addressing and preventing potential cybersecurity challenges and choose the path to a more secure and sustainable economy in an unstable, cybernetic, and conflict-prone world.

The highest levels of digital transformation and cybersecurity are observed in NATO member countries. Ensuring cybersecurity in the context of global threats, along with the joint efforts of the international community, dictates the importance of monitoring at the national level. Ukraine and Georgia, like all countries in the world, are constantly threatened by cyber-attacks and occasionally face cybersecurity challenges. The main threats to the national cybersecurity of these countries should be considered in the context of Russian information and cyber aggression, in particular, cyber-attacks on vital infrastructure. Therefore, the issue of improving the cyberspace military security systems, which would meet EU and NATO membership criteria and guarantee reliable protection of the states from cybercrime, remains urgent for both NATO aspirant countries.

REFERENCES

1. Diorditsa, I. (2017). The concept and content of cyber threats at the present stage. *Entrepreneurship, Economy and Law*, 4, 99—107 [in Ukrainian].
2. Dubov, D. (2010). Approaches to the formation of thesaurus in cybersecurity. *Political Management: Science Journal*, 5, 19—30 [in Ukrainian].
3. 2019 Cybersecurity Almanac: 100 Facts, Figures, Predictions and Statistics. URL: https://cybersecurityventures.com/cybersecurity-almanac-2019 (Last accessed: 26.12.2019).
4. Dubov, D. (2014). *Cyberspace as a new dimension of geopolitical rivalry*. Kyiv: National Institute for Strategic Studies.
5. Danyk, Yu., Vorobiienko, P., Cherneha, V. (2018). *The basics of cyber security and cyber defense*. Odessa: Odessa National Academy of Telecommunications A.S. Popov.
6. Global cybercrime-2019: development trends. URL: http://cyberfort.com.ua/analytics/globalnaja_kiberprestupnost-2019_tendentsii_razvitija.html (Last accessed: 26.12.2019).
7. Allianz Risk Barometer Top Business Risks For 2019. URL: https://www.agcs.allianz.com/content/dam/onemarketing/agcs/agcs/reports/Allianz-Risk-Barometer-2019.pdf (Last accessed: 26.12.2019).
8. Pupillo, Lorenzo (2018). EU Cybersecurity and the Paradox of Progress. *CEPS Policy Insight*, № 2018/06, February 2018. URL: https://ssrn.com/abstract=3131559 (Last accessed: 26.12.2019).
9. Cyber Security in the Deployment of the Fourth Industrial Revolution (Industry 4.0): Challenges and Opportunities for Ukraine. URL: https://niss.gov.ua/en/node/135 (Last accessed: 26.12.2019).
10. Voytsikhovkyy, A. (2018). Cybersecurity as an Important Component of the National Security System of European Countries. *The Journal of Eastern European Law*, 53, 26—37 [in Ukrainian].
11. Cyber defence / NATO-Cyber security. URL: https://www.nato.int/cps/en/natohq/topics_78170.htm (Last accessed: 26.12.2019).
12. ISO/IEC 27032. (2012). Information technology — Security techniques — Guidelines for cybersecurity. URL: https://www.sis.se/api/document/preview/915118/ (Last accessed: 26.12.2019).
13. Cyber Readiness Index 2.0. A plan for cyber readiness: a baseline and an Index. URL: https://www.belfercenter.org/sites/default/files/files/publication/cyber-readiness-index-2.0-web-2016.pdf (Last accessed: 26.12.2019).
14. The ICT Development Index (IDI): conceptual framework and methodology. URL: https://www.itu.int/en/ITU-D/Statistics/Pages/publications/mis/methodology.aspx (Last accessed: 26.12.2019).
15. Networked Readiness Index. URL: https://reports.weforum.org/global-information-technology-report-2016/networked-readiness-index (Last accessed: 26.12.2019).
16. UN E-Government Knowledgebase. URL: https://publicadministration.un.org/egovkb/en-us/Reports/UN-E-Government-Survey-2018 (Last accessed 2019.12.26).
17. Global Cybersecurity Index 2018. URL: https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2018-PDF-E.pdf (Last accessed: 26.12.2019).

18. National Cyber Security Index 2018. URL: http://ncsi.ega.ee/ncsi-index (Last accessed: 26.12.2019).
19. Petrov, V. (2018). NATO-Ukraine Cooperation on Cybersecurity International Relations. *Political Science Series*, 18—19, URL: http://journals.iir.kiev.ua/index.php/pol_n/article/download/3384/3062 (Last accessed: 26.12.2019).

Received 19.02.2020
Revised 13.04.2020
Accepted 23.02.2021

А.М. Єріна (https://orcid.org/0000-0002-3765-4441),
І.А. Гончар (https://orcid.org/0000-0002-3167-1240),
С.В. Заєць (https://orcid.org/0000-0002-6133-1087)
Київський національний університет імені Тараса Шевченка,
вул. Васильківська, 90 а, Київ, 03022, Україна,
+380 44 521 3505, kaf_stat@ukr.net

СТАТИСТИЧНІ ІНДИКАТОРИ РОЗВИТКУ КІБЕРБЕЗПЕКИ В КОНТЕКСТІ ЦИФРОВОЇ ТРАНСФОРМАЦІЇ ЕКОНОМІКИ Й СУСПІЛЬСТВА

Вступ. Масштаби й руйнівні наслідки протиправного впливу на кіберпростір є ключовою проблемою сучасної геополітики, а кібернадійність визнається суб'єктами міжнародних відносин як один з найважливіших безпекових пріоритетів.

Проблематика. Моніторинг кіберінцидентів та аномалій в інформаційно-комунікаційних системах, оперативне реагування на детерміновані кіберзагрозами ризики потребують формування системи індикаторів і критеріїв оцінювання кібербезпеки.

Мета. Узагальнення міжнародного досвіду оцінювання стану кібербезпеки, позиціонування країн за рівнем її розвитку у глобальному просторі, визначення сильних і слабких ланок в управлінні кібербезпекою та забезпечення дієвого захисту кіберпростору на національному рівні.

Матеріали й методи. Використано компонентні індекси міжнародних рейтингів, які характеризують потенціал цифрової економіки (ICT IDI, NRI, EGDI) та участь країн у сфері кібербезпеки (GCI і NCSI).

Результати. Аргументовано, що рейтинги кібербезпеки виконують роль своєрідного ідентифікатора відносних переваг і вразливих позицій національних кіберстратегій, вказують на необхідність їх перегляду з метою посилення захисту від кібератак і вдосконалення системи управління кіберризиками.

В країнах з високим рівнем економічного розвитку, який значною мірою базується на внеску IT-технологій у національне виробництво, потенціал кібербезпеки значно вищий, незалежно від геолокації. Виявлена кореляція між GCI, індексами розвитку інформаційного суспільства (IDI, NRI, EGDI) та ВВП на душу населення підтверджує, що цифрова трансформація економіки та суспільства відіграє роль ключового драйвера економічного розвитку лише за умови забезпечення інформаційної та кібербезпеки. Висвітлено найкращі практики та зазначено критично слабі сегменти національної кібербезпеки.

Висновки. За індикаторами NCSI оцінено готовність Грузії та України запобігати сценаріям реалізації фундаментальних кіберзагроз, керувати кіберінцидентами та масштабними кіберкризами.

Ключові слова: кібербезпека, кіберзагроза, кіберзлочинність, глобальний індекс кібербезпеки, національний індекс кібербезпеки, управління безпекою.