TREND EXTRAPOLATION METHOD FOR QUALITATIVE PROGNOSIS OF THE GLOBAL CYBERSECURITY INDEX IN UKRAINE

Orest Polotai, Ph.D.,
Lviv State University of Life Safety, Ukraine, e-mail: orest.polotaj@gmail.com
Andrii Lagun, Ph.D., Ass.-Prof., e-mail: andrii.e.lahun@lpnu.ua;
Nataliia Kukharska, Ph.D., Ass.-Prof.,
Lviv Polytechnic National University, Ukraine;
Volodymyr Samotyy, Dr.Sc., Prof.,
The Cracow University of Technology, e-mail: vsamotyj@gmail.com

Abstract

In the paper, the research problem of cybersecurity in Ukraine and constituent elements of the cybersecurity global index were considered. The study object is the methods of predicting the indicator of the cybersecurity global index in Ukraine based on the trend extrapolation methods using one dynamic sequence. The purpose of the work is to apply predicting methods to build a prediction of the global cybersecurity index in Ukraine. The tasks of the job are to build a global cybersecurity index prediction based on average absolute gain, building a prediction of global cybersecurity index based on the average growth rate, building a prediction of global cybersecurity index based on flowing average, assessing the quality of prediction of each method and comparing them with each other to choose the best one.

There was selected an indicator to characterize the state of cybersecurity development in Ukraine - the Global Cybersecurity Index, and a feature of using the global cybersecurity indicator and all the components on which it is built and which form it was described. Also, different values for Ukraine's five-year global cybersecurity index were formed by using official reports generated by the International Telecommunications Union located in Switzerland. Based on data of 2014-2018 years global cybersecurity index projections in Ukraine for 2019 and 2020 years have been developed. The qualitative Global cybersecurity index predicting was considered using the database of simple trend extrapolation methods. This database includes the following methods: a trend extrapolation method based on the average absolute gain, a trend extrapolation method based on the average growth factor, a trend extrapolation method based on flowing average. Also, the method of ex-post predicating to qualitatively and quantitatively compare the results of each method and determine the best of them was implemented and obtained values and made a diagram of possible future events were compared.

The obtained results give reason to hope for improvement of the global cybersecurity index in Ukraine, which maintains the provided existing trends in the development of the cybersecurity sector in the country.

Keywords

Cybersecurity, Global Cybersecurity Index, Predicting, Trend, Extrapolation

1. Introduction

The nowadays realities testify to the importance of providing effective cybersecurity as the internet becomes an integral part of our lives, from online banking to smart systems. The cybersecurity system must work for the benefit of the public for both service providers and service users. It is up to the state to take responsibility for providing access to a stability secure digital space that can be used by all citizens. To do this, the state needs to navigate the complex and cross-cutting cybersecurity field and address the complex of strategic, legal, political, technical, and organizational issues, as well as participate in multi-sectoral international cooperation.

In recent years, Ukraine has suffered significant material losses through cyber-attacks [19]. At high cost, Ukraine has understood the inadmissibility of neglecting its cybersecurity issues, because, in addition to significant material losses through the loss or distortion of strategically important information, it may provoke technological disasters, damage to civilian, financial, and military infrastructure up to the loss of state sovereignty [20]. That is why guaranteeing cybersecurity is extremely important for Ukraine, and counteraction measures to the challenges and threats in this area must be comprehensive.

2. The Current State of the Problem

Recognizing the importance of combating cybercrime, most governments of different countries have developed appropriate policies and strategies for their governments to ensure cybersecurity [18]. One of these is the method of determining the Global Cybersecurity Index (GCI), which was used in 2014 for the first time. According to official information [1], there are currently three versions of the report that contain information on the GCI:

1) v1 – 2014/2015 years;
2) v2 – 2016/2017 years;
3) v3 – 2017/2018 years.

The range of CGI values changes from 0 to 1.

Since the fourth version of the 2019-2020 years GCI Report is currently planned, it would be advisable to experiment and calculate the qualitative prediction for this year in Ukraine using simple trend extrapolation methods:

– based on analytical values of dynamic sequence;
– based on flowing average.

Many scientists are studying the issue of cybersecurity research in Ukraine. In particular, O. Trofimenko [19, 20] has considered the need for compliance at an appropriate level of cybersecurity and has shown the losses if the issues are ignored. Besides, O. Trofimenko has considered [18] the relevant global legislation and national cybersecurity development strategies that can be taken as a basis at the local state level. In his work [7] I. Voronenko has examined the keys national security indicators are in terms of the constituent development of the economy in the context of digitalization. One of the key indicators in this study is the GCI indicator. Besides, according to the results of the analysis of modern research and publications, we can conclude that the problems of ensuring the cybersecurity of Ukraine in the contemporary conditions of development of information society, actual directions of increasing the efficiency of the providing cybersecurity system, its functions and tasks have considered in scientific works of such researchers as V. Lipkan [9, 10], I. Timkin, N. Novikov [17], I. Diorditsy [7], S. Melnik, V. Kashchuk [13] and others.
The issues of cybersecurity research of the state and the development of its main indicators from the economic point of view have been considered in the works of V. Martyniuk [12], V. Zalunin [8], V. Martynenko [11], S. Dziubik [14] and others [15].
However, despite the considerable number of works on this topic, the issues of constructing a global GCI prediction based on trend extrapolation methods have received insufficient attention.

3. The Goal of the Work

That is why the purpose of the article is to build a global GCI qualitative prediction based on the trend extrapolation methods that have the following objectives:

– forming a GCI prediction based on the average absolute gain;
– forming a GCI prediction based on the average growth factor;
– forming a GCI prediction based on flowing average;
– evaluation of the quality of each method prediction and comparing them with each other.

4. Cybersecurity Prognosis Methods

Data on cybersecurity measures for computer and telecommunication networks and the creation of conditions for the safe functioning of cyberspace evaluate and use to monitor and compare the cybersecurity status of different countries in the annual international rankings, the most authoritative of which are GCI and National Cybersecurity Index (NCSI).
In today's digital reality cybersecurity threats are evolving at an accelerated pace, cybercrime is becoming more sophisticated, better organized, and transnational. Adequate tools and resources must be available at the state level to intercept information about potential threats to the country.
Global Cybersecurity Index characterizes the ability to withstand cyberattacks and ensures the working of critical digital infrastructure works in the interests of a productive and secure economy. It calculates on the base of the integral estimate of the weighted sum by categories:

– regulatory and legal regulation of cyberspace;
– economic and social context;
– technological infrastructure;
– industrial application of information and communication infrastructure in different branches [3].

The Global Cybersecurity Index was presented to the public in 2014 and substantially modified in the 2015 and 2017 reports by the International Telecommunication Union, which is a specialized agency of the United Nations for information and communication technologies [4], is a multilateral initiative aimed at determining countries' readiness to cybersecurity in the following main five areas: legal, technical, organizational, capacity development, cooperation. The calculation of the indicators used to determine the global cybersecurity index is based on the map of the cybersecurity development tree and binary response options.
The Global Cybersecurity Index contains 25 indicators and 157 questions selected on the following criteria as compliance with the five key elements of the Global Cybersecurity Index and the achievement of key goals and conceptual frameworks of Global cybersecurity programs; availability and quality of data; the possibility of cross-checking with secondary data [2]. The calculation of the indicators used to determine the global cybersecurity index is based on the map of the cybersecurity development tree and binary response options. Each of the five columns is associated with a specific color. The more in-depth path indicates a more advanced level of commitment and the column becomes of more saturated color. The concept is based on the assumption that the more is advanced cybersecurity the there is complex the observed solutions. Therefore, if the farther the treemap contains a country, confirming the presence of pre-identified cybersecurity solutions, then the more complex is the cybersecurity commitment within that country and allowing it to score a more evaluation. The rationale for using possibilities in the binary response is to eliminate assessment, which uses opinions or possible prejudices for different types of responses. Also, the binary concept is simple, according to the developers of the system opinion, because it does not require lengthy responses from countries, since the respondent only confirms the presence or absence of certain predefined cybersecurity solutions [5].
The Global Cybersecurity Index consists of five blocks, including legal, technical, organizational, capacity building, and collaboration. Now we consider these blocks. The legal block includes "legislation cybercrime", "cybersecurity regulation" and "cybersecurity training". The technical block includes national, regional, industry Computer Emergency Response Team (CERT), cybersecurity standards for organizations, child safety on the Internet. Organizational factors include strategy, public consultation, responsible agency, cybersecurity methods. Capacity development includes standardization agencies, cybersecurity research, and development programs, awareness campaigns, national education programs and curriculums, incentive mechanisms. The cooperation block includes different agreements, participation in international and bilateral forums.

Based on the data in Table 1, let us try to build an ex-post prediction of the global GCI for 2018 and a prediction for 2019 and 2020. That is, in general, the prediction model has based on five years of prehistory and contains predicted data for three years.

The predicted model has based on simple trend extrapolation methods. The trend consists of some general directions for process development (phenomenon), long-term regularity. When prediction by extrapolation methods proceed from the inertia of the phenomenon (processes) that are studied and predicted. The degree of inertia depends on the size and scale of the researched process. At the micro-level, the influence of an individual factor can instantly change the situation, while at the macro level, due to the actions of many factors that sometimes exert opposite effects on each other, the inertia is greater. With considerable inertia of the researched economic processes (phenomenon), one can expect with sufficient degree of probability that the patterns that have appeared in the "prehistory" almost not change the prediction period.

The simple prediction methods based on trend extrapolation are implemented in production management since they have several advantages:

– enough simplicity of research methods attracts a wide range of specialists;
– the ability to apply portable and simple computing tools to perform calculations;
– the big speed of calculations is effective in online mode;
– the presence of a relatively small array of information.

Now we consider the main analytical indicators of the dynamic sequences in predicting:

– average absolute gain

$$\bar{\Delta}y = \frac{y_n - y_1}{n-1} \tag{1}$$

– average growth rate

$$\bar{k}_p = \sqrt[n-1]{\frac{y_n}{y_1}} \tag{2}$$

Based on the analytical indicators that are widely used to estimate dynamic sequences, we can deduce the dependencies that can be applied to build predictions

$$\hat{y}_{n+T} = y_n + \bar{\Delta}y * T \tag{3}$$

with applying average absolute gain and

$$\hat{y}_{n+T} = y_n * \bar{k}_p^T \tag{4}$$

with using average growth rate.

The method of flowing average is based on the use of dependency:

$$\Delta y_t + 1 = \lambda_t y_t + \lambda_{t-1}\Delta y_{t-1} + \lambda_{t-2}\Delta y_{t-2} + \cdots + \lambda_{t-(n-1)}\Delta y_{t-(n-1)} \tag{5}$$

where n – is the number of prehistory years.

The coefficient λ_t is determined by the formula:

$$\lambda_t = \frac{t*\beta}{n} \tag{6}$$

where t is a number that denotes a consecutive natural sequence of "prehistory" started from the last event; β is determined by Table 1.

Table 1. Definition of value β

n	3	4	5	6	7	8
β	0,5	0,4	0,333	0,286	0,250	0,222

5. Experiments

Table 2 gives data on the global GCI indicator for the period 2014-2018. Using equation (3; 4), we build a prediction for this indicator for 2019-2020, and an ex-post prediction for 2018 to assess the quality of the prediction.

Table 2. Global Cybersecurity Index of Ukraine

Year's number, t	Global Cybersecurity Index
1	0,35
2	0,353
3	0,5
4	0,501
5	0,68

With the data for five years, we calculate indicators:

– average absolute gain $\bar{\Delta}y = 0{,}0825$
– average growth rate $\bar{k}_p = 1{,}18$

Based on dependence (3), we predict GSI, obtained with the trend extrapolation method based on the average absolute gain for 2019 and 2020 GCI $\hat{y}_{n+1} = 0{,}7625$ and $\hat{y}_{n+2} = 0{,}845$

Similarly, based on expression (4), we predict GCI $\hat{y}_{n+1} = 0{,}802$ and $\hat{y}_{n+2} = 0{,}946$

In this case, the prediction of GCI values obtained with the trend extrapolation method based on the average growth rate for 2019 and 2020 are 0.802 and 0.946.

It should be noted that the prediction quality can only be told after the event has taken place. To evaluate the reliability of the considered methods and to determine the best ones, we apply the method of "ex-post prediction". This approach

is also applicable to other quantitative predicting methods. To do this, we must determine, using these methods, the predicted values of the researched indicator under for 2018, i.e. the year for which we have a specific value.
Now we calculate the prediction of CGI values to 4 years:

– average absolute gain $\bar{\Delta}y = 0{,}05$
– average growth rate $\bar{k}_p = 1{,}12$

Based on dependence (3), we predict GCI $\hat{y}_{n+1} = 0{,}551$ – the prediction of GCI value obtained by the trend extrapolation method based on the average absolute gain for 2018.

– In this case, dependence (4) allows us to predict GCI $\hat{y}_{n+1} = 0{,}561$ – for the trend extrapolation method with the coefficient of average growth rate for 2018.
– The results of the comparison of predicted and actual data and the estimated quality of the prediction are given in Table 3 and Table 4.

Table 3 - Quality assessment prediction of GCI based on average absolute growth for 2018

Year's number, t	Actual value	Prediction value	deviation	
			absolute	relative
5	0,68	0,551	-0,129	12,9

Table 4 - Quality score prediction of GCI based on the average growth rate for 2018

Year's number, t	Actual value	Prediction value	deviation	
			absolute	relative
5	0,68	0,561	-0,119	17,5

Comparing the results of the predictions presented in table 3 and table 4, it can be concluded that usage of the average annual growth rate provides higher accuracy of the prediction, as evidenced by the absolute and relative deviation.
To form a prediction of GCI with the extrapolation method of flowing average, it is necessary to apply the dependencies (5, 6) and Table 1. Now we determine the value β for the five years. According to the data in table 2, if n = 5, then β = 0,333. Therefore $\lambda_1 = 0.067$; $\lambda_2 = 0.133$; $\lambda_3 = 0.2$; $\lambda_4 = 0.267$; $\lambda_5 = 0.333$
Using the input data (Table 2), we predict products consumption based on the flowing average method: $\Delta y_t = 0{,}179$; $\Delta y_{t-1} = 0{,}001$; $\Delta y_{t-2} = 0{,}147$; $\Delta y_{t-3} = 0{,}003$; $\Delta y_{t-4} = 0{,}05$
And finally, the predicted values of GCI for 2019 and 2020 are $\hat{y}_{t+1} = 0{,}77$ and $\hat{y}_{t+1} = 0{,}859$
Now we compare calculations of GCI prediction based on the average absolute gain, average growth rate, and flowing average. Data in table 5 suggest that prediction on the average growth rate is slightly ahead of the other two methods.
And finally, the obtained predicted values give us the possibility to construct the summary chart of the GCI indicator trend (Fig. 1).

Table 5 – Prediction of the CGI indicator which calculated of three methods

Period	Extrapolation using average absolute gain	Extrapolation using an average growth rate	Extrapolation using flowing average
2019	0,762	0,802	0,773
2020	0,845	0,946	0,859

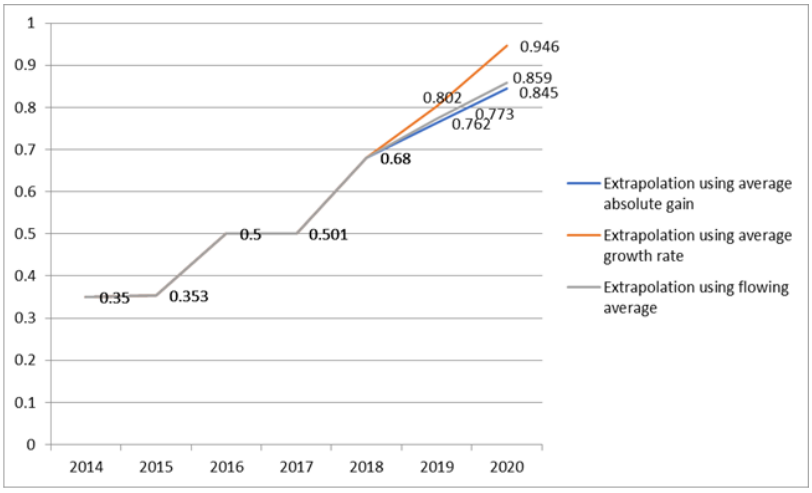

Figure 1. Diagram of predicted values of CGI indicator

6. Conclusions

The extrapolation method is one of the main prediction methods based on prediction events and the analysis of indicators that have been in the past years (at least 5 to 8 years).
A significant disadvantage of average absolute gain and average growth rate as the prediction methods based on the trend extrapolation is that their value depends entirely on the extreme levels of the dynamic range. Intermediate values,

which more determine the trend of changes in indicators, are essentially not involved in the calculations. This disadvantage is eliminated by the flowing average method.

The feature of the flowing average method is that the values of indicators which are closer to the predicted period have a greater impact on the values of the predicted indicators than through using the distant periods. This achieves by the coefficient λ.

Besides, the advantage of the flowing average method is that the values of the predicted indicators are more or less affected by all the data of the "prehistory", while the value of the average annual growth rate is determined only by extreme values of the dynamic sequences. The availability of alternative predicted options allows specialists to select the most appropriate ones based on experience, knowledge, and intuition.

The scientific novelty of the obtained results is the application of qualitative prediction methods, based on the trend extrapolation in determining the predicted value of the global cybersecurity index in Ukraine. It gives reasons to hope for improvement of the level of this indicator, provided that the existing trends in the development of the cybersecurity sphere of the state will be maintained. Based on the 2014-2018 data generated by the International Telecommunication Union, the predicted values of the Global Cybersecurity Index (GCI) in Ukraine for 2019 and 2020 has been calculated.

Also, we have compared the obtained values with each other and have made a diagram of the future development of events. In advance, it is difficult to conclude which prediction is more accurate, because currently no official values of indicators for this period have been formed yet.

8. Acknowledgments

The authors express their gratitude to the staff of the Department of Information-Measuring Technologies of Lviv Polytechnic National University, Ukraine, for the assistance in the preparation of this article.

9. Conflict of Interests

Conflict of interest while writing, preparing, and publishing the article as well as mutual claims by the co-authors is absent.

References

[1] Committed to connecting the world [Online]. Available: https://www.itu.int/en/ITU-D/Cybersecurity/ Pages/global-cybersecurity-index.aspx

[2] Global Cybersecurity Index (GCI), 2017. [Online]. Available: https://www.itu.int/en/ITU-D/ Cybersecurity/Documents/Global%20Cybersecurity%20Index%202017%20Report%20version%202.pdf

[3] Global Cybersecurity Index, 2017. International Telecommunication Union. [Online]. Available: https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2017-PDF-E.pdf

[4] ITU is the United Nations specialized agency for information and communication technologies – ICTs. [Online]. Available: https://www.itu.int/en/about/ Pages/overview.aspx

[5] I. Voronenko, "Indicators for monitoring the development of the information and telecommunication technologies market", Scientific Bulletin the National University of Life and Environmental Sciences of Ukraine, Series: Economics, Agricultural Management, Business, 2018.

[6] I. Voronenko, "Key indicators of national security as a component of digital economy development", in *Proc. 7th International Scientific and Technical Conference of Young Scientists and Students, "Current problems of modern technologies*", Ternopil, 28–29 November 2018.

[7] I. Diorditsa, The concept and content of the national cybersecurity system [Online]. Available: http://goal-int.org/ponyattya-ta-zmist-nacionalnoi-sistemi-kiberbezpeki/

[8] V. Zalunin, "Indexes and indicators of economic security of the enterprise", Innovative economy, no.3, pp.325–328, 2013.

[9] V. Lipkan, *National security of Ukraine: tutorial*. 2nd ed., Kyiv, 2009.

[10] V. Lipkan, *National and international security in definitions and concepts*. 2nd ed., Kyiv, 2008.

[11] V. Martynenko, "Prediction tendencies of Ukraine economic security development taking into account influence of globalization factors", Collection of scientific papers of the National University of the Ukraine State Tax Service, no.1, 2013, pp. 1381–49.

[12] V. Martyniuk, "Assessment of the national economy state on the basis of the integral index of the state economic security", Economics, Management, Entrepreneurship, no.25, pp.179 – 187, 2013.

[13] S. Melnyk, "Actual trends in cybercrime prevention as part of the country's cybersecurity strategy", *Collection materials of scientific-practical conference "Information Security: Challenges and Threats of Modernity"*, Kyiv, April 5, 2013, 416 p.

[14] S. Dziubyk, *Foundations of economic theory: tutorial*. 3rd ed., Kyiv, 2014.

[15] O. Polotaj, "Construction and evaluation of innovative segment prediction of Ukraine economic security", Market infrastructure Electronic scientific and practical journal, no.15, pp.209–215, 2018.

[16] O. Polotaj, "Prediction an integrated innovative indicator of economic information security", Information security, vol.21, no.2, pp.201–206, 2015.

[17] I. Timkin, Structural and functional characteristics of the Ukraine national security system. [Online]. Available: er.nau.edu.ua

[18] O. Trofymenko, "Legislative framework for cybersecurity of the state", *proc of 2nd all-Ukrainian Research Practice Conference "Cybersecurity in Ukraine: Legal and Organizational Issues"*, Odesa, November 17, 2017, pp.55–56.

[19] O. Trofymenko, Ya. Dubovoi, "Evolution of views on information wars in the information society era", Comparative and analytical law: an electronic scientific professional publication, Uzhhorod, no.1, pp.189–192, 2017.

[20] O. Trofymenko, Ya. Dubovoi, "Regarding the legal potential of safe functioning of cyberspace", *proceedings of 3rd All-Ukrainian Sciences-Practical Conference "Cybersecurity in Ukraine: Legal and Organizational Issues"*, Odesa, November 30, 2018, pp.5–7.