UDC 001.8

Comparative Analysis of the Cybersecurity Indices and Their Applications

V. M. Kravets[1]

[1] *National Academy of Security Service of Ukraine*

Abstract

The paper provides a comparative analysis of the structure, methodologies and applications of the most famous international cybersecurity indices: the Global Cybersecurity Index (GCI), the National Cybersecurity Index (NCSI), the Index of Cybersecurity (ICS). According to this survey, all these indices are determined by expert evaluation, but have different purposes. GCI and NCSI have similar pool of respondents, they are more trusted due to data verification, but have different system of indicators and evaluation. GCI includes the most extensive set of indicators, NCSI is the most accurate, reflects the up-to-date cybersecurity situation and has online tools for data processing. Data verification for ICS is not applied, but this index is unique in evaluation not countries but risks (probability of threats, activity of cyberattack actors, etc.).

An analysis of coherence of the economic activity indicators and the e-indices, including cybersecurity indices, suggests that the development of information and telecommunication technologies correlates with the development of innovation and economic activity, state power in countries with advanced information infrastructure is more stable. At the same time, there is a tendency for non-compliance of the cybersecurity level with the development of information and telecommunication infrastructure.

Keywords: international cybersecurity indices, methodology, e-indices applications.

Formulation of the problem

Today, information and communication technologies are the engine of the further society development, and science-based technological economies are more developed and rich.

In order to scientifically substantiate this hypothesis, we propose to use integrated integral indices, in particular, the so-called e-indexes which include cybersecurity indices.

Scientists, analysts and industry professionals apply different indicators and indices to assess the cybersecurity state depending on the object of protection, the purpose of such assessment and decisions are taken on their basis. In this study, we have analyzed three of the most famous international cyber security indices: Global Cybersecurity Index (GCI), National Cybersecurity Index (NCSI) and Index of Cybersecurity (ICS).

Analysis of research and publications

The vast majority of scientific publications with links to integral indices are devoted to their use in some subject area, primarily as indicators of economic activity development [1, 2, 3]. The analysis of e-indexes as indicators of the information society development is carried out by Batalova A.E., Sinyova I.S., Fenchuk M.M. [4]. In their article, the internal connections of the indicators are studied and the countries clusterization by the level of development is given.

The structure and properties research of the e-indices themselves is proposed by E. Kononova, E. Kovpak [5]. The authors of this publication have done comparative analysis and have assessed the consistency of the fourteen common e- indices, including the Information Society Index (ISI), the Knowledge Economy Index (KEI), the E-Government Development Index (EGDI), the ICT Development Index (IDI), the Networked Readiness Index (NRI), the Global Competitiveness Index (GCI), the Global Innovation Index (GII). According to this paper the most reliable, complete (contains the largest number of indicators used by other e-indices), available and trusted (with the smallest contribution of subjective evaluated indicators) is the Information and Communication Technologies Development Index [6] published by the International Telecommunication Union (ITU).

At the same time, in scientific publications, comparative analysis of international cybersecurity indices has not been carried out before.

Formulating the goals of the article

In this publication, a comparative analysis of the structure, methodologies and applications of the most famous international cybersecurity indices is carried out in order to further sharing the practice of their use in the scientific and analytical research. It is proposed to test the hypothesis of the positive impact of information and communication technologies on the development of society and national economies by using integrated indices and macroeconomic indicators.

The Global Cybersecurity Index

The Global Cybersecurity Index, GCI [7] is a trusted feature that measures at the global level how governments are implementing cyber security commitments to raise awareness of the importance and different dimensions of the problem. Since cybersecurity has a wide range of applications that penetrates various sectors and sectors, the level of cybersecurity system development in each country is assessed in five categories - legal measures, technical measures, organizational measures, capacity building and cooperation, which then are grouped together to obtain an integral evaluation.

Purpose

The long-term goal of GCI development is to stimulate further efforts to implement and integrate cybersecurity on a global scale. Comparisons of national cybersecurity strategies from different countries show which countries are upper-ranked in specific areas, and will further help implement less well-known, but more effective, cybersecurity strategies. This may contribute to improving the share information about cybersecurity to countries at different levels of development. By measuring the readiness of the cybersecurity system in various fields, the index will enable countries to assess their level of development, to realize how far they are from an acceptable level of cybersecurity, and to identify areas that need further improvement.

Methodology

To evaluate each of the five categories, a system of indicators and their corresponding questions, whose values are determined through an online survey, have been developed. Answers to the questions should be supported by additional evidence (references to documents, sites of responsible institutions, etc.). The assessment of the country's development status by a certain indicator is normalized according to its weight, as determined by experts from partner organizations (the total weight of all questions is 100 units).

The index was first introduced in 2014 (GCIv1). The second edition of the index appeared in 2017 (GCIv2). The key difference of the GCIv2 methodology is the use of a binary evaluation system (the existence or absence of a specific activity, department or measure is fixed). In 2014, a three-level system was used (existent, partially developed, absent). A number of new questions have been added in each of the five categories in order to refine the depth of research. Therefore, GCI 2014 and GCI 2017 can not be compared. In addition, the index of 2014 applies a simple average methodology, while the index in 2017 - the weighting factor for each category.

The current edition of the Global Cybersecurity Index (GCIv3) which measures the commitment of states to cybersecurity in order to raise awareness has improved the list of indicators by the involvement of more partners and an increase in the number of open consultations.

Various experts and organizations are involved in the development of the methodology and index calculation, including Interpol, the United Nations Department of Economic and Social Affairs (UNDESA), the United Nations Office on Drugs and Crime (UNDOC), the Economic Community of West African States, The European Cybersecurity Organization, the Forum of Incident Response and Security Teams (FIRST), the ITU-Arab Regional Cybersecurity Centre, the Korean Internet and Security Agency (KISA), International Social Security Association (ISSA), Global Cyber Alliance.

The National Cyber Security Index

The National Cyber Security Index, NCSI [8], is a global index that assesses the preparedness of countries to prevent cyber threats and manage cyber incidents. NCSI is also a database which contains publicly available materials and tools for proving the ability to build a national cybersecurity system. This index focuses on measurable issues of cybersecurity implemented by central governments: legislation in force (legal acts, regulations, orders, etc.) created for cybersecurity regulation, established units (existing organisations, departments, etc.), cooperation formats (committees, working groups, etc.), outcomes (policies, exercises, technologies, websites, programmes, etc.). The main categories for evaluation are: general cyber security indicators (cyber security policy development, cyber threat analysis and information sharing, education and professional development, contribution to global cyber security), baseline cyber security indicators (protection of digital services, protection of essential services, e-identification and trust services, protection of personal data), incident and crisis management indicators (cyber incidents response, cyber crisis management, fight against cybercrime, military cyber operations).

Purpose

The index is considered by developers as an instrument for providing up-to-date and accurate information on the development of national cybersecurity systems. The service gives an opportunity to compare cyberpower of countries and in the future - to get information about the best practices that guarantee high ranking positions (the process of developing services for data analysis is still ongoing).

Methodology

NCSI indicators were developed based on the fact that any national cybersecurity system should counteract the fundamental threats that directly affect the normal functioning of information and communication systems: the denial of service availability; data integrity violation; data confidentiality violation. Developers have been offered a system of indicators that would reflect the ability of countries to respond to these challenges. Each indicator has a value that shows its relative importance in the index. Estimates of indicators are provided by experts according to the following considerations: 1 point - if there is a legal act regulating a specific sphere of activity; 2-3 points - if there is a unit responsible for a particular area; 2 points - the official format of cooperation was introduced; 1-3 points – an outcome / product in a particular field of activity has been obtained. Each assessment must be confirmed by a legal act, a reference to the unit's website, service, etc.

The data is verified at least by two NCSI team members, and after inspection, database and the general rating are updated immediately.

The country index shows the percentage of the points given to the country by experts from the maximum possible value (currently 100% - 77 points).

The NCSI project was created at the e-Governance Academy (Tallinn). The NCSI team includes representatives from Estonia's government, IT industry, academics and experts in cybersecurity. NCSI was presented at the ITU workshop in April 2016.

The Index of Cyber Security

The Index of Cyber Security, ICS [9] is a sentiment-based measure of the risk to the corporate, industrial, and governmental information infrastructure from a spectrum of cybersecurity threats. It is sentiment-based in recognition of the rapid change in cybersecurity threats and postures, the state of cybersecurity metrics as a practical art, and the degree of uncertainty in any risk-centered field. In fact, the industry cybersecurity index aggregates the views of cybersecurity industry professionals as expressed through a monthly survey. The index contains the following main categories: attack actors, cyber weapons, the effect desired by attackers, attack targets, the vulnerability of available defences, overall perceptions. The ICS index is a measure of risk. A higher index value indicates a perception of increasing risk.

Purpose

This index is for cyber security industry professionals who require a continuous, methodologically transparent assessment of the cybersecurity level. Sharing information about the results of assessing the level of cyber threats risk by industry professionals promotes general awareness of society, provides an opportunity to compare own experience and threats assessment with an overall perceptions, which will undoubtedly enhance the security of information infrastructure. In addition, the consistent time series data on cyber threats risk can be used in future for scientific and analytical research to develop new security products, financial market management.

Methodology

The ICS is published since April 2011 and is updated monthly on the last day of the month. An expert survey of information security professionals (chief risk officers, chief information security officers, selected academicians engaged in field work, selected security product vendors' chief scientists) is used for evaluation. The list of respondents is not public. To guarantee comparability of the monthly estimates, developers are trying to keep the list of issues unchanged, but warn of insignificant deviations in it, due to the current state of cyber threats. The answers to the questions are formulated in a five-level system (fallen fast (-20%), fallen (-7,5%), stayed static (0%), risen (+ 7.5%) or risen fast (+ 20%) compared to the previous month). The index indicators are estimated in absolute values. Each question in the survey has a weight, and where a question has sub-questions, question's weight is divided equally between them. The absolute value matched for each question is added and divided by the number of questions in order to obtain a unified assessment from the respondent. The total monthly estimation is the average value of such indicators received from all respondents (not less than 100 experts). The ICS counts as the index for the past month, multiplied by the exponent from the total monthly estimate. The initial value of the index (in March 2011) was 1000.

Detailed reports and comparative analysis for each question are distributed only to respondents while the general level of the index is published on the site. At the same time, the reports contain only unclassified information, so respondents can share it with their colleagues.

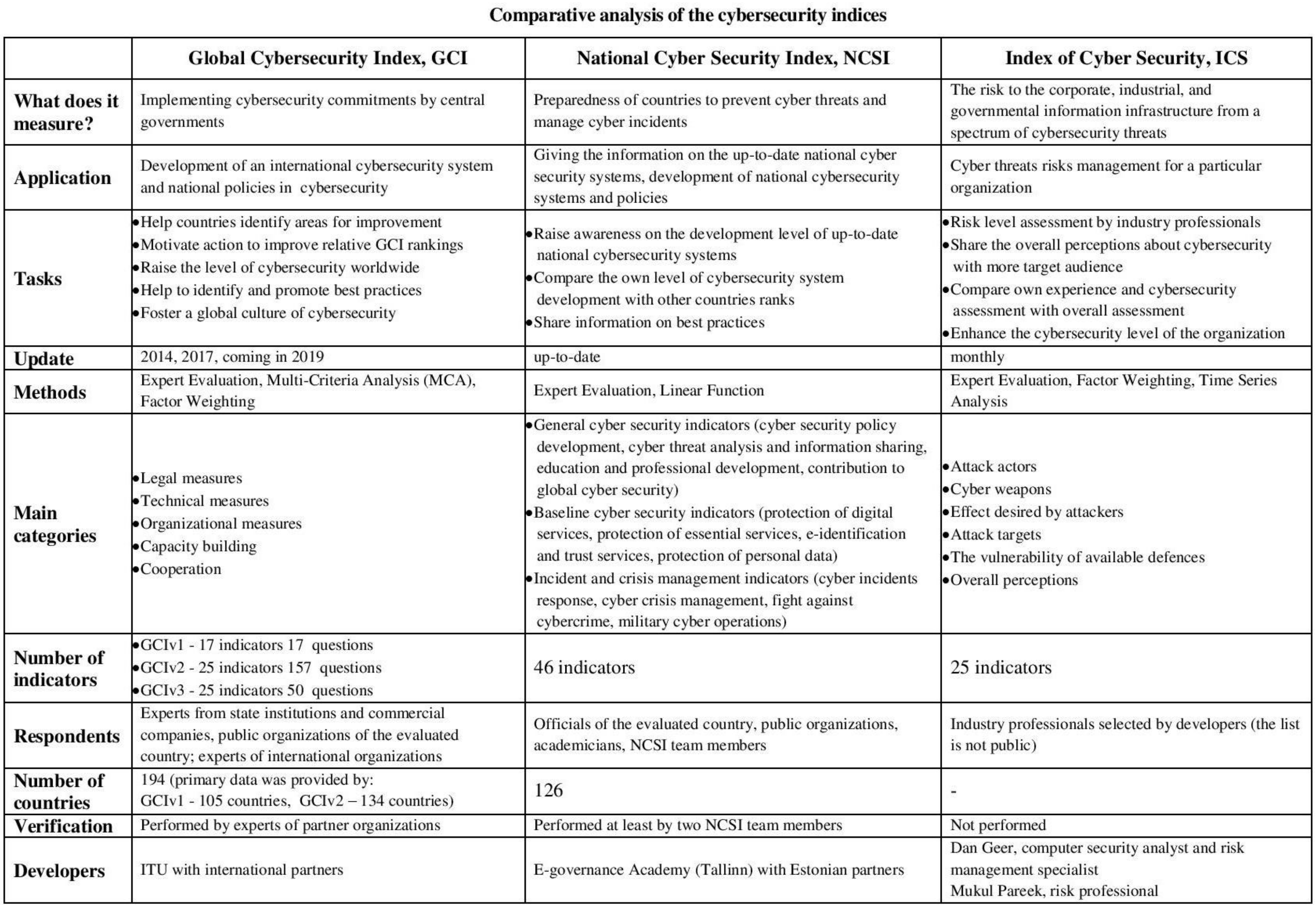
A summary comparison of the GCI, NCSI and ICS is given in Fig. 1 1.

In accordance with the above task of the study, we have made the assumption that the growth of the information and communication technologies development index will increase indicators that characterize the development of society and national economies. In our opinion, the Global Innovation Index (GII [10]) and Gross Domestic Product per capita (GDP per capita [11]) are such indicators. In addition, in order to assess the impact of information technology development on state security, we also use the Fragile States Index (FSI [12]), which characterizes the sustainability of state power in the country (the higher this indicator, the less stable is governance).

The research will be carried out by determining the coherence (paired correlation coefficients) of the indices and indicators. For this purpose, data will be used for 2017, with the exception of NCSI, which is fixed at the current moment (sample size is not less than 119 countries depending on the indicator).

With a confidence probability of at least 99%, it can be argued that there is a linear correlation between IDI and GDP per capita (0.75), between IDI and GII (0.86), which confirms the hypothesis about the positive impact of information and telecommunication technologies on the development of innovations, social and economic activity, and hence the growth of the economic activity efficiency (Table 1 1). At the same time, the development of information and communication technologies assists in the sustainability of state power, as it is fixed a reverse linear correlation between IDI and FSI (-0.87). So state structures in countries with advanced information infrastructure are less vulnerable.

The NCSI is more closely related to the Information and telecommunication technology development index (0.75) than the Global cybersecurity index (0.65),



Comparative analysis of the cybersecurity indices

	Global Cybersecurity Index, GCI	National Cyber Security Index, NCSI	Index of Cyber Security, ICS
What does it measure?	Implementing cybersecurity commitments by central governments	Preparedness of countries to prevent cyber threats and manage cyber incidents	The risk to the corporate, industrial, and governmental information infrastructure from a spectrum of cybersecurity threats
Application	Development of an international cybersecurity system and national policies in cybersecurity	Giving the information on the up-to-date national cyber security systems, development of national cybersecurity systems and policies	Cyber threats risks management for a particular organization
Tasks	•Help countries identify areas for improvement •Motivate action to improve relative GCI rankings •Raise the level of cybersecurity worldwide •Help to identify and promote best practices •Foster a global culture of cybersecurity	•Raise awareness on the development level of up-to-date national cybersecurity systems •Compare the own level of cybersecurity system development with other countries ranks •Share information on best practices	•Risk level assessment by industry professionals •Share the overall perceptions about cybersecurity with more target audience •Compare own experience and cybersecurity assessment with overall assessment •Enhance the cybersecurity level of the organization
Update	2014, 2017, coming in 2019	up-to-date	monthly
Methods	Expert Evaluation, Multi-Criteria Analysis (MCA), Factor Weighting	Expert Evaluation, Linear Function	Expert Evaluation, Factor Weighting, Time Series Analysis
Main categories	•Legal measures •Technical measures •Organizational measures •Capacity building •Cooperation	•General cyber security indicators (cyber security policy development, cyber threat analysis and information sharing, education and professional development, contribution to global cyber security) •Baseline cyber security indicators (protection of digital services, protection of essential services, e-identification and trust services, protection of personal data) •Incident and crisis management indicators (cyber incidents response, cyber crisis management, fight against cybercrime, military cyber operations)	•Attack actors •Cyber weapons •Effect desired by attackers •Attack targets •The vulnerability of available defences •Overall perceptions
Number of indicators	•GCIv1 - 17 indicators 17 questions •GCIv2 - 25 indicators 157 questions •GCIv3 - 25 indicators 50 questions	46 indicators	25 indicators
Respondents	Experts from state institutions and commercial companies, public organizations of the evaluated country; experts of international organizations	Officials of the evaluated country, public organizations, academicians, NCSI team members	Industry professionals selected by developers (the list is not public)
Number of countries	194 (primary data was provided by: GCIv1 - 105 countries, GCIv2 – 134 countries)	126	-
Verification	Performed by experts of partner organizations	Performed at least by two NCSI team members	Not performed
Developers	ITU with international partners	E-governance Academy (Tallinn) with Estonian partners	Dan Geer, computer security analyst and risk management specialist Mukul Pareek, risk professional

Fig. 1. Comparative analysis of the cybersecurity indices

Table 1. Paired correlation coefficients of the studied indicators

Indicator	IDI	GCI	GDP per capita	FSI	NCSI	GII
IDI	1	#	#	#	#	#
GCI	0,651111	1	#	#	#	#
GDP per capita	0,750521	0,564166	1	#	#	#
FSI	-0,86781	-0,5774	-0,80423	1	#	#
NCI	0,745421	0,670291	0,597095	-0,70113	1	#
GII	0,863668	0,658868	0,838098	-0,86033	0,731663	1

but this correlation is not too strong, which leads us to a disappointing conclusion - not all countries with well-developed information and telecommunication infrastructure are properly concerned with its protection, which poses risks to its functioning. It should also be noted that, according to our observations, the GCI and NCSI are not correlated to each other. On the one hand, this is due to the differences in the sets of indicators used in these indices; on the other hand, the reason may be a comparison of data series for different periods (2017 for GCI, the current situation for NCSI).

Conclusions

A comparative analysis of the current international cybersecurity indexes GCI, NCSI, ICS shows that all of them are determined through the expert evaluation, but have different purposes: the development of an international system of cyber security, the awareness on the current state of national cybersecurity systems and the risks management of cyberthreats in a particular organization. The GCI and NCSI have a similar pool of respondents, they are similar in approach to data verification, but have different systems of indicators and evaluation. The Global Cybersecurity Index is more complete, respectable and famous. At the same time, the NCSI is the most relevant, accurate and reflects the current state, but not the situation in the past. In addition, the NCSI is not a static table but is provided with modern services (software) for data processing. GCI and NCSI are also more trusted due to data verification. Verification of the ICS is not implemented at all, but it is unique because it assesses not countries but risks (probability of threats occurrence, the activity of cyberattack actors, tools for attacks, etc.).

The coherence analysis of e-indexes and economic activity indicators shows that information and telecommunication infrastructure today plays the same role for the development of society, the growth of economic prosperity as previously played the roads for stirring up the economic activity. In the information society, communication tools are a kind of transport artery. The development of information and telecommunication technologies, which correlates with the innovation's development, has a decisive value in scientific research and education, enhances the competitiveness of the national economy.

At the same time, it is observed the tendency of non-compliance of the cyber security level with the development of information and telecommunication infrastructure, which can lead to negative consequences.

The results of this study can be used to further improve the data analysis tools that characterize cybersecurity in the world.

References

[1] S. Polumiyenko, *Monitoring, ocinyuvannya ta prognozuvannya rozvytku systemy elektronnogo uryaduvannya*, vol. 6 of *Elektronne uryaduvannya ta elektronna demokratiya.* Kyiv, Ukraine: FOP Moskalenko O.M., 2017.

[2] A. Lazarev, "Mezhdunarodnyye indeksy dlya otsenki razvitiya informatsionnogo obshchestva: novyye pokazateli," *Otkrytoye obrazovaniye*, no. 4, pp. 75–84, 2011.

[3] C. Gorda, *Metody resursnogo teoretyko-igrovogo analizu procesiv regionalnogo rozvytku (Ph.D. dissertation).* Kyiv, Ukraine: Instytut telekomunikacij i globalnogo informacijnogo prostoru, Nacionalna akademiya nauk Ukrayiny, 2018.

[4] A. Batalov, I. Sineva, and M. Fenchuk, "Analiz klyuchevykh indikatorov i indeksov ikt na sovremennom etape razvitiya informatsionnogo obshchestva," *TComm*, no. 10, pp. 21–27, 2013.

[5] E. Kononova and E. Kovpak, "Statisticheskiye profili informatsionnogo obshchestva: sravnitelnyy analiz e-indeksov," *Efektivna ekonomika*, no. 5, 2015.

[6] "Ict development index 2017." International Telecommunication Union (ITU), 2017. [Online]. Available: https://www.itu.int/net4/itu-d/idi/2017/index.html.

[7] "Global cybersecurity index." International Telecommunication Union (ITU). [Online]. Available: https://www.itu.int/en/ITU-D/Cybersecurity/Pages/global-cybersecurity-index.aspx.

[8] "National cyber security index." e-Governance Academy. [Online]. Available: https://ncsi.ega.ee.

[9] D. Geer and M. Pareek, "Index of cyber security." [Online]. Available: http://cybersecurityindex.org/index.php.

[10] “Global innovation index 2017 rankings.” Global Innovation Index, 2017. [Online]. Available: https://www.globalinnovationindex.org/ UploadedFiles/ Indepths/Files/Indepths _9db22f7962064f1282db29c9aec30365.PDF.

[11] “Gdp per capita.” The World Bank. [Online]. Available: https://data.worldbank.org/indicator /NY.GDP.PCAP.CD.

[12] “Fragile states index.” The Fund For Peace. [Online]. Available: http://fundforpeace.org/fsi/data/.