10. İngilis dilli beynəlxalq mənbələr:
11. Prensky, M. (2010). Teaching Digital Natives: Partnering for Real Learning. Thousand Oaks, CA: Corwin Press.
12. Hattie, J. (2009). Visible Learning: A Synthesis of Over 800 Meta-Analyses Relating to Achievement. London: Routledge.
13. Ertmer, P. A., & Ottenbreit-Leftwich, A. T. (2010). Teacher Technology Change: How Knowledge, Confidence, Beliefs, and Culture Intersect. Journal of Research on Technology in Education, 42(3), 255–284.

DOI 10.70286/ISU-03.12.2025.003

ANALYSIS OF CYBER THREAT MEASUREMENT METRICS: ADVANTAGES AND DISADVANTAGES

Yarovenko Hanna
D.Sc., Associate Professor
Department of Economic Cybernetics
Sumy State University, Ukraine

Given the rapid growth in the number and complexity of cyber threats, measuring the level of cybersecurity at the national level is becoming increasingly critical for ensuring the resilience of states, the development of effective security policies, and the coordination of actions among the government, the private sector, and international partners. Assessing cyber threats using specialised indices allows not only to identify the strengths and weaknesses of the state cyber infrastructure, but also to compare countries with each other, determine priorities for development, and adapt strategies to the current state of the global cyber environment. To date, several indices have been developed by independent international organisations to assess cyber threats at the macro level.

The National Cybersecurity Index (NCSI) is a global ranking that shows how prepared a country (through the central government) is to prevent cyber threats and respond to cyber incidents. For its calculation, a public database was created on the existing legislative, organisational, institutional and technical means that the country has implemented to ensure cybersecurity. The index is based on 49 indicators and covers 12 subcomponents of "cybersecurity capabilities", which are grouped into three broad categories: strategic, preventive and reactive. The strategic group includes cybersecurity policy, global partnerships, education, professional development, scientific and research activity. Preventive capabilities cover the protection of critical/service and digital infrastructure, threat analysis and awareness raising, and personal data protection. The reactive category includes incident response, crisis management, cybercrime countermeasures, and military cyber defence. The NCSI score is measured as a percentage of the maximum possible "sum" of the indicators. 100% means that the country has achieved all the predicted capability indicators [1].

The NCSI has various advantages, including: the presence of strategies, response centres, legislation, data exchange mechanisms, digital resilience procedures and institutional infrastructure. Thanks to this, the NCSI ensures comparability between states, allows tracking progress and provides a relatively transparent methodology in which each criterion can be verified against open data. However, the index also has important shortcomings: it assesses formal capacity, not the actual level of protection or real incidents; relies on "declarative" factors that may not reflect the effectiveness of implementation; depends partly on the availability of data, which may distort the positions of individual countries; does not measure the technical complexity of attacks or the level of cyber threats in dynamics, which limits its use for a comprehensive analysis of the cyber environment.

The Global Cybersecurity Index (GCI) is also an international rating that assesses the level of a country's "commitment" to cybersecurity. It was developed by the International Telecommunication Union (ITU). The GCI analyses the commitments and measures that countries take in five main areas - "pillars": Legal Measures, Technical Measures, Organisational Measures, Capacity Development, and Cooperation. To assess the GCI, countries fill out questionnaires from which a set of indicators is formed. In one of the editions of the GCI, there were 20 indicators based on ≈ 83 questions. The results form an overall score/rating for countries, which allows comparing countries with each other in terms of the level of commitment and implementation of cybersecurity policies. The GCI is designed to raise awareness of the importance of cybersecurity, stimulate countries to develop appropriate policies, promote international cooperation and exchange of experience [2].

The GCI is useful in that it covers a wide range of aspects of national cyber resilience, which allows for a comprehensive assessment of cybersecurity and comparisons of countries using a unified methodology. Its advantage is its global coverage and systematic updating, which allows for monitoring the evolution of policies over time, as well as a structured model that stimulates states to develop different areas of cyber defence. At the same time, the index has disadvantages: a significant part of the data is based on self-assessments of states, which can lead to an inflated indicator; the indicators are focused mainly on the presence of strategies, regulations or institutions, rather than on the actual quality of their implementation; the methodology does not take into account the real level of threats or incident statistics; and the complexity of the structure sometimes interprets the rating less transparent for practical use.

The National Cyber Power Index (NCPI) was developed by the Belfer Center for Science and International Affairs at Harvard University and aims to assess the overall cyber potential of a state. The index analyses both the "capabilities" and the "content" of states in cyberspace, that is, not just defensive, but also potential offensive, information, economic, or espionage capabilities. The NCPI provides a comprehensive picture of the "cyber power" of a state and considers a wide range of factors: state strategy, resources, investments, the private sector, and innovation [3].

The NCPI is distinguished by the fact that it takes into account both defensive and offensive, economic, intelligence, and information capabilities of states, thereby providing a broader and more realistic view of the country's cyber potential

compared to indices that assess only the level of security. Its advantage is the comprehensiveness of the approach and the use of various sources, which allows assessing cyber power from many dimensions. At the same time, the index has limitations: its methodology is partly based on expert assessments and indirect indicators, which may reduce accuracy; it reflects more strategic potential than actual practical results; and it is also less suitable for assessing a specific level of national cybersecurity, as it focuses on force and geopolitical aspects, rather than on resilience to cyber threats.

The Cyber Readiness Index (CRI) is an international index designed to assess the readiness of states to face cyber risks. It considers the existence of a national strategy, an incident response system, laws against cybercrime, information sharing, investment in research and development, standardisation, infrastructure, etc. The CRI assesses the extent to which a country is "prepared" for cyber threats, i.e. the actual implementation of policies and procedures, not just declarations. The index covers only those countries that were included in the sample [4].

The CRI is useful because it focuses on assessing the real capacity of a state to prevent, detect and mitigate cyber incidents based on specific policies, institutions and response mechanisms, which makes it a practically oriented indicator of national cyber resilience. Its advantage is its focus on the implementation of strategies, economic risks and institutional preparation, which allows for a more applied view of a country's readiness for large-scale digital disruptions. However, the CRI has such shortcomings as the selection of criteria covers only certain aspects of cyber readiness and may not reflect the real level of technical security; the data is often based on open sources, which sometimes limits the completeness of the picture; and the very structure of the index makes it less suitable for comparing countries with very different economic or regulatory systems.

The Index of Cybersecurity (ICS) is one of the first general professional indices designed to assess the level of risk for corporate, government and industrial information infrastructure. Unlike the GCI/NCSI, which assess state readiness or state policy and capabilities, the ICS is focused on the perception of security professionals, that is, it reflects their assessment of current cyber threats. The value of the ICS changes monthly, which allows you to see trends, reactions to new threats, market excitement. This can be useful for research, sentiment analysis, and comparison of subjective but professional risk between periods or regions [5].

The ICS is not an "objective" index of state cybersecurity. It is based on surveys, so the indicators do not reflect actual resources or protection structures, but the perceptions of specialists. This means that the result is highly variable and depends on moods, news, real or potential threats, and not on formalised criteria.

In 2024, ENISA (the EU Agency for Cybersecurity) published a new tool, the EU-CSI, designed to describe the cybersecurity positions of EU Member States at the pan-European level. The ENISA EU-CSI is a composite index consisting of several qualitative and quantitative indicators grouped into "domains" that are rated on a total score of 0–100. The index allows comparing Member States by their level of cyber position, i.e. the extent to which a country meets basic requirements, has policies, resources, infrastructure, regulations, market/industry, industrial capacity, etc. [6].

As the EU-CSI is an EU-level initiative for Member States, the index provides an assessment specifically in the European context. For other countries outside the EU, the application will be indirect or irrelevant. Like other macro-indices, it does not necessarily assess the actual technical strength of systems, but rather formal readiness, policies, and institutional conditions.

An analysis of existing international indices demonstrates that modern methods for assessing cyber threats cover various aspects – from strategic and organisational to technical, institutional, operational, and even geopolitical, which makes it possible to obtain a multidimensional assessment of the cyber resilience of states. However, such indices are often based on self-assessment, open data, expert judgment, or formal indicators, which impose limitations on the accuracy, comparability, and practical interpretation of the results. The presence of these shortcomings indicates the need to refine calculation methods, increase objectivity, and unify criteria, which would allow for a more accurate and consistent comparison of the level of cybersecurity between different countries.

The work was carried out within the framework of the research topic № 0124U000544 “Cybersecurity and digital transformations of the country's wartime economy: the fight against cybercrime, corruption and the shadow sector”.

References

1. e-Governance Academy Foundation. (2025). National Cyber Security Index. e-Governance Academy Foundation. Retrieved from https://ncsi.ega.ee/ncsi-index/
2. ITU. (2025). Global Cybersecurity Index. International Telecommunication Union (ITU). Retrieved from https://www.itu.int/en/ITU-D/Cybersecurity/pages/global-cybersecurity-index.aspx
3. Voo, J., Hemani, I., & Cassidy, D. (2022). National Cyber Power Index 2022. Belfer Center for Science and International Affairs, Harvard Kennedy School. Retrieved from https://www.belfercenter.org/publication/national-cyber-power-index-2022
4. Potomac Institute for Policy Studies. (2025). Cyber Readiness Index (CRI). Potomac Institute for Policy Studies. Retrieved from https://www.potomacinstitute.us/academic-centers/cyber-readiness-index?utm_source=chatgpt.com
5. TAG Infosphere. (2025). Index of Cybersecurity. TAG Infosphere. Retrieved from https://tag-infosphere.com/ccs
6. ENISA. (2025). The EU-Cybersecurity Index 2024. European Union Agency for Cybersecurity (ENISA). https://doi.org/10.2824/7714867