STATISTICS IN TRANSITION new series and *STATISTICS OF UKRAINE, February 2023*
A New Role for Statistics: Joint Special Issue
Vol. 24, No. 1, pp. 229–258, DOI 10.59170/stattrans-2023-013
Received – 01.07.2022; accepted – 03.11.2022

Assessing the maturity of the current global system for combating financial and cyber fraud

Olha Kuzmenko[1], **Hanna Yarovenko**[2], **Larysa Perkhun**[3]

ABSTRACT

The purpose of the article is to assess the maturity of systems for counteracting financial and cyber fraud with the view of their future integration at global-level. The calculations made by the authors were based on indicators for 76 countries, which characterized each country's level of cybersecurity and its ability to combat financial fraud in 2018. After optimising the input data and selecting relevant indicators, the authors built an integrated cybersecurity index using the Sundarovsky convolution method. Sigma-limited parameterisation and Pareto-optimisation were then used to identify the determinants of the ability to counter financial and cyber fraud, which were used as predictors. Nonlinear regression was applied to determine the dependency of the integrated cybersecurity index on the government efficiency index, the ease of doing business and on the crime indices. On this basis, the authors conducted a bifurcation analysis of the maturity of current global system for combating financial and cyber fraud and produced its phase portraits. It was found to be mature ("Government Efficiency Index – Ease of Doing Business" and "Ease of Doing Business – Crime Index") and insufficient mature ("Government Efficiency Index – Crime Index"), with the components' imbalance indicating high system's sensitivity to react on changes. The constructed 'Equilibrium States' phase portraits showed non-equilibrium phase portraits of the 'saddle' type. The obtained results made it possible to identify determinants of a global integrated system's instability to combat financial and cyber fraud.

Key words: financial fraud, cyber fraud, phase portrait, bifurcation analysis.

[1] Sumy State University, Ukraine. E-mail: o.kuzmenko@biem.sumdu.edu. ORCID: https://orcid.org/0000-0001-8520-2266

[2] Sumy State University, Ukraine; University Carlos III of Madrid, Spain. E-mail: hyaroven@inf.uc3m.es. ORCID: https://orcid.org/0000-0002-8760-6835.

[3] MHP SE, Ukraine. E-mail: l.perkhun@mhp.com.ua. ORCID: https://orcid.org/0000-0002-8667-2312.

1. Introduction

One of the key tasks facing society today is to create a mechanism of protection against internal threats, which is even more urgently needed in the conditions of war with an external enemy. This is important for two main reasons. First, military conflicts in a country increase its attractiveness as a place for money laundering and the financing of terrorism (Yarovenko, 2021). Secondly, the risk of cyber fraud attacks against various elements of state and private infrastructure is increasing. For example, the number of cyber-attacks started to increase in the world in 2022 even before Russia's military aggression against Ukraine. For example, a large-scale attack against more than 70 government websites was recorded on February 14, 2022 (BBC, 2022); Ukraine's banking institutions were attacked on February 15, 2022 (Euronews, 2022). According to analytical data provided by the Quad9 DNS platform, there was a significant increase in the number of cyberattacks against Ukrainians in March. Of the 121 million malicious events recorded globally as of March 9, 2022, 4.6 million were associated with Ukraine and Poland, where 1.4 million Ukrainian citizens had been displaced by early March 2022 (Krebsonsecurity, 2022).

In addition to information attacks, there were occurrences of cyber financial fraud as well. On February 14, 2022, an 'IcedID' banking Trojan collecting personal banking data of Ukrainians was detected. In April 2022, another case of Internet fraud was discovered, where a fictitious social media page was used to collect financial assistance from EU countries through payments in violation of the confidentiality of payment card data (CyberPeace Institute, 2022).

These examples show that the issue of counteracting financial and cyber fraud is relevant and should be solved at various levels of public administration. In order to achieve it, a systematic approach should be applied, which necessitates the convergence of systems to combat financial and cyber fraud. This, in turn, is possible when their information, technical, software, and organizational integration takes place, both at the level of the state as a whole and at the level of individual business entities and the world. The need for convergence processes in the areas of money laundering and cyber fraud was identified by the US Financial Crimes Enforcement Network (FinCEN, 2009). It should occur at the level of relevant departments responsible for combating money laundering, terrorist financing, cybersecurity, and by businesses themselves. Global consulting companies Deloitte (2019) and PwC (2018) also covered this issue in their reports.

This paper deals with the issue of assessing the maturity of current global system for countering financial and cyber fraud (CFCF) in order to determine its/their

potential convergence opportunities in the future. To this end, the authors apply econometric and statistical methods that allow the assessment based on large amounts of data, taking into account temporal, spatial or other characteristics and factors.

2. Literature review

The maturity of CFCS system's depends on the advancement of specific processes and organization practices that are in place in order to ensure the system achieves desired results. In order to reach an appropriate level of maturity, it is also necessary to apply methods that can strengthen the level of protection against financial and cyber threats. Traditional methods are becoming less effective in accomplishing this goal. Matanky-Becker and Cockbain (2022) found that the widely used international three-stage money laundering model is less practical and reliable. It was used in less than a third of cases for a three-year data sample. Therefore, economic, and mathematical methods are increasingly complementing the traditional ones and or replacing them altogether. Two most powerful tools in the fight against financial and cyber fraud are artificial intelligence and machine learning, which rely on models of varying complexity that are constantly trained and retrained, and adapted to new conditions in which the research object functions. Machine learning was used by Hayble-Gomes (2022) to determine attributes needed to generate a suspicious activity report based on the transaction history of U.S. retail banking customers. Neural networks are used to identify and recognize faces of clients of financial institutions (Granados and Garcia-Bedoya, 2022), based on various data sources, such as social networks. AI tools are very effective in detecting financial crimes, including those related to money laundering, because they can be used to develop models which can identify such cases without human intervention (Rouhollahi, et al., 2021). Among different machine learning methods, the Light Gradient Boosting and Extreme Gradient Boosting have high accuracy, reaching more than 99% (Aziz, et al., 2022). Another algorithm, called Random Forest, has also been shown to very effective (94%) in modelling suspicious money laundering transactions (Tundis, Nemalikanti and Mühlhäuser, 2021).

In cases of mass financial and cyber fraud, it is possible to use models to identify group behaviour of individuals in order to identify similar characteristics and detect other cybercrimes associated with similar patterns (Mahootiha, Golpayegani and Sadeghian, 2021). An algorithm for approximating multifunctional behaviour can be used to track actions of users when they access financial transactions at their intermediate nodes (Amala Dhaya and Ravi, 2021). Genetic programming and token competition, proposed by Li and Wong (2021), have shown their effectiveness in determining objective values of individuals, which can be used to distinguishing those who differ from others. Robust regression (Riani, Corbellini and Atkinson, 2018) and logit regression (Yang and Wu, 2021) can be combined with neural networks to

detect symptoms of financial and cyber fraud. In combination with dynamic evolutionary glow-worm swarm optimization, Xia et al. (2022) proposed a biological algorithm for predicting the risk of financial fraud. Perkhun, Sorochynskyi and Izosimov (2015) researched the interaction of fraudulent attacks and tools to combat them on the basis of the modified Lotka–Volterra model. Granados and Vargas (2022) looked at how the Foreman-Ricci curvature can be used to build financial networks and quantify sets of suspicious nodes to create a strategy for detecting global financial crime and fraud. The use of data visualization is also a powerful tool for detecting abnormal operations and be used to identify fraud quickly and clearly. Tharani, et al. (2021) proposed a visualization of functions related to transactions in the Bitcoin and Ethereum networks, which helps to quickly identify cases of cyber fraud. The knowledge graph presented by Day (2021) can be used to combat the misuse of electronic payment instruments and cryptocurrencies.

The above-mentioned methods, in most cases, are used directly to detect financial and cyber fraud in individual transactions. These tools are rarely used to study processes, for example to assess the maturity of systems. This article proposes the use of bifurcation analysis and the construction of phase portraits to determine the current state of a global system and the points at which it will reach its equilibrium. It is a viral method used to study dynamic systems. This toolkit was used by Akhramovych, et al. (2022) to review the information security system in social networks and build its linear and dynamic models. Idowu, et al. (2018) described phase portraits to justify the chaos of the financial system. Sierikov and Zubova (2010) built systems of nonlinear differential equations for the market, which were based on the supply and demand model. Bystray, Lykov and Nikulina (2012) developed their own method for identifying macroeconomic risks, which involves the construction of pseudo-phase and phase portraits. Wilkens, Thomas and Fofana (2004) used phase portraits to determine price stability for technology stocks. As can be seen, bifurcation analysis and phase portraits have a wide range of applications for studying states of various systems. In this article, they are used to assess the maturity of the global system for combating financial and cyber fraud.

3. Research Methodology and Data

3.1. Research Methodology

The maturity of the current CFCF system is assessed in several stages.

Stage 1. Indicators are reduced to a single integral cybersecurity index using the Sundarovsky method, which involves the use of formula (1):

$$IS_j = \prod_{i=1}^{n} \left[a_{ij} - a_i^*\right]^{\alpha} \tag{1}$$

where IS_j - integral cybersecurity index for the *j*-th country;

a_{ij} – actual value of the *i*-th cybersecurity indicator for the *j*-th country;

a_i^*- equilibrium value of the *i*-th cybersecurity indicator for the considered set of countries;

α – constant, exponent.

In order to apply formula (1) to calculate the integral cybersecurity index, we introduce the following assumptions:

1) the absolute value of the difference between the standard deviation and the minimum allowable level is used as the equilibrium level of the constituent indicators:

$$a_i^* = \left|a_{ij} - \sigma_i\right| = \left|a_{ij} - \sqrt{\frac{\sum_{j=1}^{m} \left(a_{ij} - \underline{a_i}\right)}{n-1}}\right| \tag{2}$$

where σ_i - standard deviation of the *i*-th cybersecurity indicator;

$\underline{a_i}$ - arithmetic mean of the *i*-th cybersecurity indicator;

2) the ratio of a single value and the number of relevant indicators of cybersecurity is used as a constant value of the indicator of the degree of functional dependence (1). Considering these assumptions, formula (1) takes the form:

$$IS_j = \prod_{i=1}^{n} \left[a_{ij} - \left|a_{ij} - \sqrt{\frac{\sum_{j=1}^{m} \left(a_{ij} - \underline{a_i}\right)}{n-1}}\right|\right]^{1/n} \tag{3}$$

where n - the number of relevant indicators characterizing cybersecurity.

Stage 2. Relevant indicators characterizing the ability of countries to counteract financial fraud are determined by applying sigma-limited parameterization and Pareto optimization. We choose the integral cybersecurity index determined by the Sundarovsky method as an effective factor and indicators characterizing the ability of countries to counteract financial and cyber threats as factors of influence. Sigma-limited parametrization is performed in the form of a one-dimensional test of significance of the influence of indicators on the effective factor, and Pareto optimization is performed by constructing a Pareto diagram of t-values.

Stage 3. A non-linear regression model is built, which describes the dependence of the integral cybersecurity index on the relevant predictors identified at stage 2, and insignificant parameters are eliminated step-by-step. A combination of logarithmic and

quadratic functions as well as the multiplicative dependence of the selected indicators should be considered in this process with a view to the following bifurcation analysis of the maturity of the current system for combating financial and cyber fraud and the construction of its phase portraits.

Stage 4. A bifurcation analysis of the maturity of the current CFCF system is conducted and phase portraits of its "maturity" are constructed. This requires intermediate calculations involving the apparatus of differential calculus in order to determine partial derivatives of the function of the dependence of the integral cybersecurity index on relevant predictors and to create a system of differential equations that will serve as the basis for further analysis of the dynamic stability of the system.

Stage 5. A non-linear regression model of the dependence of the integral cybersecurity index on relevant predictors is built using a combination of power, trigonometric and multiplicative dependence of indicators with a view to conducting a bifurcation analysis of the equilibrium states of the current CFCF system and constructing its phase portraits.

Stage 6. A bifurcation analysis of the maturity of the current CFCF system phase portraits of its "equilibrium states" are constructed. This stage is performed similarly to stage 4. .

3.2. Data

To assess the maturity of thecurrent CFCF system, input data from 76 countries were collected and systematized according to two sets of indicators for 2018. One set describes the level of cybersecurity in each country at the national and global levels, and the level of its digitalization and informatization. They relate to the global cybersecurity system of world countries. The second set of indicators characterizes each country's attractiveness for money laundering and is used to make conclusions about its ability to counteract financial threats associated with money laundering and terrorist financing at the macro level. They relate to the global system of combating financial fraud in world countries. Five indicators are included in the first group (e-Governance Academy Foundation, 2022): the Global Cybersecurity Index (GCI), the ICT Development Index (ICT DI), the Network Readiness Index (NRI), the National Cyber Security Index (NCSI), and the Digital Development Level (DDL). The second set includes the Political Stability Index (PSI), the Government Efficiency Index (GEI), the Corruption Perception Index (CPI) (The GlobalEconomy, 2022), the Ease of Doing Business Index (EDB), the Crime Index (CI) (The World Bank, 2022), the Global Terrorism Index (GTI) (OCHA, 2018), and the Financial Secrecy Index (FSI) (Netzwerk Steuergerechtigkeit, 2022).

4. Empirical Results

4.1. Results of Data Analysis

It is necessary to identify causal relationships among the indicators of cybersecurity and indicators that characterize the ability of countries to counteract financial crimes. With this end in mind, a canonical analysis using the Statistica analytical package was conducted and its results are presented in Table 1.

Table 1. Results of the canonical analysis of cause-and-effect relationships between the indicators of cybersecurity and those characterizing countries' ability to counteract financial fraud

Variable	Left Set	Right Set
Variance extracted	100.00%	86.67%
Total redundancy	65.51%	49.39%
Variable 1	Global Cybersecurity Index	Political Stability Index
Variable 2	ICT Development Index	Government Effectiveness Index
Variable 3	Network Readiness Index	Ease of Doing Business
Variable 4	National Cybersecurity Index	Crime Index
Variable 5	Digital Development Level	Corruption Perceptions Index
Variable 6	-	Global Terrorism Index
Variable 7	-	Financial Secrecy Index
Canonical R	0.91	
Chi-sqr(35)	196.50	
p	0.0000	

Source: authors' calculations based on Kuzmenko, Yarovenko and Radko (2021).

As can be seen, 65.51% of the variance in the cybersecurity indicators is explained by the indicators describing countries' ability to combat financial crime. At the same time, only 49.39% of the variance in the indicators characterizing countries' ability to counteract financial threats is explained by the cybersecurity indicators. In addition, the share of variance (variability) explained by the indicators of cybersecurity is 100%, while the share of variance explained by the indicators describing countries' ability to counter financial threats is 86.67%. This means that the latter ones can be treated as the cause, while the former ones as the effect. The canonical correlation R=0.91, which corresponds to the correlation between the first canonical variables, is equal to the maximum canonical root. Its value indicates a strong relationship between groups of variables. The significance of the canonical correlation coefficient is confirmed by the values Chi-Square=196.5 and the level p=0.00.

We optimize the input data array, for which we conduct Chi-Square tests for the statistical significance of canonical roots (Table 2). The first three canonical roots can

be considered statistically significant since their values do not exceed the maximum allowable level of 0.05. Roots three and four have a canonical R-sqr value approaching zero and a p-value greater than 0.05, which means they are not statistically significant. Therefore, the first three canonical roots are considered at the next stage when the input data array is optimized.

Table 2. Chi-Square tests of canonical roots

Root Removed	Canonical R	Canonical R-sqr	Chi-sqr.	df	p	Lambda Prime
0	0.9126	0.8328	196.4981	35	0.0000	0.0568
1	0.6730	0.4530	73.9741	24	0.0000	0.3396
2	0.5662	0.3206	32.6488	15	0.0053	0.6209
3	0.2727	0.0744	6.1705	8	0.6281	0.9139
4	0.1128	0.0127	0.8765	3	0.8311	0.9873

Source: authors' calculations based on Kuzmenko, Yarovenko and Radko (2021).

To optimize the array of input data, we conduct a correlation analysis of both sets of indicators (of cybersecurity and of countries' ability to counter financial and cyber fraud). The correlation matrix of cybersecurity indicators is presented in Table 3. The resulting values indicate a significant correlation between the ICT Development Index and the Digital Development Level (the value of the correlation coefficient is 0.96). To optimize the set of input indicators in terms of cybersecurity characteristics, one of the most collinear indicators is removed from further calculations.

Table 3. Correlation matrix of a set of cybersecurity indicators

Variables	GCI	ICT DI	NRI	NCSI	DDL
GCI	1.0000	0.5358	0.7114	0.7094	0.5792
ICT DI	0.5358	1.0000	0.5834	0.6430	0.9607
NRI	0.7114	0.5834	1.0000	0.6813	0.6467
NCSI	0.7094	0.6430	0.6813	1.0000	0.6547
DDL	0.5792	0.9607	0.6467	0.6547	1.0000

Source: authors' calculations based on Kuzmenko, Yarovenko and Radko (2021).

To decide which indicator should be left in the input data array and which should be deleted, we consider the factor structure for the first three statistically significant canonical roots, selected using a piecewise linear plot and Chi-Square tests (Table 4).

Table 4. Factor structure of a set of cybersecurity indicators

Variables	Root 1	Root 2	Root 3	Root 4	Root 5
GCI	0.7935	-0.5738	0.0325	-0.1962	-0.0389
ICT DI	0.8712	0.1721	-0.3910	0.2355	-0.0550
NRI	0.8026	-0.2408	0.3794	0.3538	0.1697
NCSI	0.7257	-0.2962	-0.2189	0.0341	0.5801
DDL	0.9428	0.2574	-0.1977	0.0756	0.0015

Source: authors' calculations based on Kuzmenko, Yarovenko and Radko (2021).

Based on the analysis of the data in Table 4 it can be concluded that the indicator of the Digital Development Level has a more significant impact and should therefore be retained for further calculations.

Let us now consider the correlation matrix of the indicators describing countries' ability to counter financial and cyber fraud (Table 5).

Table 5. Correlation matrix of indicators describing countries' ability to counteract financial and fraud

Variables	PSI	GEI	EDB	CI	CPI	GTI	FSI
PSI	1.0000	0.6575	0.4557	-0.4952	0.7503	-0.6489	0.1353
GEI	0.6575	1.0000	0.8029	-0.6215	0.9037	-0.0476	0.4352
EDB	0.4557	0.8029	1.0000	-0.5826	0.6465	0.0023	0.2687
CI	-0.4952	-0.6215	-0.5826	1.0000	-0.5570	0.1732	-0.2272
CPI	0.7503	0.9037	0.6465	-0.5570	1.0000	-0.1809	0.3449
GTI	-0.6489	-0.0476	0.0023	0.1732	-0.1809	1.0000	0.2143
FSI	0.1353	0.4352	0.2687	-0.2272	0.3449	0.2143	1.0000

Source: authors' calculations based on Kuzmenko, Yarovenko and Radko (2021).

As can be seen, there is a significant correlation between the Government Efficiency Index and the Corruption Perception Index, as evidenced by the value of the correlation coefficient of 0.904. To optimize the set of input indicators in terms of countries' ability to counteract financial and cyber fraud, one of the collinear indicators is removed from further calculations.

To decide which of the two indicators (Government Efficiency Index or Corruption Perception Index) should be retained in the input data array and which should be

deleted, we consider the factor structure for the first three statistically significant canonical roots (Table 6). It can be concluded that the Government Efficiency Index has a more significant effect, which is why it is retained for further calculations.

Table 6. Factor structure of indicators of countries' ability to counteract financial and cyber fraud

Variables	Root 1	Root 2	Root 3	Root 4	Root 5
PSI	0.4314	0.6131	-0.5319	0.1180	0.0254
GEI	0.9545	0.1915	-0.1801	0.0406	-0.1027
EDB	0.8542	-0.2170	-0.2463	0.1014	0.2660
CI	-0.5569	0.0130	0.6724	-0.1198	-0.1878
CPI	0.8162	0.5048	-0.2211	-0.1246	-0.0019
GTI	0.1495	-0.6210	0.3207	-0.6026	-0.2745
FSI	0.5055	0.0899	0.3227	-0.3200	0.2829

Source: authors' calculations based on Kuzmenko, Yarovenko and Radko (2021).

4.2. Calculations Results

In the first stage, calculations were performed using formula (3). Their results are presented in Appendix, where the values in the IS column correspond to effective values of the integral cybersecurity index determined by the Sundarovsky method.

In the second stage, sigma-limited parametrization and Pareto optimization were carried out using the Statistica analytical package. The results are shown in Figures 1 and 2.

	Univariate Tests of Significance for IS (Spreadsheet1.sta) Sigma-restricted parameterization Effective hypothesis decomposition				
Effect	SS	Degr. of Freedom	MS	F	p
Intercept	15,932	1	15,932	0,19911	0,656838
Political stability index	60,262	1	60,262	0,75310	0,388504
Government effectiveness index	651,476	1	651,476	8,14157	0,005706
Ease of doing business	1068,591	1	1068,591	13,35430	0,000499
Crime Index	197,796	1	197,796	2,47187	0,120474
Global Terrorism Index	185,399	1	185,399	2,31695	0,132540
Financial Secrece Index	63,668	1	63,668	0,79566	0,375494
Error	5521,278	69	80,019		

Figure 1. One-dimensional test of the significance of the influence of indicators of countries' ability to counteract financial fraud on the integral index of cybersecurity

Source: authors' calculations.

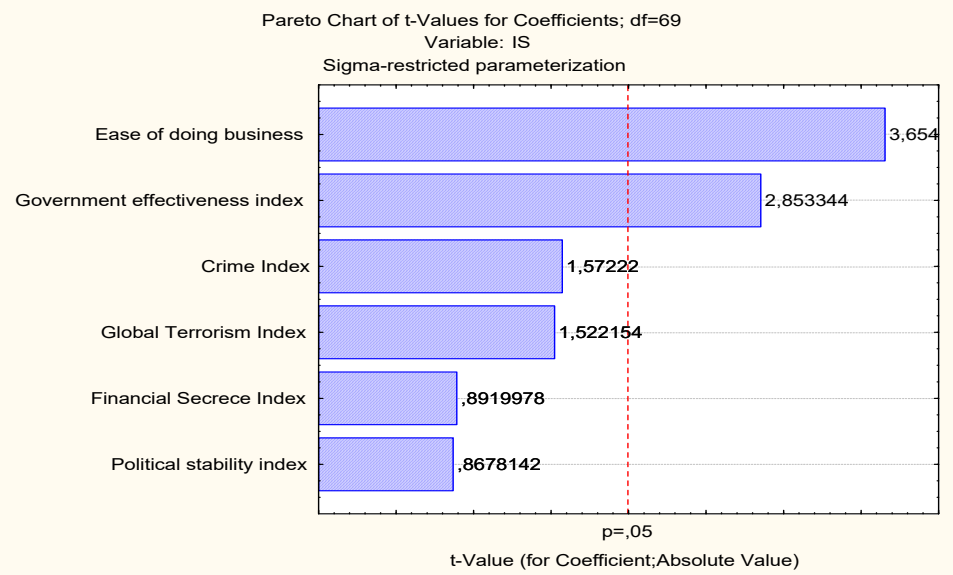

Figure 2. Pareto diagram of t-values of the significance of the influence of indicators of countries' ability to counteract financial fraud on the integral index of cybersecurity

Source: authors' calculations.

Based on the data in Figure 1, it can be argued that only two indicators have a statistically significant influence: the Government Efficiency Index and the Ease of Doing Business, since their significance levels for the Fisher criterion are less than 0.05. The Ease of Doing Business has the largest contribution to the overall model, as indicated by the largest sum of squared deviations SS (1068.59) and the smallest p-value of 0.000499. The next indicator with a statistically significant impact is the Government Efficiency Index, with SS=651.48 and the p-level of 0.0057. A three-dimensional projection is required to build a phase portrait, showing different variations: a node, a focus or a saddle.

The node corresponds to the most balanced system's state characterizing its ability to be in balance and maintain its structure. That is, the components of the cyber security system and the system of countering financial crimes are at the same level of development, which enables their easy integration. A node can be stable or unstable. Stability means the system's ability to return to a state of equilibrium after being brought out of it under the influence of various factors. For example, the emergence of armed conflicts in one country, which will increase the number of migrants, should not significantly affect the rise in crime in the countries where they migrate. Instability is the opposite of stability. A focus also corresponds to a balanced state, but its

achievement is more complicated than a node. It can also be stable and unstable. The saddle suits only for unbalanced systems, for which it is impossible to ensure the convergence of the cyber security system and the system for combating financial crimes. Systems for which the phase portrait has the appearance of a “saddle” are immature, that is, not ready for the convergence of the cyber security system and the system for countering financial fraud. “Stable node” corresponds to mature systems, and “unstable node” is mature, but some of their components are unstable. "Stable focus" characterizes systems that are not yet mature enough but have fairly balanced elements. “Unstable focus” corresponds to insufficiently mature systems with individual unbalanced components.

The use of a two-dimensional space would complicate the interpretation of the results. For this reason, further calculations are made using three indicators. The third most important indicator of countries’ ability to combat financial fraud is the Crime Index. Although its p-value is equal to 0.12, meaning it is not statistically significant, its nonlinear combination will be used in further calculations, which will be significant for the model. The significance of the factors under consideration can be visually confirmed by the Pareto diagram of t-values showing which indicators of countries' ability to counteract financial threats have a statistically significant impact on the integral cybersecurity index (Figure 2). The Pareto diagram not only shows the statistically significant influence (regressors) of the integral cybersecurity index but also orders them by the power of influence. This statistical toolkit graphically interprets the 80/20 rule, highlighting 80% of the influential environmental factors, particularly the Government Efficiency Index, Ease of Doing Business Index, and the Crime Index, which are relevant and selected for further research.

In the third stage, the Statistica software package is used to determine the specification of the nonlinear regression dependence of the integral cybersecurity index on relevant predictors: the Government Efficiency Index, the Ease of Doing Business Index, the Crime Index. By applying the stepwise inclusion method, a statistically significant dependence is revealed in the form of a square root for the Government Efficiency Index, a logarithmic dependence for the Ease of Doing Business Index, and a quadratic dependence for the Crime Index Index (Figure 3). In the case of the Government Efficiency Index, owing to the presence of negative values in the input data, we consider the dependence of the integral cybersecurity index on this indicator only as part of a multiplicative dependence.

N=58	Beta	Std.Err. of Beta	B	Std.Err. of B	t(53)	p-level
Regression Summary for Dependent Variable: IS (Spreadsheet1.sta) R= ,80929115 R?= ,65495216 Adjusted R?= ,62891081 F(4,53)=25,150 p<,00000 Std.Error of estimate: 9,2027						
Intercept			-229,789	67,41833	-3,40840	0,001255
LN-V9	0,421814	0,111687	61,729	16,34451	3,77675	0,000404
SQRV8	0,401105	0,126867	17,088	5,40484	3,16163	0,002595
V10**2	-0,187681	0,088620	-0,003	0,00128	-2,11782	0,038898
1/V8	0,150132	0,093801	0,172	0,10727	1,60054	0,115423

Figure 3. Results of regression statistics of dependence of the integral cybersecurity index on relevant predictors: Government Efficiency Index, Ease of Doing Business Index, Crime Index

Source: authors' calculations.

Based on the results of the specification of the dependence of the integral cybersecurity index on relevant predictors, which is expressed as logarithmic, quadratic functions, and the multiplicative dependence of the three indicators, we formalize the indicated nonlinear dependence. The results are presented in Table 7.

Table 7. Results of statistical analysis of the dependence of the integral cybersecurity index on relevant predictors

Specification	Coefficients	Standard error	t-statistics	p-value	Lower 95%	Upper 95%
Y- cross section	-108.6929	56.5889	-1.9207	0.0587	-221.5009	4.1151
ln(EDI)	35.3774	13.2591	2.6682	0.0094	8.9459	61.8089
CI^2	-0.0019	0.0012	-1.6080	0.1122	-0.0037*	-0.00004*
GEI*EDI*CI	0.0028	0.0008	3.5848	0.0001	0.0012	0.0043

** The confidence level is 88%.*

Source: authors' calculations.

Based on data in Table 7 the following regression model can be formulated (4):

$$IS = -108.69 + 35.3774 \cdot \ln(EDI) - 0.00188 \cdot CI^2 + 0.00277 \cdot GEI \cdot EDI \cdot CI \quad (4)$$

where IS – the integral cybersecurity index;

GEI – the Government Efficiency Index,

EDI – the Ease of Doing Business Index,

CI – the Crime Index.

The statistical significance of ln(EDI) and GEI*EDI*CI was confirmed with p less than 0.05. The p-value for CI^2 exceeds 0.05, but this excess is not critical enough, so statistical significance can be defined for a confidence interval. It was found that the confidence interval with a probability of 88% does not contain a zero value, enabling the use of CI^2 to construct a phase portrait. The coefficient of determination for this model is 62.73%, while the value of the Fisher criterion of 40.40 exceeds the critically acceptable level.

In the fourth stage, the MathCAD application software package was used. The following analysis of the dynamic stability of a CFCF system and the construction of phase portraits of its/their maturity is based on the non-linear function (5), obtained based on the non-linear model (4):

$$f(gei, edi, ci) := -108.693 + 35.37739 \cdot \ln(edi) - 0.00188 \cdot ci^2 + 0.002774 \cdot gei \cdot edi \cdot ci \qquad (5)$$

Based on function (5), we model a system of differential equations (6) that characterize the behaviour of a dynamic CFCF system:

$$\begin{aligned} &\frac{d}{dgei} f(gei, edi, ci) \rightarrow 0.002774 ci \cdot edi \\ &\frac{d}{dedi} f(gei, edi, ci) \rightarrow \frac{35.37739}{edi} + 0.002774 ci \cdot gei \\ &\frac{d}{dci} f(gei, edi, ci) \rightarrow -0.00376 ci + 0.002774 edi \cdot gei \end{aligned} \qquad (6)$$

The above three differential equations (6) can be used to establish relationships between variables GEI (Government Performance Index), EDI (Ease of Doing Business), CI (Crime Index) and their first partial derivatives $\frac{d}{dgei} f(gei, edi, ci), \frac{d}{dedi} f(gei, edi, ci), \frac{d}{dci} f(gei, edi, ci)$.

Based on the non-linear approach underlying bifurcation theory, we construct phase portraits of the integral cybersecurity index, where phase trajectories are represented as projections on pairwise planes: the Government Efficiency Index – the Ease of Doing Business, the Ease of Doing Business – the Crime Index,

the Government Efficiency Index – the Crime Index. Equations (7) were constructed using the MathCad mathematical analysis software:

$$
\begin{aligned}
&\mathrm{Faza}(gei0, edi0, ci0, dt, N) := \left| \begin{array}{l}
\left(gei_0 \leftarrow gei0 \quad edi_0 \leftarrow edi0 \quad ci_0 \leftarrow ci0\right) \\
\text{for } k \in 0..N \\
\quad \left| \begin{array}{l}
fff \leftarrow f\left(gei_k, edi_k, ci_k\right) \\
gei_{k+1} \leftarrow \left[gei_k + dt \cdot \left(0.002774\, ci_k \cdot edi_k\right)\right] \\
edi_{k+1} \leftarrow \left[edi_k + dt \cdot \left(\dfrac{35.37739}{edi_k} + 0.002774\, ci_k \cdot gei_k\right)\right] \\
ci_{k+1} \leftarrow \left[ci_k + dt \cdot \left(-0.00376\, ci_k + 0.002774\, edi_k \cdot gei_k\right)\right]
\end{array} \right. \\
(gei \quad edi \quad ci)
\end{array} \right. \qquad (7)
\end{aligned}
$$

To visualize formula (7), which represents "phase portraits" of the state of a CFCF system, and subsequently identify its state as one of the three types (saddle, node, or focus), we consider various possible values as factors (Government Efficiency Index, Ease of Doing Business, Crime Index), and the value of the function of the integral cybersecurity index with a given level of accuracy based on the specified number of implementation points:

$$
\begin{aligned}
(gei1 \quad edi1 \quad ci1) &:= \mathrm{Faza}(1.6, 80, 42, 0.01, 100) \\
(gei2 \quad edi2 \quad ci2) &:= \mathrm{Faza}(1.45, 78, 20, 0.01, 100) \\
(gei3 \quad edi3 \quad ci3) &:= \mathrm{Faza}(0.18, 68, 36, 0.01, 100) \\
(gei4 \quad edi4 \quad ci4) &:= \mathrm{Faza}(0.43, 56, 51, 0.01, 100) \\
(gei5 \quad edi5 \quad ci5) &:= \mathrm{Faza}(-0.32, 50, 52, 0.01, 100) \\
(gei6 \quad edi6 \quad ci6) &:= \mathrm{Faza}(-0.45, 57, 70, 0.01, 100) \qquad (8)
\end{aligned}
$$

We plug the actual values of the input data (formulas 8) into relationships in order to formalize the phase portraits (7). As a result, we visualize (the first ratio of formulas (8)) the nonlinear dependence of the integral cybersecurity index on relevant factors in the pairwise planes "Government Efficiency Index – Ease of Doing Business" (left fragment of Figure 4) and "Ease of Doing Business - Crime Index" (right fragment of Figure 4).

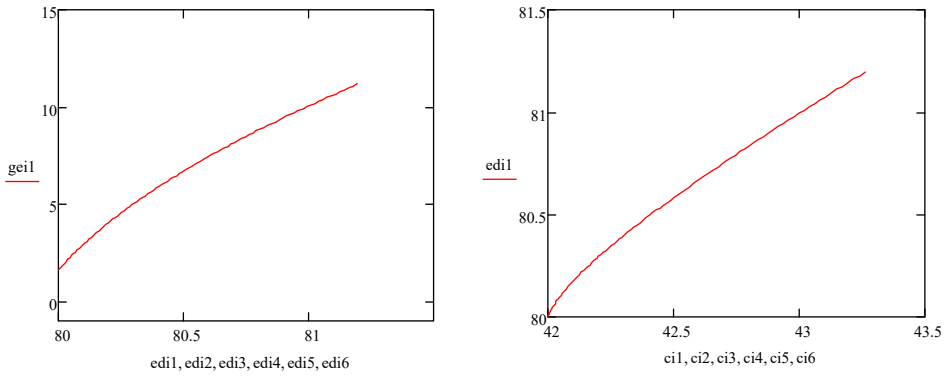

Figure 4. Curves of nonlinear dependence of the integral cybersecurity index on the relevant factors in the planes "Government Efficiency Index - Ease of Doing Business" (left box) and "Ease of Doing Business – Crime Index" (right box)

Source: authors' calculations.

Let us now analyse the phase portraits of a dynamic CFCF system on the entire set of values of input indicators (formulas (8)). First, we consider the system's phase portrait represented in the plane "Government Efficiency Index – Ease of Doing Business" (Figure 5). This phase portrait shows the bifurcation type classified as "unstable focus", i.e., the unstable state of the system. If one parameter changes significantly and the value of another parameter is fixed, the system is in a state of non-equilibrium.

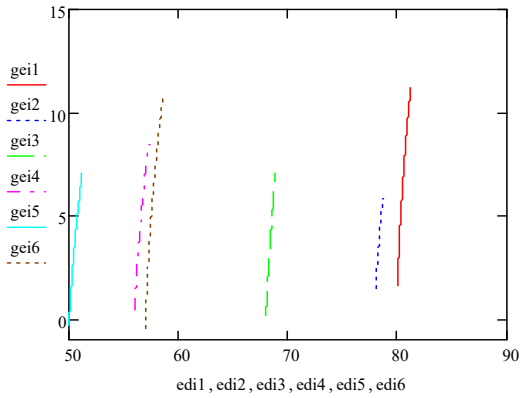

Figure 5. Phase portrait ("unstable focus") of a dynamic CFCF system in a state of non-equilibrium represented in the plane "Government Efficiency Index – Ease of Doing Business"

Source: authors' calculations.

Let us now consider the phase portrait of a dynamic CFCF system represented in the plane "Ease of Doing Business – Crime Index" (Figure 6). Once again, it is in a state of non-equilibrium, classified as "unstable focus".

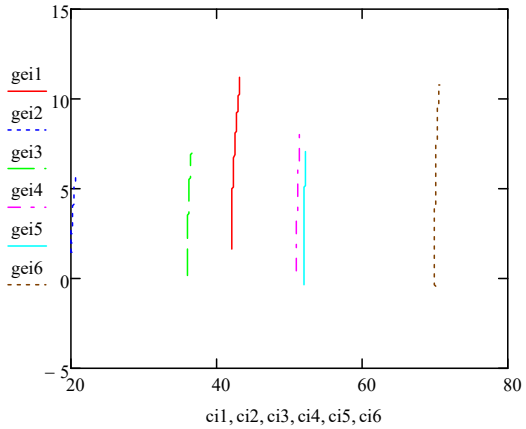

Figure 6. Phase portrait ("unstable focus") of a dynamic CFCF system in a state of non-equilibrium represented in the plane "Ease of Doing Business – Crime Index"

Source: authors' calculations.

The non-equilibrium state of a dynamic CFCF system in the form of a phase portrait classified as "unstable node" can be observed in the plane "Government Efficiency Index – Crime Index", which is shown in Figure 7.

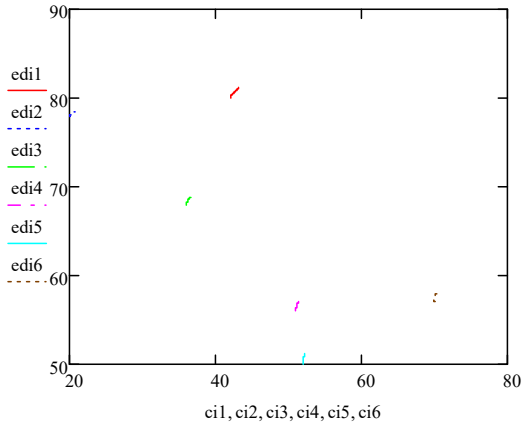

Figure 7. Phase portrait ("unstable node") of a dynamic CFCF system in a state of non-equilibrium represented in the plane "Government Efficiency Index – Crime Index"

Source: authors' calculations.

Bifurcation analysis of the maturity of the current global CFCF system and its phase portraits classified as "unstable focus" and "unstable node" (Figures 5-7) indicate the system under consideration is in a state of maturity, but an incomplete balance of the components in the plane of "Government Efficiency Index – Ease of Doing Business" and "Ease of Doing Business – Crime Index", as well as insufficient maturity and incomplete balance of the "Government Efficiency Index – Crime Index" elements.

In the fifth stage, we determine the specification of the non-linear regression dependence of the integral cybersecurity index on relevant predictors: the Government Efficiency Index, Ease of Doing Business, and the Crime Index. We define the specification from the first relevant feature – the Government Efficiency Index. The integral cybersecurity index determined by the Sundarovsky method is chosen as the resultant feature, and the polynomial (second and third steps), inverse, trigonometric dependencies of the Government Efficiency Index are chosen as factorial ones. The results of the regression analysis are presented in Table 8.

Table 8. Results of statistical analysis of the dependence of the integral cybersecurity index on the Government Efficiency Index

Specification	Coefficients	Standard error	t-statistics	p-value	Lower 95%	Upper 95%
Y- cross section	47.8568	43.4523	1.1014	0.2746	-38.8281	134.5417
GEI*EDI*CI	0.0004	0.0015	0.2402	0.8109	-0.0026	0.0033
GEI^2	-5.1192	18.2560	-0.2804	0.7800	-41.5390	31.3006
GEI^3	1.7633	2.0450	0.8623	0.3915	-2.3163	5.8428
1/GEI	0.08037	0.09631	0.83447	0.40690	-0.1118	0.2725
Sin(GEI)	14.1229	6.3637	2.21929	0.0298	1.4276	26.8182
Cos(GEI)	-16.857	43.9954	-0.3832	0.7028	-104.625	70.9114

Source: authors' calculations.

Given the p-value of 0.0298 (Table 8), the variable sin(GEI) is statistically significant at the alpha level of 0.05. Therefore, a sinusoid is selected as a specification of the dependence of the integral cybersecurity index on the government efficiency index in further calculations.

Next we define the specification of the non-linear dependence of the integral cybersecurity index on the second relevant feature – the Ease of Doing Business. As in the previous case, we treat the integral cybersecurity index determined by the

Sundarovsky method as an effective feature, and polynomial (second and third steps), inverse, logarithmic, square root, trigonometric dependencies of the Ease of Doing Business as factorial ones. Applying the regression analysis tools, we obtain the result presented in Table 9.

Given the p-values in Table 9, it can be argued that there is no statistically significant variable at the alpha level of 0.05. However, a confidence interval calculated for the cubic dependence of the performance attribute on the Ease of Doing Business variable (the smallest p-value equal to 0.1773) does not contain a zero value with a relatively high probability of 82%, which means it can be regarded as statistically significant under the given conditions. Therefore, a cubic dependence is selected as the specification of the dependence of the integral cybersecurity index on the Ease of Doing Business in further calculations.

Table 9. Results of statistical analysis of the dependence of the integral cybersecurity index on the Ease of Doing Business

Specifi-cation	Coefficients	Standard error	t-statistics	P-value	Lower 95%	Upper 95%
Y-cross section	-215579.91	167427.8	-1.2876	0.202	-549676.79	118516.97
EDI^2	5.39	4.03	1.3386	0.185	-2.65	13.44
EDI^3	-0.02	0.01	-1.3634	0.177	-0.0373*	-0.0001*
1/EDI	890050.46	692798.4	1.2847	0.203	-492407.17	2272508.10
ln(EDI)	99794.06	77102.97	1.2943	0.200	-54062.51	253650.63
$EDI^{0,5}$	-28814.34	22124.27	-1.3024	0.197	-72962.64	15333.95
Sin(EDI)	0.24	1.78	0.1359	0.892	-3.31	3.80
Cos(EDI)	0.86	1.62	0.5323	0.596	-2.36	4.08

** The confidence level is 82%.*

Source: authors' calculations.

Finally, we define the specification of the nonlinear dependence of the integral cybersecurity Index on the third relevant feature – the Crime Index. We treat the integral cybersecurity index determined by the Sundarovsky method as a resultant feature, and polynomial (second and third degree), inverse, trigonometric dependencies of the Crime Index as factorial ones. Applying the regression analysis tools, we obtain the result presented in Table 10.

Table 10. Results of statistical analysis of the dependence of the integral cybersecurity index on the Crime Index

Specification	Coefficients	Standard error	t-statistics	P-value	Lower 95%	Upper 95%
Y-cross section	7828.5624	5651.85	1.3851	0.1705	-3449.52	19106.65
CI^2	-0.5685	0.40	-1.4118	0.1626	-1.37	0.24
CI^3	0.0027	0.00	1.3904	0.1690	-0.00	0.01
1/CI	-24362.1135	18011.51	-1.3526	0.1807	-60303.52	11579.29
ln(CI)	-4624.8443	3329.88	-1.3889	0.1694	-11269.52	2019.83
$CI^{0,5}$	1679.5597	1203.49	1.3956	0.1674	-721.97	4081.08
Sin(CI)	-3.2419	2.36	-1.3765	0.1732	-7.94	1.46
Cos(CI)	5.7206	2.37	2.4112	0.0186	0.99	10.45

Source: authors' calculations.

Given the p-value of 0.0186 (Table 10), the variable Cos(CI) is statistically significant at the alpha level of 0.05. Therefore, a cosine wave is selected as the specification of the dependence of the integral cybersecurity Index on the Crime Index in further calculations.

Thus, having defined the specification of the dependence of the integral cybersecurity index on relevant predictors (Government Efficiency Index, Ease of Doing Business, Crime Index) in the form of a sinusoid, cubic dependence, cosine wave, respectively, and also introducing an additional variable of multiplicative influence on the performance feature of all three relevant factors, we construct a nonlinear regression dependence. The results are presented in Table 11.

Table 11. Results of statistical analysis of the dependence of the integral cybersecurity index on relevant predictors

Specification	Coefficients	Standard error	t-statistics	P-value	Lower 95%	Upper 95%
Y-cross section	10.8979	4.1283	2.6398	0.0102	2.6663	19.1294
Sin(GEI)	9.9771	5.0902	1.9601	0.0539	-0.1724	20.1266
EDI^3	0.0001	0.0000	5.6383	0.0000	0.0001	0.0001
Cos(CI)	3.4013	1.6051	2.1191	0.0376	0.2009	6.6017
GEI*EDI*CI	-0.0006	0.0012	-0.4738	0.6371	-0.0030	0.0018

Source: authors' calculations.

Based on the coefficients in Table 11, we construct a regression dependence of the integral cybersecurity index on the relevant predictors: Government Efficiency Index, Ease of Doing Business, Crime Index in the form of the following equation:

$$IS = 10{,}8989 + 9{,}9771 \cdot \quad sin\,(GEI) \; + 0.00008 \cdot EDI^3 + 3.4013 \cdot cos\,(CI) \; - 0.00057 \cdot GEI \cdot EDI \cdot CI \tag{9}$$

The validity and accuracy of equation (9) is confirmed based on the following criteria. The coefficients of the variables are statistically significant, since their p-values are below the alpha level of 0.05, except the coefficient before the variable of the multiplicative influence of the three factors. We retain this variable in the model in the bifurcation analysis of the maturity of the current CFCF system and take into account when building phase portraits of its "equilibrium states" since the multiplicative effect of the three factors is required in a qualitative analysis of bifurcations. The coefficient of determination is equal to 70.59%, which means that 70.59% of the variation of the effective feature of the integral cybersecurity index is explained by the variation of the selected factor features, which is a good result.

In the sixth stage of our study, we construct a nonlinear function (10) using equation (9):

$$f(gei, edi, ci) \coloneqq 10.8978783 + 9.977087 sin\,(gei) \; + 7.643510 \cdot 10^{-5} \cdot (edi^3) + 3.40130281 cos\,(ci) - 0.00057478 gei \cdot edi \cdot ci \tag{10}$$

Based on function (10), we model a system of differential equations that characterize the behaviour of a dynamic CFCF system to construct phase portraits of "equilibrium states":

$$\frac{d}{dgei} f(gei, edi, ci) \rightarrow 9.97708769 \cdot \cos(gei) + -0.00057478 \cdot ci \cdot edi$$

$$\frac{d}{dedi} f(gei, edi, ci) \rightarrow 0.000229305 \cdot edi^2 + -0.00057478 \cdot ci \cdot gei$$

$$\frac{d}{dci} f(gei, edi, ci) \rightarrow -3.40130281 \cdot \sin(ci) + -0.00057478 \cdot edi \cdot gei \tag{11}$$

The above three differential equations (11) are used to established relationships between variables GEI (Government Efficiency Index), EDI (Ease of Doing Business), CI (Crime Index) and their first partial derivatives $\frac{d}{dgei} f(gei, edi, ci), \frac{d}{dedi} f(gei, edi, ci), \frac{d}{dci} f(gei, edi, ci)$.

Taking the non-linear approach underlying bifurcation theory, we construct phase portraits of the "equilibrium states" of the integral cybersecurity index where phase trajectories are represented as projections on pairwise planes: the Government Efficiency Index – the Ease of Doing Business, the Ease of Doing Business – the Crime Index, the Government Efficiency Index – the Crime Index. The phase portraits are constructed on the basis of the system of differential equations (12) using the MathCad mathematical analysis software:

$$
\begin{aligned}
&\text{Faza}(gei0, edi0, ci0, dt, N) := \\
&\quad \left(gei_0 \leftarrow gei0 \quad edi_0 \leftarrow edi0 \quad ci_0 \leftarrow ci0\right) \\
&\quad \text{for } k \in 0..N \\
&\quad\quad fff \leftarrow f\left(gei_k, edi_k, ci_k\right) \\
&\quad\quad gei_{k+1} \leftarrow \left[gei_k + dt\cdot\left(9.97708769\cos\left(gei_k\right) + -0.00057478ci_k\cdot edi_k\right)\right] \\
&\quad\quad edi_{k+1} \leftarrow \left[edi_k + dt\cdot\left[0.000229305\left(edi_k\right)^2 + -0.00057478ci_k\cdot gei_k\right]\right] \\
&\quad\quad ci_{k+1} \leftarrow \left[ci_k + dt\cdot\left(-3.40130281\sin\left(ci_k\right) + -0.00057478edi_k\cdot gei_k\right)\right] \\
&\quad (gei \quad edi \quad ci)
\end{aligned}
\tag{12}
$$

To visualize the phase portraits of the "equilibrium states" of the CFCF system using formula (12) and then identify its state as one of the three types (saddle, node, or focus), we consider various possible values of the three factors (Government Efficiency Index, Ease of Doing Business, Crime Index) and the value of the function that describes the integral Cybersecurity Index with a given level of accuracy based on the specified number of implementation points:

$$
\begin{aligned}
(gei1 \quad edi1 \quad ci1) &:= \text{Faza}(1.6, 80, 42, 0.01, 100) \\
(gei2 \quad edi2 \quad ci2) &:= \text{Faza}(1.45, 78, 20, 0.01, 100) \\
(gei3 \quad edi3 \quad ci3) &:= \text{Faza}(0.18, 68, 36, 0.01, 100) \\
(gei4 \quad edi4 \quad ci4) &:= \text{Faza}(0.43, 56, 51, 0.01, 100) \\
(gei5 \quad edi5 \quad ci5) &:= \text{Faza}(-0.32, 50, 52, 0.01, 100) \\
(gei6 \quad edi6 \quad ci6) &:= \text{Faza}(-0.45, 57, 70, 0.01, 100)
\end{aligned}
\tag{13}
$$

We plug the actual values of the input data (formulas 13) into the relationships in order to formalize the phase portraits (12) and determine the equilibrium points represented in the plane "Government Efficiency Index – Ease of Doing Business" (Figure 8). The equilibrium state of the CFCF system corresponds to the following values of its parameters (the intersection points of the graphs shown in Figure 8): the Government Efficiency Index – 1.4838, Ease of Doing Business – 80.183.

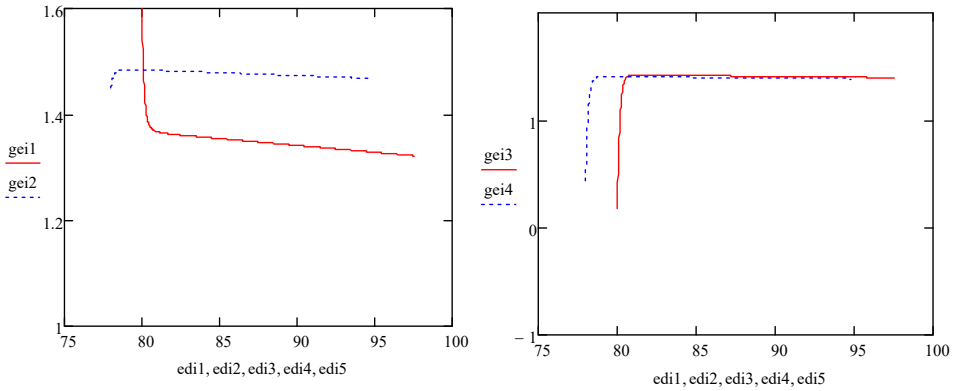

Figure 8. Equilibrium points of the CFCF system represented in the plane "Government Efficiency Index - Ease of Doing Business"

Source: authors' calculations.

Let us now analyse the phase portraits of the dynamic CFCF system on the entire set of values of input indicators (formulas (13)). We first consider the phase portrait of the system represented in the plane "Government Efficiency Index – Ease of Doing Business" (Figure 9). This phase portrait demonstrates the presence of an saddle point characterizing a non-equilibrium state of the CFCF system.

Moving on to the phase portrait represented in the "Ease of Doing Business – Crime Index" plane (Figure 10), we observe that it is in a non-equilibrium state classified as a "saddle". This type of bifurcation indicates an unstable state of the system, i.e., if one parameter changes significantly and the value of another parameter is fixed, the system is in a state of non-equilibrium.

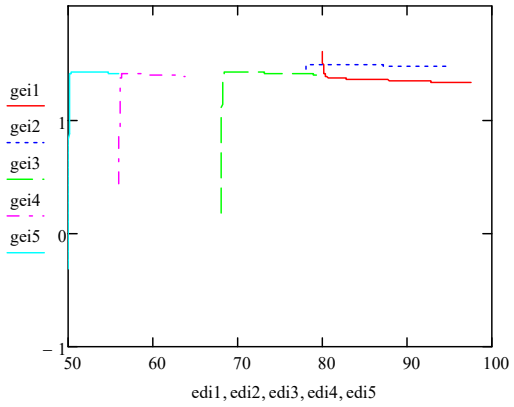

Figure 9. Phase portrait ("saddle") of the dynamic CFCF system represented in the plane "Government Efficiency Index - Ease of Doing Business"

Source: authors' calculations.

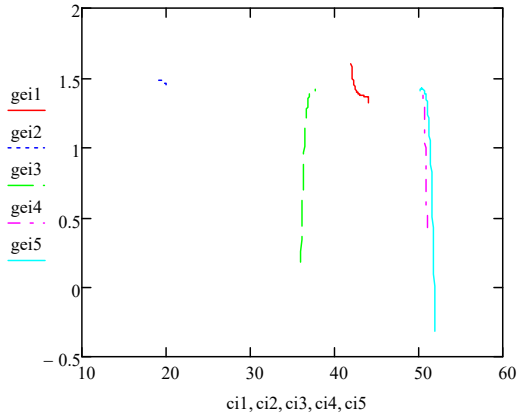

Figure 10. Phase portrait ("saddle") of the CFCF dynamic system, which is in a non-equilibrium state, represented in the plane "Ease Of Doing Business – Crime Index"

Source: authors' calculations.

The non-equilibrium state of the dynamic CFCF system as evidenced by a phase portrait classified as "saddle" can also observed in the plane "Government Efficiency Index – Crime Index", which is shown in Figure 11.

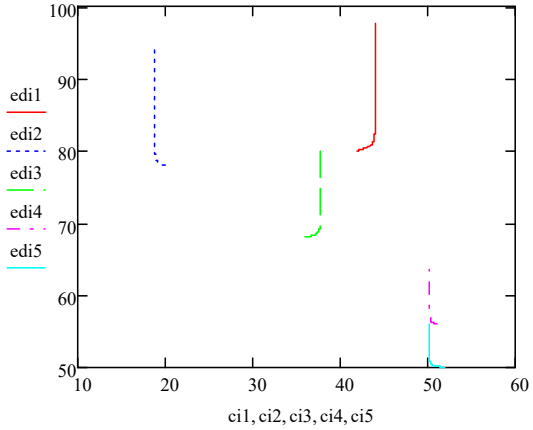

Figure 11. Phase portrait ("saddle") of the dynamic CFCF system, which is in a non-equilibrium state, represented in the plane "Government Efficiency Index – Crime Index"

Source: authors' calculations.

The above bifurcation analysis of the maturity of the current CFCF system based on its phase portraits (Figures 9–11) reveals states of non-equilibrium classified as "saddle" for all projections – "Government Efficiency Index - Ease of Doing Business", "Ease Of Doing Business – Crime Index" and "Government Efficiency Index – Crime Index". .

5. Conclusions

The purpose of the above analysis was to assess the maturity of the global system for combating financial and cyber fraud with a view to determining its readiness for integration at different levels of state management. Since the studied system is dynamic, i.e. change under the influence of various external and internal factors, a bifurcation analysis was performed involving the construction of phase portraits of its maturity and equilibrium. The resulting phase portraits of the CFCF system's "maturity" were classified as "unstable focus" when represented in the planes "Ease of Doing Business – Crime Index" and "Government Efficiency Index – Ease of Doing Business." A phase portrait classified as "unstable node" was obtained for the plane "Government Efficiency Index – Crime Index".

The results show that the global CFCF system is quite mature according to obtained node and focus phase portraits but unstable. That is, it is significantly affected by the level of crime in a given country, the inefficiency of government decisions, and the lack of opportunities for business development and organization. However, factors such as financial secrecy, political stability, the level of corruption and terrorism do not cause fluctuations. They do not lead to significant changes in the cybersecurity system. The CFCF system based on the integration of cybersecurity and combating financial fraud systems, above all, requires legislative changes, which should improve the living standards of the population and reduce crime in general and financial and cyber fraud in particular. Another strategic factor which must be considered is the creation of opportunities for business development also positively affects the countries' economic processes and foster their economic growth.

The proposed methodology makes it possible to determine points where the system's equilibrium will be reached, but phase portraits classified as "saddle" points indicate that the CFCF system cannot reach a state of equilibrium. (constructed in the context of the respective threeplanes). Changing only one of the parameters will affect this state, provided that another factor has a fixed value. The preliminary conclusions about the system's instability and its lack of its equilibrium are thus confirmed.

To sum up, the detected states of maturity and equilibrium of the CFCF system indicate its sufficient level of maturity, but at the same time, its inability to recover in the planes of "Government Efficiency Index - Ease of Doing Business", "Ease Of Doing Business - Crime Index" and "Government Efficiency Index - Crime Index". That is, there is a need to improve the processes of business regulation and state policy formation in the world countries to counter financial and cybercrimes. In the future, this approach can be recommended to relevant government agencies to form initiatives for developing public financial monitoring and national cybersecurity , as well as to international organizations to improve the strategy of global countermeasures against financial and cybercrimes.

Acknowledgement

This research was funded by the grant from the Ministry of Education and Science of Ukraine (No. s/r 0121U109559, 0121U100467).

References

Akhramovych, V., Shuklin, G., Pepa, Y., Muzhanova, T. and Zozulia, S., (2022). Devising a procedure to determine the level of informational space security in social networks considering interrelations among users. *Eastern-European Journal of Enterprise Technologies*, [e-journal], 1(9–115), pp. 63–74; 10.15587/1729-4061.2022.252135.

Amala Dhaya, M. D. and Ravi, R., (2021). Multi feature behavior approximation model based efficient botnet detection to mitigate financial frauds. *Journal of Ambient Intelligence and Humanized Computing*, [e-journal], 12(3), pp. 3799–3806; 10.1007/s12652-020-01677-w.

Aziz, R. M., Baluch, M. F., Patel, S. and Ganie, A. H., (2022). LGBM: a machine learning approach for Ethereum fraud detection. *International Journal of Information Technology* (Singapore), [e-journal]; 10.1007/s41870-022-00864-6

BBC, (2022). Ukraine cyber-attack: Russia to blame for hack, says Kyiv. [online] Available at: https://www.bbc.com/news/world-europe-59992531 [Accessed 31 May 2022].

Bystray, G. P., Lykov, I. A. and Nikulina, N. L., (2012). Risks assessment and forecasting long time rows of economic indicators. *Economy of Region*, [e-journal] 3, pp. 240–249; 10.17059/2012-3-24.

CyberPeace Institute, (2022). Ukraine: Timeline of Cyberattacks on critical infrastructure and civilian objects. [online] Available at: https://cyberpeaceinstitute.org/ukraine-timeline-of-cyberattacks/, [Accessed 31 May 2022].

Day, M.-Y., (2021). Artificial intelligence for knowledge graphs of cryptocurrency anti-money laundering in fintech. In: Proceedings of the 2021 IEEE/ACM International Conference on Advances in Social Networks Analysis and Mining, 13th IEEE/ACM International Conference on Advances in Social Networks Analysis and Mining, ASONAM 2021. Virtual, Online, 8 November 2021. New York: Association for Computing Machinery; 10.1145/3487351.3488415.

Deloitte, (2019). The connected defense: Elevating the fight against financial crime. Using 4IR technologies to prevent and detect the growing ecosystem of financial crime. [online] Available at: https://www2.deloitte.com/content/dam/Deloitte/nl/Documents/financial-services/deloitte-nl-fsi-elevating-the-fight-against-financial-crime.pdf, [Accessed 31 May 2022].

e-Governance Academy Foundation, (2022). National Cyber Security Index. [online] Available at: https://ncsi.ega.ee/ncsi-index/, [Accessed 31 May 2022].

Euronews, (2022). Ukraine's defence ministry and two banks targeted in cyberattack. [online] Available at: https://www.euronews.com/my-europe/2022/02/15/ukraine-s-defence-ministry-and-two-banks-targeted-in-cyberattack, [Accessed 31 May 2022].

FinCEN, (2009). Mortgage Loan Fraud Connections with Other Financial Crime: An Evaluation of Suspicious Activity Reports Filed By Money Services Businesses, Securities and Futures Firms, Insurance Companies and Casinos. [online] Available at: https://www.fincen.gov/sites/default/files/shared/ mortgage_fraud.pdf, [Accessed 31 May 2022].

Granados, O. and Garcia-Bedoya, O., (2022). Deep Learning-Based Facial Recognition on Hybrid Architecture for Financial Services. In S. Misra, A.K. Tyagi, V. Piuri, L. Garg, ed. 2022. Artificial Intelligence for Cloud and Edge Computing. Springer: Cham. pp. 51-70. 10.1007/978-3-030-80821-1_3.

Granados, O., Vargas, A., (2022). The geometry of suspicious money laundering activities in financial networks. EPJ Data Science, [e-journal], 11(1), article number 6; 10.1140/epjds/s13688-022-00318-w.

Hayble-Gomes, E., (2022). The use of predictive modeling to identify relevant features for suspicious activity reporting. Journal of Money Laundering Control, [e-journal] ahead-of-print; 10.1108/JMLC-02-2022-0034.

Idowu, B. A., Vaidyanathan, S., Sambas, A., Olusola, O. I. and Onma, O. S., (2018). A new chaotic finance system: Its analysis, control, synchronization and circuit design. In: V.-T. Pham, S. Vaidyanathan, C. Volos, T. Kapitaniak, ed. 2018. Nonlinear Dynamical Systems with Self-Excited and Hidden Attractors. Springer: Cham, pp. 271–295; 10.1007/978-3-319-71243-7_12.

Krebsonsecurity, (2022). Report: Recent 10x Increase in Cyberattacks on Ukraine. [online] Available at: https://krebsonsecurity.com/2022/03/report-recent-10x-increase-in-cyberattacks-on-ukraine/, [Accessed 31 May 2022].

Kuzmenko, O., Yarovenko, H. and Radko, V., (2021). Poperednii analiz protsesu konverhentsii system kiberbezpeky ta finansovoho monitorynhu krain *[Preliminary analysis of the convergence process of cyber security systems and financial monitoring of countries. Economy and society]*, [e-journal], 32; 10.32782/2524-0072/2021-32-37. [in Ukrainian].

Li, H., Wong, M.-L., (2021). Grammar-Based Multi-objective Genetic Programming with Token Competition and Its Applications in Financial Fraud Detection. *Natural Computing Series*, [e-journal], pp. 259–285; 10.1007/978-3-030-79553-5_11.

Mahootiha, M., Golpayegani, A.H. and Sadeghian, B., (2021). Designing a New Method for Detecting Money Laundering based on Social Network Analysis. In: 26th International Computer Conference, Computer Society of Iran, 26th International Computer Conference, Computer Society of Iran, CSICC 2021. Tehran, 3 March 2021. New York: Institute of Electrical and Electronics Engineers (IEEE); 10.1109/CSICC52343.2021.9420621.

Matanky-Becker, R., Cockbain, E., (2022). Behind the criminal economy: using UK tax fraud investigations to understand money laundering myths and models. Crime, *Law and Social Change*, [e-journal], 77(4), pp. 405-429; 10.1007/s10611-021-09997-4.

Netzwerk Steuergerechtigkeit, (2022). Financial Secrecy Index - 2018 Results. [online] Available at: https://www.netzwerk-steuergerechtigkeit.de/wp-content/uploads/2018/01/6_fsi-ranking_incl-_eu-tax-havens.pdf, [Accessed 31 May 2022].

OCHA, (2018). Global Terrorism Index (2018). [online] Available at: https://reliefweb.int/report/world/global-terrorism-index-2018, [Accessed 31 May 2022].

Perkhun, L., Sorochynskyi, O., Izosimov, O., (2015). Systema vzaiemodii shakhraiskykh atak ta instrumentiv borotby z nymy. *Scientific Bulletin of National Academy of Statistics*, *Accounting and Audit*, [e-journal], 1, pp. 50–65; http://194.44.12.92:8080/jspui/handle/123456789/3813. [in Ukrainian].

PwC, (2018). Building a united front on financial crimes. [online] Available at: https://www.pwc.com/gx/en/financial-services/pdf/united-front-financial-crimes-2018-pwc.pdf, [Accessed 31 May 2022].

Riani, M., Corbellini, A. and Atkinson, A.C., (2018). The Use of Prior Information in Very Robust Regression for Fraud Detection. International Statistical Review, [e-journal], 86(2), pp. 205–218; 10.1111/insr.12247.

Rouhollahi, Z., Beheshti, A., Mousaeirad, S. and Goluguri, S., (2021). Towards Proactive Financial Crime and Fraud Detection through Artificial Intelligence and

RegTech Technologies. In: ACM International Conference Proceeding Series, 23rd International Conference on Information Integration and Web Intelligence, iiWAS 2021. Virtual, Online, 29 November 2021 through 1 December 2021. New York: Association for Computing Machinery; 10.1145/3487664.3487740.

Sierikov, A. V., Zubova, O.O., (2010). Marketing as a necessary condition for synergetic management of economic activity. Actual Problems of Economics, 5, pp. 276–283.

Tharani, J.S., Charles, E.Y.A., Hou, Z., Palaniswami, M., and Muthukkumarasamy, V., (2021). In: Proceedings - Conference on Local Computer Networks, 46th IEEE Conference on Local Computer Networks, LCN 2021. Edmonton, 4 October 2021. New York: Institute of Electrical and Electronics Engineers (IEEE); 10.1109/LCN52139.2021.9524878.

The GlobalEconomy, (2022). List of available indicators. [online] Available at: https://www.theglobaleconomy.com/indicators_list.php, [Accessed 31 May 2022].

The World Bank, (2022). World Development Indicators; [online] Available at: https://databank.worldbank.org/reports.aspx?source=2&series=SI.POV.GINI&country=#, [Accessed 31 May 2022].

Tundis, A., Nemalikanti, S. and Mühlhäuser, M., (2021). In: ACM International Conference Proceeding Series, 16th International Conference on Availability, Reliability and Security, ARES. Virtual, Online, 17 August 2021. New York: Association for Computing Machinery; 10.1145/3465481.3469196.

Wilkens, K., Thomas, N. and Fofana, M.S., (2004). Stability of technology stock prices: Evidence of rational expectations or irrational sentiment? Managerial Finance, [e-journal] 30(12), pp. 33–54; 10.1108/03074350410769380.

Xia, P., Ni, Z., Zhu, X., He, Q. and Chen, Q., (2022). A novel prediction model based on long short-term memory optimised by dynamic evolutionary glowworm swarm optimisation for money laundering risk. *International Journal of Bio-Inspired Computation*, [e-journal], 19(2), pp. 77–86; 10.1504/IJBIC.2022.121233.

Yang, Y. and Wu, M., (2021). Explainable Machine Learning for Improving Logistic Regression Models. In: IEEE International Conference on Industrial Informatics, 19th IEEE International Conference on Industrial Informatics, INDIN 2021. Mallorca, 21 July 2021. New York: Institute of Electrical and Electronics Engineers (IEEE); 10.1109/INDIN45523.2021.9557392.

Yarovenko, H., (2021). Informatsiina bezpeka yak draiver rozvytku natsionalnoi ekonomiky | Information security as a driver of national economy development. DSc. Sumy State University. Available at: essuir.sumdu.edu.ua/handle/123456789/83664, [Accessed 31.05.2022]. [in Ukrainian].

Appendix

Final calculations of the integral cybersecurity index, determined by the Sundarovsky method

Country	IS	Country	IS
Australia	57,03	Liberia	3,33
Austria	57,70	Lithuania	60,61
Bahrain	29,76	Luxembourg	58,97
Barbados	12,32	Malaysia	55,41
Belgium	61,32	Malta	39,17
Bolivia	15,94	Mauritius	44,16
Botswana	15,75	Mexico	31,91
Brazil	35,78	Montenegro	33,17
Brunei Darussalam	28,56	Netherlands	65,46
Bulgaria	42,09	New Zealand	53,48
Canada	55,98	North Macedonia	39,64
Chile	37,39	Norway	59,60
China	36,02	Panama	29,08
Costa Rica	12,15	Paraguay	33,70
Croatia	54,06	Philippines	29,63
Cyprus	39,86	Poland	51,48
Czech Republic	50,66	Portugal	53,06
Denmark	63,60	Romania	42,83
Dominica	22,71	Russian Federation	50,74
Dominican Republic	26,45	Saudi Arabia	50,99
Estonia	65,41	Seychelles	14,84
Finland	65,08	Singapore	65,94
France	63,45	Slovakia	51,23
Germany	62,90	Slovenia	46,79
Ghana	22,17	South Africa	27,30
Greece	46,64	Spain	60,68
Grenada	13,80	Sweden	55,84
Guatemala	12,02	Switzerland	61,78
Hungary	49,49	Tanzania	17,16
Iceland	40,08	Thailand	39,41
India	37,28	Trinidad and Tobago	9,65
Indonesia	34,80	Turkey	46,17
Ireland	54,54	Ukraine	43,00
Israel	55,18	United Kingdom	64,85
Italy	53,19	United States	65,35
Japan	58,31	Uruguay	42,02
Kenya	29,73	Vanuatu	13,21
Latvia	52,54	Venezuela	20,47