Journal of
Risk and Financial Management

MDPI

Article

Ensuring Financial System Sustainability: Combating Hybrid Threats through Anti-Money Laundering and Counter-Terrorist Financing Measures

Antonín Korauš [1,*], Eva Jančíková [2], Miroslav Gombár [3], Lucia Kurilovská [4] and Filip Černák [3]

[1] Academy of the Police Force in Bratislava, Sklabinská 1, 835 17 Bratislava, Slovakia
[2] Faculty of International Relation, University of Economics in Bratislava, Dolnozemská cesta 1, 852 35 Bratislava, Slovakia; eva.jancikova@euba.sk
[3] Faculty of Management and Business, University of Prešov in Prešov, Konštantínova 16, 080 01 Prešov, Slovakia; miroslav.gombar@unipo.sk (M.G.)
[4] Faculty of Law, The Comenius University in Bratislava, Šafárikovo nám. 6, 818 06 Bratislava, Slovakia; lucia.kurilovska@flaw.uniba.sk
* Correspondence: antonin.koraus@akademiapz.sk

Abstract: This paper deals with ensuring the sustainability of the financial system and combating hybrid threats in relation to anti-money laundering and counter-terrorist financing (AML/CTF) measures. International cooperation in the field of combating hybrid threats is only at the beginning, and in many ways, the experience of international cooperation in the fight against money laundering and terrorist financing, which is based on many years of experience in the institutional and legislative fields, could be used. Hybrid threats are constantly changing and evolving, which means our response to them must also constantly evolve and adapt. The aim of the presented study is the analysis of the problem of the legalization of income from criminal activity and the financing of terrorism and their possible relationship with the fight against hybrid threats and maintaining the stability of the financial system.

Keywords: sustainability; hybrid threats; anti-money laundering; counter-terrorist financing

Citation: Korauš, Antonín, Eva Jančíková, Miroslav Gombár, Lucia Kurilovská, and Filip Černák. 2024. Ensuring Financial System Sustainability: Combating Hybrid Threats through Anti-Money Laundering and Counter-Terrorist Financing Measures. *Journal of Risk and Financial Management* 17: 55. https://doi.org/10.3390/jrfm17020055

Academic Editor: Svetlozar (Zari) Rachev

Received: 18 November 2023
Revised: 10 January 2024
Accepted: 26 January 2024
Published: 31 January 2024

1. Introduction

The financial environment, on a global scale, with its manifestations of international interconnection and interdependence, together with financial technologies, not only maintains the pace of economic growth and international trade but also exposes the financial system to many new risks, mainly in the form of hybrid threats. Frequent cyber-attacks pose a high risk to the stability and sustainability of financial systems around the world. The necessity of strengthening resistance to hybrid threats and the sustainability of the financial system is the topic of the day, exploring the critical intersection between the sustainability of the financial system and the ongoing fight against hybrid threats and the significant requirement that is being transformed into a system of anti-money laundering and counter-terrorist financing measures to ensure the integrity and sustainability of the global financial infrastructure. Recently, international efforts have been focused on the creation of regulatory frameworks and mechanisms aimed at combating money laundering and terrorist financing, which has also played a significant role in mitigating the broader risks associated with hybrid threats. This article provides an analysis of the multifaceted challenges that hybrid threats pose to the sustainability of the financial system. Ultimately, the sustainability of the financial system is inextricably linked to its ability to adapt, evolve, and effectively counter emerging threats. By analyzing the complicated and challenging relationship between hybrid threats, money laundering, terrorist financing,

and the sustainability of financial systems, this article can open a debate and inform policy makers, financial institutions, and security experts regarding preparing, solving, and creating effective scenarios to combat hybrid threats.

The development of new technologies in recent years has fundamentally affected the security situation in the world. Hybrid threats are increasingly being discussed, which are defined as a set of coercive and subversive activities through conventional and non-conventional and military and non-military methods that can be used by state and non-state entities in a coordinated manner to achieve specific goals without a formal declaration of war and below the threshold for a usual response (Concept for the Fight of the Slovak Republic against Hybrid Threats 2022). Even the war conflict in Ukraine shows how, in addition to direct military operations, many non-military means are also used, of which we can mainly mention enemy propaganda, support for extremism, use of national or religious communities dissatisfied with their position in society, and support for criminal activities, but mainly attacks on critical infrastructure. The increasing damage caused by cyber-attacks, along with their estimated rapid increase in the coming years, makes it critical to study them and document their origins, effects, the APTs perpetrating them, and the greater cybercrime economy (Riggs et al. 2023).

By building human resources and technical capacities and implementing educational and communication activities, resistance to various forms of hybrid threats in the respective domains can be significantly increased. System weaknesses in hybrid activities will be filled through a vulnerability audit and subsequent proposals for amending and supplementing regulatory frameworks. In addition, Slovakia's resistance to hybrid threats will be increased by the implementation of a complex set of measures, which include the optimization of processes in public administration entities, increasing educational capacities, and the acquisition of new competencies and skills by public bodies through a system of professional training (Koraus et al. 2022).

Experience from the fight against criminal activity shows the important role played by financial institutions. Sustainable fraud detection comprises the use of sustainable and ethical practices in the detection of fraudulent activities in the financial sector (Maashi et al. 2023; Kurshan and Shen 2020; Leonov et al. 2019; Antwi et al. 2023; Alnasser Mohammed 2021). The research (Kumar and Seetharama 2022) objectives have been to determine the impact of the exogenous construct on anti-money laundering implementation in banks. The impact of AML regulations on economic growth, as well as how AML regulations affect the foreign direct investment (FDI) growth link for 165 economies worldwide, have been the subject of scientific studies (Ofoeda et al. 2022a, 2022b, 2022c; Ofoeda 2022; Ofoeda et al. 2024). It is no different with hybrid threats. On the one hand, the financial system can be used or abused in the financing of these activities, and on the other hand, the financial system can be the target of hybrid threats, since in every society a healthy financial system has been the basis of the functioning of the economy. In recent years, also due to the influence of economic and political developments, the issues of hybrid threats in the context of financial systems have started to be discussed, mainly from the point of view of their vulnerability and especially their sustainability. Political and economic developments due to globalization have brought new challenges to which it is necessary to respond at the national and international level; as the research emphasizes, some specific measures should be taken to increase financial sustainability (Herman and Zsido 2023).

The aim of our contribution is to map the risks associated with financial systems and define measures for their sustainable protection with an emphasis on experience in the fight against money laundering and terrorist financing. When processing this contribution, we used scientific and professional articles on the given issue and available official sources of the EU and the Slovak Republic, which we subjected to analysis.

2. Hybrid Threats in Relation to Sustainable Financial Systems

The challenge of hybrid threats has become a key aspect of security policy discourse (Bajarūnas 2020), and activities associated with hybrid threats often require relatively

complex financing, which is carried out through the existing financial system, which plays a similar role to AML or CTF (Aho et al. 2020). Similar tools are used and often implemented by the same participants. Therefore, in this post, we will look for ways to use knowledge from the fight against money laundering (ML) and terrorist financing (TF).

In relation to the threats facing financial systems, we must mention the development of financial technologies, which can be a source of potential hybrid activities. An important fact is that financial technology firms are often relatively small firms compared to traditional banks, but they can have a large impact on the healthy and sustainable functioning of the financial system. Their effort to quickly obtain cheap capital can also be a problem which can lead to a potential hybrid threat. Although banks still dominate the market for payment transactions, innovation in payments is often associated with non-bank firms located abroad. The security threats of these new payment systems should by no means be underestimated (Hamed 2023).

The financial system, which consists of financial institutions, markets, tools, and services, has the task of ensuring the smooth functioning of the state. An attack on such a system can have major destabilizing effects and seriously threaten the functioning of any industry. The financial market reacts to every threat, and confidence in the financial markets is extremely important for financial stability. It is trust that is the target of hybrid threats, whether through misinformation or a through specific attacks on the banking system, growing civil unrest, a decrease in trust in financial markets, increasing withdrawals from banks, and increasing the probability of an economic crisis. An attack on a bank, investment fund, telecommunications/ATM network, SWIFT, or central banks would be a direct hit and could result in significant damage. It could be the failure of credit cards and other payment systems or the unavailability of online banking, cash, payments, and reliable bank account information. Banks may lose their ability to trade with each other, and consequently, all parts of society would be affected. As digitization increases, so do cyber-attacks on publicly listed financial services companies. Cyber-attacks affect all types of entities, and by July 2019, attacks against many public institutions in Spain, Germany, the United Kingdom, Finland, Lithuania, Bulgaria, and Croatia were reported. Large financial institutions are aware of cyber risks and have built backup systems and taken measures to reduce vulnerabilities. Nevertheless, there are several reasons why the current level of protection may be insufficient from the EU's point of view (Demertzis and Wolff 2019). Unlike potential man-made attacks, a hybrid operation may be better prepared to overwhelm the defense system and wreak havoc using artificial intelligence. The effect could be even more devastating if it were a coordinated hybrid operation that would hit critical infrastructure and supply chains (Savolainen 2019).

In the modern world, almost all financial activities are conducted in digital format and real physical money loses its meaning. The increased digitization of the financial system has highlighted cyber vulnerabilities, where remote actors can interfere with national systems, often anonymously. The basic source of risk for the EU financial system is the already mentioned security policy under national competence. Financial requirements fall to the ECB; however, security issues, such as cyber-attacks, fall under national security authorities. There is a lack of coordination between the ECB and national authorities; although attacks are reported to the ECB, information from the ECB is not provided to individual institutions. In this context, the ECB could play a more positive role and act as a mediator of information. One of the big challenges in the cyber protection of financial institutions is improving the quality of cooperation. Given the extensive financial integration, an attack on a member state can have significant cascading effects within the EU financial system, and therefore, one of the big challenges is precisely the improvement of cooperation in the cyber protection of financial institutions. In addition, when assessing cyber-attacks, operational risks are mainly taken into account—they are mainly threats resulting from attacks by private criminal actors, i.e., individual attacks, and there is a lack of a certain systemic view which would include coordinated hybrid threats targeting individual entities or the financial system as a whole and, consequently, the economy of the country. Another problem is

that companies that have been attacked often cover up these attacks to avoid possible financial losses and bad reputations. This, on the other hand, has the consequence that many companies may not be aware of the seriousness of the situation and do not make sufficient use of the possibilities of insuring against these risks (Antwi et al. 2023).

ML/TF are now considered a classic form of criminal activity that is connected to the functioning of the financial system. These activities often lead to a chain of various illegal activities, from the financing of organized crime to the destabilization of governments and the violation of the integrity of financial institutions.

To ensure the governments act in the best interest of their citizens and to realize the United Nations Sustainable Development Goals (SDGs), governments and public sector entities need to efficiently prevent different organizational pathologies in which money laundering plays a very important role (Dobrowolski and Sułkowski 2020).

Subsequent recovery would require time, especially in the case of damage, manipulation, or the unavailability of data. The financial system plays an important role in the development of the economies of individual countries, and it is an important tool for the development of international economic relations, especially when it comes to international financial relations. From its beginning, the positive developments in international financial relations were also accompanied by various forms of abuse of the system for various illegal activities connected with money laundering and terrorist financing. These objectives, which have not been studied previously, represent an important contribution because real sustainable concerns in banking did not emerge until recently, mainly with the adoption of the Sustainable Development Goals, which should be reached by 2030 (Cantero-Saiz et al. 2023).

In the last decade, there has been a significant rise in cryptocurrencies on the market. Several studies provide high-level analysis of the intersection of the cryptocurrency sector with anti-money laundering (AML) regulations and the risk-based anti-money laundering systems maintained by financial institutions (Faccia Alessio et al. 2020; Al-Tawil 2023; Al-Tawil and Younies 2021; Dyntu and Dykyi 2018; Barone and Masciandaro 2019; Dupuis and Gleason 2021; Alarab et al. 2020; Kshetri 2021; Jayasekara 2020; Kirimhan 2023).

Virtual assets present unique AML/CTF risks that have historically been overlooked by global regulation. The potential of virtual assets as a new way of exchanging value and the need for effective AML/CTF regulation is intriguing, but emerging issues that will increase risks and the current global regulatory response, including reliance on centralized intermediaries, may be holding back this potential (Schmidt 2022).

AML/CFT, covering regulatory requirements and guidelines, aim to combat fund generation from unlawful activities. Market intermediaries receive infringement notices for guideline breaches. Despite strengthened policies and procedures, assessing the effectiveness of AML/CFT legislation remains crucial (Khan et al. 2021).

The Financial Action Task Force (FATF) is an independent intergovernmental body focused on developing global policies to combat money laundering, terrorist financing, and the financing of weapons of mass destruction. Despite its shift from rule-based to holistic risk-based assessment during their 30-year history, the effectiveness of FATF's framework in preventing the criminal abuse of financial institutions remains uncertain. Artificial intelligence (AI) holds promise in enhancing these risk-based assessments, potentially making AML measures faster, cheaper, and more efficient for FIs by improving identification, response, communication, and the monitoring of suspicious activities (Sultana 2020; Goldbarsht 2022; Begishev 2021; Huarte 2020; Alessa 2019; Summerfield 2018; Chan and Moses 2017).

The transformation of sustainability in global financial services aimed at addressing sustainability-related risks has been long overdue and is of fundamental importance to the future development of financial services. The call for sustainability transformation in financial services emerged from the Paris Agreement and the UN Sustainable Development Goal agenda (Tuyon et al. 2023).

3. Data and Methodology

The fight is against the threat of ML/TF to global security and for the integrity of the financial system and sustainable growth. The European Commission conducts risk assessments to identify and respond to risks affecting the EU internal market. It advocates the adoption of global solutions to respond to these threats at the international level. The European Union has adopted strong anti-money laundering and anti-terrorist financing legislation that contributes to this international effort. The Commission ensures the effective application of this legislation by reviewing the transposition of the EU and cooperating with networks of competent authorities (Directive (EU) 2018/1673 2018; Directive (EU) 2018/843 2018; Directive (EU) 2019/1153 2019; European Commission 2019a, 2019b, 2020).

The Treaty on the European Union serves as the legal foundation for adopting directives that aim to harmonize laws among member states, particularly in creating and sustaining the internal market, which includes adjusting anti-money laundering measures. European legislation was enacted to guarantee the effective operation of the financial system and internal markets. Due to the evolving nature of money laundering and terrorist financing threats, coupled with the continuous technological advancements available to perpetrators, there remains a necessity to adapt the legal framework to address these evolving challenges.

As part of the analysis of the problem of money laundering and terrorist financing, we will focus on the indicator defined by the global Basel AML index, which assesses the risk of money laundering (ML) and terrorist financing (TF) in countries by amalgamating data from publicly available sources like the Financial Action Group, Transparency International, the World Bank, and the World Economic Forum (Manning et al. 2021). It incorporates 15 indicators related to AML/CFT compliance, covering areas such as corruption, financial standards, policy disclosure, and the rule of law to generate an overall risk score. This Total Risk Score offers a comprehensive evaluation of a country's resilience against money laundering and terrorist financing, considering both structural and functional elements. The scores are aggregated into a composite index using qualitative and expert rankings, resulting in a final country ranking. The data should be read in conjunction with the analysis and description of the methodology and indicators. Without this background, the results can be easily misunderstood or distorted. The Basel AML Index does not measure the actual amount of money laundering or terrorist financing, rather it is aimed at assessing the risk of such activity. ML/TF risk is understood as a broad area of risk in relation to a country's vulnerability to ML/TF and its capabilities to counter them. The source of the data is the annual reports of The Foundation of the Basel Institute on Governance (Basel AML Index 2012). The analysis of the Basel AML index itself covers the period from 2012 to 2020 in 23 selected EU countries and Great Britain. The average value of the Basel AML index in the monitored period is 4.445 ± 0.103, while Finland (3.019 ± 0.341), followed by Estonia (3.163 ± 0.383), Slovenia (3.593 ± 0.229), and Bulgaria (3.761 ± 0.260). On the contrary, the country with the highest ML/TF risk in the observed period is Luxembourg (5.584 ± 0.445), followed by Greece (5.424 ± 0.780), Italy (5.232 ± 0.226), and Germany (5.113 ± 0.445). Figure 1 provides a graphical representation of the change in the value of the Basel AML index in the monitored period and in selected EU countries.

As a part of the analysis, we will try to define the relationship between the risk of the legalization of income from criminal activity and the financing of terrorism (Basel AML) and the global indices CPI, EFI, SEDA, and DBI, which will act as independent predictors. The basic problem is therefore the analysis of the relationship:

$$\text{Basel AML} = f(\text{CPI}, \text{EFI}, \text{SED}A, \text{DBI})_{2012-2020} \quad (1)$$

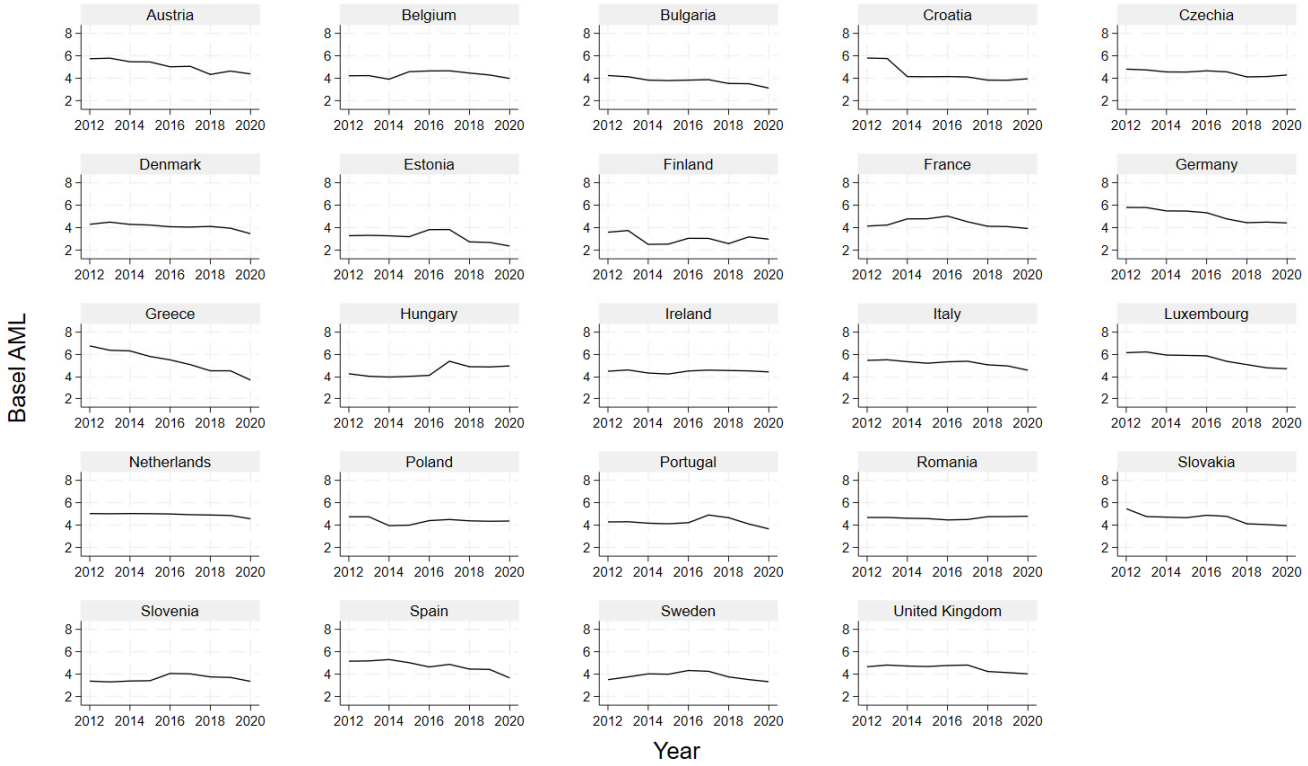

Figure 1. Change in the value of the Basel AML index in the monitored period from 2012 to 2020 in selected EU countries.

Therefore, the basic input predictors are the following selected global indices, which evaluate the risk of corruption, economic freedom, the prosperity of the country, and the ease of conducting business, i.e., predictors where we assume their significant influence on ML/TF risk.

1. CPI—The Corruption Perceptions Index is an index that focuses on the perception of the existence of corruption among public administration officials and politicians and defines corruption as the abuse of public authority for personal gain. The index ranges from 0 to 100, with a value of 0 representing a very corrupt country and a value of 100 representing a country without corruption or with a minimum of corruption (Wilhelm 2002). The average value of this index in the monitored period from 2012 to 2020 in selected EU countries is at the level of 65.579 $\pm$ 2.035, while the highest average values and thus the lowest levels of corruption are recorded from available sources in Denmark (89.222 $\pm$ 1.374), Finland (87.000 $\pm$ 1.675), the Netherlands (82.556 $\pm$ 0.558), and Luxembourg (81.222 $\pm$ 1.262). On the contrary, the highest average levels of corruption are recorded in Bulgaria (42.444 $\pm$ 0.950), Romania (45.222 $\pm$ 1.574), Greece (46.000 $\pm$ 2.578), and Hungary (47.778 $\pm$ 3.233).

2. EFI—The Index of Economic Freedom by the Heritage Foundation evaluates countries based on twelve factors: property rights, judicial effectiveness, government integrity, tax burden, government spending, fiscal health, business freedom, labor freedom, monetary freedom, trade freedom, investment freedom, and financial freedom (Dialga and Vallée 2021). The EFI Index evaluates the level of economic freedom based on the following 12 quantitative and qualitative factors grouped into four broad categories or pillars of economic freedom: 1. rule of law (property rights, government integrity, judicial effectiveness), 2. government size (government spending, tax burden, fiscal health), 3. effectiveness of legal regulations (freedom of business, labour freedom, monetary freedom), 4. open markets (freedom of trade, freedom of investment, financial freedom). Each of the twelve economic freedoms within these categories is rated on a scale of 0 to 100. A country's overall score is derived from the average of these twelve economic freedoms, giving

equal weight to each. The average value of the index of economic freedom in the monitored period from 2012 to 2020 is 69.595 ± 0.809, while the highest average values are recorded in the countries of Ireland (78.356 ± 1.727), Estonia (77.233 ± 0.960), Great Britain (77.089 ± 1.400), and Denmark (76.533 ± 0.871). Conversely, the lowest average values of the EFI index in selected EU countries in the monitored period are in Greece (56.456 ± 1.852), Croatia (60.944 ± 0.854), Italy (62.133 ± 0.891), and Slovenia (63.378 ± 2.484).

3. SEDA—Sustainable Economic Development Assessment. The SEDA score aids in assessing the effectiveness of countries in transforming their wealth (expressed in per capita income) into prosperity. This assessment is represented by the wealth-to-prosperity ratio, comparing a country's SEDA score to the expected score based on its GNI per capita. The coefficient serves as a relative indicator, with a value of 1.0 indicating welfare aligned with expected income levels. Countries with a coefficient above 1.0 provide higher well-being than expected, while those below 1.0 generate lower prosperity than anticipated (Huang et al. 2012). The average value of the SEDA index in selected EU countries in the monitored period of 2012–2020 reaches the level of 73.556 ± 1.124. Among the countries with the highest values of the SEDA index are Finland (84.422 ± 0.300), Denmark (83.978 ± 0.245), Sweden (83.978 ± 0.501), and Luxembourg (83.622 ± 0.693). The countries with the lowest SEDA index values include Romania (56.900 ± 0.939), Bulgaria (58.000 ± 1.087), Greece (63.411 ± 0.614), and Croatia (63.411 ± 0.753).

4. DBI—Doing Business Index. The DBI quantifies scores by calculating percentiles for individual indicators, followed by determining the arithmetic mean for each monitored dimension in the business environment. The resulting country ranking is determined by re-averaging these average percentiles and ordering them mathematically from the smallest to the largest percentile (Gürler 2023). The evaluated areas and indicators include starting a business, dealing with construction permits, obtaining electricity, registering property, obtaining credit, protecting minority investors, paying taxes, trading across borders, enforcing contracts, and resolving insolvency. The average value of the DBI index in selected EU countries in the monitored period of 2012–2020 reaches the level of 75.441 ± 0.677. The countries with the highest values of the DBI index, i.e., countries with a simple business environment, include Denmark (84.756 ± 0.312), Great Britain (83.533 ± 0.409), Sweden (81.978 ± 0.223), and Finland (80.378 ± 0.551). The countries where the DBI index acquires the lowest value in the monitored period are Greece (66.289 ± 1.643), Luxembourg (68.667 ± 0.942), Croatia (70.467 ± 2.749), and Hungary (70.922 ± 1.964).

We apply neural networks and the STATISTICA program to the analysis of relation (1) within the submitted contribution. An artificial neural network (ANN) is made up of mathematical neurons, primitive units, where each one processes weighted input signals and generates an output. A neural network represents a topological arrangement of individual neurons in a structure that communicates using oriented, graded connections. Thus, each artificial neural network is, among other things, characterized by the type of neurons, their topological arrangement, and the strategy of adaptation during the training (learning) of the network. It is called "forward" because the signal propagates unidirectionally from the input to the output of the network. We divide the data file intended for analysis into:

- Training set of data—a randomly selected part of the data that is used for learning the network;
- Test set of data—another part of the data that is used to stop training so that the network is not overdetermined;
- Validation set of data—the remaining part of the data with which we will verify the final quality of the model. These are data that were not available to the model either during training or during testing.

In the case of poorly chosen sets, there may be problems with the resulting model; e.g., the model may be over specified for one of the data sets. In general, if the network

contains a small number of neurons, its ability to capture and describe the dependencies in the training data is weaker. If, on the other hand, the network contains too many neurons, this network will probably have no problem finding and representing dependencies in the training data, but its ability to generalize, that is, the ability to find the correct result for new data, may be worse. We call such a phenomenon overfitting of the network. Overdetermination can occur when the model contains too many input parameters and relatively few observations. The goal is therefore not to maximize network performance on training data but a reasonable compromise between training performance and the ability to generalize knowledge in new data. Therefore, it seems important to divide the data into the three basic groups mentioned above. Typically, this division is made in the ratio of 50-25-25, or 70-15-15. The performance on each of these sets is then reported in the results, while we generally choose a model that does not have fluctuations that are too large on individual sets. The data file represents a matrix (216 × 5), while the data are distributed in the proportion 70% (Train):15% (Test):15% (Validation). Due to the prevalence of this approach to data analysis, we will not deal with the theoretical side of the issue of artificial neural networks in more detail. The five most suitable networks (ANN1 to ANN5) were used for the analysis of the investigated problem, the basic characteristics of which are listed in Table 1.

Table 1. Basic characteristics of applied neural networks.

Statistics	ANN_1	ANN_2	ANN_2	ANN_4	ANN_5
Network name	MLP 4-22-1	MLP 4-26-1	RBF 4-13-1	MLP 4-4-1	MLP 4-26-1
Training performance	0.735386	0.636932	0.551740	0.605559	0.631275
Test performance	0.695341	0.646213	0.510110	0.677413	0.573129
Validation performance	0.600524	0.454051	0.364583	0.586650	0.387612
Training error	0.136460	0.176423	0.212416	0.188096	0.178552
Test error	0.167681	0.209995	0.241033	0.181624	0.217556
Validation error	0.147947	0.185556	0.294384	0.160012	0.201938
Training algorithm	BFGS 71	BFGS 38	RBFT	BFGS 19	BFGS 83
Error function	SOS	SOS	SOS	SOS	SOS
Hidden activation	Tanh	Tanh	Gaussian	Logistic	Tanh
Output activation	Identity	Tanh	Identity	Logistic	Sine

The best characteristics of the generated neuron structures are shown primarily in MLP (Multilayer Perceptron) networks and in one RBF (Radial Basis Function) network. Artificial neural networks are defined in the hidden layer by a minimum of 4 and a maximum of 26 neurons. The sum of squares function is used as the error function in all generated networks, and Gaussian function and logistic function or hyperbolic tangent were used to activate the output function, constant function, logistic function, hyperbolic tangent function, or sine function. The BFGS (Broyden–Fletcher–Goldfarb–Shanno) algorithm was used as the basic training algorithm. The BFGS algorithm stands out as a variant of the second-order optimization technique, leveraging the second-order derivative of the objective function. Classified as a quasi-Newtonian method, it falls within the category of algorithms that approximate the second derivative, commonly referred to as the Hessian. This approach becomes particularly valuable in optimization problems, where quantifying the second derivative proves challenging. Widely acknowledged as the most employed second-order algorithm for numerical optimization, the BFGS algorithm typically finds application in adapting machine learning algorithms. It originates from the family of algorithms extending the Newton method optimization algorithm, collectively referred to as quasi-Newton methods. The Newton method, also a second-order optimization algorithm, relies on the Hessian matrix. However, its limitation lies in the need to calculate the inverse of the Hessian matrix. This operation is not only computationally expensive but may lack stability depending on the attributes of the objective function. Quasi-Newton methods are among the most widely used methods of nonlinear optimization. They are incorporated into several software libraries, proving effective in finding solutions to a wide variety of small

to medium-sized problems, especially when the Hessian version is difficult to compute. The primary difference between the various quasi-Newton optimization algorithms lies in the particular method employed to quantify the approximation of the inverse Hessian. The BFGS algorithm offers an outstanding approach to updating the inverse Hessian calculation without the need for recomputing each iteration. It, along with its extensions, may be one of the most widely used quasi-Newton or second-order optimization algorithms in numerical optimization. The advantage of using the Hessian, if available, lies in its capability to decide both the direction and the step size necessary to alter the input parameters strategically minimizing or maximizing the objective function. Quasi-Newton strategies, like the BFGS algorithm, approximate the inverse Hessian, enabling them to determine the direction of movement. However, the challenge stems from the absence of step-size information. This is the hurdle that the BFGS algorithm solves by looking up rows in the selected direction to determine the optimal distance to move. In-depth information about the BFGS algorithm can be found in studies such as those conducted by Wu et al. (2020) and Nezhad et al. (2013).

To select the most suitable neural network (ANN1–ANN5), we apply basic deviations between the values calculated using neural networks and real data. We present these basic statistical characteristics of deviations in Table 2.

Table 2. Descriptive statistics of deviations of applied neural networks.

Variable	ANN_1	ANN_2	ANN_3	ANN_4	ANN_5
Valid N	216	216	216	216	216
Mean	−0.368%	0.480%	−0.367%	0.817%	0.221%
Median	−1.905%	−0.173%	0.079%	−0.655%	−1.111%
Minimum	−34.068%	−33.134%	−43.388%	−35.581%	−30.691%
Maximum	37.048%	40.478%	35.589%	43.192%	40.098%
Lower Q	−8.012%	−8.108%	−9.984%	−8.820%	−9.578%
Upper Q	6.803%	9.437%	9.114%	9.041%	8.902%
Range	71.116%	73.612%	78.977%	78.773%	70.789%
Quartile R	14.815%	17.546%	19.099%	17.861%	18.480%
Std.Dev.	12.630%	13.997%	14.730%	13.851%	14.189%
Skewness	0.345926	0.334813	0.018631	0.466462	0.387799
Kurtosis	0.648217	0.293565	−0.098713	0.474595	0.103286

The smallest deviation of the predicted and actual data is shown by the neural network ANN5 (MLP 4-26-1) and reaches 0.221 ± 1.892%, with the second highest value of the non-parametric showing position measure, which is the median at the level of −1.111%. This analyzed neural network is also the lowest value of the range, i.e., the difference between the minimum and maximum value at the level of 70.789%, with the smallest minimum value at the same time (−30.691%). However, the interquartile range of the deviation shows the second highest value (18.480%) and the second highest value of the standard deviation (14.189%). If we analyze only the validation group of data (N = 32) of the neural network ANN5 (MLP 4-26-1), then the average deviation value is 1.391 ± 5.176%, with a median value at the level of 1.542%. The value of the margin of deviation is 64.188% and the value of the interquartile range is 18.887% for this network. ANN3 (MLP 4-4-1) shows the second lowest average deviation of predicted and real values for the entire data set at the level of 0.367 ± 1.964%, with the lowest value of the median deviation at the level of −0.079%. However, the minimum deviation value represents −43.388% and the deviation range represents the highest value compared to the other considered neural networks and reaches 78.997%, with the highest value of the interquartile range at the level of 19.099%. Based on the results shown in Table 2 and at the same time based on the analysis of deviations between predicted and real data of individual data groups (training, testing, validation), we will choose the ANN5 neural network (MLP 4-26-1). The selected neural network with label ANN5 (MLP-4-26-1) is characterized as

follows: MAE = 0.167, MAPE = 8.217%, MSE = 0.234, RMSE = 0.315. The stated values give a good starting point for drawing relevant conclusions.

4. Results and Discussion

The first partial conclusion of the analysis is the result of the sensitivity analysis. From the above analysis, it follows that the most significant predictor in terms of model (1), which significantly affects the conditional value of the studied variable Basel AML, is the global CPI index, which, as we have already stated above, focuses on the perception of the existence of corruption among public administration officials and politicians and defines corruption as the abuse of public power for personal gain. The share of this index (CPI) in the total change in the Basel AML value is 37.620%. The second most significant regressor within model (1) is the global SEDA index, with a share in the change in the value of the investigated variable at the level of 27.860%. The third most important regressor of model (1) is the global DBI index, with 20.866% influence, and finally, the smallest influence is the index of business freedom, i.e., the global EFI index, with 13.654% influence. The analysis of the selected interrelationships of the input variables (CPI, SEDA, DBI, EFI) and their influence on the change in the value of the investigated response, which is the global Basel AML index, is presented in Figures 2–4.

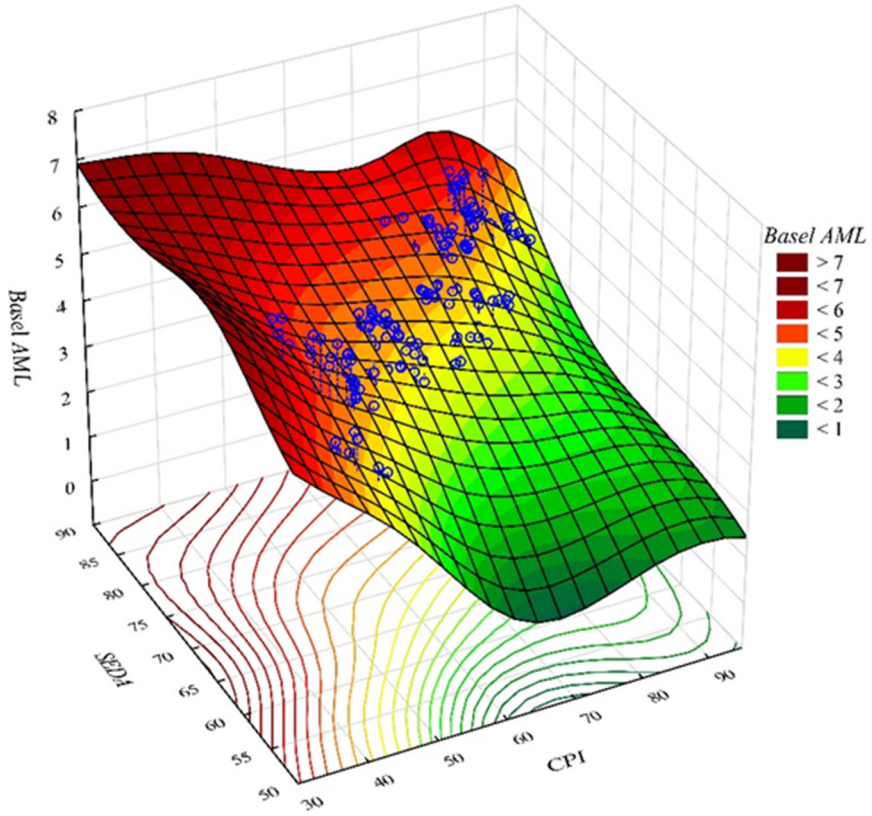

Figure 2. Predicted impact of the global CPI and SEDA indices on the change in the value of the Basel AML index.

The graphic representation of the two most significant predictors of model (1) that influence the change in the value of the Basel AML index is the perception of the risk of corruption among public administration officials and politicians and defines corruption as the abuse of public power for one's own benefit, expressed by the CPI index and the ability of countries to transform their wealth into prosperity, while this ability, as defined by the global SEDA index in the monitored period of 2012 to 2020 in 23 selected EU countries and Great Britain, is shown in Figure 2. The first conclusion, which is based on the nature of the predictors used, is the fact that by increasing the value of the CPI index, i.e., a lower

level of corruption risk, the value of the Basel AML index decreases globally. At the same time, Figure 2 shows the dominant influence of the CPI index on the overall change in the monitored variable. Figure 2 further shows that even if the value of the SEDA index is at its maximum level, and at the same time the CPI index is at the lower interval of values, the risk of the legalization of income from criminal activity is minimal. At the same time, the smallest predicted value of the Basel AML index is at values of the CPI index in the interval of about 65 to 72 and subsequently at the maximum values of this index. On the other hand, the maximum predicted value of the risk of the legalization of income from criminal activity and the financing of terrorism is at the maximum value of the SEDA index, i.e., in the case where countries are able to transform their wealth into prosperity very effectively, but at the same time, there is the highest risk of corruption, which is expressed by the minimum value of the CPI index.

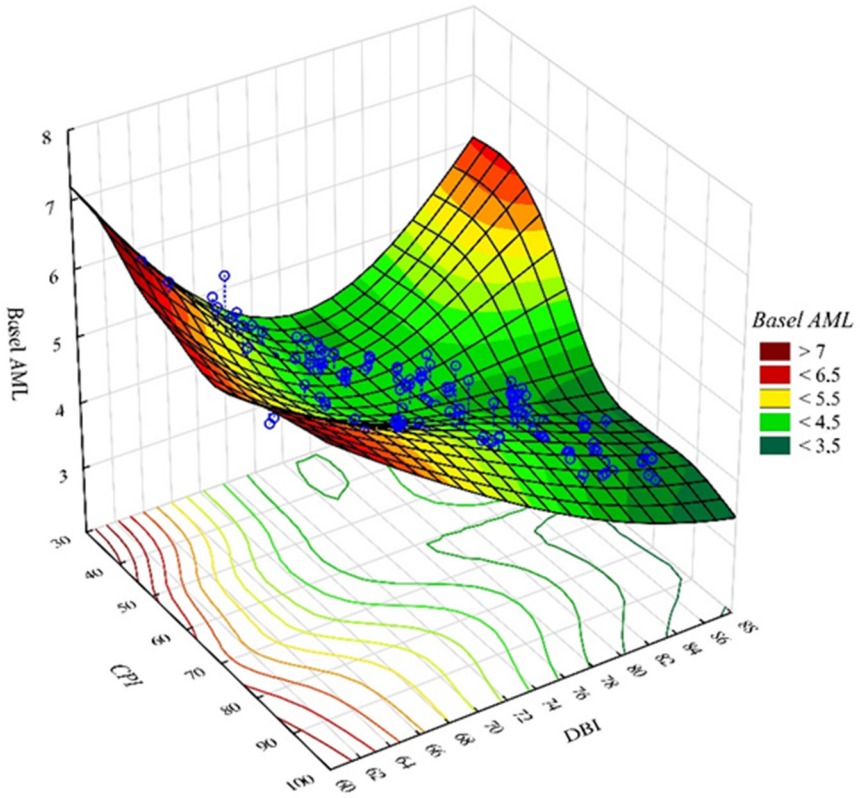

Figure 3. Predicted impact of the global CPI and DBI indices on the change in the value of the Basel AML index.

The second analyzed pair of predictors of model (1) and their influence on the conditional predicted value of the Basel AML index is the CPI index and the DBI index, which essentially expresses the ease of conducting business (Figure 3). Even in this case, it is possible to identify a significant influence of corruption risk perception (CPI) on the change in the value of the ML/TF problem (Basel AML).

Figure 3 shows that the minimum predicted values of the Basel AML index are achieved in the case of the lowest level of corruption risk (CPI), and at the same time, a high value of the DBI index, i.e., in countries where the business environment is simple. The minimum ML/TF risk values are therefore at a value of the CPI index greater than 65 and at a value of the DBI index higher than 83. On the contrary, the highest values of the predicted value of the Basel AML index are observed at a value of the DBI index lower than 63, but also in the case where the business environment is simple, but at the same time, there is a high risk of corruption by civil servants and politicians.

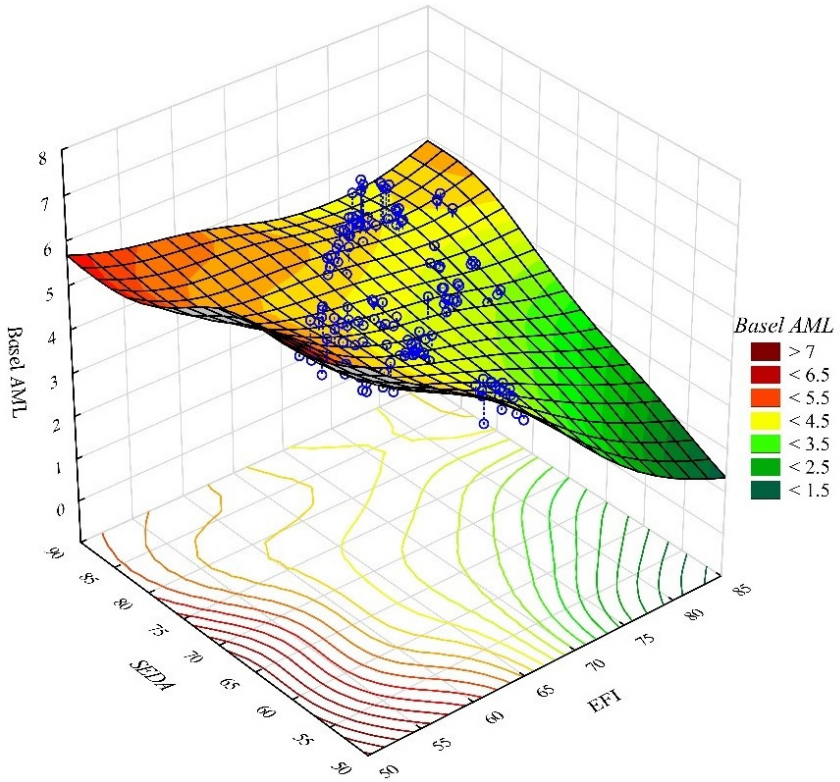

Figure 4. Predicted impact of the SEDA and EFI global indices on the change in the value of the Basel AML index.

The last analyzed pair of predictors of model (1) and their influence on the change in the ML/FT perception value (Basel AML) is the global index SEDA and EFI, i.e., freedom of business (Figure 4).

Figure 4 shows that the predicted value of the Basel AML index, i.e., the highest level of ML/FT risk, is at high values of the EFI index, i.e., in countries with a high degree of business freedom. At the same time, however, it is necessary to be aware of the fact that ML/TF risk has an increasing tendency even in countries that have a low level of business freedom, but at the same time, the value of the SEDA index, i.e., the country's ability to transform its wealth into prosperity, is decreasing. The ML/TF risk prediction problem is a complex problem, and within the analysis, we focused only on the basic input factors that could influence the value of the Basel AML index.

5. Conclusions

In the current era, which has typical manifestations of interconnectedness and interdependence within the global financial system, the manifestations and risks of hybrid threats are becoming more frequent. The sustainability and stability of financial systems in the global environment is destabilized through cyber-attacks from terrorist financing. The comprehensive research carried out in some contexts revealed the interdependencies of the sustainability of the financial system and the ongoing fight against hybrid threats. The key role played by AML/CTF measures as an integral part of ensuring the integrity and existence of the global financial infrastructure was emphasized.

An important step and contribution were the implementation of the international community in the form of the creation of regulatory frameworks and mechanisms to combat ML/TF. The United Nations Sustainable Development Goals (SDGs), adopted in 2015, are the most relevant global agreements on 17 of the most important issues that are crucial to all countries and their societies. The achievement of all SDGs requires a reduction in the scale of money laundering destabilizing domestic economies (Dobrowolski and Sułkowski 2020).

The impact of these measures was not only aimed at limiting illegal financial flows but also aimed at mitigating the impact of hybrid threats. However, our contribution revealed persistent challenges and vulnerabilities in the financial system, especially due to permanent developments in the area of malicious attacks and threats, which need to be responded to operationally and systematically in the innovation process of AML and CTF measures. In this context, it is important to emphasize that the sustainability of the financial system is the joint responsibility of representatives of the state sector, legislators, regulators, financial institutions, and security and IT experts and their holistic and adaptive approach to the sustainability of the financial system. By analyzing the complicated connections between hybrid threats, money laundering, terrorist financing, and the financial system, the current challenges for stakeholders have been raised, which can result in informed decision-making, support for cooperation between stakeholders, and better decision-making processes directed towards such innovations, which will minimize the impacts and consequences of hybrid threats.

Hybrid threats have become an everyday part of our society, and therefore, the fight against hybrid threats must be continuous and comprehensive. The EU and NATO have adopted several measures that we have also implemented in our practice. We cooperate closely at the international level but also at the national level. The agenda of the fight against hybrid threats is a priority of several ministries, of which the Ministry of Foreign Affairs and European Affairs of the Slovak Republic, the Ministry of Defence of the Slovak Republic, and the Ministry of the Interior of the Slovak Republic have the most significant share. In recent years, several fundamental documents have been adopted that regulate the fight against hybrid threats. In 2022, the Action Plan was adopted, which deals with the most important tasks that a company must solve in six segments. An important role is also played by the academic sector, which participates in the analysis of the situation, proposes measures, and helps in their implementation. We see an irreplaceable role in the education of citizens of all age categories, especially in developing their critical thinking and resistance to the misinformation that currently surrounds us. In these contexts, it is necessary to emphasize the significance and importance of education in the areas of AML, hybrid threats, and sustainability, to which several scientific research and publication outputs are devoted (Alsuwailem and Saudagar 2020; Pourhabibi et al. 2020; Jensen and Iosifidis 2023). It is also important that the measures are accepted and supported by most of the population.

In connection with hybrid threats, it is necessary to use institutional and legal safeguards against money laundering and terrorist financing. The fight against money laundering has been associated with 50 years of experience, which has been extended for 20 years by the fight against the financing of terrorism. Despite many years of experience, issues related to money laundering and terrorist financing are still relevant and new challenges are emerging that need to be addressed.

Author Contributions: Conceptualization, E.J. and A.K.; methodology, M.G.; software, F.Č.; validation, E.J. and L.K.; formal analysis, E.J. and M.G.; investigation, A.K.; resources, A.K. and L.K.; data curation, M.G. and F.Č.; writing—original draft preparation, E.J. and M.G.; writing—review and editing, E.J. and A.K.; visualization, F.Č. and L.K.; supervision, A.K. and E.J.; project administration, F.Č. and L.K.; funding acquisition, A.K. All authors have read and agreed to the published version of the manuscript.

Funding: This contribution was created as part of the national project "Increasing Slovakia's resistance to hybrid threats by strengthening public administration capacities", project code ITMS2014+: 314011CDW7. This project is supported by the European Social Fund.

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Data Availability Statement: Data are contained within the article.

Conflicts of Interest: The authors declare no conflict of interest.

References

Aho, Aleksi, Catarina Midões, and Arinis Šnore. 2020. *Hybrid Threats in the Financial System*. Helsinki: The European Centre of Excellence for Countering Hybrid Threats. ISBN 978-952-7282-63-2.

Alarab, Ismail, Simant Prakoonwit, and Mohamed Ikbal Nacer. 2020. Competence of graph convolutional networks for anti-money laundering in bitcoin blockchain. Paper presented at 2020 5th International Conference on Machine Learning Technologies, Beijing, China, June 19–21; New York: Association for Computing Machinery, pp. 23–27. [CrossRef]

Alessa, R. 2019. Webinar-An Executive Guide on How to Use Machine Learning and AI for AML Compliance. Available online: https://www.youtube.com/watch?v=k46 (accessed on 25 January 2024).

Alnasser Mohammed, Sulaiman Abdullah Saif. 2021. Money laundering in selected emerging economies: Is there a role for banks? *Journal of Money Laundering Control* 24: 102–10. [CrossRef]

Alsuwailem, Alhanouf Abdulrahman Saleh, and Abdul Khader Jilani Saudagar. 2020. Anti-money laundering systems: A systematic literature review. *Journal of Money Laundering Control* 23: 833–48. [CrossRef]

Al-Tawil, Tareq Na'el. 2023. Anti-money laundering regulation of cryptocurrency: UAE and global approaches. *Journal of Money Laundering Control* 26: 1150–64. [CrossRef]

Al-Tawil, Tareq Na'el, and Hassan Younies. 2021. The implications of the Brexit from EU and bitcoin. *Journal of Money Laundering Control* 24: 137–49. [CrossRef]

Antwi, Effah Kwabena, John Boakye-Danquah, Wiafe Owusu-Banahene, Anna Dabros, Ian Eddy, Daniel Abraham Silver, Evisa Abolina, Brian Eddy, and Richard S. Winder. 2023. Risk assessment framework for cumulative effects (RAFCE). *Front. Environ. Sci.* 10: 1055159. [CrossRef]

Bajarūnas, Eitvydas. 2020. Addressing hybrid threats: Priorities for the EU in 2020 and beyond. *European View* 19: 62–70. [CrossRef]

Barone, Raffaella, and Donato Masciandaro. 2019. Cryptocurrency or usury? Crime and alternative money laundering techniques. *European Journal of Law and Economics* 47: 233–54. [CrossRef]

Basel AML Index. 2012. Available online: https://index.baselgovernance.org (accessed on 25 January 2024).

Begishev, Ildar R. 2021. Criminological classification of robots: Risk-based approach. *Law Enforcement Review* 5: 185–201. [CrossRef]

Cantero-Saiz, María, Begoña Torre-Olmo, and Sergio Sanfilippo-Azofra. 2023. Sustainable banking, financial strength and the bank lending channel of monetary policy. *Journal E&M Ekonomie a Management* 26: 165–85. [CrossRef]

Chan, Janet, and Lyria Bennett Moses. 2017. Making Sense Of Big Data For Security. *British Journal of Criminology* 57: 299–319. [CrossRef]

Concept for the Fight of the Slovak Republic against Hybrid Threats. 2022. Available online: https://www.nbu.gov.sk/wp-content/uploads/PHHD/Koncepcia-boja-SR-proti-hybridnym-hrozbam.pdf (accessed on 25 January 2024).

Demertzis, Maria, and Guntram B. Wolff. 2019. Hybrid and Cybersecurity Threats and the European Union's Financial System. Policy Contribution Issue n°10. Available online: https://www.bruegel.org/wp-content/uploads/2019/09/PC-10_2019.pdf (accessed on 25 January 2024).

Dialga, Issaka, and Thomas Vallée. 2021. The index of economic freedom: Methodological matters. *Studies in Economics and Finance* 38: 529–61. [CrossRef]

Directive (EU) 2018/1673 of the European Parliament and of the Council of 23 October 2018 on Combating Money Laundering by Criminal Law. 2018. Available online: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32018L1673 (accessed on 25 January 2024).

Directive (EU) 2018/843 of the European Parliament and of the Council of 30 May 2018 amending Directive (EU) 2015/ 849 on the Prevention of the Use of the Financial System for the Purposes of Money Laundering or Terrorist Financing and Amending Directives 2009/138/EC and 2013/36/EU. 2018. Available online: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:32018L0843 (accessed on 25 January 2024).

Directive (EU) 2019/1153 of the European Parliament and of the Council of 20 June 2019 Laying Down Rules Facilitating the Use of Financial and Other Information for the Prevention, Detection, Investigation or Prosecution of Certain Criminal Offences. 2019. Available online: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32019L1153 (accessed on 25 January 2024).

Dobrowolski, Zbysław, and Łukasz Sułkowski. 2020. Implementing a sustainable model for anti-money laundering in the United Nations development goals. *Sustainability* 12: 244. [CrossRef]

Dupuis, Daniel, and Kimberly Gleason. 2021. Money laundering with cryptocurrency: Open doors and the regulatory dialectic. *Journal of Financial Crime* 28: 60–74. [CrossRef]

Dyntu, Valeriia, and Oleh Dykyi. 2018. Cryptocurrency in the system of money laundering. *Baltic Journal of Economic Studies* 4: 75–81. [CrossRef]

European Commission. 2019a. Assessment of Recent Alleged Money Laundering Cases Involving EU Credit Institutions' COM. Available online: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52019DC0373 (accessed on 25 January 2024).

European Commission. 2019b. Assessment of the Risk of Money Laundering and Terrorist Financing Affecting the Internal Market and Relating to Cross-Border Activities' COM. Available online: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52019DC0370 (accessed on 25 January 2024).

European Commission. 2020. Action Plan for a Comprehensive Union Policy on Preventing Money Laundering and Terrorist Financing' COM. Available online: https://www.dlapiper.com/en/insights/publications/2021/10/anti-money-laundering-and-countering-terrorism-financing (accessed on 25 January 2024).

Faccia Alessio, Narcisa Roxana Moşteanu, Luigi Pio Leonardo Cavaliere, and Leonardo Jose Mataruna-Dos-Santos. 2020. Electronic Money Laundering, The Dark Side of Fintech: An Overview of the Most Recent Cases. Paper presented at ICIME 2020: 2020 12th International Conference on Information Management and Engineering, Amsterdam, The Netherlands, September 16–18; pp. 29–34. [CrossRef]

Goldbarsht, Doron. 2022. Artificial Intelligence and Financial Integrity: The Case of Anti-money Laundering. *Journal of Banking and Finance Law and Practice* 33: 21–36.

Gürler, Cem. 2023. Ease of doing business in European Union countries and candidates. *Pamukkale University Journal of Social Sciences Institute/Pamukkale Üniversitesi Sosyal Bilimler Enstitüsü Dergisi* 57: 81–93. [CrossRef]

Hamed, Ruba. 2023. The role of internal control systems in ensuring financial performance sustainability. *Sustainability* 15: 10206. [CrossRef]

Herman, Emilia, and Kinga-Emese Zsido. 2023. The Financial Sustainability of Retail Food SMEs Based on Financial Equilibrium and Financial Performance. *Mathematics* 11: 3410. [CrossRef]

Huang, Chu-Long, Jonathan Vause, Hwong-Wen Ma, and Chang-Ping Yu. 2012. Using material/substance flow analysis to support sustainable development assessment: A literature review and outlook. *Resources, Conservation and Recycling* 68: 104–16. [CrossRef]

Huarte, E. G. 2020. Uncertain causation in civil liability arising from artificial intelligence. *Revista General de Derecho Europeo*. [CrossRef]

Jayasekara, Sisira Dharmasri. 2020. Deficient regimes of anti-money laundering and countering the financing of terrorism: Agenda of digital banking and financial inclusion. *Journal of Money Laundering Control* 24: 150–62. [CrossRef]

Jensen, Rasmus Ingemann Tuffveson, and Alexandros Iosifidis. 2023. Qualifying and raising anti-money laundering alarms with deep learning. *Expert Systems with Applications* 214: 119037. [CrossRef]

Khan, Norziaton Ismail, Mohamad Asri Abdul Jani, and Anis Asfarina Zulkifli. 2021. The Effectiveness of Anti-Money Laundering/Counter Financing of Terrorism Requirements in Fund Management Companies. *International Journal of Service Management and Sustainability* 6: 53–76. [CrossRef]

Kirimhan, Destan. 2023. Importance of anti-money laundering regulations among prosumers for a cybersecure decentralized finance. *Journal of Business Research* 157: 113558. [CrossRef]

Koraus, Antonín, Lucia Kurilovská, and Stanislav Šišulák. 2022. Increasing the Competnecies and Awareness of Public Administration Worker in the Context of Current Hybrid Threats. In *Conference Proceedings RELIK 2022. Reproduction of Human Capital—Mutual Links and Connections*. Praha: Vysoká škola Ekonomická. ISBN 978-80-245-2466-5.

Kshetri, Nir. 2021. The role of artificial intelligence in promoting financial inclusion in developing countries. *Journal of Global Information Technology Management* 24: 1–6. [CrossRef]

Kumar, Nishant, and A. Seetharama. 2022. Adoption of anti-money laundering by banks. *International Journal of Early Childhood Special Education* 14: 10541–47.

Kurshan, Eren, and Hongda Shen. 2020. Graph computing for financial crime and fraud detection: Trends, challenges and outlook. *International Journal of Semantic Computing* 14: 565–89. [CrossRef]

Leonov, Serhiy, Hanna Yarovenko, Anton Boiko, and Tetiana Dotsenko. 2019. Prototyping of information system for monitoring banking transactions related to money laundering. *SHS Web of Conferences* 65: 04013. [CrossRef]

Maashi, Mashael, Bayan Alabduallah, and Fadoua Kouki. 2023. Sustainable financial fraud detection using garra rufa fish optimization algorithm with ensemble deep learning. *Sustainability* 15: 13301. [CrossRef]

Manning, Matthew, Gabriel T. W. Wong, and Nada Jevtovic. 2021. Investigating the relationships between FATF recommendation compliance, regulatory affiliations and the Basel Anti-Money Laundering Index. *Security Journal* 34: 566–88. [CrossRef]

Nezhad, Ali Mohammad, Roohollah Aliakbari Shandiz, and Abdolhamid Eshraghniaye Jahromi. 2013. A particle swarm–BFGS algorithm for nonlinear programming problems. *Computers &Operations Research* 40: 963–72. [CrossRef]

Ofoeda, Isaac. 2022. Anti-money laundering regulations and financial inclusion: Empirical evidence across the globe. *Journal of Financial Regulation and Compliance* 30: 646–64. [CrossRef]

Ofoeda, Isaac, Elikplimi Agbloyor, and Joshua Yindenaba Abor. 2024. Financial sector development, anti-money laundering regulations and economic growth. *International Journal of Emerging Markets* 19: 191–210. [CrossRef]

Ofoeda, Isaac, Elikplimi Komla Agbloyor, and Joshua Yindenaba Abor. 2022a. How do anti-money laundering systems affect FDI flows across the globe? *Cogent Economics & Finance* 10: 2058735. [CrossRef]

Ofoeda, Isaac, Elikplimi Komla Agbloyor, Joshua Yindenaba Abor, and Kofi A. Osei. 2022b. Anti-money laundering regulations and financial sector development. *International Journal of Finance & Economics* 27: 4085–104. [CrossRef]

Ofoeda, Isaac, Elikplimi Komla Agbloyor, Joshua Yindenaba Abor, and Kofi Osei Achampong. 2022c. Foreign direct investment, anti-money laundering regulations and economic growth. *Journal of International Development* 34: 670–92. [CrossRef]

Pourhabibi, Tahereh, Kok-Leong Ong, Booi H. Kam, and Yee Ling Boo. 2020. Fraud detection: A systematic literature review of graph-based anomaly detection approaches. *Decision Support Systems* 133: 113303. [CrossRef]

Riggs, Hugo, Shahid Tufail, Imtiaz Parvez, Mohd Tariq, Mohammed Aquib Khan, Asham Amir, Kedari Vineetha Vuda, and Arif I. Sarwat. 2023. Impact, vulnerabilities, and mitigation strategies for cyber-secure critical infrastructure. *Sensors* 23: 4060. [CrossRef]

Savolainen, Jukka. 2019. Hybrid Threats and Vulnerabilities of Modern Critical Infrastructure—Weapons of Mass Disturbance (WMDi)? Working Paper 2019. The European Centre of Excellence for Countering Hybrid Threats. Available online: https://www.hybridcoe.fi/wp-content/uploads/2019/11/NEW_Working-paper_WMDivers_2019_rgb.pdf (accessed on 25 January 2024).

Schmidt, Alicia. 2022. Virtual assets: Compelling a new anti-money laundering and counter-terrorism financing regulatory model. *International Journal of Law and Information Technology* 29: 332–63. [CrossRef]
Sultana, Shirin. 2020. Role of financial intelligence unit (FIU) in anti-money laundering quest Comparison between FIUs of Bangladesh and India. *Journal of Money Laundering Control* 23: 931–47. [CrossRef]
Summerfield, R. 2018. Strengthening AML Protection through AI. Financier Worldwide Magazine. Available online: www.financierworldwide.com/strengthening-aml-protection-through-ai#.YV6BGi0Rrw4 (accessed on 25 January 2024).
Tuyon, Jasman, Okey Peter Onyia, Aidi Ahmi, and Chia-Hsing Huang. 2023. Sustainable financial services: Reflection and future perspectives. *Journal of Financial Services Marketing* 28: 664–90. [CrossRef]
Wilhelm, Paul G. 2002. International validation of the corruption perceptions index: Implications for business ethics and entrepreneurship education. *Journal of Business Ethics* 35: 177–89. [CrossRef]
Wu, Jian-Ying, Yuli Huang, and Vinh Phu Nguyen. 2020. On the BFGS monolithic algorithm for the unified phase field damage theory. *Computer Methods in Applied Mechanics and Engineering* 360: 112704. [CrossRef]