

ENSURING FINANCIAL SYSTEM SUSTAINABILITY: COMBATING HYBRID THREATS THROUGH ANTI- MONEY LAUNDERING AND COUNTER-TERRORISM FI- NANCING MEASURES

Antonín Koraus^{1*}, Eva Jančíková², Miroslav Gombár³, Lucia Kurilovská⁴ and Filip Černák⁵

¹ Academy of the Police force in Bratislava, Sklabinská 1, 835 17 Bratislava, Slovak Republic.

antonin.koraus@akademiapz.sk

² University of Economics in Bratislava, Faculty of International Relation; Dolnozemska cesta 1, 852 35 Bratislava 5 Slovak Republic eva.jancikova@euba.sk

³ Department of Management, Faculty of Management and Business, University of Prešov, 080 01 Prešov, Slovak Republic; miroslav.gombar@unipo.sk

⁴ Faculty of Law, The Comenius University in Bratislava, Šafárikovo nám. 6. 818 06 Bratislava. Slovak Republic. lucia.kurilovska@flaw.uniba.sk

⁵ Faculty of Management and Business, University of Prešov in Prešov, Konštantínova 16, 080 01 Prešov, Slovak Republic. fcernak@sitno.sk

* Correspondence: antonin.koraus@akademiapz.sk

Abstract: The paper deals with ensuring the sustainability of the financial system and combating hybrid threats in relation to anti-money laundering and terrorist financing 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 legalization of income from criminal activity and 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, money laundering and terrorist financing, The Financial Action Task Force (FATF)

1. Introduction

The financial environment on a global scale with its manifestations of international interconnection and interdependence together with financial technologies not only maintain the pace of economic growth and international trade, but also expose 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 (AML) and counter-terrorist financing (CTF) measures in ensuring 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 financial system is inextricably linked to its ability to adapt, evolve, and effectively counter emerging threats. By analysing the complicated and challenging relationship between hybrid

Citation: To be added by editorial staff during production.

Academic Editor: Firstname Last-name

Received: date

Revised: date

Accepted: date

Published: date



Copyright: © 2023 by the authors. Submitted for possible open access publication under the terms and conditions of the Creative Commons Attribution (CC BY) license (<https://creativecommons.org/licenses/by/4.0/>).

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 towards 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, conventional and non-conventional, 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 of a usual response [1]. 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, support of criminal activities, but mainly attacks on critical infrastructure. The increasing damages caused by cyber-attacks, along with their estimated rapid increase in the coming years, make it critical to study them and document their origins, effects, the APTs perpetrating them, and the greater cybercrime economy. [2]

By building human resources, 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 by 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 optimization of processes in public administration entities, increasing educational capacities, acquisition of new competencies and skills by public bodies through a system of professional training. [3]

Experience from the fight against criminal activity shows the important role played by financial institutions. The sustainable fraud detection comprises the use of sustainable and ethical practices in the detection of fraudulent activities in the financial sector [4 - 8]. The research [9] objectives were to determine the impact of the exogenous construct on anti-money laundering implementation in banks. The impact of anti-money laundering (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 [10 - 14]. 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 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. [15]

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 the 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 [16] and activities associated with hybrid threats often require relatively complex financ-

ing, which is carried out through the existing financial system, which plays a similar role to money laundering or terrorist financing. 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 and terrorist financing.

As with money laundering and terrorist financing, it is true for hybrid threat financing that they copy legal procedures, and it is often difficult to identify them in the mass of legal transactions. The 1990s brought an increase in globalization and an increased movement of funds and capital was associated with it; initially this movement was directed from developed countries to developing and developing countries. In recent decades, the situation has changed, and China is currently one of the biggest creditors. Certain geopolitical ambitions are also associated with economic expansion. The European Union, built on economic integration, is currently in a situation where it has a centralized economic policy, but geopolitical issues and security are dealt with at the national level. In this, it differs from other economic powers, in which the economy, foreign policy and security form a whole, the EU has these activities divided and the question is to what extent it should increase their coordination. Currently, there is a debate in the EU about the further direction towards greater federalization or the strengthening of national elements. [17]

One of the biggest problems in this area is the relationship with China as a global player, which officially became the largest creditor in the world, surpassing traditional official creditors such as the World Bank, the IMF or all the creditors of the OECD countries together. Official Chinese loans and investments reach almost 10% of global GDP. Unlike other economies that are based on private ownership, Chinese capital is almost always controlled by the government. The main creditors are banks and enterprises owned or controlled by the state. [18]

During the crisis in the Eurozone, Chinese capital became very attractive to EU member states, for example in the case of Italy they bought government bonds and invested in strategic enterprises. Portugal has become the country with the largest Chinese investment per capita. [19] The biggest problem with Chinese investments is their non-transparency. The unclear origin of financial flows and the ultimate owners of companies operating in EU countries is a problem that was also addressed in the latest EU directives related to money laundering and terrorist financing. Even before the military conflict in Ukraine some institutions drew attention to the risks associated with too high dependence on Russia especially in the field of energy raw materials and also on the transfer of some production activities to Russia. One of the main political tools of the EU and Western liberal democracies is the application of sanctions against countries with authoritarian regimes. However, many studies show that the success of these sanctions can be limited, if the sanctions concern private companies, which often do not share the official views of their government officials and try to circumvent the sanctions. Experts are still analysing whether sanctions can be effective when applied to large economies that have important mineral resources (Russia) or control supply chains (China). Supply chain disruptions during the Covid crisis have shown the vulnerability of many industries. [7]

3. Options for minimizing hybrid threats in relation to sustainable financial systems

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. [20]

Money laundering and terrorist financing 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 to act in the best interest of their citizens and to realize the United Nations Sustainable Development Goals (SDGs), governments and public sector entities need efficiently to prevent different organizational pathologies in which money laundering plays a very important role. [21]

The financial system, which consists of financial institutions, markets, tools and services, which have 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 attack 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, 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 well 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. [22] Unlike potential man-made attacks, a hybrid operation may be better prepared to overwhelm the defence 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. [23] Subsequent recovery would require time, especially in case of damage, manipulation or unavailability of data.

In 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-attack, fall under national security authorities. There is a lack of coordination between the ECB and national authorities, although attacks are reported to the ECB, but information from the ECB to individual institutions is not provided. 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 on 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 reputation. Which, 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. [7]

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.

The financial system plays an important role in the development of the economies of individual countries, 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 development in international financial relations was 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 that should be reached by 2030. [24]

In the last decade, there has been a significant rise of cryptocurrencies on the market. Many research 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. [25 - 34]

Virtual assets present unique anti-money laundering and countering the financing of terrorism (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. [35]

Anti-Money Laundering / Counter Financing of Terrorism (AML/CFT) broadly encompasses regulatory requirements, acts and guidelines designed to curtail the practice of generating funds through unlawful or criminal activities. Several infringement notices were issued to market intermediaries due to provision breaches of the guidelines. Although policies and procedures have been tightened up to the level of satisfaction, assessing the effectiveness of AML/CFT legislation is still necessary. [36]

Artificial intelligence has had a major impact on organisations from Banking through to Law Firms. The rate at which technology has developed in terms of tasks that are complex, technical, and time-consuming has been astounding. The purpose of this paper is to explore the solutions that AI, RegTech and CharityTech provide to charities in navigating the vast amount of anti-money laundering and counter-terror finance legislation so that they comply with the requirements and mitigate the potential risk they face but also develop a more coherent and streamlined set of actions. [37]

The Financial Action Task Force (FATF) is an independent intergovernmental body that develops and promotes policies to protect the global financial system against money laundering, terrorist financing, and the financing of the proliferation of weapons of mass destruction. The FATF recommendations are recognised as the global anti-money laundering (AML) standard. However, more than 30 years after the inception of the FATF, it is not clear that the organisation's framework fully succeeds in realising its potential in mitigating the criminal abuse of financial institutions (FIs), even after it has shifted its focus from rule-based methods that are on their own deficient to an approach that adopts holistic risk-based assessments. Artificial intelligence (AI) has the potential to optimise these risk-based assessments and make AML measures faster, cheaper, and more efficient for FIs. It can potentially help to identify risks and respond to, communicate, and monitor suspicious activity more effectively. [38 -44]

In 1988, the United Nations Convention against Illicit Traffic in Narcotic Drugs and Psychotropic Substances was adopted, which aimed to support the international cooper-

ation of the organizations involved and the adoption of the necessary legislative and administrative measures. [45]

In the following year, the international organization Financial Action Task Force on Money Laundering was established with the aim of analysing money laundering trends and how to minimize them. An important result of their activity was the formulation of 40 recommendations to combat money laundering. These recommendations were supplemented by 9 recommendations related to the financing of terrorism. In February 2012, the FATF published revised recommendations that address issues such as the financing of weapons of mass destruction. This integrated 9 special recommendations on terrorist financing with anti-money laundering measures, resulting in a comprehensive set of 40 FATF recommendations. Since 2012, the FATF has continued to refine and strengthen its recommendations to ensure that countries have the strongest possible tools to combat money laundering, terrorist financing and the financing of the proliferation of weapons of mass destruction. In June 2019, the FATF revised its standards to include binding measures for the regulation and supervision of activities and service providers related to virtual assets or cryptographic assets. In 2022, the FATF further strengthened the global beneficial ownership rules in the FATF Standards to prevent criminals from hiding their illegal activities and dirty money behind secretive corporate structures. We can consider FAFT's recommendations as a comprehensive strategy to combat money laundering and terrorist financing. FAFT currently has 39 member states (Russian Federation has suspended the membership since 24/02/2023) and cooperates with other countries within regional organizations. [46 - 47]

Egmont Group is also an important organization in the fight against money laundering, which ensures cooperation in the safe exchange of intelligence information and experience between 170 national financial intelligence units. Financial intelligence units are uniquely positioned to support national and international efforts to combat the financing of terrorism. The sharing of financial intelligence is of paramount importance, and it is fundamental to international efforts to combat money laundering and terrorism. The Egmont Group supports the efforts of international partners and other stakeholders to implement the resolutions and statements of the UN Security Council, the Financial Action Task Force (FATF) and the G20 Finance Ministers. [48]

Within Europe, the Committee of Experts for the Evaluation of Measures Against Money Laundering and Terrorist Financing - MONEYVAL, is a permanent monitoring body of the Council of Europe tasked with assessing compliance with basic international standards for combating money laundering and terrorist financing and the effectiveness of their implementation, as well as tasked with making recommendations to national authorities regarding the necessary improvements to their systems. Through a dynamic process of mutual evaluations MONEYVAL aims to improve the capacities of national authorities to fight money laundering and terrorist financing more effectively. MONEYVAL aims to ensure that its member states have effective systems in place to combat money laundering and terrorist financing and comply with relevant international standards. [49]

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 [50]

4. The EU in the fight against money laundering and terrorist financing

The fight against money laundering and terrorist financing contributes to global security, 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 launder-

ing 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 acquis and cooperating with networks of competent authorities [51–56].

The Treaty on the European Union provides the legal basis for the adoption of directives on the approximation of the laws of member states, the subject of which is the creation and functioning of the internal market, including the adjustment of anti-money laundering measures. In order to ensure the proper functioning of the financial system and the internal market, European legislation was adopted. Given the changing nature of the money laundering and terrorist financing threat, supported by the constant development of technology and means available to perpetrators, there is still a need to adapt the legal framework in response to these threats.

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 measures the risk of ML / TF (Money Laundering / Terrorist Financing) in countries using data from publicly available sources, such as the Financial Action group (FATF), Transparency International, the World Bank, and the World Economic Forum [57]. A total of 15 indicators of countries' AML / CFT compliance at levels such as corruption, financial standards, policy disclosure and rule of law are combined into one overall risk score. By combining these data sources, the Total Risk Score provides a holistic assessment addressing the structural as well as functional elements of a country's resilience against money laundering and terrorist financing. Scores are aggregated as a composite index using qualitative and expert ranking to create 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. The analysis of the Basel AML index itself covers the period from 2012 to 2020 in selected 23 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). Fig. 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.

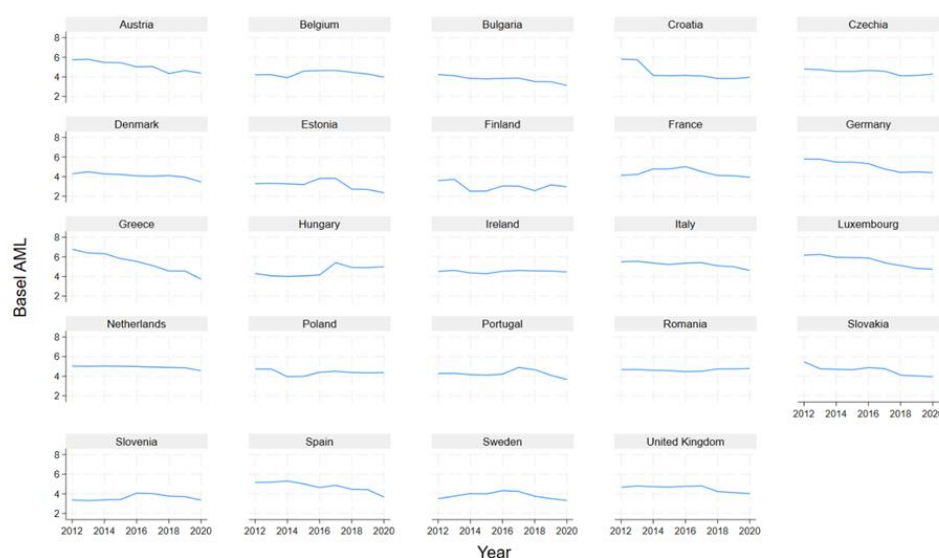


Figure 1. Change in the value of the Basel AML index in the monitored period from 2012 to 2020 in selected EU countries

As a part of the analysis, we will try to define the relationship between the risk of legalization of income from criminal activity and 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:

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

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 doing business, i.e. predictors where we assume their significant influence on ML/TF risk:

1. CPI - 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 a country without corruption, or with a minimum of corruption [58]. 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 value and thus the lowest level of corruption are recorded from available sources in Denmark ($89,222 \pm 1,374$), Finland ($87,000 \pm 1,675$), the Netherlands (82.556 ± 0.558) and Luxembourg (81.222 ± 1.262). On the contrary, the highest average level of corruption is 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 - 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, Financial freedom [59]. 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. Based on the SEDA score, it is possible to examine to what extent countries are able to transform their wealth (expressed in per capita income) into prosperity. The results are displayed using an indicator called the wealth-to-prosperity ratio. This coefficient compares a country's SEDA score to the score that would be expected given the country's GNI (gross national income) per capita. Thus, the coefficient provides a relative indicator of how well a country has transformed its wealth into the well-being of its population. Countries with a coefficient of 1.0 generate welfare in line with what would be expected given their income levels [60]. Countries that have a coefficient greater than 1.0 provide a higher level of well-being than would be expected given their GNI, while countries below 1.0 generate a lower level of prosperity than would be expected. 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 value 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 value 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 methodology for quantifying the score is set in such a way that the percentile in which the economy is located is first calculated for individual indicators. The arithmetic mean is then calculated from the results, which gives us information about the average percentile for each monitored dimension of the business environment [61]. The resulting order (ranking) of the countries is determined by re-averaging these average percentiles of the monitored dimensions for each economy and mathematically ordering them from the smallest to the largest percentile. The evaluated areas and indicators include: Starting a business, Dealing with construction permits, Getting electricity, Registering property, Getting credit, Protecting minority investors, Paying taxes, Trading across borders, Enforcing contracts, 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 value 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 ($66,289 \pm 1,643$), Luxembourg ($68,667 \pm 0,942$), Croatia ($70,467 \pm 2,749$), and Hungary ($70,922 \pm 1,964$).

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 into 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 training (learning) of the network. We demonstrate the basic idea of the term neural network based on the principle of the most commonly used feedforward neural 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 data that is used for learning the network,

- test set of data – another part of data that is used to stop training so that the network is not overdetermined,
- validation set of data – the remaining part of the data on which we will verify the final quality of the model. This is data that was 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 on 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 75-15-15. The performance on each of these sets is then reported in the results, while we generally choose a model that does not have too large fluctuations on individual sets. 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. In total, more than 3700 different artificial neural networks were analysed, while the 5 most suitable networks (ANN1 to ANN5) were used for the analysis of the investigated problem, the basic characteristics of which are listed in tab.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 networks (Multilayer Perceptron) and in one RBF network (Radial Basis Function). 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. Gaussian function, Logistic function or. Hyperbolic tangent and to activate the output function, constant function, logistic function, hyperbolic tangent function or sine function.

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 tab. 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 $0.221 \pm 1.892\%$ with the second highest value of the non-parametric shows position measure, which is the median at the level of -1.111% . This analysed neural network 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 also the second highest value of the standard deviation (14.189%). If we analyse only the validation group of data ($N=32$) of the neural network ANN5 (MLP 4-26-1), then the average deviation value is $1.391 \pm 5.176\%$ 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 $0.367 \pm 1.964\%$ 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 tab.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 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 Fig. 2 to Fig. 4.

Graphic representation of the two most significant predictors of the 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 is defined by the global SEDA index in the monitored period of 2012 to 2020 in 23 selected EU coun-

tries and Great Britain is shown in Fig. 2. The first conclusion, which is based on the nature of the used predictors, 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, Fig. 2 shows the dominant influence of the CPI index on the overall change of the monitored variable. Fig. 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 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 legalization of income from criminal activity and 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.

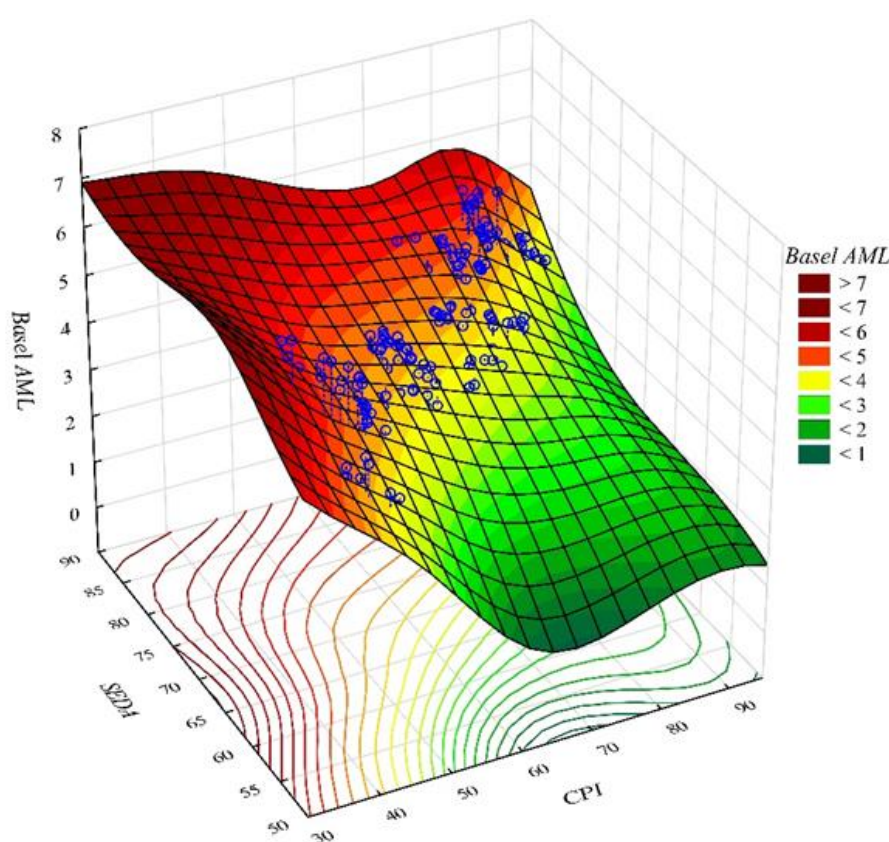


Figure 2 Predicted impact of the global CPI and SEDA indices on the change in the value of the Basel AML index

The second analysed 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 doing business (Fig. 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).

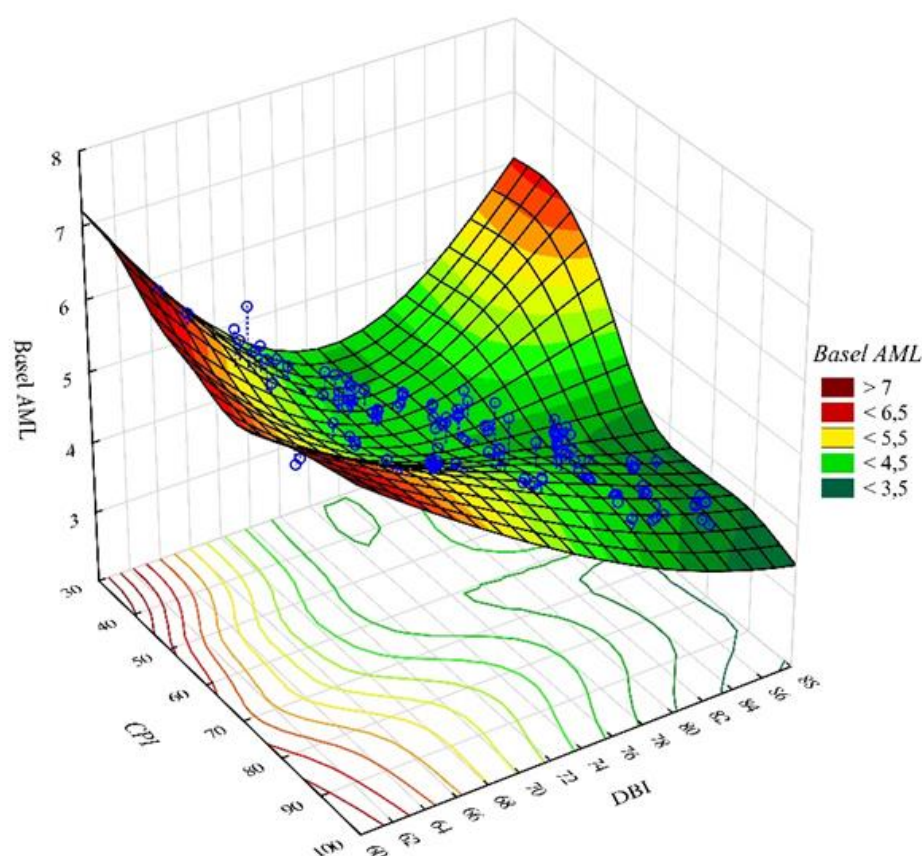


Figure 3 Predicted impact of the global CPI and DBI indices on the change in the value of the Basel AML index

Fig. 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 if the business environment is simple but at the same time there is a high risk of corruption by civil servants and politicians.

The last analysed 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 (Fig. 4).

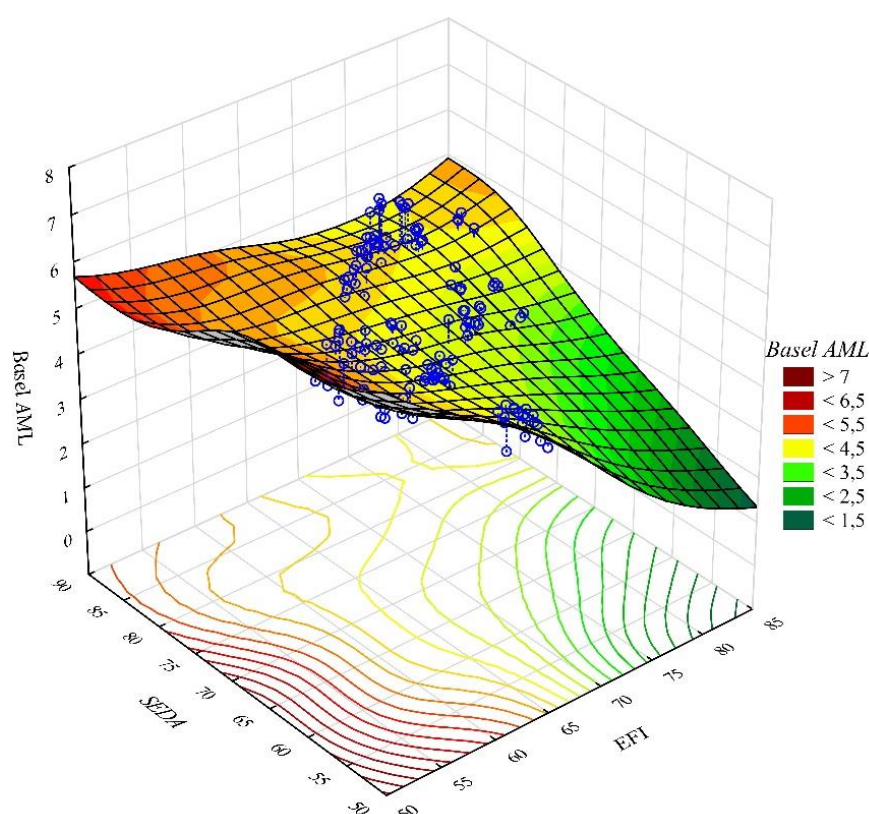


Figure 4. Predicted impact of the SEDA and EFI global indices on the change in the value of the Basel AML index

Fig. 4 shows that the predicted value of the Basel AML index, i.e. the highest level of ML/TF 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, 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 to 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 anti-money laundering (AML) and anti-terrorist financing (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 money laundering and terrorist financing. 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. [62].

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 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 analysing the complicated connections between hybrid threats, money laundering, terrorist financing and the financial system, current challenges for stakeholders have been raised, which can result in informed decision-making, support of cooperation between stakeholders, better decision-making process directed towards such innovations that will minimize impacts and consequences 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 a number of 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 the 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 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. [63 - 65]. It is also important that the measures are accepted and supported by most of the population.

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

Funding: The 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: Not applicable.

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

References

1. Concept for the fight of the Slovak Republic against hybrid threats, (2022). <https://www.nbu.gov.sk/wp-content/uploads/PHHD/Koncepcia-boja-SR-proti-hybridnym-hrozbam.pdf>

2. Riggs, H.; Tufail, S.; Parvez, I.; Tariq, M.; Khan, M.A.; Amir, A.; Vuda, K.V.; Sarwat, A.I. (2023) Impact, vulnerabilities, and mitigation strategies for cyber-secure critical infrastructure. *Sensors*, 23, 4060. <https://doi.org/10.3390/s23084060>
3. Koraus, A.; Kurilovská L.; Šišulák, S. (2022). Increasing the Competencies 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.
4. Maashi, M.; Alabdullah, B.; Kouki, F. (2023) Sustainable financial fraud detection using garra rufa fish optimization algorithm with ensemble deep learning. *Sustainability*, 15, 13301. <https://doi.org/10.3390/su151813301>
5. Kurshan, E.; Shen, H.D. (2020). graph computing for financial crime and fraud detection: trends, challenges and outlook. *International journal of semantic computing* 14 (04) , pp.565-589. DOI: [10.1142/S1793351X20300022](https://doi.org/10.1142/S1793351X20300022)
6. Leonov, S.; Yarovenko, H.; Boiko, A.; Dotsenko, T. (2019) Prototyping of information system for monitoring banking transactions related to money laundering © SHS Web of Conferences 65(1):04013. DOI: [10.1051/shsconf/20196504013](https://doi.org/10.1051/shsconf/20196504013)
7. Antwi,S.; Tetteh, A.B.; Armah P.; Dankwah, E.O. (2023) Anti-money laundering measures and financial sector development: Empirical evidence from Africa, *Cogent Economics & Finance*, 11:1, 2209957, DOI: [10.1080/23322039.2023.2209957](https://doi.org/10.1080/23322039.2023.2209957)
8. Mohammed, S.A.S.A. (2019) Money laundering in selected emerging economies: is there a role for banks? *Journal of money laundering control*. DOI: 10.1108/JMLC-12-2019-0096
9. Kumar, N.; Seetharaman, A. (2022) Adoption of anti-money laundering by banks. *Journal: International journal of early childhood special education*. Volume 14. Issue 3. Page 10541-10547. DOI [10.9756/INT-JECSE/V14I3.1238](https://doi.org/10.9756/INT-JECSE/V14I3.1238)
10. Ofoeda, I.; Agbloyor, E.K.; Abor, J.Y.; Achampong, K.O. (2022) Foreign direct investment, anti-money laundering regulations and economic growth. *Journal of international development*. Volume 34. Issue 3. Page 670-692. DOI [10.1002/jid.3582](https://doi.org/10.1002/jid.3582)
11. Ofoeda, I.; Agbloyor, E.K.; Abor, J.Y. (2022) How do anti-money laundering systems affect FDI flows across the globe? *Cogent economics & finance* 10 (1). <https://doi.org/10.1080/23322039.2022.2058735>
12. Ofoeda, I. (2022) Anti-money laundering regulations and financial inclusion: empirical evidence across the globe. *Journal of financial regulation and compliance*. Volume 30. Issue 5. Page 646-664. DOI [10.1108/JFRC-12-2021-0106](https://doi.org/10.1108/JFRC-12-2021-0106)
13. Ofoeda, I.; Agbloyor, E.; Abor, J.Y. (2022) Financial sector development, anti-money laundering regulations and economic growth. *Journal: International journal of emerging markets*. DOI [10.1108/IJOEM-12-2021-1823](https://doi.org/10.1108/IJOEM-12-2021-1823)
14. Ofoeda, I.; Agbloyor, E.K.; (...); Osei, K.A. (2022) Anti-money laundering regulations and financial sector development. *International journal of finance & economics* 27 (4) , pp.4085-4104. <https://doi.org/10.1080/23322039.2023.2209957>
15. Herman, E.; Zsido, K.E. (2023). The Financial Sustainability of Retail Food SMEs Based on Financial Equilibrium and Financial Performance. *Mathematics*, Volume 11, Issue 15 DOI [10.3390/math11153410](https://doi.org/10.3390/math11153410)
16. Bajarūnas, E. (2020). Addressing hybrid threats: Priorities for the EU in 2020 and beyond. In *European view*, 19(1), s. 62–70. <https://doi.org/10.1177/1781685820912041>
17. Aho, A.; Midões, C.; Šnore, A. (2020) Hybrid threats in the financial system. *The European Centre of excellence for countering hybrid threats*. Helsinki. ISBN 978-952-7282-63-2
18. Horn, S.; Reinhart, C.; Trebesch, C. (2021) China's overseas lending, In *Journal of international economics*. Volume 133. 103539. <https://doi.org/10.1016/j.jinteco.2021.103539>
19. Tavares da Silva, J.; Pereira, R. (2020) China and the Portuguese Atlantic: The BRI's last puzzle pieces. In *Leandro, F., Duarte, P.. The Belt and Road Initiative – An Old Archetype of a New Development Model*. Palgrave Macmillan. DOI: [10.1007/978-981-19-6700-9_42](https://doi.org/10.1007/978-981-19-6700-9_42)

20. Hamed, R (2023) The role of internal control systems in ensuring financial performance sustainability. *Journal Sustainability*. Volume 15, Issue 13. [DOI 10.3390/su151310206](https://doi.org/10.3390/su151310206)
21. Dobrowolski, Z.; Sułkowski, Ł. (2020) Implementing a sustainable model for anti-money laundering in the United Nations development goals. *Sustainability*, 12, 244. <https://doi.org/10.3390/su12010244>
22. Demertzis M. and Wolff, G. (2019) Hybrid and cybersecurity threats and the European Union's financial system. Policy Contribution Issue n°10. https://www.bruegel.org/wp-content/uploads/2019/09/PC-10_2019.pdf.
23. Savolainen, J. (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. https://www.hybridcoe.fi/wp-content/uploads/2019/11/NEW_Working-paper_WMDivers_2019_rgb.pdf.
24. Cantero-Saiz, M. ; Torre-Olmo, B. ; Sanfilippo-Azofra, S. (2023) Sustainable banking, financial strength and the bank lending channel of monetary policy. *Journal E & M ekonomie a management*. Volume 26, Issue 1, Page 165-185. [DOI: 10.15240/tul/001/2023-1-010](https://doi.org/10.15240/tul/001/2023-1-010)
25. Faccia, A.; Mocteanu, N.R.; (...); Mataruna-Dos-Santos, L.J. (2020) Electronic Money Laundering, The Dark Side of Fintech: An Overview of the Most Recent Cases. ICIME 2020: 2020 12th International Conference on Information Management and Engineering. ICIME 2020: Proceedings of the 2020 12th International Conference on Information Management and Engineering, pp.29-34. [DOI: 10.1145/3430279.3430284](https://doi.org/10.1145/3430279.3430284)
26. Al-Tawil, T.N. (2022) Anti-money laundering regulation of cryptocurrency: UAE and global approaches. *Journal Of Money Laundering Control*. [DOI 10.1108/JMLC-07-2022-0109](https://doi.org/10.1108/JMLC-07-2022-0109)
27. Al-Tawil, T.N.; Younies, H. (2020) The implications of the Brexit from EU and bitcoin. *Journal of money laundering control*. [DOI: 10.1108/JMLC-05-2020-0050](https://doi.org/10.1108/JMLC-05-2020-0050)
28. Dyntu, V.; Dykyi, O. (2018) Cryptocurrency in the system of money laundering. *Baltic journal of economic studies* 4 (5) , pp.75-81. [DOI: 10.30525/2256-0742/2018-4-5-75-81](https://doi.org/10.30525/2256-0742/2018-4-5-75-81)
29. Barone, R.; Masciandaro, D. (2019) Cryptocurrency or usury? Crime and alternative money laundering techniques. *European journal of law and economics* 47 (2) , pp.233-254. [DOI: 10.1007/s10657-019-09609-6](https://doi.org/10.1007/s10657-019-09609-6)
30. Dupuis, D.; Gleason, K. (2021) Money laundering with cryptocurrency: Open doors and the regulatory dialectic. *Journal of Financial Crime* 28 , pp.60-74. [DOI: 10.1108/JFC-06-2020-0113](https://doi.org/10.1108/JFC-06-2020-0113)
31. Alarab, I.; Prakoonwit, S. and Nacer, M. I. (2020) Competence of graph convolutional networks for anti-money laundering in bitcoin blockchain. *Proc. 5th Int. Conf. Mach. Learn. Technol. Acm int c proceeding* , pp.23-27. [DOI: 10.1145/3409073.3409080](https://doi.org/10.1145/3409073.3409080)
32. Kshetri, N. (2021) The role of artificial intelligence in promoting financial inclusion in developing countries. *Journal of global information technology management* 24 (1) , pp.1-6. <https://doi.org/10.1080/1097198X.2021.1871273>
33. Jayasekara, S.D. (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*, Vol. 24 No. 1, pp. 150-162, [DOI: 10.1108/JMLC-04-2020-0035](https://doi.org/10.1108/JMLC-04-2020-0035).
34. Kirimhan, D. (2023) Importance of anti-money laundering regulations among prosumers for a cybersecure decentralized finance. *JOURNAL OF BUSINESS RESEARCH*. Volume 157. [DOI 10.1016/j.jbusres.2022.113558](https://doi.org/10.1016/j.jbusres.2022.113558)
35. Schmidt, A. (2022) Virtual assets: compelling a new anti-money laundering and counter-terrorism financing regulatory model. *International journal of law and information technology*. Volume 29. Issue 4. Page 332-363. [DOI 10.1093/ijlit/eaac001](https://doi.org/10.1093/ijlit/eaac001)
36. Khan, N. I.; Abdul Jani, M. A.; Zulkifli, A. A.. (2021) The Effectiveness of Anti-Money Laundering / Counter Financing of Terrorism Requirements in Fund Management Companies. *Int. J. Serv. Manag. Sustain.* 6 (2) , pp.53. [DOI: 10.24191/ijsms.v6i2.15572](https://doi.org/10.24191/ijsms.v6i2.15572)
37. Singh, C.; Lin, W.W. (2021) Can artificial intelligence, RegTech and CharityTech provide effective solutions for anti-money laundering and counter-terror financing initiatives in charitable fundraising. *Journal of money laundering control* 24 (3) , pp.464-482. [DOI: 10.1108/JMLC-09-2020-0100](https://doi.org/10.1108/JMLC-09-2020-0100)
38. Sultana, S. (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 (4), pp.931-947. [DOI: 10.1108/JMLC-04-2022-0060](https://doi.org/10.1108/JMLC-04-2022-0060)

39. Goldbarsht, D. (2022) Artificial Intelligence and Financial Integrity: The Case of Anti-money Laundering. *Journal of banking and finance law and practice*. Volume 33. Issue 1. Page 21-36. <https://researchers.mq.edu.au/en/publications/artificial-intelligence-and-financial-integrity-the-case-of-anti-> 736
737
40. Begishev, I.R. (2021) Criminological classification of robots: risk-based approach pravoprimenenie-law enforcement review. DOI: 10.52468/2542-1514.2021.5(1).185-201 738
739
41. Huarte, E.G. (2020) Uncertain causation in civil liability arising from artificial intelligence. *Revista general de derecho europeo*. ISBN: 978-92-846-7127-4. DOI: 10.2861/737677 740
741
42. Alessa R.(2019) Webinar-An Executive Guide on How to Use Machine Learning and AI for AML Compliance. [URLhttps://www.youtube.com/watch?v=k46](https://www.youtube.com/watch?v=k46) 742
743
43. Summerfield, R. (2018) Strengthening AML Protection through AI. *Financier Worldwide Magazine*. [URL/www.financierworldwide.com/strengthening-aml-protection-through-ai#YV6BGi0Rrw4](https://www.financierworldwide.com/strengthening-aml-protection-through-ai#YV6BGi0Rrw4) 744
745
44. Chan, J.; Moses, L.B. (2017) Making Sense Of Big Data For Security. *British journal of criminology* 57 (2), pp.299-319. DOI:10.1093/bjc/azw059 746
747
45. UN Office on Drugs and Crime, About the United Nations Office on Drugs and Crime. 2023 <https://www.unodc.org/unodc/en/about-unodc/index.html>. 748
749
46. The Financial Action Task Force (FATF), 2023, The Financial Action Task Force (FATF) leads global action to tackle money laundering, terrorist and proliferation financing. <https://www.fatf-gafi.org/en/publications/Fatfrecommendations/Fatf-recommendations.html> 750
751
47. FATF (2017) Anti-money laundering and terrorist financing measures and financial inclusion: with a supplement on customer due diligence. FATF/OECD Guidance, pp.2. <https://www.fatf-gafi.org/en/publications/Fatfgeneral/Financial-inclusion-cdd-2017.html> 752
753
48. EGMONT GROUP (2023) <https://egmontgroup.org/> 754
755
49. Moneyval (2023) Committee of Experts on the Evaluation of Anti-Money Laundering Measures and the Financing of Terrorism. <https://www.coe.int/en/web/moneyval> 756
757
50. Tuyon, J; Onyia, O.P. ; Ahmi, A. ; Huang, CH. (2022) Sustainable financial services: reflection and future perspectives. *Journal Of Financial Services Marketing* DOI 10.1057/s41264-022-00187-4 758
759
51. Directive (EU) 2018/1673 of the European Parliament and of the Council of 23 October 2018 on combating money laundering by criminal law. <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32018L1673> 760
761
52. 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. <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32018L0843> 762
763
53. 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. <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32019L1153> 764
765
54. European Commission (2020) Action Plan for a comprehensive Union policy on preventing money laundering and terrorist financing' COM. <https://www.dlapiper.com/en/insights/publications/2021/10/anti-money-laundering-and-counterterrorism-financing> 766
767
55. European Commission (2019) Assessment of recent alleged money laundering cases involving EU credit institutions' COM. <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52019DC0373> 768
769
56. European Commission (2019) Assessment of the risk of money laundering and terrorist financing affecting the internal market and relating to cross -border activities' COM. [https://www.eba.europa.eu/sites/default/documents/files/document_library/Publications/Guidelines/2023/1054144/Guidelines%20on%20MLTF%20risk%20management%20and%20access%20to%20financial%20services.p](https://www.eba.europa.eu/sites/default/documents/files/document_library/Publications/Guidelines/2023/1054144/Guidelines%20on%20MLTF%20risk%20management%20and%20access%20to%20financial%20services.pdf) 770
771
772
773
774
775
776
777
778
779
780
781
57. Manning, M.; Wong, G.T.W.; Jevtovic, N. (2021) Investigating the relationships between FATF recommendation compliance, regulatory affiliations and the Basel Anti-Money Laundering Index. *Secur J* 34, 566–588. <https://doi.org/10.1057/s41284-020-00249-z> 782
783
784

58. Wilhelm, P.G. (2002) International validation of the corruption perceptions index: implications for business ethics and entrepreneurship education. *Journal of business ethics* 35, 177–189. <https://doi.org/10.1023/A:1013882225402>
59. Dialga, I. and Vallée, T. (2021), "The index of economic freedom: methodological matters", *Studies in Economics and Finance*, Vol. 38 No. 3, pp. 529-561. <https://doi.org/10.1108/SEF-07-2015-0181>
60. Chu-Long Huang, Jonathan Vause, Hwong-Wen Ma, Chang-Ping Yu. (2012) Using material/substance flow analysis to support sustainable development assessment: A literature review and outlook, *Resources, Conservation and Recycling*. Volume 68. Pages 104-116, ISSN 0921-3449, <https://doi.org/10.1016/j.resconrec.2012.08.012>
61. Gürler, C. (2023) Ease of doing business in European Union countries and candidates. *Pamukkale University Journal of Social Sciences Institute / Pamukkale Üniversitesi Sosyal Bilimler Enstitüsü Dergisi* [online], 57, 81-93. ISSN 13082922. [DOI:10.30794/pausbed.1214548](https://doi.org/10.30794/pausbed.1214548)
62. Dobrowolski, Z.; Sulkowski, L. (2020) Implementing a sustainable model for anti-money laundering in the United Nations development goals. *Sustainability* 12 (1) <https://doi.org/10.3390/su12010244>
63. Alsuwailem, A.A.S.; Saudagar, A.K.J. (2020) Anti-money laundering systems: a systematic literature review. *Journal of money laundering control* 23 (4) , pp.833-848. [DOI: 10.1108/JMLC-02-2020-0018](https://doi.org/10.1108/JMLC-02-2020-0018)
64. Pourhabibi, T; Ong, KL; (...); Boo, YL. (2020) Fraud detection: A systematic literature review of graph-based anomaly detection approaches. *Decision Support Systems* 133(4):113303 [DOI: 10.1016/j.dss.2020.113303](https://doi.org/10.1016/j.dss.2020.113303)
65. Jensen, R.I.T.; Iosifidis, A. (2023) Qualifying and raising anti-money laundering alarms with deep learning. *Journal: Expert Systems With Applications*. Volume 214. [DOI 10.1016/j.eswa.2022.119037](https://doi.org/10.1016/j.eswa.2022.119037)

Disclaimer/Publisher's Note: The statements, opinions and data contained in all publications are solely those of the individual author(s) and contributor(s) and not of MDPI and/or the editor(s). MDPI and/or the editor(s) disclaim responsibility for any injury to people or property resulting from any ideas, methods, instructions or products referred to in the content.