SOCIAL SCIENCES

MANAGEMENT ECONOMICS EDUCATION

APPLICATION OF INFORMATION TECHNOLOGIES

MEST JOURNAL

VOL. 13

NO. 1

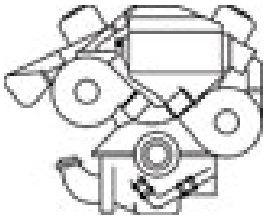
January 2025

ISSN 2334-7171

EDITED BY

Zoran Čekerevac

ISSN 2334-7058 (Online) DOI 10.12709/issn.2334-7058



ISSN 2334-7171
ISSN 2334-7058 (Online)
DOI 10.12709/issn.2334-7058
This issue:
DOI 10.12709/mest.13.13.01.00

MEST Journal

Management
Economics
Society
Technologies

Edited by
Zoran Čekerevac

CIP – Каталогизација у публикацији
Народна библиотека Србије, Београд

005+37+3+66

MEST Journal : Management, Education, Science & Society, Technologies / editor-in-chief Zoran P. Čekerevac. – [Štampano izd.]. – Vol. 13, no. 1 (2025) – – Belgrade : MESTE NGO; Toronto : SZ & Associates, 2013- (Belgrade : ICIM+). – 30 cm
Polugodišnje. - Drugo izdanje na drugom medijumu: MEST Journal (Online) = ISSN 2334-7058
ISSN 2334-7171 = MEST Journal (Štampano Izd.)

COBISS.SR- ID 196182028

Circulation: 100 copies

FBIM Transactions DOI 10.12709/issn.2334-704X
ISSN 2334-704X (Online) ISSN 2334-718X (Print)

As of September 2022, the FBIM Transactions has been incorporated and merged with MEST Journal. Since then, they have been published under the common name **MEST Journal**.

MEST Journal online
www.mest.meste.org
DOI 10.12709/issn.2334-7058
Current Issue: DOI 10.12709/mest.13.13.01.00

MEST Journal is an international academic journal, the official journal of the non-profit organization MESTE, published online, as well as print, which publishes scientific and professional research articles and reviews in the English language. MEST Journal is published from Belgrade - Serbia and Toronto - Canada. The focal point of the journal is at international level, with the view on matters from a global perspective, but, also, some papers concerning some local specific events could be published. The science and technological advancements and their socio-political impact that happens all over the world can find a place in the MEST Journal. The journal is indexed by Index Copernicus in ICI Journals Master List ICV from 2015, in ERIH PLUS from 2017, in EBSCO, Google Scholar, CrossRef, COBIS.SR, COBIB.RS, Kobson, Scilit, CiteFactor, etc.

Publishers

- **MESTE NGO** – Belgrade
- **SZ & Associates**, Toronto, Canada

Editorial board – Scientific Board:

Editorial staff – Production:

Editor-in-chief:	Prof. Dr. Dr. h. c. **Zoran Čekerevac**, MESTE, Belgrade, RS
Technical editor:	**Damjan Čekerevac**, MSc, University of Coimbra, Coimbra, Portugal
Technical editor:	**Slavko Zdravković**, MSc, SZ & Assoc.- Toronto, Canada
Lector:	**Sanja Manojlović**, MA, Faculty of Business and Law, Belgrade, Serbia
Manager:	**Milanka Bogavac,** PhD, Dr. h. c., Faculty of Business and Law, Belgrade, Serbia
Design:	SZ & Assoc. – Toronto, Canada

Printed by: **Planeta print, Belgrade** Circulation: 100 copies
The journal was published online at URL: https://www.meste.org/ojs/index.php/mest/index

The MEST Journal is registered in doiSerbia of the National Library of Serbia, COBIB.SR, Matica Srpska Library, COBISS.SR, Google Scholar, CrossRef, OALIB, EleCas base of KoBSON, the Index Copernicus ICI Journals Master List from 2015 (*ICV 2022 =100.00*), EBSCO, Scilit, ROAD, ERIH PLUS, CiteFactor, and in the ResearchBib (IF: 2023 Evaluation Pending).

All published papers have been internationally reviewed

Two issues of journal are published annually, on January 15th, and July 15th.

ISSN 2334-7058 (Online) &
ISSN 2334-7171

THEMATIC AREAS

Economics

Management in economics

Public management

Management in industry

Entrepreneurship

Management in crisis situations

Management in transport

Technologies and quality tools in management

IT use in the management

Management in ecology

Management in sport

Economic education and teaching

Information security and information system security

Business information system

Innovation and technology

Legal aspects of management

Economics and Law

These are basic, but not exclusive themed areas.

MEST Journal
DOI 10.12709/mest.13.13.01.01

GDP AND BUSINESS CREATION RELATIONSHIP IN ROMANIAN DEVELOPMENT REGIONS

Daniel Badulescu
University of Oradea, Department of Economics and Business, Oradea, Romania
https://orcid.org/0000-0001-8653-0149

Dragos Dianu
University of Oradea, Oradea, Romania

Ramona Simut
University of Oradea, Department of Economics and Business, Oradea, Romania
https://orcid.org/0000-0003-1673-3586

Alina Badulescu
University of Oradea, Department of Economics and Business, Oradea, Romania
https://orcid.org/0000-0002-0090-9340

JEL Category: **M13, L26, R11**

Abstract

The relationship between economic growth, most commonly measured by Gross Domestic Product (GDP), and the rate of business creation is central to understanding how new businesses contribute to economic development and how economic conditions influence entrepreneurial activities. The literature emphasizes the significant role of small and medium-sized enterprises (SMEs) in economic growth, highlighting the importance of the type of entrepreneurship (opportunity or necessity), the economic context, the role of support measures, and entrepreneurial education. New businesses contribute to innovation, productivity, and job creation but the quality and intensity of these contributions significantly varies across regions. Countries and regional disparities affect the rate of business creation and economic growth. Moreover, innovative regions demonstrate greater resilience to economic crises and possess an enhanced ability to resume economic growth and diversification swiftly. In this research, we set out to identify a unidirectional or bidirectional long-term and short-term relationship between GDP variables and the rate of establishment of companies at the level of Romania, respectively at

Address of the corresponding author:
Daniel Badulescu
dbadulescul@uoradea.ro

the component development region, based on the statistical data available for the period 2006-2021. We found a long-term relationship between GDP and the establishment rate of companies in Romania and most of the component regions. This relationship is not statistically significant in the short term. While the rate of new firm establishment does impact economic growth in certain areas over the short and long term, our findings indicate that economic growth more significantly influences the establishment of new firms in the long term. However, the varied results suggest that further analysis is needed.

Keywords: *GDP, Business Creation, Economic Growth, Entrepreneurship, Regional Disparities, SMEs, Innovation*

1 INTRODUCTION

The relationship between the evolution of GDP and the firms' formation rate has been intensively studied in the economic literature, revealing a complex interaction between economic growth, entrepreneurial activity, and business creation. Studies have shown that new companies contribute to GDP growth by stimulating innovation, creating jobs, and increasing productivity. Audretsch and Keilbach (2003) highlight that regions with higher levels of entrepreneurial activity tend to experience faster economic growth due to either the spillover effects of innovation and increased competition (Aparicio, Urbano, & Gomez, 2023) or institutional structures of support (Bosma & Levie, 2010). Similarly, Acs & Audretsch (2010) emphasize the importance of entrepreneurial ecosystems and the spillover effects of knowledge and innovation from new ventures to wider economic structures (Munyo & Veiga, 2024). Several studies on the relationship between economic growth and business creation, whether at the European level (European Commission, 2023) or specifically in Romania (Dianu, Gavriluț, Badulescu, Simut, & Herte, 2019; International Finance Corporation, 2023), indicate a complex, bidirectional relationship, often influenced by various factors, varying and uneven across different regions.

This paper investigates the connection between economic growth and business formation rates in Romania, both at the regional and national levels, to identify specific trends and characteristics of the SME sector's contribution to economic growth, thereby providing valuable insights for effective policy-making and supporting entrepreneurship and business creation.

2 LITERATURE REVIEW

Most of the studies of the last decades coherently emphasize the significant role of entrepreneurial activity in stimulating economic growth, also highlighting the significance of the type of entrepreneurship and the economic context in which it occurs. For example, fast-growing startups, often referred to as "gazelle", have a more substantial impact on economic growth compared to small businesses (Abdinnour & Adeniji, 2023), where the founder rather wants to ensure a certain level of income and image in the community (life-style entrepreneurship) or those severely constrained by the access to financing, hostile economic environment or lack of growth prospects (Badulescu & Badulescu, 2014). This distinction is crucial because it underscores the importance of supporting high-potential businesses that can drive significant economic change. Interpreting the empirical evidence on the relationship between private initiative and economic growth, Carree & Thurik (2010) highlight that the impact varies depending on the type of entrepreneurial activity and the stage of economic development. Stam & van Stel (2011) find that opportunity entrepreneurship has a significant positive impact on GDP growth compared to necessity entrepreneurship. Opportunity entrepreneurship prevails in developed countries reinforcing the contributions of Wennekers et al. (2005), according to which all types of entrepreneurship contribute to economic growth. However, the contribution of new, dynamic enterprises to GDP growth is better highlighted in developed countries.

New businesses play an important role in the economy by introducing new products and services and increasing competition, productivity, and innovation, which are essential for economic growth. Probably the most visible and expected contribution of new firms is the creation of (new) jobs. They come not only to solve a pressing economic-social and political challenge (reducing unemployment) but the employment opportunities and individual incomes generated by these businesses can lead to an increase in consumer spending, which in turn stimulates economic growth (Munyo & Veiga, 2024). However, the

contribution of the employment of new companies, and especially of their majority, usually less innovative, should not be overestimated. Along with the creation of fresh positions in emerging firms, an equally important number of jobs disappear due to the discontinuation of many small firms lacking experience and resources. (Aga, Francis, & Meza, 2015). The quality of jobs created by new businesses also matters. High-quality jobs that offer good wages and careers, with a substantial impact on economic growth, are generated by a small fraction of new entrants.

Startups and new businesses often bring innovative products and services to market, driving productivity improvements and economic expansion. The rate of technology adoption and the ability to scale innovations are critical factors that determine the impact of new ventures on GDP growth (Munyo & Veiga, 2024). A stable environment, supportive policies, and favorable regulations that reduce barriers to entry and support enterprises in their diversity can enhance the positive impact of new ventures on economic growth and stimulate the desire to establish new companies (Aparicio, Urbano, & Gomez, 2023). Streamlined business registration processes, access to finance, and protection of intellectual property rights are essential components of such an environment. The regulatory environment and business regulation associated with the labor market (Loayza, Oviedo, & Serven, 2005), (Jalilian, Kirkpatrick, & Parker, 2007), tax burden, trade barriers, bankruptcy and contract enforcement, reforms in the economy (Haidar, 2012) are undoubtedly important factors in the growth or stagnation of the SMEs sector, affecting the new entrants flow (Badulescu, Badulescu, Sipos-Gug, Herte, & Gavrilut, 2020), (Munyo & Veiga, 2024).

Finally, different cultural attitudes towards entrepreneurship and the availability of entrepreneurship education and training can influence, positively or negatively, the rate of new business establishment and its impact on economic growth (Walter & Block, 2016), (Ndofirepi, 2020), (Patrício & Ferreira, 2024). Research has shown that the impact of new businesses on GDP growth can vary across sectors – high-tech and knowledge-intensive ones often have a more significant contribution to GDP from new enterprises compared to traditional sectors, highlighting the effects of agglomeration and location economies (Bosma, van Stel, & Suddle, 2008), and the importance of local and regional factors (Audretsch & Fritsch, 1994), (Reynolds, Storey, & Westhead, 1994).

The relationship between the evolution of GDP and the firms' creation rate varies significantly across regions and is influenced by local economic conditions, institutional frameworks, and innovation capacities (Badulescu, et al., 2024). Studies highlight that regions with robust entrepreneurial ecosystems tend to experience higher GDP growth rates due to the positive impact of new business formation on job creation, innovation, and productivity (Capello, 2019). Research indicates that regional disparities, influenced by factors such as access to capital, infrastructure, and skilled labor, affect the rate of new business creation and economic growth (Floerkemeier, Spatafora, & Venables, 2021). For example, regions identified as innovation leaders in Europe recovered faster after the financial crisis of 2007-2008 (Bristow & Healy, 2018), and this resilience is attributed to the ability of innovative regions to adapt and reinvent their economic structures.

3 DATA AND METHODOLOGY

Romania is divided into eight development regions (NUTS2 level, see Figure 1) (Eurostat, 2021), ranked by GDP per capita as follows: the capital region, Bucharest-Ilfov, with over 28,400 EUR per capita, followed by the West Region (12,200 EUR per capita), Center Region (11,600 EUR per capita), North-West Region (10,500 EUR per capita), South-East Region (10,100 EUR per capita), South-West Region (9,400 EUR per capita), South-Muntenia Region (9,390 EUR per capita), and North-East Region (7,900 EUR per capita) (National Institute of Statistics (Romania), 2024).

The number of enterprises has grown steadily but slowly over the analyzed period, from around 555,000 in 2008-2010 to approximately 671,900 in 2022. Nearly a quarter of all companies registered in Romania (24.1%) are in the capital region, Bucharest-Ilfov, followed by the North-West Region (15%), Center, North-East, South-East, and South regions (each between 11% and 12%), while the South-West and North-East regions have the lowest percentages, between 7% and 9% each (National Institute of Statistics (Romania), 2024).

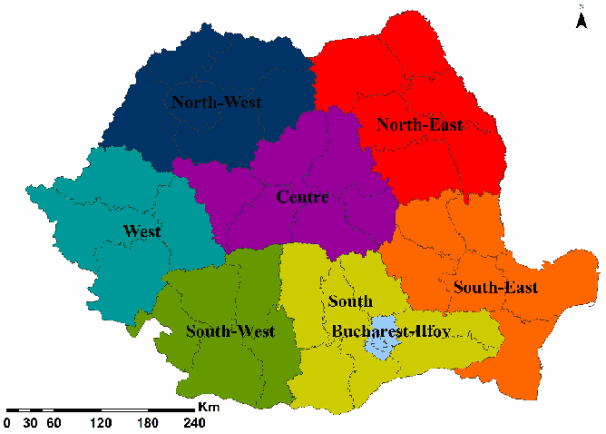


Fig. 1 The Development Regions of Romania (Muntean, Caranfil, & Ilovan, 2021)

This study investigates whether a unidirectional or bidirectional relationship exists, in both short-term and long-term contexts, between GDP and the rate of company creation across Romania and its development regions. For this, we used the annual data provided by Eurostat/ National Institute of Statistics (Romania) for the period 2006-2021 (Eurostat, 2024), (National Institute of Statistics (Romania), 2024). Given that the two variables have different measurement units, to process and interpret the results, the statistical data were logarithmized.

To analyze the relationship between the two variables, we tested their stationarity using the Augmented Dickey-Fuller (ADF) test (Dickey & Fuller, 1979, p. 427). We applied Johansen's cointegration method to assess the existence of a long-term equilibrium relationship. Based on these results, we used the appropriate model and tested for Granger causality between the variables.

As long as there is at least one unit root, the model is non-stationary, and we proceed with the cointegration tests application, such as the Johansen test. Otherwise, a VAR (Vector Autoregression) model will be used to explain the relationship between the variables. If the variables are cointegrated, the most appropriate model is the VECM (Vector Error Correction Model), which captures both the short-term dynamics and the long-term equilibrium relationship. Then, causality between the variables can be tested using the Granger causality test within this framework. If there is no cointegration relationship between the variables, the VAR model in first differences (VARD) will be applied, and subsequently, the Granger causality test will be performed. To investigate the presence of a long-term relationship, we will begin by testing the stationarity of the variables using the ADF (Augmented Dickey-Fuller) test. Identifying non-stationarity is essential to proceed with cointegration analysis and establish long-term equilibrium relationships.

4 RESULTS AND DISCUSSION

In Table 1, we presented the results obtained after applying the ADF test for the two logarithmic variables, GDP and the rate of establishment of companies, at the level of Romania and each region.

Table 1. Testing the stationarity of the variables

Variable	Test for a unit root in Level		Test for a unit root in the first difference	
	t-statistic (ADFcalc)	Test critical value	t-statistic (ADFcalc)	Test critical value
Romania				
LGDP	-1.901457	1% (-2.771926) 5% (-1.974028) 10% (-1.602922)	-1.684449	1% (-2.771926) 5% (-1.974028) 10% (-1.602922)
LSetup Rate	-2.740895	1% (-4.004425) 5% (-3.098896) 10% (-2.690439)	-6.556934	1% (-4.057910) 5% (-3.119910) 10% (-2.701103)
București – Ilfov Region				
LGDP	-2.078852	1% (-2.771926) 5% (-1.974028) 10% (-1.602922)	-1.993195	1% (-2.771926) 5% (-1.974028) 10% (-1.602922)
LSetup Rate	-2.374950	1% (-4.004425) 5% (-3.098896) 10% (-2.690439)	-4.458577	1% (-4.200056) 5% (-3.175352) 10% (-2.728985)

Variable	Test for a unit root in Level		Test for a unit root in the first difference	
	t-statistic (ADFcalc)	Test critical value	t-statistic (ADFcalc)	Test critical value
Centre Region				
LGDP	-3.101218	1% (-2.771926) 5% (-1.974028) 10% (-1.602922)	-1.976044	1% (-2.771926) 5% (-1.974028) 10% (-1.602922)
LSetup Rate	-2.965717	1% (-4.004425) 5% (-3.098896) 10% (-2.690439)	-6.913363	1% (-4.057910) 5% (-3.119910) 10% (-2.701103)
North–East Region				
LGDP	-2.693614	1% (-2.771926) 5% (-1.974028) 10% (-1.602922)	-1.979014	1% (-2.771926) 5% (-1.974028) 10% (-1.602922)
LSetup Rate	-2.991062	1% (-4.004425) 5% (-3.098896) 10% (-2.690439)	-6.718423	1% (-4.057910) 5% (-3.119910) 10% (-2.701103)
North–West Region				
LGDP	-1.364899	1% (-2.771926) 5% (-1.974028) 10% (-1.602922)	-2.055575	1% (-2.771926) 5% (-1.974028) 10% (-1.602922)
LSetup Rate	-2.714270	1% (-4.004425) 5% (-3.098896) 10% (-2.690439)	-5.977316	1% (-4.057910) 5% (-3.119910) 10% (-2.701103)
South-East Region				
LGDP	-1.040191	1% (-2.771926) 5% (-1.974028) 10% (-1.602922)	-3.390554	1% (-2.771926) 5% (-1.974028) 10% (-1.602922)
LSetup Rate	-2.679612	1% (-4.004425) 5% (-3.098896) 10% (-2.690439)	-6.924296	1% (-4.057910) 5% (-3.119910) 10% (-2.701103)
South–Muntenia Region				
LGDP	-0.925052	1% (-2.771926) 5% (-1.974028) 10% (-1.602922)	-3.994241	1% (-2.771926) 5% (-1.974028) 10% (-1.602922)
LSetup Rate	-2.605983	1% (-4.004425) 5% (-3.098896) 10% (-2.690439)	-6.723960	1% (-4.057910) 5% (-3.119910) 10% (-2.701103)
South-West Region				
LGDP	-1.257590	1% (-2.771926) 5% (-1.974028) 10% (-1.602922)	-1.654585	1% (-2.771926) 5% (-1.974028) 10% (-1.602922)
LSetup Rate	-2.771612	1% (-4.004425) 5% (-3.098896) 10% (-2.690439)	-5.478159	1% (-4.057910) 5% (-3.119910) 10% (-2.701103)
West Region				
LGDP	-0.241383	1% (-2.771926) 5% (-1.974028) 10% (-1.602922)	-1.996789	1% (-2.771926) 5% (-1.974028) 10% (-1.602922)
LSetup Rate	-2.920577	1% (-4.004425) 5% (-3.098896) 10% (-2.690439)	-6.758486	1% (-4.057910) 5% (-3.119910) 10% (-2.701103)

Based on the results presented in Table 1, it can be concluded that, in the level form of the variables LGDP and LSetup Rate, the null hypothesis of a unit root cannot be rejected at any of the three significance levels (1%, 5%, or 10%). Given the non-stationarity of the series, their first differences were computed to ensure stationarity, both in the case of Romania (total) and the case of the 8 regions. This time, in the case of the variables studying the rate of establishment of companies, it is observed that the null hypothesis (H0) is rejected both for 1% (|ADFcalc| > |ADFtab| = 4.057910) and for 5% (|ADFcalc| > |ADFtab| = 3.119910), respectively 10% (|ADFcalc| > |ADFtab| = 2.701103). For the other variables, the null hypothesis is only rejected for 10% or 5%. Thus, regarding the LGDP variable at the level of Romania, respectively at the level of the 8 regions, we can state the following: the first-order differenced series of the LGDP variable achieves stationarity across all three significance levels (1%, 5%, and 10%) for the South-Muntenia and South-East regions. For the Bucharest-Ilfov, Center, North-East, North-West, and West regions, the first-order differenced series becomes stationary at the 5% and 10% significance levels. In contrast, for the South-West region and Romania as a whole, stationarity is achieved only at the 10% significance level.

Using the results of the ADF test, we can determine the order of integration (I) for these variables by identifying the presence or absence of unit roots. In this context, Table 2 has been constructed to present the findings.

Table 2. The order of integration of the model variables

	LGDP	LSetup Rate
1% critical value	I = 1 (South-East Region and South Muntenia Region)	I = 1 (Romania and the 8 component regions)
5% critical value	I = 1 (Bucharest -Ilfov, Center, North-East, North-West, West, South-East and South Muntenia Regions)	I = 1 (Romania and the 8 component regions)
10% critical value	I = 1 (Romania and the 8 component regions)	I = 1 (Romania and the 8 component regions)

We notice that the variables LSetup Rates have the order of integration equal to 1 at the 1%, 5%, and 10% significance levels. The variables LGDP have the order of integration equal to 1 at the level of Romania and the level of the 8 regions only at a 10% significance level. If the variables have the same order of integration, the possibility of co-integration relationships exists within the models to be estimated.

To identify the relationship between GDP and the rate of establishment of firms, we will develop two models for each region. The first model will contain the rate of establishment of firms as the dependent variable and the GDP as the independent variable. The second model will include GDP as the dependent variable, while the rate of establishment of companies represents the independent variable Thus, we will continue to apply the Johansen integration test to identify a possible long-term relationship within the models for the 8 regions of Romania, and respectively for Romania as a whole. Depending on the results of the Johansen integration test, we can decide whether the application of the VEC model is optimal for each region. The presence of cointegration between variables indicates a long-term relationship between them. Therefore, the Error Correction Model (VECM) can be applied. In Tables 3 and 4 we have presented the long-term relationship and the short-term relationship between the two variables, GDP and the rate of establishment of firms.

Table 3. VECM and Granger Causality – Firm establishment rate (dependent variable)

Causality direction	Error correction term (long-term) (EC) [t-statistic] (std. error)	Coefficient of the independent variable (short-term) [t-statistic] (std. error)	Coefficient of the first-order lag [t-statistic] (std. error)	R-squared (F-statistic)
GDP → RATE OF ESTABLISHMENT OF COMPANIES				
Romania (total)	-0.764815 (0.50239) [-1.52235]	-0.191053 (1.88425) [-0.10140]	-0.187930 (0.33532) [-0.56045]	0.51043 (3.1279)
Center Region	-0.644878 (0.44953) [-1.43455]	2.239538 (2.25896) [0.99140]	-0.299243 (0.32878) [-0.91015]	0.51660 (3.206132)
North-East Region	-0.760796 (0.45766) [-1.66236]	0.182799 (1.80743) [0.10114]	-0.221649 (0.32776) [-0.67625]	0.51753 (3.218025)
North-West Region	-1.050595 (0.48255) [-2.17717]	0.152224 (1.40546) [0.10831]	-0.001311 (0.33110) [-0.00396]	0.53485 (3.449581)
Bucharest-Ilfov Region	-1.044215 (0.30473) [-3.42670]	-0.574532 (0.75655) [-0.75941]	0.152147 (0.25816) [0.58934]	0.66909 (6.066021)
South-East Region	-0.075284 (0.17951) [-0.41938]	-1.890721 (0.96835) [-1.95251]	-0.545287 (0.24278) [-2.24603]	0.57815 (4.11598)
South-Muntenia Region	-0.546116 (0.41249) [-1.32394]	-1.724174 (1.18919) [-1.44987]	-0.358362 (0.30177) [-1.18754]	0.58597 (4.2459)
South-West Region	-0.943080 (0.46513) [-2.02754]	0.640993 (1.62567) [0.39429]	0.012259 (0.33574) [0.03651]	0.45748 (2.52977)
West Region	-0.699374 (0.42412) [-1.64902]	2.116935 (2.00081) [1.05804]	-0.370720 (0.32318) [-1.14710]	0.53691 (3.47827)

The results show that the causal effect of GDP on the rate of establishment of firms is significant in the long term in Romania, the error correction term being statistically significant at 10% significance level. Moreover, the negative sign of this coefficient indicates that the relationship between the mentioned variables is characterized by a long-term equilibrium. The value of the estimated coefficient (EC) indicates that approximately 76% of the imbalance is corrected in a year. Therefore, the results confirm a long-term relationship between GDP and the rate of establishment of firms. On the other hand, regarding the short-term causal effect, it is observed that, at the level of Romania, this relationship is not supported, as the coefficient is not statistically significant (t-statistic = 0.10140). Also, the results show that the establishment rate of firms in period t-1 does not influence the establishment rate in period t. At the level of the 8 development regions of Romania, a relatively similar evolution can be observed. Thus, in the Center, North-East, North-West, Bucharest Ilfov, South-West, and West regions, the causal effect of GDP on the rate of establishment of companies is significant in the long term, at the 10% significance level. We also note that the sign of the coefficients is negative, which confirms a long-term relationship. However, the results show

that in the South-East Region and the South-Muntenia Region, this long-term relationship is not confirmed for the total population, as the t-statistic value is lower than the critical value from the statistical table. However, the short-term coefficients indicate convergence and significant results from GDP to the establishment rate of firms in the two regions. In the other areas analyzed, the coefficients are not statistically significant. Therefore, in the Center, North-East, North-West, Bucharest Ilfov, South-West, and West regions, we did not identify a short-term relationship between GDP and the rate of establishment of companies. Moreover, based on the coefficients of the independent variable (in the short term), we can conclude that GDP has a negative relationship with the rate of firm establishment in the two regions. Thus, when the GDP increases by 1%, the establishment rate of companies decreases by 1.89% in the South-East Region and by 1.72% in the South-Muntenia Region. As in the case of Romania, at the level of the 8 regions, it can be observed that the establishment rate of firms in period t-1 does not influence the establishment rate of firms in period t, except for the South-East Region.

Table 4. VECM and Granger Causality – GDP (dependent variable)

Causality direction	**Error correction term (long-term) (EC) [t-statistic] (std. error)**	**Coefficient of the independent variable (short-term) [t-statistic] (std. error)**	**Coefficient of the first-order lag [t-statistic] (std. error)**	**R-squared (F-statistic)**
RATE OF ESTABLISHMENT OF COMPANIES → GDP				
Romania (total)	-0.100250 (0.05495) [-1.82432]	0.095021 (0.06654) [1.42796]	0.654133 (0.37392) [1.74938]	0.343103 (1.56692)
Center Region	-0.075686 (0.04456) [-1.69838]	0.075307 (0.05254) [1.43326]	0.627991 (0.36100) [1.73958]	0.334685 (1.509144)
North-East Region	-0.044877 (0.03770) [-1.19023]	0.057775 (0.06016) [0.96033]	0.500168 (0.33176) [1.50763]	0.281658 (1.176282)
North-West Region	-0.044730 (0.05183) [-0.86299]	0.102876 (0.08479) [1.21323]	0.413648 (0.35993) [1.14923]	0.202869 (0.76499)
Bucharest-Ilfov Region	-0.054463 (0.02790) [-1.95217]	0.128941 (0.11366) [1.13444]	0.282824 (0.33308) [0.84911]	0.365226 (1.726090)
South-East Region	-0.214334 (0.11013) [-1.94614]	0.082128 (0.07596) [1.08120]	0.079573 (0.30298) [0.26264]	0.304346 (1.312487)
South-Muntenia Region	-0.072361 (0.06385) [-1.13337]	0.121812 (0.08140) [1.49647]	-0.175944 (0.32078) [-0.54849]	0.249234 (0.9959)
South-West Region	-0.053617 (0.05400) [-0.99286]	0.041884 (0.07470) [0.56072]	0.410512 (0.36168) [1.13500]	0.171425 (0.620675)
West Region	-0.106416 (0.04637) [-2.29490]	0.042594 (0.05869) [0.72578]	0.648384 (0.36333) [1.78456]	0.433606 (2.29667)

Starting from the results obtained following the application of the model (GDP as the dependent variable, it can be concluded that the long-term causal effect of the rate of company establishment on GDP is statistically significant at the 10% significance level for Romania, the Central Region, the Bucharest-Ilfov Region, the South-East Region, and the West Region. In the other regions, North-East, North-West, South Muntenia, and South-West, although we obtained a negative coefficient, these coefficients are not statistically significant. Therefore, we can state that in Romania, the relationship between the rate of establishment of companies and GDP is characterized by a long-term equilibrium and the value of the estimated coefficient (EC) indicates that approximately 10% of the imbalance is corrected in a year. Regarding the short-term relationship, we observe that both at the level of the entire country and the level of the Center and South-Muntenia regions, the establishment rate of companies significantly influences the GDP. Thus, when the rate increases by 1%, the GDP increases by 0.9% at the country level, 7% in the Center Region, and 12% in the South-Mountain Region.

5 CONCLUSIONS

The literature suggests a strong and positive relationship between the evolution of GDP and the creation rate. However, this relationship is more complex and influenced by various factors, including the type of entrepreneurial activity, the institutional context, and the level of economic development. The regional perspective on the relationship between the evolution of GDP and the rate of establishment of companies underlines the importance of local conditions and targeted policies in stimulating economic growth and reducing disparities.

In this paper, we aimed to analyze the relationship between economic growth and business formation rates in Romania, from a regional and national perspective to highlight possible particularities and trends regarding the contribution of the SME sector to economic growth. We tried to answer an important question in economic theory and practice, namely, does GDP evolution determine the pace of new firm formation or, conversely, does the formation of new firms influence GDP evolution? We were interested in finding out, in the case of Romania and its component regions:

- if the relationship between these variables exists,
- what is the meaning of this relationship,
- how it behaves in the short or long term, and
- if there are regional particularities within these relationships.

We found that the causal effect of GDP on the firm formation rate is significant and balanced in the long term at the national level. In the short term, however, this relationship does not hold. At the level of Romania's development regions, the evolution is somewhat similar to the national level. Thus, in six of the eight regions (Center, North-East, North-West, Bucharest Ilfov, South-West, and West) the GDP evolution significantly influences the long-term company formation rate. In the South-East and South Muntenia regions, this long-term relationship is not confirmed. In the short term, in the Center, North-East, North-West, Bucharest-Ilfov, South-West, and West regions, we did not identify a relationship between GDP and the company formation rate, and, surprisingly, in the South-East Region and Sud-Muntenia Region, we found that GDP growth has a negative relationship with the rate of company creation.

On the other hand, when researching whether the companies' formation rate influences economic growth, we found that the causal effect is significant in the long term in the case of Romania, and, respectively, in the case of the Central, Bucharest - Ilfov, South-East and West Regions. In the other regions (North-East, North-West, South Muntenia, and South-West), we obtained a negative coefficient, but not statistically significant. In the short term, we observe that, both at the national level and in the Center and South-Muntenia regions, the rate of company establishment significantly influences GDP. Its effect is not statistically significant in the other six.

As an overall conclusion, we can say that, rather, economic growth determines, in the long term, the availability of launching new firms, and not the contrary (that the new firms' creation would stimulate, directly and noticeably, economic growth). This statement must be discussed and accompanied by exemptions or particular behaviors. Consistent with other our previous research on this topic (Dianu, Gavriluț, Badulescu,

Simut, & Herte, 2019), (Simut, Badulescu, & Dianu, 2021), (Badulescu, Badulescu, Simut & Dianu, 2025) we can observe several differences between Romania's regions in terms of their potential and orientation towards sustained economic growth. However, these differences are not significant enough to suggest expressively divergent development paths or a notably faster progression for any particular region toward European averages compared to others. However, the metropolitan Region (i.e. Bucharest-Ilfov) stands out as an exception, exhibiting a significantly higher growth rate. Our forecasts indicate that this trend will persist, further widening the gap between this region and the other regions of Romania.

Practical and theoretical utility and economic policy recommendations derived from this research could be focused on the imperative effective regional policies supporting entrepreneurship, innovation, and infrastructure development to reduce regional disparities and promote balanced economic growth. Location-based policies that address the specific needs of lagging regions can help promote a more inclusive economic environment (Floerkemeier, Spatafora, & Venables, 2021), and policymakers concerned with stimulating economic growth should consider these factors to create proper environment support and nurture entrepreneurial activity.

WORKS CITED

Abdinnour, S., & Adeniji, S. (2023). Empirical analysis of the impact of entrepreneurial activity on economic growth of Global Entrepreneurship Monitor (GEM) countries. *Journal of Global Entrepreneurship Research, 13*(12), https://doi.org/10.1007/s40497-023-00355-3.

Acs, Z., & Audretsch, D. (2010). *Handbook of Entrepreneurship Research Book. An Interdisciplinary Survey and Introduction* (2nd edition). New York: Springer.

Aga, G., Francis, D., & Meza, J. (2015). *SMEs, Age, and Jobs. A Review of the Literature, Metrics, and Evidence.* Washington, D.C.: World Bank Group, Development Economics, Policy Research Working Paper 7493.

Aparicio, S., Urbano, D., & Gomez, D. (2023). Entrepreneurial Activity and Economic Growth: A Literature Review. In S. Aparicio, D. Urbano, & D. Gomez (Eds.), *Driving Complexity in Economic Development* (https://doi.org/10.1007/978-3-031-34386-5_2). Cham: Palgrave Macmillan.

Audretsch, D., & Fritsch, M. (1994). The Geography of Firm Births in Germany. *Regional Studies, 28*(4), 359-365, DOI: 10.1080/00343409412331348326.

Audretsch, D., & Keilbach, M. (2003). *Entrepreneurship Capital and Economic Performance.* London, UK: Centre for Economic Policy Research, Discussion Paper No. 3678.

Badulescu, D., & Badulescu, A. (2014). *Antreprenoriatul. Cum, cine, când?/ Entrepreneurship. How, who, when?* Cluj Napoca, Romania: Editura Presa Universitară Clujeană.

Badulescu, D., Badulescu, A., Sipos-Gug, S., Herte, A., & Gavrilut, D. (2020). Knowledge Intensive Business Services and their Economic Role in European Union: A Brief Analysis. *Oradea Journal of Business and Economics, 5*(1), 72-85.

Badulescu, D., Gavrilut, D., Simut, R., Bodog, S.-A., Zapodeanu, D., Toca, C.-V., & Badulescu, A. (2024). The Relationship between Sustainable Economic Growth, R&D Expenditures and Employment: A Regional Perspective for the North-West Development Region of Romania. *Sustainability, 16*, 760, https://doi.org/10.3390/su16020760.

Badulescu, D., Badulescu, A., Simut, R. & Dianu, D. (2025). Firm size distribution and economic growth. Evidence from Romanian development regions. *Forthcoming*.

Bosma, N., & Levie, J. (2010). *Global Entrepreneurship Monitor 2009 Executive Report.* Global Entrepreneurship Research Association (GERA).

Bosma, N., van Stel, A., & Suddle, K. (2008). The geography of new firm formation: Evidence from independent start-ups and new subsidiaries in the Netherlands. *International Entrepreneurship and Management Journal, 4*, 129–146, https://doi.org/10.1007/s11365-007-0058-8.

Bristow, G., & Healy, A. (2018). Innovation and regional economic resilience: an exploratory analysis. *The Annals of Regional Science, 60*, 265–284, https://doi.org/10.1007/s00168-017-0841-6.

Capello, R. (2019). Regional Development Theories and Formalised Economic Approaches: An Evolving Relationship. *Italian Economic Journal, 5*, 1–16, https://doi.org/10.1007/s40797-019-00085-0.

Carree, M., & Thurik, A. (2010). The Impact of Entrepreneurship on Economic Growth. In Z. Acs, & D. Audretsch (Eds.), *Handbook of Entrepreneurship Research* (pp. 557-594, DOI: 10.1007/978-1-4419-1191-9_20). New York: Springer.

Dianu, D., Gavriluț, D., Badulescu, D., Simut, R., & Herte, D. (2019). Business Formation, Discontinuity and Economic Growth in Romania. Madrid: The 34th International Business Information Management Association Conference (IBIMA).

Dickey, D., & Fuller, W. (1979). Distribution of the Estimators for Autoregressive Time Series with a unit root. *Journal of the American Statistical Association, 74*(366), 427-431.

European Commission. (2023). *Economic forecasts and trends*. Retrieved 10 10 2024, from https://commission.europa.eu/statistics/economic-forecasts-and-trends_en.

Eurostat. (2021). *NUTS - Nomenclature of territorial units for statistics*. Retrieved 04 20, 2024, from https://ec.europa.eu/eurostat/web/nuts/background.

Eurostat. (2024). *Business Demography. Database*. Retrieved 11 09 2024, from https://ec.europa.eu/eurostat/web/business-demography/database.

Floerkemeier, H., Spatafora, N., & Venables, A. (2021). *Regional Disparities, Growth, and Inclusiveness.* Washington, D.C.: International Monetary Fund, Institute for Capacity and Development, WP/21/39.

Haidar, J. (2012). The Impact of Business Regulatory Reforms on Economic Growth. *Journal of the Japanese and International Economies, 26*(3), 285-307.

International Finance Corporation (2023). *Strong Private Sector Key to Drive Romania's Economic Growth, Says New IFC-World Bank Report*. Retrieved 10 10, 2024, from https://www.ifc.org/en/pressroom/2023/strong-private-sector-key-to-drive-romanias-economic-growth-says.

Jalilian, H., Kirkpatrick, C., & Parker, D. (2007). The Impact of Regulation on Economic Growth in Developing Countries: A Cross-Country Analysis. *World Development, 35*(1), 87-103.

Loayza, N., Oviedo, A., & Serven, L. (2005). *Regulation and macroeconomic performance.* Washington, DC: World Bank, WPS3469.

Muntean, A.-D., Caranfil, R.-A., & Ilovan, O.-R. (2021). Urban Bioregions and Territorial Identities in Romania. The Role of Information and Communication Technology. *Journal of Settlements and Spatial Planning, 8*, 78-93, https://doi.org/10.24193/JSSPSI.2021.8.

Munyo, I., & Veiga, L. (2024). Entrepreneurship and Economic Growth. *Journal of the Knowledge Economy, 15*, 319-336, https://doi.org/10.1007/s13132-022-01032-8.

National Institute of Statistics (Romania). (2024). *Tempo Online. Domain*. Retrieved 09 09, 2024, from http://statistici.insse.ro:8077/tempo-online/#/pages/tables/insse-table.

Ndofirepi, T. (2020). Relationship between entrepreneurship education and entrepreneurial goal intentions: psychological traits as mediators. *Journal of Innovation and Entrepreneurship, 9*(2), https://doi.org/10.1186/s13731-020-0115-x.

Patrício, L., & Ferreira, J. (2024). Unlocking the connection between education, entrepreneurial mindset, and social values in entrepreneurial activity development. *Review of Managerial Science, 18*, 991–1013, https://doi.org/10.1007/s11846-023-00629-w.

Reynolds, P., Storey, D., & Westhead, P. (1994). Cross-national Comparisons of the Variation in New Firm Formation Rates: An Editorial Overview. *Regional Studies, 28*(4), 343-356.

Simut, R., Badulescu, A., & Dianu, D. (2021). Do Entrepreneurial Dynamics Influence Economic Growth and Employment? Evidence for Romania. *Oradea Journal of Business and Economics*, 6(2), pp. 98-110. https://doi.org/10.47535/1991ojbe133.

Stam, E., & van Stel, A. (2011). 4 Types of Entrepreneurship and Economic Growth. In A. Szirmai, W. Naudé, & M. Goedhuys (Eds.), *Entrepreneurship, Innovation, and Economic Development*, https://doi.org/10.1093/acprof:oso/9780199596515.003.0004. Oxford: Oxford University Press.

Walter, S., & Block, J. (2016). Outcomes of entrepreneurship education: An institutional perspective. *Journal of Business Venturing, 31*(2), 216-233, https://doi.org/10.1016/j.jbusvent.2015.10.003.

Wennekers, S., van Stel, A., Thurik, R., & Reynolds, P. (2005). Nascent Entrepreneurship and the Level of Economic Development. *Small Business Economics, 24*, 293–309, https://doi.org/10.1007/s11187-005-1994-8.

Received for publication: 28.11.2024
Revision received: 03.12.2024
Accepted for publication: 08.01.2025.

How to cite this article?

Style – **APA** *Sixth Edition:*

Badulescu, D., Dianu, D., Simut, R., & Badulescu, A. (2025, 01 15). GDP and Business Creation Relationship in Romanian Development Regions. (Z. Cekerevac, Ed.) *MEST Journal, 13*(1), 1-12. doi:10.12709/mest.13.13.01.01

Style – **Chicago** *Sixteenth Edition:*

Badulescu, Daniel, Dragos Dianu, Ramona Simut, and Alina Badulescu. "GDP and Business Creation Relationship in Romanian Development Regions." Edited by Zoran Cekerevac. *MEST Journal* (MESTE) 13, no. 1 (01 2025): 1-12.

Style – **GOST** *Name Sort:*

Badulescu Daniel [et al.] GDP and Business Creation Relationship in Romanian Development Regions [Journal] // MEST Journal / ed. Cekerevac Zoran. - Belgrade – Toronto : MESTE, 01 15, 2025. - 1 : Vol. 13. - pp. 1-12.

Style – **Harvard** *Anglia:*

Badulescu, D., Dianu, D., Simut, R. & Badulescu, A., 2025. GDP and Business Creation Relationship in Romanian Development Regions. *MEST Journal,* 15 01, 13(1), pp. 1-12.

Style – **ISO 690** *Numerical Reference:*

GDP and Business Creation Relationship in Romanian Development Regions. **Badulescu, Daniel, et al.** [ed.] Zoran Cekerevac. 1, Belgrade – Toronto : MESTE, 01 15, 2025, MEST Journal, Vol. 13, pp. 1-12.

MEST Journal
DOI 10.12709/mest.13.13.01.02

REJOINDER TO RECTENWALD ON SUPPOSED ISRAELI WAR CRIMES

Walter E. Block
Harold E. Wirth Eminent Scholar Endowed Chair and Professor of Economics, Loyola University New Orleans, New Orleans, LA, USA
https://orcid.org/0000-0003-2215-4791

JEL Category: **Z0**

Abstract

In the view of Rectenwald (2024), in its 2023-2024 war against Hamas, Israel is guilty of "war crimes" and I am guilty of supporting this uncivilized behavior of that country. In so doing I am besmirching the good name of libertarianism, with which I have long been associated. The present paper is my attempt to refute these charges of that author. Specifically, Rectenwald maintains that I make unjustified demands for evidence, that I have improperly renounced by anarcho-capitalist philosophy, and that I have more than just several times contradicted myself. My claim against him involves the argument that he gives insufficient weight to sectarianism and completely avoids the fact that Hamas uses Gazan civilians as shields. Further, I refute his claim that the IDF targets innocent civilians. Rectenwald defends DiLorenzo's critique of my analysis of the Israel-Hamas war, and I take issue with the analysis of the latter scholar. Rectenwald is particularly exercised that the IDF can accurately estimate the number of civilians who are likely to be killed in an attack; I show the irrelevance of this criticism. We engage in a "war of words" over the statements of the leaders of the two warring parties. We also take issue with each other over US funding of Israel and its abrupt cessation; over shape shifting and silver linings.

Keywords: *Israel, Hamas, genocide, war crimes*

REJOINDER TO RECTENWALD ON SUPPOSED ISRAELI WAR CRIMES

It is important to demonstrate the fallacies of Rectenwald (2024).[1] If so eminent a scholar as he can be so wrong on Israel's conduct in its war with Hamas, there is little hope that those with more modest intellectual accomplishments can be brought around to entertaining a correct view on this matter. On the other hand, if this former New York University professor can be refuted, then the probability of the latter occurring is thereby markedly increased, so important a public figure is

Address of the author:
Walter E. Block
wblock@loyno.edu

[1] All my references to this author, unless otherwise mentioned, will be to this one essay of his, Rectenwald (2024)

he. That is precisely the purpose of the present paper: to do just that.

Our author starts off on the wrong foot. He maintains that "Block makes impetuous demands for evidence…" That is more than passing curiosity. Can a "demand for evidence" in a contentious issue[2] ever been "impetuous?" Hardly. Evidence, along with logic is the be all and end all of science, social science, history, philosophy, and other such callings.

Rectenwald next maintains that "In the case of Israel, the erstwhile anarcho-capitalist[3] abandons his anarcho-capitalist perspective and principles, contradicts himself repeatedly…"

There is a little story that must be told at this point. Murray N. Rothbard is/was my mentor, my guru, my friend, my guide, my inspiration in all matters of economics and libertarian political philosophy. In Rothbard (1967) he strongly inveighed against "sectarianism." This is the fallacy that infected many libertarian anarchists. Since from this perspective all governments violate the non-aggression principle of libertarianism, they are all illicit and all condemned. Rothbard had none of this. He emphasized the point that, yes, all states are evil, but some are much more so than others. In other words, it is sectarian to say, as would the anarchist libertarian who Rothbard (1967) is criticizing: "Hamas is evil, Israel is evil," and leave matters there. If one wants to take seriously Rothbard's rejection of sectarianism, as I do, then he cannot do so as an anarcho-capitalist. He must do so under the aegis of some other version of libertarianism.

I have chosen the classical-liberal perspective of this philosophy as the jumping off point in an attempt to be responsive to the clarion call of Rothbard's, as exemplified in the title of my book Block and Futerman (2021). Thus, I concede to Rectenwald: I am indeed "contradicting myself." Ordinarily, in virtually all my writings, speeches, interviews, I articulate the anarcho-capitalist point of view. However, when it comes to issues as to which criminal government entity is worse than the other, I do not say, as a sectarian, "a pox on both your houses." Instead, I put on my classical liberal libertarian hat and ask which is *worse* than the other.[4]

He denies that he "suffer[s] from 'Israel Derangement Syndrome…'" I shall demonstrate below that he is indeed infected with this intellectual malady. Rectenwald is not merely an intelligent man. He is a world class scholar. His ethics are beyond reproach. Yet, he takes the side of that terrorist organization, Hamas, vis a vis the Israeli government which, to be sure, is not perfect, far from it, but in this case is fighting an entirely defensive war. How, else, then, to account for his erroneous analysis other than by resort to this syndrome?

Rectenwald puts the case against Israel, and me by extension, very powerfully:

"… if someone firebombs my apartment and I know what neighborhood they live in but not their exact address, I would not be justified in firebombing their entire neighborhood in response. In fact, I would not even be justified in bombing their home. The only justifiable use of force would be to prevent them from bombing my apartment and/or to bring them, and only them, to justice." The implication here, of course, is that Israel has gone far beyond limiting itself to pursuing, capturing, punishing, those individual Hamas members who were specifically responsible for the carnage of October 7, 2023.

This illustrious commentator reckons in the absence of shield theory (Block, 2010, 2011A, 2019). Consider the following. Jones has a knife and has attached to himself two-year-old son placed in front of him in a baby hold-all. Jones runs

[2] If the Israeli-Hamas war is not a contentious issue, there is no such thing as a contentious issue. There is probably more hatred, more disparagement, more cancellation, even more divorces over this issue than any other, even including abortion. I cannot believe other than that Rectenwald would agree with me in this claim.

[3] That is, moi. Rectenwald is indeed correct in this contention. I do indeed support the anarcho-capitalist version of libertarianism. For example, see Block, 2007, 2011B, 2021; Block and Fleischer, 2010; Block and Futerman, 2020-2021; Futerman and Block, 2019

[4] Contrary to Rectenwald, I do so not only in the Israel-Hamas context, but, also, regarding any other dispute between two governments as in the case of Russia and Ukraine: Block, 2022A, 2022B, 2022C

at Smith, with blood in his eye, yelling he is going to kill the latter, who has a gun. Smith cannot run away; Jones is faster than him. Smith has his back to the wall in any case. However, this would be victim has a gun. If Smith does not shoot Jones, he will himself be killed. And here is the crucial point: the only way Smith can shoot Jones is through the body of Jones' totally innocent son. Jones represents Hamas, Smith, Israel. A knife is deadly, but a gun is even more powerful. Hamas can indeed strike murderous blows against Israel, but Israel is stronger than Hamas.

So, what should Smith (Israel) do? If he does nothing, he will be committing suicide; Jones (Hamas) will murder him. To save his own life, he must kill Jones, in self-defense. But if he does any such thing, Jones' two-year-old baby son will also be killed, and there can be no doubt that this toddler is the paradigm case of an innocent person.

Let us consider the case where Smith kills the two Joneses. We need not worry too much about the adult Jones; he is killed in the act of murder. Even an Israel hater such as Rectenwald will, presumably, acquiesce in this notion. But what about Jones Junior? He is collateral damage. Who is responsible for his unjustified death? Rectenwald says Smith is the guilty party. He is imposing "collective punishment" in Rectenwald's view, on baby Jones.[5] And in a sense, a superficially correct sense, which is why this author is so confused on the matter, my debating partner is correct! After all, it is the bullet emanating from the gun of Smith that pierces the body of the Jones baby. But even a moment's reflection should convince any fair-minded commentator that the entire blame rests with father, Jones. No, he did not directly shoot his son, but he is solely responsible for his death regardless of that fact. And yes, Smith shot and killed baby Jones, and, yet he is in no way responsible for his death.

How many babies may Jones use as a shield? If he has two, three or perhaps even four such young children strapped to himself when he charges at Smith, the same analysis holds. How about 20,000, or 200,000, or two million, the approximate population of Gaza? Would Smith, Israel that is, be entitled to shoot them all? Of course not. It is inconceivable that any one man could physically control so many people, most of whom of course were not babies, but rather adult shields. What is the correct number? To what extent may Smith (Israel) properly engage in the killing of civilians in self-defense?

We have here a continuum problem (Block and Barnett, 2008), and there is no one correct answer. However roughly and approximately, the mathematics of the situation fully incline in favor of Israeli practice. For, how many Hamas fighters are there? Estimates vary, but we may safely estimate the figure at in the neighborhood of 100,000. Are these terrorists, all together, more than sufficient to terrorize the entire population? Of course they are. The proof is in the pudding: they have, at least to the date of the present writing[6], succeeded in staying in power in the face of the devastation and mass killing that has so far afflicted that unhappy corner of the world.

This quote from a former Prime Minister of Israel is very pertinent. Stated Golda Meir: "When peace comes, we will perhaps in time be able to forgive the Arabs for killing our sons, but it will be harder for us to forgive them for having forced us to kill their sons. Peace will come when the Arabs will love their children more than they hate us."[7] I really should not do this, but that quote is so pertinent, so apropos, so profound, that for the sake of Rectenwald, and in the hope that he reads it carefully, I will repeat it right here once again: "When peace comes we will perhaps in time be able to forgive the Arabs for killing our sons, but it will be harder for us to forgive them for having forced us to kill their sons. Peace will come when the Arabs will love their children more than they hate us."

So much for Rectenwald's opposition to "firebombing their entire neighborhood." He completely misconstrues what is going on in the Middle East. In his case, innocent people are

[5] According to the good professor: "The NAP excludes the initiation of force and the collective punishment of those not involved in the original aggression." That is true enough.

[6] August 2024

[7] https://www.goodreads.com/quotes/664790-when-peace-comes-we-will-perhaps-in-time-be-able

being killed alright, but it is solely the fault of the bombers, for there are no shields in place. He never so much as even contemplates such a situation. That is not at all the case in Israel, where Hamas places rocket launchers in schools, Mosques, hospitals, playgrounds, residential areas, and then complains, bitterly, when the IDF defends itself in the only way it can. It first sends leaflets, warning of incipient attacks, urging civilians to vacate the area. Hamas forbids such migration, and garners world support when Israel kills the Jones baby; that is the children and other innocent civilians in Gaza.

This former NYU professor then states as follows: "Block's response to DiLorenzo is that he never endorsed any such war crimes or the targeting of civilians, or admitted that any targeting has happened: 'Where did I ever say or write that the Israeli government intentionally targeted civilians?' But this was not DiLorenzo's point at all. DiLorenzo's point is that the IDF *does* target civilians—women and children—and that in supporting and cheerleading Israel's onslaught in Gaza, whether based on ignorance or not, Block thereby sanctions and encourages such targeting. In supporting Israel's onslaught in Gaza, Block endorses war crimes."

With the Jones - Smith case in mind, we are now in a position to put paid to this claim. First, the IDF does not "target civilians." Au contraire, it does everything humanly possible, perhaps more than any other military in the entire history of warfare, to avoid this. Does that mean it will not bomb a building with a rocket launcher in it, after it has warned civilians of its intention and thus knowingly inflicts collateral damage? No, it does not refrain from such acts. Does this mean that in the mind of the IDF, no innocents will perish as a result of these actions? No, again. But, contrary to Rectenwald, this does not mean that the Israeli military "targets" civilians. Instead, it is shooting Jones' baby in self-defense. In Rectenwald's view, if a bank robber came to alleviate this organization of its funds, and had a baby strapped to him, the bank guards would be legally and morally obligated not to forcibly stop him if the only way they could do so would be to mow down both. Thus, the bank guards would be at the mercy of the bank robbers. This is highly problematic.

This scholar is by no means finished with his critique. He next avers:

"DiLorenzo has raised Block's ire by stating: 'He [Block] is no longer an unpaid senior fellow at the Mises Institute not because he is 'pro-Israel,' as some uninformed or dishonest commentators have asserted. It is because the Mises Institute cannot be associated with such a well-known, prolific, public advocate of the intentional targeting and killing of Palestinian women, children, and babies.'

"Block accuses DiLorenzo of intellectual dishonesty and insists that he never wrote or said such a thing. He never advocated targeting and killing Palestinian women, children, and babies. But again, the point is not that Block has stated that he supports the targeting and killing of Palestinian women, children, and babies but rather that he is either unaware of such targeting, is in denial about it, or dismisses the reality of the same. Likewise, his support of the onslaught on Gaza amounts to such advocacy."

DiLorenzo is a world class Austrian economist and historian who relies on facts and logic. He ought to know better than this. There is a world of difference between statement A: "Israel bombed a residential area of Gaza" and statement B: "Israel purposefully targeted civilians who occupied that residential area." A is a statement of objective fact. We can all see the rubble that is now Gaza. No one can deny A. But B is an entirely different matter. It calls for an intention of the IDF, something not obviously apparent from the mere objective act depicted in A. There could have been many other motives underlying this act for all that DiLorenzo, Rectenwald or anyone else for that matter mentioned. For example, C: "The IDF bombed the residential area in spite of the fact that it knew there were civilians ensconced there." Or D: "The IDF bombed the residential area as an act of self-defense since Hamas had placed rocket launchers therein, which were murdering innocent civilians." Rectenwald is not an economist, so, perhaps, he can be excused for not taking cognizance of this economic[8] distinction. It is more difficult to do so in the case of DiLorenzo.

[8] But also a matter of common sense

Our esteemed scholar makes this charge: "Certainly, the evidence of our senses, as seen in endless photographs and videos, confirms that the IDF indiscriminately slaughters civilians." Yes, we have all seen the rubble that is now Gaza, which followed the unwarranted, depraved and vicious attack launched against Israel on October 7, 2023. This is objective. This is undeniable. But "indiscriminate" is entirely a different matter. It does not at all logically follow from the fact that many buildings were destroyed, and many lives lost that the IDF acted in an indiscriminate manner. As for "slaughter" that properly describes what had occurred on that day of infamy October 7, 2023, not in regard to Israel's defensive response.

Rectenwald appears particularly exercised at the fact that "… the [Israeli] army significantly expand[ed] its bombing of targets that are not distinctly military in nature. These include private residences as well as public buildings, infrastructure, and high-rise blocks …"

But this is precisely where Hamas has placed it military weaponry. If these areas are ruled off limits because there are shields located there, that baby Joneses may be found in the vicinity, Israel might as well surrender in its war against Hamas. Is that what Rectenwald wishes? It is difficult to avoid this conclusion.

Something else that sticks in Rectenwald's craw is the claim that the IDF full well knows "… the number of civilians who are likely to be killed in an attack on a particular target. This number is calculated and known in advance to the army's intelligence units, who also know shortly before carrying out an attack roughly how many civilians are certain to be killed."

The proper answer to this is "so bloody what." The Israel military has done all that any civilized army could do to minimize civilian deaths. It does not at all want to kill baby Jones. It sends out leaflets before attacks to reduce the probability of that occurring. It appreciates the fact that Hamas will prevent these innocents from leaving these areas. Yet, in self -defense it must terminate the missile launchings from these places. How else can it do so apart from bombing them? The fact that it can accurately estimate the harm to the baby Jones shields is entirely irrelevant to these considerations, Rectenwald to the contrary notwithstanding.

Our author is upset that the IDF was "… *not interested in killing [Hamas] operatives only* when they were in a military building or engaged in a military activity…" Rather, these terrorists were targeted at times when they were using their families as shields. Rectenwald does not at all incorporate the lesson learned from the Jones Smith example. He completely ignores this reality. He maintains that these terrorists should be safe from IDF targeting when they are surrounded by baby Joneses. For him, it is morally required that the IDF should attempt to bring to justice these terrorists only when they are actively engaged in their terroristic activities. This means that murderers and rapists can only be arrested when they are in the midst of conducting their foul deeds. They cannot be arrested when "innocently" sitting at a restaurant or night club. One can only wonder, in dismay, at this position of Rectenwald's.

Our learned author is aghast at the charge that "… more children were killed in the Gaza Strip in just over four months than were killed in four years in all other conflicts around the world, combined."

Stipulate, arguendo, that this and these other charges are true. All this means is that there were many, many baby Joneses in Gaza who were used as shields. Who is responsible for their deaths? Those who directly killed them by pulling triggers, or releasing bombs aimed at terrorists (Israel), or those who set up these innocent children as buffers, in positions such that the only way, the only way, that Israel could defend itself would be by killing them (Hamas)? Rectenwald blames Israel. No fair-minded commentator would do any such thing.

Next, Rectenwald marshals a series of intemperate remarks made by Israeli officials and asserts: "Expressed intent is a valid indicator of genocidal goals." Many of these statements were made in the immediate aftermath of the atrocities of October 7, 2023. Some were made even more recently, while Hamas still holds Israeli hostages, some of whom who have already perished under captivity. What do you expect when people are devastated by the next worst calamity to have ever overtaken the Jewish people? Sweetness and light?

But actions speak louder than words. The word "leaflet" appears nowhere in his essay; he does not seem cognizant of the fact that the Israeli *actions* are an attempt to minimize civilian deaths the very opposite of genocide; that if there is any purposeful slaughter of civilians, it is due to Hamas behavior. This is clear in their attack on the peaceful concert goers on that evil day.

However, if words are so important to Rectenwald, let him consider the most important document of these despicable human beings. The Hamas covenant invokes this injunction: "The Day of Judgment will not come about until Muslims fight Jews and kill them. Then, the Jews will hide behind rocks and trees, and the rocks and trees will cry out: 'O Muslim, there is a Jew hiding behind me, come and kill him.'"[9]

These were not off the cuff angry remarks, made amidst tears. They appeared in the very covenant of these people. This document is akin for them to the US Constitution for Americans or to the bible for religious people.

The next critique offered by Rectenwald is as follows:

"As for the US's funding and arming of Israel, Block at first suggests that Israel's war on Gaza is none of the US's business. Citing DiLorenzo, he writes:

"'[Block] complain[s] … bitterly about the Biden administration's pause in sending more bombs to Israel to be dropped on the Gazan population, calling it 'treachery.' He therefore is fully in favor of using the US government's powers of legalized theft (aka taxation) to pay for more bombs for Israel'…

"First of all [writes Block], I oppose all US foreign aid to any and all countries and this certainly includes Israel.

"Yet only a few paragraphs later, Block contradicts himself by arguing that since the US has promised Israel foreign aid, it should deliver on said promise: Third, it is even more egregious to stop the foreign aid that had been promised to a recipient country such as Israel. Yes, it is true, from an anarcho-capitalist point of view that all such government contracts are invalid upon their face. However, from the classical liberal perspective from which I often write about Israel, they are valid, and the US is derelict in this regard (emphasis mine).

"So, Block argues that since the US has promised to extort its taxpayers to send arms and military aid to Israel, it should follow through with said extortion and send the aid and arms. That's the equivalent of saying that a thief who's promised to give a third party stolen goods should follow through with his theft to make good on his promise to the intended recipient of the stolen goods."

Not so fast. The US government should not exist at all, based on my anarcho-capitalist point of view. Since it exists, it should not be sending foreign aid to anyone. However, right now, the US transfers far more money to all Arab countries put together than to Israel alone, although to be sure, that nation receives more foreign aid[10] than any other single country. Given that the US will continue to send massive amount of foreign aid to all the Arab countries, it would be unfair, unjust, to cut out such largesse to Israel, alone. It is even more egregious to stop this aid to Israel that has already been promised to that country right in the middle of a war, a just war, that Israel is now conducting. In other words, the situation is more complicated than that contemplated by this critic of mine. If the US shut off all financial and other transfers of funds to Israel, and as well to all other countries in the Middle East, that would be perfectly acceptable. But to do so with its most important ally in the region, and to no one else, that is a different matter, one beyond the ken of Rectenwald's.

It is one thing to support stopping all US aid to Israel. That is a no brainer for libertarians; all must agree. It is quite another to favor abruptly pulling the rug out from under that country's feet by stopping promised aid while continuing to support Israel's enemies. That is an entirely different matter.

Let us make this point from a different perspective. All libertarians must agree to the privatization of

[9] https://irp.fas.org/world/para/docs/880818a.htm

[10] I feel I should apologize to Peter Bauer whenever I use this phrase. See on this Bauer, 1954, 1972, 1981, 1982, 1984, 1987; Bauer and Yamey, 1957

the bus service. This is a micro-libertarian issue, not one of macro-libertarianism.[11] But how shall the privatization actually take place? Suppose there is a public bus on the route from one city in Alaska to another. It is now right in the middle of the two, 300 miles away from both. The temperature is 60 degrees below zero. All passengers have paid for their tickets. Suddenly, the bus driver halts, is picked up by a government helicopter and leaves all the passengers to die in the freezing temperature. Must libertarians acquiesce in this type of privatization? Of course not. Consider another example. It is another foundational principle of the freedom philosophy that all hospitals should be privatized. A man is now unconscious, lying on the operating table; his heart has just been removed from him, and he is now in the process of receiving a replacement. Suddenly privatization takes place; all the doctors and nurses immediately leave the operating room, and this patient dies. Must libertarians support this type of privatization? Of course not. But Rectenwald would be logically obligated to do so based upon these comments of his.

He would have to opine something along these lines: "… since the US has promised to extort its taxpayers to run buses and hospitals, it should follow through with said extortion and continue to do so. That's the equivalent of saying that a thief who's promised to give a third party stolen goods should follow through with his theft to make good on his promise to the intended recipient of the stolen goods."

The point is, just because a cessation of government operations is justified, is more than justified, it does not logically follow, as per this author, that any and all methods of so doing are warranted.[12] Privatization is one thing. It is entirely justified. Immediate privatization is quite another matter. A sophisticated libertarian must be cautious is supporting it. Similarly, ending foreign aid is one thing. It is entirely justified. Immediate cessation of government-to-government transfers of aid is quite another matter. A sophisticated libertarian must be cautious in supporting it. Rectenwald is a libertarian. But caution is not his middle name.

Rectenwald avers of me: "He has previously stated that he opposes all foreign aid, yet he does not reject foreign aid where Israel is concerned. Hello?"

Let it be said, loud and clear, as a libertarian, I oppose all foreign aid. But that does not imply that all precipitous withdrawals are defensible, whether regarding buses, hospitals, or Israel.

Rectenwald continues his negative appraisal of my perspective:

"In the carve-out exception he makes for Israel, it is telling that Block changes his stripes from anarcho-capitalism, under which taxation is theft, to classical liberalism, under which it is not considered theft. Why, when it comes to Israel, does Walter Block change from an anarcho-capitalist to a classical liberal? This shapeshifting is a convenient excuse for making an exception for Israel…"

Why do I engage in this "shape shifting?" It is due to my appreciation of Rothbard (1967) who inveighs against "sectarianism," as mentioned above. Thus, there is nothing untoward here. I am a staunch anarcho-capitalist, opposed to all governments, per se. However, when comparing states and state-like entities, such as Israel and Hamas, unless I am content to condemn them both, I must approach this issue from a different libertarian perspective. I have chosen classical liberalism as a vantage point from which to do this.

Whereupon my critic takes issue with the fact that "Block suggests that the Biden administration's refusal (albeit temporarily) to send bombs to Israel defeats the administration's stated purpose for the refusal—to save Gazan lives. This is the case, Block argues, because the bombs that were withheld are precision bombs and would kill less civilians. Here, I merely point to the evidence cited above, which makes clear that the IDF is not concerned with sparing the lives of non-

[11] See McMaken (2024). For a response, Block (2024A)

[12] Why is it that the Biden Administration ceased its support for Israel? Was it due to libertarian considerations which reject foreign aid? Not a bit of it. Rather, it was because the IDF was not following US orders which undermined its effectiveness in pursuing the Hamas terrorists.

combatants, regardless of the types of bombs being guided by AI systems."

This "logic" goes way over my head. Yes, precision munitions will allow more Gazan civilian lives to be saved. The US refuses to continue to send them. If the IDF wishes to defend its country with inferior weaponry, more civilians will perish. This proves that the Israeli military "is not concerned with sparing the lives of non-combatants"? Under what logical system can this even come close to being true? Maybe logic operates differently at NYU. Rectenwald seems to saying that since the Israeli military can no longer have this precision armament, if they were really "concerned with sparing the lives of non-combatants" they would altogether cease operations against Hamas, that is, commit national suicide. A rational person can only react with dismay at this illogic.

Whereupon Rectenwald launches upon the following:

"Then, our anarcho-capitalist-turned-classical-liberal-in-the-case-of-Israel-only makes a stunning reversal. Withholding said aid and arms to Israel is beneficial after all: However, I must concede, there is indeed one benefit that flows from this backstabbing cessation of armaments: the US will further solidify its reputation for international unreliability. This is all to the good since on net balance and here I expect my opponent will agree with me, the interference of the US in world affairs has been a detriment to peace and prosperity, and thus its limitation will

be positive...

"Let's get this straight. Withholding aid and arms to Israel is bad because of the reasons Block has just given: 1) it would harm Israel; 2) it represents a double standard (because DiLorenzo and, I suppose, other commentators, didn't mention cutting all foreign aid); 3) the US promised the aid and arms; 4) Israel is a US client state, and the US has a bad reputation for reneging on its promises with respect to its client states, reputational damage that will only be exacerbated by refusing Israel aid and arms; and 5) cutting said aid and arms will end up endangering more Gazan lives.

"But, but, but … withholding of said aid and arms is nevertheless beneficial — because it will solidify the reputation of the US as an unreliable international partner. Here, Block transparently contradicts point number 4.

"Then, Block stunningly admits: 'the interference of the US in world affairs has been a detriment to peace and prosperity, and thus its limitation will be positive.'"

Evidently, this author has never heard of the concept of "silver lining." What, pray tell, is that? For his edification, it stems from the statement: "Every cloud has a silver lining." For example, it is raining outside, and this will ruin our plans for a picnic. However, it has been hot around here lately, and at least the rain will cool things down. Or, I hate to clean up my apartment; it is a pain in the neck. But in so doing I found my wristwatch, which I thought I had lost. The cooler weather, and the timepiece are the silver-linings, benefit which stem from an otherwise unsatisfactory situation. Or more pertinent to the case at hand, US foreign policy has been an utter disaster for many, many years.[13] The latest failure has been it sticking a knife in the back of Israel (Block, 2024B) by suddenly, precipitously, abruptly, stopping shipments of promised precision military aid. But at least there is some benefit, some silver lining, in this sorry state of affairs: the US reputation for reliability in foreign affairs will be further besmirched, and this country will be even less trusted than before, and thus less able to ruin things in future. This seems like a perfectly coherent claim. It might even be false. But Rectenwald perceives a logical contradiction in it. I just cannot for the life of me understand how an intelligent person, an accomplished scholar such as he, can draw that conclusion.

This author ends his essay by bewailing "… the deaths of over 35,000 people, the displacement of 2.3 million people, and the hundreds of thousands facing starvation…" involved in the present war of Israel against Hamas. I join him in this regret. Fervently so. Among the missing is possibly a modern-day Mozart. Or Einstein. Or the person who would have cured cancer 20 years earlier than when it would be actually alleviated thus

[13] Let us stipulate, arguendo, that this is true

saving not millions but billions of further precious lives.

But which organization started this war? Which is responsible for this carnage? Obviously, Hamas. And we precisely set the date at which this occurred: October 7, 2023. Had they not done so, the present carnage would not be occurring. Rectenwald is busily attacking Israel for defending itself, and me for justifying the role that Israel and the IDF have played. He should be ashamed of himself.

Nevertheless, I am grateful to him for this irrational, tendentious, evil, malignant essay of his. Without it, I could not have written this reply, and further made the case on behalf of the only almost fully civilized country in the Middle East and its present entirely justified war.

WORKS CITED

Bauer, P. T. (1954 [1967]). *West African Trade*. New York, N.Y.: Augustus M Kelley Pubs

Bauer, P. T. (1972). *Dissent on Development*. Cambridge, MA: Harvard University Press

Bauer, P. T. (1981). *Equality, the Third World, and Economic Delusion*. Cambridge: Harvard University Press

Bauer, P. T. (1982). Ecclesiastical Economics is Envy Exalted. *This World*, (1), Winter/Spring.

Bauer, P. T. (1984). *Reality and Rhetoric: Studies in the Economics of Development*. Cambridge Mass., Harvard University Press.

Bauer, P. T. (1987, Nov). Population Scares. *Commentary*, *84*(5), 39-42.

Bauer, P. T., & Yamey, B. S. (1957). *The Economics of Underdeveloped Countries.* The University of Chicago Press, Chicago

Block, W. E. (2007). Anarchism and Minarchism; No Rapprochement Possible: Reply to Tibor Machan. *Journal of Libertarian Studies, 21*(1), 91-99; Retrieved from: https://mises.org/journals/jls/22_1/22_1_37.pdf

Block, W. E. (2010). Response to Jakobsson on human body shields. *Libertarian Papers*. Retrieved from: https://libertarianpapers.org/2010/25-block-response-to-jakobsson-on-human-body-shields/

Block, W. E. (2011A). The Human Body Shield. *Journal of Libertarian Studies*, *22*(1), 625-630. Retrieved from: https://mises.org/journals/jls/22_1/22_1_30.pdf

Block, W. E. (2011B). Governmental Inevitability: Reply to Holcombe. *Journal of Libertarian Studies, 19*(3), 667-688. Retrieved from : https://mises.org/journals/jls/22_1/22_1_34.pdf

Block, W. E. (2019). Human shields, missiles, negative homesteading and libertarianism. *Ekonomia Wroclaw Economic Review*, *25*(1), 9-22. doi: 10.19195/2084-4093.25.1.1

Block, W. E. (2021). Murray Rothbard, Anarchist. *Histori Filozofii (Studies in the History of Philosophy), 12*(4), 7-41. doi: 10.12775/szhf.2021.018

Block, W. E. (2024A, Jun 27). *US should stop micromanaging the Israeli war.* Retrieved from Israel Hayom: https://www.israelhayom.com/opinions/us-should-stop-micro-managing-the-israeli-war/

Block, W. E. (2024B, May 15). *Backstabbing Israel.* Retrieved from Israel Hayom: https://www.israelhayom.com/opinions/backstabbing-israel/

Block, W. E., & Fleischer, M. (2010, Oct 13). *How Would an Anarchist Society Handle Child Abuse?* Retrieved from LewRockwell.com: http://archive.lewrockwell.com/block/block167.html

Block, W. E. (2022A, Mar 5). *Russia and Ukraine.* Retrieved from Ron Paul Institute: https://ronpaulinstitute.org/russia-and-ukraine/

Block, W. E. (2022B, Apr 27). *Nuclear War*. Retrieved from Ron Paul Institute: https://ronpaulinstitute.org/nuclear-war/

Block, W. E. (2022C, May 19). *How will human life on earth end, and what to do about this?* Retrieved from Ron Paul Institute: https://ronpaulinstitute.org/how-will-human-life-on-earth-end-and-what-to-do-about-this/

Block, W. E., & Barnett W. (2008). Continuums. *Journal Etica e Politica / Ethics & Politics, X*(1), 151-166, Retrieved from: https://www.openstarts.units.it/handle/10077/5251

Block, W. E., & Futerman, A. G. (2020-2021). Rejoinder to Miller on Anarcho Capitalism. *Quinnipiac Health Law Journal, 24*(1), 1-27. Retrieved from : https://heinonline.org/HOL/LandingPage?handle=hein.journals/qhlj24&div=5&id=&page=

Block, W. E., & Futerman, A. (2021). *The Classical Liberal Case for Israel. With commentary by Benjamin Netanyahu*. Springer Publishing Company

Futerman, A., & Block, W. E. (2019). The Fallacy of A Priori Statism. *Stetson Law Review. 49*, 73-91; Retrieved from: https://www2.stetson.edu/law-review/wp-content/uploads/2020/01/3.-49.1-FutermanBlock.pdf

McMaken, R. (2024, Apr 29). The Problem with Microlibertarianism. Retrieved from LewRockwell.com: https://www.lewrockwell.com/2024/04/ryan-mcmaken/the-problem-with-microlibertarianism/

Rectenwald, M. (2024, Jul 1). *A Chip Off the Old Block.; Walter Block's Flawed and Malignant Support for Israeli War Crimes*. X.com. Retrieved from X.com: https://x.com/RecTheRegime/status/1807797101390090675

Rothbard, M. N. (1967, Spring-Autumn). War guilt in the Middle East. *Left and Right, 3*(3), 20-30. Retrieved from MisesInstitute: https://mises.org/journals/lar/pdfs/3_3/3_3_4.pdf

Received for publication: 23.07.2024
Revision received: 27.07.2024
Accepted for publication: 08.01.2025.

How to cite this article?

Style – **APA** *Sixth Edition:*

Block, W. E. (2025, 01 15). Rejoinder to Rectenwald on Supposed Israeli War Crimes. (Z. Cekerevac, Ed.) *MEST Journal, 13*(1), 13-22. doi:10.12709/mest.13.13.01.02

Style – **Chicago** *Sixteenth Edition:*

Block, Walter E. "Rejoinder to Rectenwald on Supposed Israeli War Crimes." Edited by Zoran Cekerevac. *MEST Journal* (MESTE) 13, no. 1 (01 2025): 13-22.

Style – **GOST** *Name Sort:*

Block Walter E Rejoinder to Rectenwald on Supposed Israeli War Crimes [Journal] // MEST Journal / ed. Cekerevac Zoran. - Belgrade – Toronto : MESTE, 01 15, 2025. - 1 : Vol. 13. - pp. 13-22.

Style – **Harvard** *Anglia:*

Block, W. E., 2025. Rejoinder to Rectenwald on Supposed Israeli War Crimes. *MEST Journal,* 15 01, 13(1), pp. 13-22.

Style – **ISO 690** *Numerical Reference:*

Rejoinder to Rectenwald on Supposed Israeli War Crimes. **Block, Walter E.** [ed.] Zoran Cekerevac. 1, Belgrade – Toronto : MESTE, 01 15, 2025, MEST Journal, Vol. 13, pp. 13-22.

MEST Journal
DOI 10.12709/mest.13.13.01.03

REJOINDER TO BIONIC MOSQUITO ON ISRAEL

Walter E. Block
Harold E. Wirth Eminent Scholar Endowed Chair and Professor of Economics, Loyola University New Orleans, New Orleans, LA, USA
https://orcid.org/0000-0003-2215-4791

JEL Category: **Q15**

Abstract

Mosquito (2018, 2023) is a rejoinder to Block, Futerman, and Farber (2016), as well as to Futerman, Farber, and Block (2016). The latter two essays heavily support Israel, and criticize Rothbard (1967) which, in turn, is highly critical of Israel. The present publication is an attempt to refute Mosquito's two rejections of the case on behalf of Israel and thus supports the only Jewish state on the planet. The issue of contention in Mosquito's first essay has mainly to do with private property rights and homesteading. The debate concerns how far back in history it is legitimate to go in the determination of which group of people are the rightful owners of land under dispute. This is crucially important since the very existence of Israel is at stake. If the views of Mosquito and Rothbard are correct, that pretty much spells the end of Israel, since the land it claims to rule over properly belongs to Arabs, Palestinians, and other enemies of this country. Mosquito's second essay involves his rejection of Israel's conduct in the present war in the Middle East. All parties to this debate are libertarians, who predicate this philosophy on Lockean (1948) homesteading theory. This makes it all the more remarkable that we come to such widely disparate conclusions as to this matter.

Keywords: *Palestinians, Israelis, homesteading, land titles, justification, statutes of limitation.*

1 INTRODUCTION

Mosquito (2018, 2023) has written two important essays criticizing the very existence of the state of Israel. The first is based upon the homesteading theory of libertarianism; the second constitutes his criticism of Israel's activities since October 7, 2023.

What is libertarianism? Briefly, it is the view that just law is predicated upon two principles: first, non-aggression. It should be illegal to engage in the threat of actual violence against innocent people. Force is only justified in defense, not offense.[1] Secondly, legitimate property rights are initially based upon the homesteading of virgin

Address of the author:
Walter E. Block
wblock@loyno.edu

[1] See on this Bergland (1986); Block (2008, 2009); Hoppe (1993); Huebert (2010); Kinsella (1995, 1996); Narveson (1988); Nozick (1974); Rothbard (1973, 1978, 1982); Woolridge (1970).

territory,[2] and any voluntary interaction thereafter, such as buying, selling, trading, lending, gambling, gift giving, etc.[3]

In section II we refute Mosquito's (2018) in which he claims that at the very best Israel is only 7 percent legitimate. Section III is given over to a rejection of Mosquito (2023) in which this author is "not surprised" that my analysis of the Israel-Hamas war is incompatible with libertarian theory. We conclude in section IV.

2 IS ISRAEL 7 PERCENT LEGITIMATE?

Our author starts this essay of his as follows:

"After noting the anti-Israel sentiment in the Arab world, the authors comment: 'What is much more vexing is that a similar attitude is pervasive among the libertarian community (and, even, shonda, amongst, happily, a very small percentage of Jews) where Israel is often picked out as a particularly pernicious state relative to almost all others.'

"It is interesting – one might consider such descriptors from a nationalist or religious viewpoint, like 'what a disgrace that some Jews hold an anti-Israel position'; but why would this be true from a libertarian standpoint? Just because a libertarian happens to be Jewish, does that preclude him from looking negatively at the creation and/or existence of the state of Israel?"

Mr. Mosquito is absolutely correct: there is no logical contradiction in a Jew, whether libertarian or not, taking a harshly anti-Israel position. However, the three authors he upbraids for this viewpoint are all Jewish. There is no logical inconsistency, either, as Jews bewailing Jewish opponents of the one country in the world dedicated to the preservation of this group of people. To be sure, we did not write that particular point as libertarians; we wrote it qua members of the Hebrew community. The one does not preclude the other.

Mosquito[4] is quite right again when he attributes the "troubling"[5] fact that "some libertarians hold a special hatred of the Israeli state" to Rothbard (1967). This latter author is the leader of the entire libertarian movement, widely and justly known as "Mr. Libertarian." Since he was adamantly opposing the only democracy in the Middle East, it should occasion little surprise that many admirers of his should follow his lead in this matter.

This author goes further than Rothbard in condemning Israel. Whereas the latter says that this country is "'uniquely pernicious' in that it was supposedly founded on massive land theft and expropriation from Arabs," the former opines that:

"Well, it wasn't 'supposedly' founded in such a manner – it was specifically founded in such a manner." Mosquito also takes us to task for our "neglect to point out the terrorism that was also present in the founding."

My claim then and now is that Israel is the rightful owner of the land under contention between the two sides, and thus that while there was indeed "massive land theft and expropriation" it was not by Jews against Palestinians, it was the other way around. As for there being terrorism at the founding of Israel in 1948, once again I applaud Mosquito's keen observatory powers in discerning this. However, it was launched not by Jews against Arabs, but, once again, the inverse. There have been pogroms against Jews from time immemorial, in many, many lands, and the Arabs have not proven themselves behindhand in following up on this tradition.

Mosquito is once again correct in maintaining that "Our thesis…is that Rothbard did not go far back enough in time in analyzing legitimate land claims…." He is to be congratulated for putting his

[2] First come, first served, or, first in time, first in right.

[3] For literature on this matter, consult Block (1990, 2002A, 2002B); Block & Edelstein (2012); Block & Nelson (2015); Block & Yeatts (1999-2000); Block vs Epstein (2005); Bylund (2005, 2012); Gordon (2019A, 2019B); Grotius (1625); Hoppe (1993, 2011); Kinsella, (2003, 2006A, 2006B, 2007, 2009A, 2009B, 2009C); Locke (1948); McMaken (2016); Paul (1987); Pufendorf (1673); Rothbard (1969, 1973); Rozeff (2005); Watner (1982).

[4] This of course is the nom de plume of an accomplished libertarian scholar. I shall not be revealing his identity here or anywhere else.

[5] To me, not to him

finger precisely on this crucially important issue in this debate. My co-authors and I did and do indeed claim that "Much of the land currently under dispute was homesteaded by Jews before the territory was even called 'Palestine,' when it was in fact called 'Judea.'"

But this scholar strenuously objects to the fact that we look back to "Roman times" in an attempt to justify Jewish land ownership at present. Our critic agrees with us that there can be "no man-made statute of limitations in libertarianism." Thus, our claim cannot be summarily rejected on the grounds that the clock undermines it. This is an important point. To be sure, there is a natural statute of limitations under libertarianism: the further back you go in history, the more difficult it is to prove anything, and I must acknowledge that two millennia or more stretch things quite a bit.

I do maintain however that "Jews can prove descent from the original Jewish homesteaders" and that this can be done "both culturally and genetically." Mosquito objects quite strenuously to the former: "Culturally? What on earth does this mean? Westerners share certain cultural characteristics with ancient Greeks. What does this prove about land claims?"

We are trying to dredge up every bit of evidence we can from long, long ago. This scholar is quite right that culture in and of itself will not suffice. But, along with genetic and other evidence, a similar culture, and similar religious practices, can indeed shed light on Jews today and their forebears and thus buttress these claims.

Nor has he any use for genetic evidence. "Genetically? I am quite certain that virtually every one of Mediterranean ancestry (including the Palestinian Arabs) has traces of Jewish genes going back to the time of Christ; throw in the expanse of the Ottoman Empire in more recent years and you pretty much cover all of Southern Europe, northern Africa, the Middle East and Central Asia. Do they all have a claim to this land?"

No, of course not. But some of them do. The perfect is the enemy of the good. What other evidence? Consider the fact that the Al Aqsa Mosque lies above the Hebrew Second Temple, not below it. This edifice was built by the Kohanim, and there are certainly Jews in the modern day with that genetic code. It might have skipped Mosquito's attention, but this is clear evidence, both genetically and architecturally, that the forefathers of the modern Jews were there before the Palestinians. Further evidence for this contention is that the beginning of the Islamic religion dates from the birth and life of Mohammad,[6] which took place in the sixth century, something in the order of 1800 years ago. Jews were around, in sharp contrast, at least double that amount of time. What were the people of the book doing for all those centuries? Surely, among their studies of the Torah, they were also homesteading not only land in general but the very territory now under contention.

Mosquito's response to this explanation? "This is nonsense; correction, this is nonsense on stilts. To lay claim, an individual must demonstrate prior ownership by an ancestor – a specific ancestor; ownership of property that was stolen. Can you imagine the chaos if culture or genes over thousands of years is sufficient to establish a claim?"

Here, my debating partner can be shown to be in error. Consider the following. At present, in the US, the population is around 360 million. Yet the land is virtually empty. If you take a plane from Boston to Los Angeles, you will see a few lights at 30,000 feet, east of the Mississippi. But west of this river, until you reach the coast, the land is virtually empty, apart from Denver and Las Vegas.

How many Indians were there in this territory when the Europeans arrived? The best estimate is 3-10 million. If even 360 million people cannot fill up the entire country, those few could hardly fully occupy it. Thus, there is no case to be made that according to homesteading theory, whites, and blacks too, must vacate, and give all the land back to the native peoples.

If we can extrapolate from what Mosquito says in the Middle Eastern context to the American one, the Indians properly own not one single solitary square inch of the entire continent. Why not? This

[6] According to one estimate, he was born on 29 August 570 CE. See on this: (Kadir, 1997)

is due to the fact that these tribesmen did not own the land they undoubtedly homesteaded on an individual basis. Rather, they owned it communally, collectively, or tribally. It is a highly problematic viewpoint that Mosquito takes upon himself that these people owned no property at all. I cannot believe that proper libertarian theory leads anywhere near that conclusion. And, as for "the chaos" that this author fears, that is a mere pragmatic concern, entirely apart from the doctrine of libertarianism that we both share. Nor will this necessarily ensue. If this case were adjudicated by a libertarian court, and all contending parties were civilized, no such thing would occur.[7]

Next, our author casts doubt on "'Prodigious evidence' from 2000 years ago. Evidence that connects specific individuals to specific land claims?" The relative placement of the Al Aqsa Mosque and the Second Temple seems very "prodigious" to me. As to matching specific people and land titles, that requirement undermines 100% of Indian land claims. I do not think that this viewpoint can be sustained.

At this juncture, our world-class scholar makes the following very important point:

"'Original homesteaders'? Why stop at the fall of Judea? Did Joshua lead the Jews into an unoccupied land? This site identifies 12 battles of Joshua, eleven of which were instigated by the Israelites. I guess we could go back even further, but you get the point; the point is that the argument presented by the authors is pointless – it is never-ending."

No, it is not at all "never-ending." If there are such folk out there, let them make their claim. If they can prove historical precedence over the Israelis, the latter should concede their prior rights. Mr. Mosquito seems to have lost sight of the libertarian principle of "first in time, first in right" and that there are no formal time limits. If someone can prove that he is descended from the Neanderthals and that the Jews stole land from them, their claims should be respected and acted upon. My claim is that this author does not fully understand the libertarian principle of land claims. There is no formal statute of limitations. Yes, the process is "never-ending" in that sense. If it were "ending" there would be no statute of limitations. But, as said before, there is a natural ending to the process: the further back we go in history, the more difficult it is to prove anything. The Jews have proven prior ownership in numerous ways, the most dramatic being the placing of the Second Temple vis a vis that of the Al Aqsa Mosque. Those who preceded the Jews, including the Neanderthals, can also take up the quest. All they need to do is present evidence backing up their claims. They have not done so. Therefore the process has ended; temporarily that is. It is always open and "never-ending" in that if new evidence arises, it must be considered, weighed, and respected.

We now arrive at Mosquito's charge of the "mass expulsion of Arabs during the 1948 War of Independence, we concede that this did indeed happen in certain isolated cases."

Mosquito's response: "There were 750,000 refugees. This is 'isolated'"?

There are two responses here. First, three-quarters of a million Palestinians departed; not all of these constituted unjustified expulsions. Some of them, perhaps a goodly number of them,[8] left as part and parcel of an attempt at genocide to be conducted by the five invading Arab armies against the Jews. The latter sent messages to these soon-to-become refuges, to leave their premises, on the ground that these armies could then better and more efficiently be able to slaughter the Jews. If the Palestinians remained, it would be more difficult to conduct this planned genocidal pogrom.

At virtually the same time, virtually the same number of Jews were expelled from Egypt, Syria, Lebanon, and the other invading armies. These people were totally innocent. They were not at all cooperating with any army intent upon mass murder of civilians. They were not traitors to their countries. One wonders why Mosquito, an otherwise splendid student of history, totally ignored this parallel mass, and in this case only,

[7] As to which is "civilized," Hamas or Israel, the former purposefully aims to murder civilians, the latter does what it can to preserve civilian lives.

[8] There are no statistics available on this phenomenon

forced emigration. If there were any rough justice to come out of this situation, given that Israel would not accept the return of these turncoats, there would have been a massive switch: the departing Palestinians would have taken over the properties vacated by the fleeing Jews, and they would have been given those of the emigrating Palestinians. Israel welcomed those Jews who escaped with their lives from the Arab countries, while the latter set up refugee camps to demonstrate the heartlessness of Israel.

Second, "But the point is, did they [the Palestinians] have a right to these areas in the first place?" Yes, "Arabs lived in the land continuously for thousands of years; multiple generations can be specifically traced and identified." But as we have demonstrated above, the Jews were there long before they arrived on this scene, so, no, they most certainly did not "have a right to these areas in the first place."

Mosquito claims that the "Zionists of Israel no doubt cooperated fully in the Jewish expulsion from Arab lands – as they had regarding Jews throughout Europe." This is more than passing curious. Our author offers not one shred of evidence to back up this claim. It seems highly problematic on its face that the Zionists were encouraging European nations to ban Jews. For one thing, this occurred long before Zionism was even started.[9]

States Mosquito: "Finally, regarding the legitimacy of Israel as a state, even according to Israel's most vociferous critics of which Rothbard was one, 7% of pre-1948 Palestine was purchased legitimately by Jews. As noted in the title, Israel is 7% legitimate."

Let us engage in a little bit of contrary-to-fact history on this point. Suppose that this country was set up based on only this small amount of territory. What would have then occurred? It takes no great imagination to posit that the same five Arab armies that did attack the larger Israel would have attacked this smaller version. They opposed the state of Israel per se, even if it were limited to one square inch of territory.[10] What would then have taken place? The Jews, a first-world high-technology community, would have beaten the Arabs, a low-tech third-world group of nations. Israel would have been roughly the same size that it is now. This would have been justified on libertarian grounds: when an invading army loses, and the victors occupy some of its territory, they may keep it. Rothbard, and Mosquito, would not have been exactly happy with this result. This demonstrates that there is something more than the libertarian theory that emanates from their viewpoints.

In his conclusion, Mosquito avers: "Every single person on earth, if the ancestry is traced back far enough (and 2000 years is more than far enough – a few hundred years is probably far enough), has a history of both victim and perpetrator. What are we supposed to do with that? The authors have made a libertarian case for a war of all against all."

This is not at all the case. Rather, we go back to the earliest claimants. Those are the Jews, in this case. Are there yet earlier claimants? If so, we have not yet heard from them, and no evidence, none at all, however, imperfect, is forthcoming from any such quarter.

Hoppe (2024) commits the same error of thinking that only individuals can homestead, or own, property.[11] This Hoppe-Mosquito thesis completely trashes the idea of homeowners' associations, cooperatives, condominiums, partnerships, corporations, and other such collectivist forms of ownership. It denies that Indian tribes can own any property at all. This constitutes a powerful reductio ad absurdum against this thesis.[12]

---

[9] Zionism begun in 1897 (Britannica, 2024). Pogroms and mass expulsions of Jews in Europe dated long before that time.

[10] The covenant of the Palestinians, which they have never renounced, calls for the murder of all Jews, not just those in the Middle East. "The Day of Judgement will not come about until Muslims fight the Jews, when the Jew will hide behind stones and trees. The stones and trees will say O Muslims, O Abdullah, there is a Jew behind me, come and kill him." (Cohen, 2021)

[11] For a refutation of Hoppe on this and many other points, see Block and Futerman (2024).

[12] There is something deeply fallacious about methodological collectivism. Only individuals, never groups, can engage in human action. However, it is invalid, as these two experts on Austro-libertarianism

3 NOT SURPRISED

Mosquito starts off this essay of his by citing the claim of my co-authors and myself that "Israel is entitled to do whatever it takes to uproot this evil, depraved culture that resides next to it."

In his view, this is incompatible with libertarianism, which, certainly, precludes certain acts that are indeed contrary to the NAP of this philosophy. He does not read in between the lines. "Whatever it takes" written by libertarians means something quite different from when written by others. We mean, "Whatever it takes among other things that is compatible with the non-aggression principle." The purposeful slaughter of civilians is the genocidal approach of Hamas, not Israel, and no libertarian would wish the latter country to adopt this practice of the former. Regrettably, collateral damage occurs in all wars, despite the IDF's best efforts to preserve civilian Gazan life by showering leaflets in all directions. But this is undermined by Hamas using such folk as shields, locating armaments and rocket launchers in hospitals, schools, Mosques, etc.

States my learned friend: "Hamas needs to be destroyed, just as the Nazis were – the Walter Block libertarian campaign for carpet bombing Dresden."

Note, he does not quote me in support of this latter activity. Instead, he puts words into my mouth, attributing to me views I do not hold. It is not proper scholarship to set up a straw man, attribute it to a rival theorist, and then demolish it. I might as well take the position, with no evidence at all, that Mosquito believes that 2+2=5, and then castigate him as irrational for that belief. If he believes I favor "carpet bombing Dresden" he should offer evidence that I favor such a monstrous activity.

Here, Mosquito waxes eloquently: "Of course, such a war would engulf, at minimum, Iran, Syria, Egypt, Saudi Arabia, and Iraq. A few hundred million people – no big deal, not too big a price to pay. But, I wonder, once this is done, how many billion more people will feel hatred toward Israel – and the United States. This path will lead to about 7.5 billion people dead, and the rest dying. But you go for it, Walter. Whatever it takes. And it will entirely be the fault of Hamas – all those tens-of-thousands or tens-of-millions or several billion dead. Hamas started it (they didn't, but this is Walter's lie), so everything that follows is on their head."

Let us take the last assertion first. Hamas did not start this conflagration on October 7? That is a "lie" on my part to say that it did? Whatever, then, did occur on this day of infamy? If murdering some 1200 innocent Israelis, and taking over 200 more as hostages does not count as "starting" anything, one wonders what would count. Of course, Hamas would be responsible for the horrid occurrences that ensued afterward. If not for them, we would not now be in the present situation in the Middle East.

Now for the first claim. These words of his were published on November 1, 2023. Presumably, this author first wrote them a few days before that. Almost a year has passed since then. Just when is this Armageddon supposed to take place? This author vouchsafes us no answer. It would appear, then, that he has not met his intellectual burden. None of these predictions have yet come true. Nothing has come even close. Mosquito is thus rendered as a poor prognosticator. One wonders if he is now ready to take back these rather hysterical words of his.

Next in the batter's box is this statement: "And it isn't enough just for Israel to win. They must win so conclusively that they will never have to face another war – a war to end all wars. Where have we heard that one before? How did that work out?"

Is there something wrong, then, for wishing for complete and total peace? Just because this goal has not yet "worked out" does not mean it never can. Even if we never attain this wonderful objective, that is no justification for sneering at it. Israel has been at war with its neighbors, apart for a few months here and there, almost continuously since 1948. There is nothing amiss, Mosquito to the contrary notwithstanding, for wishing for an end to all such hostilities. Stated Prime Minister of Israel Benjamin Netanyahu: "If the Arabs put down their weapons today, there would be no more

do, to extrapolate this insight to a rejection of political collectivism.

violence. If the Jews put down their weapons today, there would be no more Israel." (Netanyahu, n.d.) No truer words were ever said.

Mosquito now joins a list of distinguished and long-term libertarians who maintain I can no longer make this claim[13] on my own behalf:

"Can we finally give up the pretense that Walter is a libertarian…? This may be one of the more unhinged pieces of writing I have read on this topic."

Let us stipulate, arguendo, that Mosquito is 100% in the right on this debate we are having regarding Israel v. Hamas, and that I am totally wrong. Does my error on this one occasion logically imply I am no longer a libertarian? Of course not. Consider the fact that Murray Rothbard is pro-choice and that Ron Paul is pro-life on the issue of abortion. They are 180 degrees apart from each other on this vitally important issue. Two more prominent leaders of our philosophy can hardly be imagined. If Mosquito is correct in rejecting my libertarian credentials based on my (supposed) error regarding our present controversy, he must also maintain that either Rothbard or Paul, either one of them, is also not a libertarian. That on its face constitutes a reductio ad absurdum of his position.[14]

As for "unhinged,"[15] may I remind this author that we are all scholars here. At least we are supposed to fit into this category. Part and parcel of this undertaking is that evidence, logic, not name-calling, will bring us that proverbial one-millionth of an inch closer to the Truth with a capital T. This sort of verbiage only detracts from this undertaking; it adds nothing positive.

In the view of Mosquito:

"I have been clear about my position on this conflict; it is the position that I find consistent with libertarian political theory, but it strikes me as the most appropriate position to take for any human being with an ounce of decency in him or her: a pox on all political leaders on both sides of this conflict, as well as a pox on the political leaders of those states that support and have allowed this conflict to fester for seventy-five years and more."

Both sides are wrong here, he avers. In this claim, Mosquito commits what Rothbard (1967) properly characterized as the "sectarian fallacy." He urged libertarians to take a clear stand on the issues of the day, lest they become irrelevant and even more powerless to change them than now we are. If we confine ourselves to castigating all, equally, "a pox on all your houses," we cannot affect the world. My debating partner clearly falls into this trap.

Mosquito concludes on this note:

"Walter has asked me several times to work with him on different projects, etc. I have even had people take me to task for not taking advantage of such a noble offer from Walter. First, I have always been cautious about linking my work with that of another. Second, specifically with Walter, while we agree on the ninety-five percent of minor topics, I find him completely and dangerously wrong on the five percent of important ones."

I have two problems with these parting words of his. First, co-authors need not agree on everything under the sun, merely on the limited number of papers that bear both their names. Second, in my view, the Israeli-Hamas war is the only, single, issue upon which we disagree. I have shared many a meal with Mosquito, and to the best of my recollection, there are no other issues that divide us. Evidently, he was too busy with other important work of his to even name one of these other issues in this five percent of disagreements between the two of us.

---

[13] See on this Hoppe (2024); DiLorenzo (2024); McMaken (2024); Rectenwald (2024). For refutations, respectively, see Block and Futerman (2024) (on Hoppe, 2024). Block (2024A, 2024B, 2024C) (on DiLorenzo, 2024); Block (2024D) (on McMaken, 2024); Block 2024E (on Rectenwald, 2024)

[14] As it happens, again utilizing Mosquito's "insight," I claim that neither deserves the libertarian appellation, since evictionism (Block 2014A, 2014B, 2018, 2021) is the only correct libertarian position on this matter. Both libertarian leaders are wrong on this one issue; therefore, neither can any longer be considered a libertarian.

[15] Hoppe (2024) also employs such unscholarly language

WORKS CITED

Bergland, D. (1986). *Libertarianism In One Lesson*. Orpheus Publications.

Bionic Mosquito. (2018, Jan 4). Israel: 7 Percent Legitimate. https://bionicmosquito.blogspot.com/2018/01/israel-7-percent-legitimate.html

Bionic Mosquito. (2023, Nov 1). Not Surprised. https://bionicmosquito.blogspot.com/2023/11/not-surprised.html

Block, W. E. (1990). Earning Happiness Through Homesteading Unowned Land: a comment on 'Buying Misery with Federal Land' by Richard Stroup. Journal of Social Political and Economic Studies, 15(2), 237-253.

Block, W. E. (2002a). Homesteading City Streets; An Exercise in Managerial Theory. Planning and Markets, 5(1), 18-23. http://www-pam.usc.edu/volume5/v5i1a2s1.html

Block, W. E. (2002b). On Reparations to Blacks for Slavery. *Human Rights Review, 3*(4), 53-73.

Block, W. E. (2008 [1976]). *Defending the Undefendable*. Auburn, AL: The Mises Institute. http://mises.org/books/defending.pdf

Block, W. E. (2009). The Privatization of Roads and Highways: Human and Economic Factors; Auburn, AL: The Mises Institute

Block, W. E. (2010). Review of Huebert's Libertarianism Today. *Libertarian Papers*. Retrieved from https://libertarianpapers.org/2010/19-block-review-of-hueberts-libertarianism-today/

Block, W. E. (2014A). Evictionism and Libertarianism. *Journal of Medicine and Philosophy,* 35(2), 290-294;

Block, W. E. (2014B). Toward a libertarian theory of evictionism. *Journal of Family and Economic Issues*, 35(2), 290-294. Retrieved from https://link.springer.com/article/10.1007%2Fs10834-013-9361-4

Block, W. E. (2018). Judith Jarvis Thomson on abortion; a libertarian critique. *DePaul Journal of Health Care Law, 19*(1), 1-17, Article 3

Block, W. E. (2021). *Evictionism: The compromise solution to the pro-life pro-choice debate controversy.* Springer Publishing Company.

Block, W. E. (2024A, 07 15). Anti-war? A rejoinder to Antiwar.com, Lew Rockwell, Tom DiLorenzo, and the Mises Caucus of the Libertarian Party. (Z. Cekerevac, Ed.) *MEST Journal, 12*(2-SE), SE-8-13. doi:10.12709/mest.12.12.SE.02

Block, W. E. (2024B, 04 18). The charge of Israeli cynicism is false. Retrieved from Israel Hayom https://www.israelhayom.com/opinions/the-charge-of-israeli-cynicism-is-false/

Block, W. E. (2024C, 07 15). From Friend and Co-Author to Mad Critic. (Z. Cekerevac, Ed.) *MEST Journal, 12*(2-SE), SE-14-29. doi:10.12709/mest.12.12.SE.03

Block, W. E. (2024D, 07 15). Micro and macro libertarianism: Rejoinder to McMaken. (Z. Cekerevac, Ed.) *MEST Journal, 12*(2-SE), SE-1-7. doi:10.12709/mest.12.12.SE.01

Block, W. E. (2024E). Rejoinder to Rectenwald on supposed Israeli war crimes. *MEST Journal*, Retrieved from https://www.meste.org/mest/M/a_m.html

Block, W. E. & Edelstein, M. R. (2012). Popsicle sticks and homesteading land for nature preserves. *Romanian Economic and Business Review, 7*(1), 7-13. Retrieved from https://www.rebe.rau.ro/REBE%207%201.pdf

Block, W., Epstein, R. (2005). Debate on Eminent Domain. *NYU Journal of Law & Liberty, 1*(3), 1144-1169

Block, W. E., & Futerman, A. G. (2024, 07 15). Rejoinder to Hoppe on Israel Versus Hamas. (Z. Cekerevac, Ed.) *MEST Journal, 12*(2-SE), SE-30-86. doi:10.12709/mest.12.12.SE.04

Block, W. E., Futerman, A. G., & Farber, R. (2016, Jun). A Libertarian Approach to the Legal Status of the State of Israel. *Indonesian Journal of International and Comparative Law, 3*(3), 435-553. Retrieved from https://thejewishlibertarian.com/tag/the-legal-status-of-the-state-of-israel/

Block, W. E., & Nelson, P. L. (2015). *Water Capitalism: The Case for Privatizing Oceans, Rivers, Lakes, and Aquifers.* New York City, N.Y.: Lexington Books; Rowman and Littlefield;

Block, W., & Yeatts, G. (1999-2000). The Economics and Ethics of Land Reform: A Critique of the Pontifical Council for Justice and Peace's 'Toward a Better Distribution of Land: The Challenge of Agrarian Reform'. *Journal of Natural Resources and Environmental Law, 15*(1), 37-69

Britannica. (2024, Sep 5). Zionism. Retrieved from Britannica https://www.britannica.com/topic/Zionism

Bylund, P. (2005, June). *Man and Matter: A Philosophical Inquiry into the Justification of Ownership in Land from the Basis of Self-Ownership.* Master thesis, Lund University. Retrieved from https://www.uppsatser.se/uppsats/a7eb17de8f/

Bylund, P. (2012). Man and matter: how the former gains ownership of the latter. *Libertarian Papers, 4*(1). Retrieved from https://libertarianpapers.org/articles/2012/lp-4-1-5.pdf

Cohen, B. (2021, Sep 24). 'There is a Jew hiding behind me — come and kill him'. Retrieved from *Pittsburgh Jewish Chronicle* https://jewishchronicle.timesofisrael.com/there-is-a-jew-hiding-behind-me-come-and-kill-him/

DiLorenzo, T. (2024). "From Mad (Social) Scientist to Mad Zionist." June 1; Retrieved from Lew Rockwell https://www.lewrockwell.com/2024/06/thomas-dilorenzo/from-mad-socialscientist-to-mad-zionist/

Futerman, A. G., Farber, R., & Block, W. E. (2016, Oct 13). The Libertarian Case for Israel. Retrieved from Forward https://forward.com/scribe/351957/tk-tk/

Gordon, D. (2019A, Nov 8). Locke vs. Cohen vs. Rothbard on Homesteading. Retrieved from Mises Institute https://mises.org/wire/locke-vs-cohen-vs-rothbard-homesteading

Gordon, D. (2019B, Dec 13). Violence, Homesteading, and the Origins of Private Property. Retrieved from Mises Institute https://mises.org/wire/violence-homesteading-and-origins-private-property

Grotius, H. (1625). *Law of War and Peace (De Jure Belli ac Pacis)*, 3 volumes, translated by A.C. Campbell, London, 1814

Hazlitt, H. (2008 [1946]). *Economics in One Lesson*. Auburn, AL: Mises Institute. Retrieved from https://mises.org/books/economics_in_one_lesson_hazlitt.pdf

Hoppe, H-H. (1993). *The Economics and Ethics of Private Property: Studies in Political Economy and Philosophy*. Boston: Kluwer

Hoppe, H-H. (2011). Of Private, Common, and Public Property and the Rationale for Total Privatization. *Libertarian Papers, 3*(1), 1-13. Retrieved from https://libertarianpapers.org/2011/1-hoppe-private-common-and-public-property/

Hoppe, H. (2024, Jan 31). An Open Letter to Walter E. Block. Retrieved from LewRockwel https://www.lewrockwell.com/2024/01/hans-hermann-hoppe/breaking-up-is-hard-to-do-but-sometimes-necessary/

Huebert, J. (2010). *Libertarianism Today*. Santa Barbara, CA.: Praeger

Kadir, S. (1997, Jul 22). Quran readings, songs to mark Prophet birthday. Retrieved from *The Straits Times*, p. 8, https://eresources.nlb.gov.sg/newspapers/Digitised/Article/straitstimes19970722-1.2.87.11.2

Kinsella, S. (1995). Legislation and the Discovery of Law in a Free Society. *Journal of Libertarian Studies 11*(2), 132-181.

Kinsella, S. N. (1996, Fall). New Rationalist Directions in Libertarian Rights Theory. *Journal of Libertarian Studies 12*(2), 313-326. Retrieved from https://www.mises.org/journals/jls/12_2/12_2_5.pdf

Kinsella, S. N. (2003). A libertarian theory of contract: title transfer, binding promises, and inalienability. *Journal of Libertarian Studies, 17*(2), 11–37. Retrieved from http://www.mises.org/journals/jls/17_2/17_2_2.pdf

Kinsella, S. N. (2006A, May 26). Thoughts on Intellectual Property, Scarcity, Labor-ownership, Metaphors, and Lockean Homesteading. Retrieved from Mises Institute https://mises.org/wire/thoughts-intellectual-property-scarcity-labor-ownership-metaphors-and-lockean-homesteading

Kinsella, S. N. (2006B, Sep 7). How We Come to Own Ourselves. Retrieved from Mises Daily https://mises.org/library/how-we-come-own-ourselves

Kinsella, S. N. (2007, Aug 15). Thoughts on the Latecomer and Homesteading Ideas; or, why the very idea of "ownership" implies that only libertarian principles are justifiable. Retrieved from Mises Wire https://mises.org/wire/thoughts-latecomer-and-homesteading-ideas-or-why-very-idea-ownership-implies-only-libertarian

Kinsella, S. N. (2009A, Aug 21). What Libertarianism Is. Retrieved from Mises Institute https://mises.org/library/what-libertarianism

Kinsella, S. N. (2009B). What Libertarianism Is, in Jörg Guido Hülsmann & Stephan Kinsella, eds., *Property, Freedom, and Society: Essays in Honor of Hans-Hermann Hoppe* (Auburn AL: Mises Institute)

Kinsella, S. N. (2009C, May 22). Homesteading, Abandonment, and Unowned Land in the Civil Law. http://blog.mises.org/10004/homesteading-abandonment-and-unowned-land-in-the-civil-law/

Locke, J. (1948). An Essay Concerning the True Origin, Extent, and End of Civil Government. In E. Barker (Ed.), Social Contract (pp. 17-19). New York: Oxford University Press.

McMaken, R. (2016, October 19). How the Feds Botched the Frontier Homestead Acts. https://mises.org/wire/how-feds-botched-frontier-homestead-acts

McMaken, R. (2024, April 29). The Problem with Microlibertarianism. LewRockwell.com. https://www.lewrockwell.com/2024/04/ryan-mcmaken/the-problem-with-microlibertarianism/

Narveson, J. (1988). The Libertarian Idea. Philadelphia: Temple University Press.

Netanyahu, B. (n.d.) Quotable Quote. Retrieved from Goodreads https://www.goodreads.com/quotes/513129-if-the-arabs-put-down-their-weapons-today-there-would

Nozick, R. (1974). Anarchy, State, and Utopia. New York: Basic Books.

Paul, E. F. (1987). Property Rights and Eminent Domain. Livingston, New Jersey: Transaction Publishers.

Pufendorf, S. (1673). Natural law and the law of nations. Buffalo, NJ: Hein.

Rand, A. (1957). Atlas Shrugged. New York, NY: Random House.

Rectenwald, M. (2024, July 1). A Chip Off the Old Block: Walter Block's Flawed and Malignant Support for Israeli War Crimes.

Rothbard, M. N. (1967). War guilt in the Middle East. Left and Right. http://mises.org/journals/lar/pdfs/3_3/3_3_4.pdf

Rothbard, M. N. (1969, June 15). Confiscation and the Homestead Principle. The Libertarian Forum, 1(6). https://www.panarchy.org/rothbard/confiscation.html

Rothbard, M. N. (1973). *For a New Liberty*. New York: Macmillan

Rothbard, M. N. (1998). The Ethics of Liberty. New York: New York University Press.

Rozeff, M. S. (2005, September 1). Original Appropriation and Its Critics. Retrieved from http://www.lewrockwell.com/rozeff/rozeff18.html

Watner, C. (1982). The Proprietary Theory of Justice in the Libertarian Tradition. Journal of Libertarian Studies, 6(3-4), 289-316. Retrieved from http://mises.org/journals/jls/6_3/6_3_6.pdf

Woolridge, W. C. (1970). Uncle Sam the Monopoly Man. New Rochelle, N.Y.: Arlington House.

Received for publication: 10.09.2024
Revision received: 14.09.2024
Accepted for publication: 08.01.2025.

How to cite this article?

Style – **APA** *Sixth Edition:*

Block, W. E. (2025, 01 15). Rejoinder to Bionic Mosquito on Israel. (Z. Cekerevac, Ed.) *MEST Journal, 13*(1), 23-33. doi:10.12709/mest.13.13.01.03

Style – **Chicago** *Sixteenth Edition:*

Block, Walter E. "Rejoinder to Bionic Mosquito on Israel." Edited by Zoran Cekerevac. *MEST Journal* (MESTE) 13, no. 1 (01 2025): 23-33.

Style – **GOST** *Name Sort:*

Block Walter E Rejoinder to Bionic Mosquito on Israel [Journal] // MEST Journal / ed. Cekerevac Zoran. - Belgrade – Toronto : MESTE, 01 15, 2025. - 1 : Vol. 13. - pp. 23-33.

Style – **Harvard** *Anglia:*

Block, W. E., 2025. Rejoinder to Bionic Mosquito on Israel. *MEST Journal,* 15 01, 13(1), pp. 23-33.

Style – **ISO 690** *Numerical Reference:*

Rejoinder to Bionic Mosquito on Israel. **Block, Walter E.** [ed.] Zoran Cekerevac. 1, Belgrade – Toronto : MESTE, 01 15, 2025, MEST Journal, Vol. 13, pp. 23-33.

MEST Journal
DOI 10.12709/mest.13.13.01.04

SECURITY RISKS FROM THE MODERN MAN-IN-THE-MIDDLE ATTACKS

Zoran Cekerevac
MESTE, Belgrade, Serbia
https://orcid.org/0000-0003-2972-2472

Petar Cekerevac
Independent researcher, Belgrade, Serbia
https://orcid.org/0000-0001-6100-5938

Lyudmila Prigoda
Maikop State Technological University, Maikop, Russia
https://orcid.org/0000-0002-4762-3892

Fawzi Al-Naima
Al-Kut University College, Wasit, Iraq, and Department of Computer Eng., Al-Nahrain University, Baghdad, Iraq
https://orcid.org/0000-0003-0930-5073

JEL Category: **G32, M15**

Abstract

This paper presents a detailed analysis of Man-in-the-Middle (MITM) attacks, covering their technology, historical examples, economic consequences, and managerial prevention activities. The study overviews modern Internet trends and discusses the weaknesses of current security measures, such as Secure Sockets Layer and Transport Layer Security protocols, and the complexity of two-way trust relationships. Various techniques for launching MITM attacks are considered, including Address Resolution Protocol cache poisoning, Domain Name Server spoofing, session hijacking, and Secure Sockets Layer hijacking. A chronological overview of some well-known MITM attacks highlights a shift from laptops to mobile devices. It emphasizes the vulnerability of Bluetooth low-energy devices, estimating around 80% of such devices are susceptible to MITM attacks. Overall, this paper provides a perceptive analysis of MITM attacks, their past and current manifestations, and the significant economic impact they can have on computer systems and users and underscores the crucial need for robust security measures.

Keywords: *Babington Plot, computer applications, computer networks, Internet, MITM.*

Address of the corresponding author:
Zoran Cekerevac
zoran@cekerevac.eu

1 INTRODUCTION

In 2011, Cisco predicted that by 2020, there would be 50 billion devices connected to the Internet. The widespread deployment of the Internet of Things (IoT) was expected to lead to a significant transformation in our comprehension and the evolution of the Internet (Evans, 2011). It seems that expectations were too optimistic. In the meantime, unexpected events took place and greatly influenced the development of the Internet, devices, and applications. As reported by Statista, about 15.14 billion IoT devices were used worldwide in 2023 (Vailshery, 2023). We can add approximately seven billion mobile phones and two billion personal computers. It is easy to conclude that the Internet was connecting over 24 billion devices in 2023.

New software applications emerged alongside the widespread use of new devices. They enhanced the quality of life, but also brought about a significant increase in risks.

It is fine when everything is connected to the Internet and can exchange data according to user wishes. But, on its way to its final destinations, data passes through all TCP/IP model layers where many risks lurk. One can add a new potential risk layer, the extensive use of Cloud storage. The possibility of an attack on this layer is high, starting with brute force attacks at password-based attacks and including possible data change at the Session layer using man-in-the-middle (MITM)[1] attacks.

This paper presents famous MITM attack cases and their economic consequences. For those unfamiliar with MITM attack technology, in Section 3, we explained an example of a communication scheme shown in Fig. 1. We also recommended other literature sources with more in-depth details to enhance comprehension of MITM attacks.

2 METHODS AND HYPOTHESES

The methodology applied in this research includes the systemic-functional approach to the phenomena analysis. In justification of theoretical propositions and findings, the authors used the hypothetico-deductive method, axiomatic method, analytical-deductive method, comparative method, scientific induction and deduction, synthesis, and comparative analysis.

At the turn of the century, research efforts were directed towards MITM attacks. With the advancements in computer protection technology, the authors of this paper proposed a research question:

Are MITM attacks still a threat?

They entered the research with the following hypothesis:

H_o – The MITM attack is an old and outdated technology that cannot harm modern computer systems and their users, so it is no longer in use.

The authors also set the alternative hypothesis:

H_a – MITM attacks still exist and can harm modern computer systems and their users.

3 MITM TECHNOLOGY

An MITM attack can be visualized as a game of the broken telephone when words are passed from the first participant to a row of participants up to the final participant. The message often reaches the last person in the row modified, consciously or unconsciously. In an MITM attack, an intermediate participant manipulates the messages of two legitimate participants.

Man-in-the-middle attacks have been happening since ancient times. Only the means were different. One of the most famous MITM attacks was the Babington Plot. It took place in 1568. Communications between Mary Stuart and her supporters regarding the plot to assassinate Queen Elizabeth I were intercepted by a third party (Sir Francis Walsingham). Altering the contents of the messages revealed the identities of those involved in the plot and resulted in their execution (Ecuron, 2023).

Most modern Internet applications use encrypted connections provided by SSL/TLS protocols to provide services securely. SSL/TLS can create a two-way trust relationship, but it is rather complex for administration. Often, only one party

[1] Also known as Manipulator-in-the-Middle or Machine-in-the-Middle

authenticates the connection. That represents a weakness that an attacker can exploit.

A modern MITM attack employs various techniques to intercept communication between two nodes. The attacker can usurp the proxy role by disconnecting their victims' communication.

The MITM attack example in Fig. 1 was thoroughly analyzed in the paper by Cekerevac, Dvorak, Prigoda, & Cekerevac (2017). The attacker's idea is to replace the public keys of Victim A (bank client) and Victim B (bank) in victims' communication with his public key. The attacker's main challenge is how to get involved in communication. Once successfully positioned, he can manipulate communications or use eavesdropping.

How it might look in the case of an attack on Office 365 is shown in Fig. 2. In credential phishing, the MITM server acts as a proxy. It presents the destination's login page to the victim and passes on any received username and password to the destination URL. In the case of multi-factor authentication (MFA), it presents the MFA request to the user for further input and forwards any responses to the destination. Because the MITM server is between secure connections, it can decrypt data from the user and extract the username and password. It then re-encrypts the traffic and sends it to the destination website. When authentication is completed, the final step is for the destination website to send a session cookie to the user. Session cookies are valuable as they manage all the information that needs to be stored during the victim's interaction with the website. An attacker can decrypt and extract the session cookie before sending it to the user (Arndt, 2023).

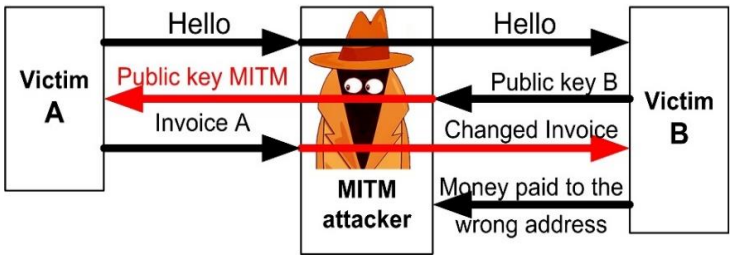


Fig. 1 An example of the MITM attack (Cekerevac, Dvorak, Prigoda, & Cekerevac, 2017)

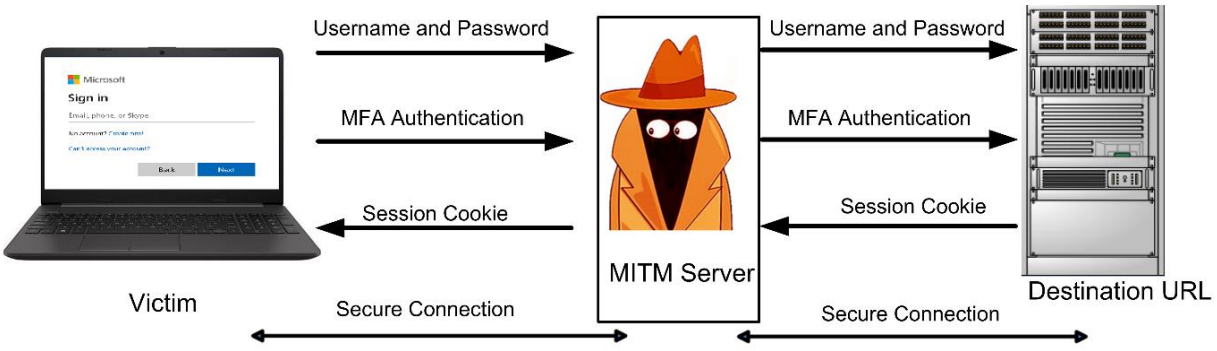


Fig. 2 The MITM server intercepts all steps of authentication. (Source: Authors, based on (Arndt, 2023))

The MITM attacks can start with (Cekerevac, Dvorak, Prigoda, & Cekerevac, 2017):

- Address Resolution Protocol (ARP) cache poisoning. The attacker manipulates ARP tables to intercept and redirect network traffic between two parties.
- DNS spoofing. The attacker forges DNS responses to redirect users to malicious websites or intercept sensitive information.
- Session hijacking, including side-jacking, evil twin, and sniffing. The attacker steals or impersonates a user's session token to gain unauthorized access or perform actions on their behalf.

- SSL Hijacking. The attacker intercepts and decrypts SSL/TLS encrypted communications by presenting fake certificates.

Here are some other common examples of Man-in-the-Middle (MITM) attacks, such as:

- Wi-Fi pineapple attacks - The attacker exploits Wi-Fi vulnerabilities to intercept and manipulate network traffic.
- IP spoofing - The attacker manipulates the source IP address to impersonate another person or device on the network.
- Evil Twin attacks - The attacker creates a fraudulent wireless access point (AP) to trick users into connecting and intercepting their traffic.
- Email interception - The attacker intercepts and reads email messages exchanged between two email servers.
- SSL stripping - The attacker downgrades an encrypted connection to an unencrypted one, allowing them to intercept sensitive information.
- Bluetooth hijacking - The attacker intercepts and manipulates Bluetooth communication between devices.

In the past, MITM attacks predominantly targeted laptops, but now mobile phones are becoming the main target of attacks. The risk is increasing because many users do not even think about their data protection. Significant risks also arise from the Internet of Things (IoT) inclusion in networks. Each of the connected devices is a possible point of intrusion into the network.

MITM attacks can be performed in many ways using a variety of tools. Some of such tools are:

- Ettercap – a comprehensive suite for MITM attacks that includes many features for network and host analysis and supports the dissection of many protocols (Ornaghi & Valleri, 2015).
- evilgrade – a modular framework that allows injecting fake updates and making hostname redirections (Amato & Kirschbaum, 2010).
- Dsniff – “a collection of tools for network auditing and penetration testing. Sshmitm and webmitm implement active MITM attacks against redirected SSH and HTTPS sessions by exploiting weak bindings in ad-hoc PKI” (Song, 2001).

There is also a risk in Bluetooth communication. Some say that the Bluetooth operating range is small and an MITM attacker must be close to both attacked devices. That is true, but Bluetooth Low Energy (BLE) devices can have a working range of more than 100m. Furthermore, in some cases, the devices do not even need to be close to each other. The attacker can relay packets remotely via the Internet (Cekerevac, Dvorak, Prigoda, & Cekerevac, 2017).

Many Bluetooth devices used for keyless entry and mobile point-of-sales systems are vulnerable to MITM attacks. The BLE specification provides secure connections through link-layer encryption, device whitelisting, and bonding. But "companies too often do not implement correctly that protection and this lack could allow attackers to clone BLE devices” (Jasek, 2016). “Jasek estimates that 80% of BLE smart devices are vulnerable to MITM attacks” (Spring, 2016). Per this research, 80% of reviewed devices were incorrectly configured. That allows hackers to use tools like GATTacker to perform an MITM attack.

It is interesting to see how MITM attacks have adapted to today's circumstances. Here are some experiences (Cekerevac, Dvorak, Prigoda, & Cekerevac, 2017):

- Man-in-the-cloud (MITC). Cloud computing has become a standard for many users. Storage capacities are large enough and do not demand users to log on for each data transmission session. After the first authentication, they use a session token saved on the user's local computer. If an attacker steals the token, he can fully control the account.
- Man-in-the-browser (MITB). Many people use e-banking. In the MITB attacks, an attacker in some way inserts a Trojan into the victim's computer. When the victim attempts to visit the targeted URL, the malware injects specific HTML code into the original web page code to trick the user. If the user is not careful, he will not notice minor differences between the current and original user interface. After that, "banking services" will be "provided" by the attacker.

- Man-in-the-mobile (MITMO). Many users prefer to make their financial transactions over their smartphones. The MITMO attack focuses on mobile transaction authentication numbers (mTANs) and transaction authentication codes. This attack intercepts SMS traffic and forwards the captured codes to the attacker. The MITMO is a real and significant challenge for out-of-band authentication systems (Gregg, 2015A).
- Man-in-the-app (MITA). Mobile apps can be vulnerable. MITA implies that an application does not perform certificate validation properly. An attacker inserts a self-signed certificate and exploits how the applications handle trust. He can communicate with the app directly. Then, the hacker can intercept application data, steal information, or impersonate the victim on the application (Gregg, 2015).
- MITM attacks on IoT. With the increasing development of IoT, MITM attacks have become a much bigger challenge. For example, close-to-home devices could be IoT refrigerators that display a user's Google calendar. Research showed that they did not validate SSL certificates. This slip could result in the mounting of an MITM attack and the user's Google credentials stolen (Gregg, 2015A).

After a successful MITM attack, an attacker can use it for identity theft, surveillance, financial exploitation, malware infection, business sabotage, and/or network exploitation (Martens, 2023).

4 RESEARCH RESULTS

Advances in encryption technology and network security have made MITM attacks more difficult to carry out. However, many successful MITM attacks resulted in identity theft, malware infiltration, and financial losses. Cofense Intelligence has identified trends in MITM attacks based on several tell-tale signs (Arndt, 2023):

- MITM attacks increased by 35% in volume, reaching inboxes between Q1 2022 and Q1 2023.

It has been found that the majority of MITM credential phishing attacks, specifically 94%, were aimed at O365 authentication.

At least one URL redirection was used in 89% of campaigns, while 55% used two or more.

After conducting extensive research, we have identified several major MITM attacks that occurred in the last decade.

4.1 DNSChanger botnet: 2007 – 2018

The DNSChanger botnet was a notorious cybercriminal operation active from 2007 to 2011. Initially, the botnet infected millions of computers globally, primarily targeting Windows-based systems. It spreads through various means, such as malicious email attachments, drive-by downloads, and software vulnerabilities. The cybercriminals behind the operation used the botnet for nefarious purposes, including distributing malware, injecting malicious advertisements, and conducting fraudulent activities.

In late 2009, NASA OIG and the FBI opened a joint criminal investigation against Rove Digital, a company suspected of being the source of DNSChanger botnet fraud. This botnet allowed the attackers to redirect millions of victims to websites of the attacker's choice, instead of the websites that victims intended to visit. The malware forced more than one hundred NASA computers to use Rove Digital's DNS servers instead of NASA's DNS servers, which placed them into a sort of botnet under the control of Rove Digital. The NASA OIG checked security records and determined that Session hijacking caused them losses that exceeded $65,000. Millions of computers were believed to be infected worldwide. Seven persons were charged with computer intrusions, wire fraud, and money laundering. Millions of dollars in accounts in Estonia, the United States, Cyprus, Denmark, and Austria have been frozen. In Estonia, real estate and other assets belonging to the defendants were seized (Zadig, 2012-2013).

DNSChanger botnet targeted the Domain Name System (DNS) responsible for translating human-readable domain names into IP addresses. It aimed to redirect users to malicious servers, allowing the attackers to control and manipulate internet traffic for their gain.

The DNSChanger botnet attacked numerous devices worldwide, including computers, routers, and other networked devices. It achieved this by

exploiting security vulnerabilities and spreading malware through infected websites or malicious email attachments.

Activated botnet changed the DNS settings within compromised devices, pointing them to rogue DNS servers controlled by the attackers. Victims' requests were redirected to malicious servers under the attackers' control instead of legitimate websites or online services. This setup allowed the attackers to intercept and monitor internet traffic, potentially leading to various malicious activities like phishing, data theft, and spreading further malware.

The impact of the DNSChanger MITM attack was extensive, affecting both individuals and organizations. Organizations faced risks from compromised internal traffic, compromised data integrity, and the potential for sensitive information leakage.

To combat the threat, cybersecurity organizations and law enforcement agencies worked together to dismantle the botnet infrastructure. With court approval, they arrested and prosecuted the individuals responsible for operating the DNSChanger botnet. Law enforcement also helped victims remove the malicious DNS settings from their devices and restore normal functionality. The security experts advised users on protection against similar MITM attacks and reducing the spread of malware across networks.

In 2011, with the help of a multinational collaboration between law enforcement agencies and cybersecurity organizations, the botnet was suppressed. However, some infected devices remained active because their users did not take any action to clean their systems.

In 2016, Proofpoint experts discovered several improvements in the implementation of the DNSChanger attack, including (Proofpoint, 2016):

- External DNS resolution for internal addresses.
- Steganography for concealment.
- Adding dozens of recent router exploits. At the end of 2016, there were 166 fingerprints, some working for several router models (in 2015 there were 55 fingerprints). Some were a few weeks old (13/09/2016) when the attack started around 28 October.
- When possible (in 36 cases) the exploit kit modifies network rules so the administrative ports are accessible from external addresses. It exposed the router to additional attacks like the Mirai botnet (Vailshery, 2023).
- The adware chain also accepted Android devices.

As of December 16th, 2016, DNSChanger EK appeared to be offline, and the malicious campaign stopped. However, any previously compromised routers (at least 56,000) were potentially still under the attacker's control. The campaign was widespread internationally, mostly in the USA (14%), Indonesia (12.9%), and Brazil (7.4%). Non-mobile computers were mostly attacked (68.4%). Mobiles followed (30.3%). Attacked visitors mostly used the Chrome browser (73.9%). From mobiles, visitors mostly used Android phones (66.5%) and tablets (11.5%). 12% of visitors used iPhones, and 9.8% used iPads (Proofpoint, 2016).

In 2017, law enforcement agencies and cybersecurity experts discovered that remnants of the botnet were still infecting computers worldwide. To combat this ongoing threat, cybersecurity experts launched a campaign to raise awareness and assist affected users in removing the botnet from their devices. The campaign provided resources for individuals to identify if their system was infected and offered guidance on how to mitigate the botnet's impact.

In 2018 a massive new DNS changing issue appeared. Chinese cybersecurity uncovered an ongoing malware campaign that hijacked over 100,000 home routers and modified their DNS settings to steal users' login credentials by redirecting them to malicious web pages, especially when they visited banking sites.

The campaign dubbed GhostDNS has many similarities with the infamous DNSChanger malware. According to the cybersecurity firm Qihoo 360's NetLab, just like the regular DNSChanger campaign, GhostDNS scans for the IP addresses of routers that use weak or no passwords. Then, it accesses the router's settings and changes the router's default DNS address to the one controlled by the attackers (Rocha, 2018).

The DNSChanger botnet attack served as a reminder of the critical role of DNS in Internet

communication and the risks associated with compromised DNS settings. To avoid such attacks users are advised to always use the latest firmware version and a strong password for their router.

4.2 MITM attack on Yahoo: 2011 – 2016

The largest-known breach of any company's computer network happened with Yahoo! in 2013. (Senouci, 2023) Digital thieves have taken over all 3 billion Yahoo user accounts data by that attack. In 2014, the company also disclosed a separate attack that affected 500 million accounts. Attackers came into a position to take data including names, birth dates, phone numbers, passwords, security questions, and backup email addresses. The data was encrypted with easy-to-crack security (Perlroth, 2017).

In 2016, Yahoo faced a significant security breach caused by the MITM attack. Yahoo admitted that one billion accounts were compromised (Khandelwal, 2016) (Henriques, 2016). The attackers employed various methods to carry out the MITM attack on Yahoo. It is believed that they exploited a combination of social engineering tactics, vulnerabilities within Yahoo's systems, and sophisticated techniques. By infiltrating Yahoo's network, the attackers were able to gain access to highly sensitive user information, including names, email addresses, telephone numbers, dates of birth, and passwords of millions of Yahoo users.

Furthermore, the attackers targeted Yahoo's "Account Management" tool, which enabled them to forge "cookies".[2] These forged cookies allowed the attackers to impersonate Yahoo users without needing their passwords and gain access to their accounts, potentially exposing further personal information.

The consequences of the Yahoo MITM attack were substantial. Apart from the immediate breach of personal data, the incident compromised user trust and had far-reaching implications. Customers' private information became vulnerable to misuse, such as identity theft, phishing attacks, and other fraudulent activities. The breach also impacted Yahoo's reputation, leading to public scrutiny and negative publicity.

Yahoo responded to the attack by launching an investigation, notifying affected users, and advising them to change their passwords. They also invalidated the forged cookies, patched security vulnerabilities, and enhanced their security measures to prevent future breaches. The incident prompted Yahoo to collaborate with law enforcement agencies and cybersecurity experts to identify the attackers and hold them accountable.

Court proceedings have also been initiated against Yahoo and Aabaco Small Business, LLC, which resulted in a proposed class-action settlement regarding data hacking incidents that occurred from 2013 to 2016, as well as in connection with data breaches that occurred at least from January to April 2012, although it does not appear that hackers took the data in that case. The settlement applies to those who had a Yahoo account at any time from January 1, 2012, to December 31, 2016 and resided in the USA or Israel. Under the Settlement terms, Yahoo has enhanced, or, through its successor, Oath Holdings Inc., continues to improve its business practices to improve the security of its users' personal information stored in its databases. Yahoo and Aabaco Small Business are obligated to pay $117,500,000 into the Settlement Fund, which is regulated to provide a minimum of two years of credit monitoring services to protect Settlement Class Members from future damages, or a cash alternative for those already have credit monitoring or identity protection. The settlement fund is obligated to provide monetary payments to individuals who incurred expenses, including loss of time, as well as to Yahoo users who paid for ad-free or premium Yahoo Mail services, and to users of Aabaco Small Business services, including business email. The settlement fund will also cover any costs related to the court process. In return, plaintiffs will drop their claims related to the Incidents (Case No. 5:16-MD-02752-LHK, 2020).

In conclusion, the 2016 MITM attack on Yahoo highlighted the critical importance of robust cybersecurity measures and the potential

[2] Small files that authenticate users and keep them logged in to their accounts.

consequences of large-scale data breaches. It served as a wake-up call for Internet users and organizations to prioritize personal information protection and strengthen their defenses against evolving cyber threats.

Verizon bought Yahoo for $4.48 billion in June 2017, but the price was reduced by $350 million from the original deal because of the breaches. Also, Verizon and Yahoo agreed to share certain legal and regulatory liabilities because of data breaches incurred by Yahoo (Tran, 2017).

The Verizon 2023 Data Breach Investigations Report (Hylender, Langlois, Pinto, & Widup, 2023) showed that:

- 74% of all breaches include the human element (via error, privilege misuse, stolen credentials, or social engineering).
- 83% of breaches involved external actors. The primary attackers' motivation is overwhelmingly financially driven at 95% of breaches.
- The primary methods that attackers use are stolen credentials, phishing, and exploitation of vulnerabilities.

Social Engineering attacks are very effective and highly lucrative for cybercriminals. Business Email Compromise (BEC) attacks have almost doubled across incident datasets.

4.3 Superfish: 2014

Superfish was a high-profile security incident and involved some Lenovo laptops sold between 2014 and 2015 (CISA, 2016). This incident was caused by the pre-installed adware program called Superfish, which had severe implications for user privacy and security. Superfish was designed to inject targeted advertisements into users' web browsers by analyzing images on websites. To achieve this, Superfish utilized an MITM attack.

Superfish installed a self-signed root certificate on affected laptops to inject the ads. This certificate allowed Superfish to intercept and decrypt secure HTTPS connections between the user's browser and websites. Superfish undermined https security by acting as a proxy and decrypting the traffic without the user's knowledge or consent (Goodin, 2015).

By conducting an MITM attack, Superfish could inject its ads into websites, even if they were not designed to show ads. This invasive behavior compromised users' browsing experience, flooded their screens with unwanted advertisements, and potentially exposed them to malicious content.

The use of a self-signed root certificate presented significant security risks. Normally, trusted certificate authorities issue SSL/TLS certificates to ensure the authenticity of encrypted communications. Superfish's self-signed certificate bypassed this crucial step. Attackers can exploit vulnerabilities to perform malicious acts. This exposes users to potential attacks by cybercriminals who exploit security gaps. Utilizing the same certificate, attackers could impersonate legitimate websites, intercept sensitive data such as login credentials or financial information, and launch other nefarious activities.

Once the Superfish controversy came to light, it sparked widespread concern among users, security experts, and the technology community. Lenovo faced significant backlash for pre-installing such intrusive adware on their devices. They apologized and promptly released a removal tool to uninstall Superfish and remove the root certificate from affected laptops.

The aftermath of the Superfish incident showed manufacturers and users the potential threats posed by pre-installed software and the need for transparency and security checks within the supply chain.

4.4 Cloudflare Heartbleed: 2017

The public became aware of the Heartbleed bug in 2014. It was a major security flaw in the OpenSSL encryption software those days. That vulnerability was easy to exploit. In addition, it was difficult to detect if an attacker used it.

OpenSSL is one of the best-known SSL implementations. It enables systems to communicate using SSL encryption. The initial release was in 1998, and OpenSSL worked correctly until 2011 when Robin Seggelmann added the faulty Heartbeat feature in an experimental software version. That version passed reviews and went into use. Neither reviewers nor users noticed it. It has been discovered that an OpenSSL vulnerability was present and active between March 2012 and April 2014. Those using older versions (before 1.0.1) were not at risk (Kiprin, 2021).

Heartbleed was a flaw within the implementation of the OpenSSL's Transport Layer Security (TLS) heartbeat feature. This feature allowed secure communication between servers and clients by periodically sending small packets of data to verify that the connection was still active. However, due to a coding error in OpenSSL, an attacker could send a specially crafted malicious heartbeat request, causing the server to leak random chunks of its memory.

The exploit enabled the attacker to retrieve sensitive information from the server's memory, which could include usernames, passwords, private digital keys, and even decrypted data. This kind of attack facilitated potential unauthorized access to confidential information and enabled cybercriminals to present themselves as trusted servers.

In 2017, the Cloudflare Heartbleed incident showcased a potential vulnerability in the widely used OpenSSL cryptographic software library. This vulnerability allowed attackers to carry out an MITM attack, potentially exposing sensitive data transferred between servers and clients.

The Cloudflare Heartbleed incident specifically refers to the impact that this vulnerability had on Cloudflare's content delivery network (CDN). As one of the largest CDN providers, Cloudflare's infrastructure was widely used by numerous websites, making the potential scale of the attack significant.

Upon the discovery of the vulnerability, Cloudflare immediately acted to remediate the issue by patching the affected systems and deploying the necessary security measures. They informed their customers, advised them to update their SSL certificates and private keys, and recommended that users change their passwords as a precautionary measure. Cloudflare has revoked and reissued over 100,000 certificates (Sullivan, 2021).

While the full extent of the exposure and any potential unauthorized access remains unclear, the impact of the Cloudflare Heartbleed incident raised awareness regarding the importance of promptly patching software vulnerabilities and conducting thorough security audits.

Although the Cloudflare Heartbleed attack itself is not an MITM attack, it is significant because in the attack exploited vulnerability can be used in MITM attacks to compromise the security of client-server communications. The Heartbleed incident served as a reminder that even widely trusted and well-established security protocols can contain flaws that cybercriminals can exploit. Unfortunately, it turns out that it is still common for systems to be vulnerable to Heartbleed (Venter, 2023).

4.5 KRACK Attack: 2017

The KRACK attack (Key Reinstallation Attack), discovered in 2018, targeted the WPA2 (Wi-Fi Protected Access II) protocol, which is widely used for securing Wi-Fi networks. It exploited vulnerabilities in the four-way handshake process of the WPA2 protocol and an attacker can use it in an MITM attack.

The KRACK attack leverages the fact that a four-way handshake, used to establish a secure connection between a client and an access point, can be manipulated. By forcing the reuse of a one-time encryption key during the handshake, an attacker can trick the client device into reinstalling a previously used key. This key reinstallation vulnerability allows the attacker to decrypt and/or forge data packets transmitted over the Wi-Fi network (Vanhoef & Piessens, Key Reinstallation Attacks: Breaking WPA2 by forcing nonce reuse, 2017). Attackers can intercept and view sensitive information transmitted over Wi-Fi, such as passwords and credit card details. Additionally, the attacker could inject malicious content into the data stream, potentially leading to further compromise or exploitation.

The KRACK attack had a significant impact on a vast number of devices and Wi-Fi networks worldwide. Both client devices (such as smartphones, laptops, and IoT devices) and Wi-Fi access points were vulnerable to the attack. The attack vector did not rely on any specific software or implementation flaw but rather exploited weaknesses in the WPA2 protocol itself.

Once the KRACK vulnerability was discovered, major technology companies and vendors, including device manufacturers and network equipment providers, released patches and updates to address the issue. They advised users to apply these updates promptly to stay protected.

The KRACK attack highlighted the importance of using updated software and firmware, regular

security patching, and following best practices for securing Wi-Fi networks. It also reinforced the need for end-to-end encryption and the use of additional security measures like VPNs (Virtual Private Networks) to protect data transmitted over Wi-Fi networks, mitigating the risk of MITM attacks.

Currently, the most convenient, although not complete, solution for authentication, and prevention of KRACK and offline dictionary attacks is the WPA3 wireless security standard, which is not supported by all devices. Unfortunately, even WPA3 is not immune to all threats. Vanhoef and Ronen (2019) published several security flaws in WPA3 in 2019. This is about a set of security protocol vulnerabilities collectively known as Dragonblood (Irei & Scarpati, 2022). It refers to physical and temporal attacks that allow an attacker to force devices to revert to WPA2 or enable offline dictionary attacks.

4.6 Efail Attack: 2018

The Efail attack, discovered in 2018, targeted encrypted email communications and exploited vulnerabilities in the way certain email clients handle the OpenPGP and S/MIME encryption standards. It was an MITM attack that took advantage of how email clients handle encrypted content. It relied on manipulating the HTML rendering of encrypted emails to extract the plaintext content from the encrypted sections. By altering specific parts of the encrypted email, the attacker could trick the email client into sending the decrypted content or its metadata back to the attacker's server (EFAIL, 2018).

The vulnerability is directed against the content of the email and not against the recipient, The attack exploited both the design limitations and implementation flaws in certain email clients, particularly those that automatically decrypted or parsed encrypted email content for the convenience of the user. This allowed adversaries to bypass the inherent security provided by OpenPGP and S/MIME encryption standards. The Efail attack has been thoroughly analyzed by Poddebniak and colleagues in their research paper (2018).

The impact of the Efail attack was significant since it affected various email clients. However, it is important to note that the attack did not directly target the encryption algorithms themselves but rather the email client's handling of the encrypted content.

Once the Efail vulnerability was disclosed, the first recommendation was to disable PGP/GPG or S/MIME in email clients (Ashford, 2018). Researchers collaborated with affected email client vendors to address the issue and release necessary patches. In response, many email clients added necessary security improvements to prevent further vulnerability exploitation.

To protect against Efail and similar MITM attacks, users must keep their email clients up to date. Additionally, adopting secure communication protocols like TLS and using end-to-end encrypted messaging platforms can add an extra layer of protection to email communications.

The Efail attack highlighted the importance of continuous security assessments and improvements in encryption standards and the need for users and organizations to stay vigilant and proactive in safeguarding their confidential email communications.

4.7 Exodus: 2019

In 2019, security officers of Lookout discovered a significant cyber-attack, on iOS and Android, the "Exodus" attack that can be used in MITM attacks. It involved sophisticated techniques for intercepting and manipulating encrypted communications between users and servers (Vijayan, 2019).

The attack got its name after the malicious mobile malware utilized to carry out the attack. It involved the installation of malicious software on the compromised devices, which allowed the attackers to gain control over the encrypted connections. Once installed, the malware could intercept and redirect encrypted traffic, decrypt it, and then re-encrypt it before forwarding it to its intended destination. The attackers got a chance to intercept and manipulate the encrypted data by compromising the security and privacy of the victims. The Android version had full root access to the device, whereas the iOS version could only extract a limited set of data accessible via iOS APIs. Exodus for Android could keep running even when the screen is switched off.

The attackers achieved that by exploiting vulnerabilities in the targeted systems or leveraging social engineering techniques to trick users into downloading and installing a seemingly legitimate application previously bundled with malicious software. Google removed those apps after the company was notified of the problem. Security Without Borders estimated that there were potentially one thousand or more infections. Lookout said that their telemetry showed the attacks focused purely on Italian IP addresses, and the risk for other users was negligible (Vijayan, 2019).

Exodus was particularly concerning because it targeted encrypted communications commonly considered secure. By compromising trust, the attackers undermined the effectiveness of encryption protocols and put sensitive data at risk.

To protect against Exodus, it is crucial to adhere to security best practices such as keeping software and devices up to date, being cautious when downloading applications or clicking on suspicious links, using strong encryption protocols, and regularly monitoring network traffic for any signs of malicious activity.

4.8 Adversary-in-the-Middle: 2023

Recently, cybersecurity experts at Microsoft Defender detected a sophisticated attack that targeted banks and financial services organizations. This attack involved two stages - an adversary-in-the-middle[3] (AITM) phishing attack and a subsequent business email compromise (BEC) activity. What is concerning about this incident is that it exploited trusted relationships and came from a compromised vendor (Microsoft, 2023).

The attackers used an indirect proxy, which is different from the usual reverse proxy techniques. That allowed them to have control over phishing pages and steal session cookies. They also employed session replay attacks and took advantage of weak multifactor authentication (MFA) policies to modify MFA methods without being challenged. Furthermore, they conducted a second-stage phishing campaign that targeted the contacts of the initial victim, sending out over 16,000 emails.

Dealing with this attack requires more than standard measures to address identity compromise. Organizations affected by this attack need to revoke session cookies, undo any MFA modifications made by the attackers, and actively hunt for similar threats. The attackers, in this case, were associated with the Storm-1167 threat actor, according to Microsoft's classifications (Microsoft, 2023).

Adversary-in-the-middle attacks aim at intercepting and compromising user authentication processes for malicious purposes. In this attack, the adversaries positioned themselves between users and the targeted service, obtaining credentials and intercepting MFA to obtain session cookies. With these stolen session cookies, they gained access to user resources, carried out business email compromises, and engaged in other malicious activities.

Unlike previous campaigns, this attack did not rely on the reverse proxy method commonly used by AITM kits. Instead, it used an indirect proxy approach, which involved the target application's login page on a cloud service impersonating. By controlling the phishing website, the attackers could modify content and avoid detection. There were no proxy HTTP packets used between the victim and the website during the AITM attack unlike traditional attacks (Microsoft, 2023).

When the victim entered their login information, a fake multi-factor authentication page was displayed. The attackers obtained the MFA token from the user and used it to access the session token, starting a session with the authentication provider. Then, the victim was redirected to another page.

This attack underscores the complexity of AITM attacks and emphasizes the need for comprehensive security defenses. Organizations must remain vigilant and implement robust security measures to mitigate the risks posed by these evolving threat techniques. Storm-1167

[3] An adversary-in-the-middle (AitM) attack is also known as a man-in-the-middle (MITM) attack. (Hypr, 2023) (Rowe, 2023)

attack technology is discussed in detail in the Microsoft Security Blog (Microsoft, 2023).

4.9 BLUFFS attack

Researchers from Eurecom have recently discussed a new set of attacks called 'BLUFFS' that have the potential to compromise the secrecy of Bluetooth sessions, paving the way for MITM attacks. These attacks target two newly found architectural flaws within the Bluetooth standard that specifically impact the derivation of session keys used for decrypting data during communication. These vulnerabilities are not limited to any hardware or software configuration, as they stem from fundamental design weaknesses in Bluetooth. Due to the widespread usage of Bluetooth as a wireless communication standard, BLUFFS attacks can affect laptops, smartphones, and other mobile devices (Toulas, 2023).

The primary objective of BLUFFS is to undermine the forward and future secrecy of Bluetooth sessions, thereby compromising the confidentiality of data exchanged between devices. That is accomplished through capitalizing on flaws in the session key derivation process. Through these vulnerabilities, an attacker can launch a brute-force attack and force the derivation of a short, weak, and predictable session key (SKC) to decrypt past communications and manipulate future ones. The attack takes place in several phases, see Fig. 3.

To successfully execute a BLUFFS attack, the perpetrator must be within Bluetooth range of the targeted victims and pose as one of the devices involved in the session. By impersonating one device, an attacker can negotiate with the other device to establish a weak session key by proposing the lowest possible key entropy value while using a constant session key diversifier.

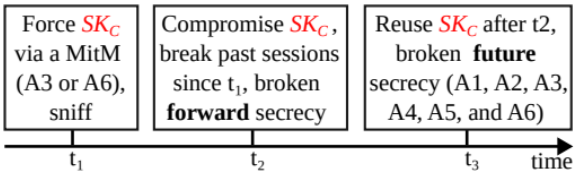


Fig. 3 Attack steps (Antonioli, 2023)

The BLUFFS attack can be of six different types, encompassing various combinations of impersonation and MITM techniques. These attacks are effective regardless of whether the targeted devices support Secure Connections (SC) or Legacy Secure Connections (LSC). BLUFFS impacts all versions of Bluetooth up to and including Bluetooth 5.4, released in February 2023, and Bluetooth 4.2, released in December 2014. The research conducted by Eurecom involved the efficacy of BLUFFS testing on different devices. All of them were susceptible to at least three of six BLUFFS attacks.

Bluetooth SIG, the organization responsible for licensing Bluetooth technology, advised implementing measures to mitigate the risks posed by the BLUFFS attacks. These measures include rejecting connections with low key strengths below seven octets, utilizing 'Security Mode 4 Level 4' to ensure strong encryption, and operating in “Secure Connections Only” mode while pairing (Toulas, 2023).

4.10 Mobile-in-the-middle

In sensitive information searches, fraudsters often use the proven MITM method of attack (Stockley, 2021). Due to the prevalence of mobile devices, MITM attacks often use so-called "evil twins" wireless networks. Compromised networks use the same name as legitimate ones. Therefore, they can easily trick victims and their devices that they belong to legitimate users.

MITM attacks are hard to detect because they are not in the victim's mobile device. During communication, the victim's mobile device and legitimate systems think they are communicating directly although the communication is over the attacker. One of the most significant MITM risks for smartphone users is communication over public wireless networks. Traced's research found that 5% of public networks were subject to an active MITM attack (Stockley, 2021). The attack can be by directly compromising a legitimate router, which allows the attacker to control the victim's connections to everything on the network. Router vulnerabilities allowed criminals to own hundreds of thousands of routers. MITM attacks that alter DNS traffic and lead victims to fake sites are just one of the possible burdens when attackers own the victim's gateway.

Not only Wi-Fi networks but also 5G networks are vulnerable to MITM attacks. At Black Hat 2019, security professionals demonstrated that it is possible to communicate with devices using a fake

base station. In doing so, it is possible to collect critical information about the device, including the type, operating system, version, and IMSI number[4]. Some MITM attacks do not require the presence of the mobile device owner. They can record the messages the device sends and play them back later. That was the case with Apple when it introduced the ability to buy transport tickets without unlocking the phone. Researchers at the University of Birmingham have found a way to reproduce a payment message, changing it so it can be sent to any wireless payment reader. That would allow an attacker to pay anything, in any amount, and at any time.

Working from home has become a permanent reality, so protecting against MITM attacks has become an obligation, not an option. If the company wants secure communication with its employees, the employees should use a reliable VPN for their mobile to connect to the company's VPN. That can prevent attackers from infiltrating the session. Another layer of defense is obtained with appropriate app installation, e.g., the Trustd mobile, which will check a potential victim's local WiFi connection for MITM activity and alert it. The business-focused Traced solution simultaneously informs the company's IT administrator, who should ensure secure communication. Although the protection against MITM is crucial, only 8% of companies in 2021 took technical measures to protect employees from risky Wi-Fi connections. According to a survey, over 20% of companies experienced a mobile device breach in 2020-2021. (Verizon, 2021 Mobile Security Index, 2021)

5 MANAGING MITM PROTECTION

In 2019, 11% of companies reported being affected by MITM attacks, according to the Fortinet State of Operational Security Report 2020 (Fortinet, 2020). As a protective measure against MITM attacks, 27% of websites were using HTTP Strict Transport Security (HSTS) as of December 11, 2023. (W3Techs, 2023) Additionally, according to Verizon (2023), 7% of users did not take any measures to protect their home Wi-Fi.

According to a survey by Enterprise Management Associates, close to 80% of internet TLS certificates are vulnerable to MITM attacks, with 25% of all certificates having already expired (Goldstein, 2023).

After the COVID-19 pandemic, many employees continue to work hybrid schedules and potentially use unsecured public Wi-Fi networks. They remain vulnerable to MITM attacks. There are ways one can try defending himself without knowing about MITM attacks in detail. A good idea is to check if the lock symbol exists in the address bar. When analyzing how to prevent MITM attacks, the best are often the most basic cybersecurity tools. They include (Poremba, 2022):

- Firewalls and VPNs.
- SSL and security certificates.
- Multi-factor authentication to control access.
- Employing hardline connections for sensitive devices to critical networks.
- Deploying endpoint security to protect IoT devices directly.

Institutions, companies, or cities can offer public Wi-Fi but separate it from the internal networks, which should use strong-wired equivalent privacy (WEP) and Wi-Fi-protected access (WAP). WEP/WAP encryption can help prevent attackers from attacking.

Every user should use the Internet by (Gregg, 2015), (Martens, 2023), (Microsoft, 2023):

- using security defaults to improve identity security. For additional control, users can define conditional risk-based access policies.
- continuous access evaluation implementation.
- installing antivirus software that can block MITM malware and monitor networks, browsers, firewalls, dark web, etc.
- encrypted connections use.
- avoiding free and unsafe Wi-Fi hotspots for sensitive transactions.
- avoiding HTTP websites, using only the encrypted version of websites, and installing a browser plugin like "HTTPS Everywhere."

[4] IMSI - International mobile subscriber identity, a unique number that identifies the device owner through its SIM card.

- using a home Wi-Fi router with WPA2 encryption and resetting the default password to a strong one.
- not visiting websites when the browser warns about a site's certificate problem.
- updating the operating system, applications, and antivirus on all used devices.
- using a dedicated laptop for online banking.
- setting up two-factor authentication on all accounts if possible.
- continuous monitoring accounts for any suspicious or anomalous activity (for example, location, ISP, user agent, and use of anonymizer services).

Almost half of all security breaches occur due to human behavior. Therefore, organizations need to consider the human aspect when educating their staff on preventing MITM attacks. Security awareness training that aims to prevent MITM attacks should cover the following topics (Poremba, 2022):

- Why should users avoid public and open
- Wi-Fi networks?
- Why the use of secure websites (HTTPS) is a necessity?
- How to spot fake websites?
- How to avoid phishing scams?

However, to prevent MITM attacks, education is not sufficient. The policy measures need to be implemented. The MSI[5] showed that (Poremba, 2022):

- around one-half (52%) of organizations do anything to enforce their policy measures.
- 8% of organizations do not use a VPN when using public Wi-Fi.
- nearly one-half (46%) of VPN clients are out of date or misconfigured.
- Less than one-third of organizations (32%) ban the use of public Wi-Fi.

When any identity compromise appears, the first measure is to reset the password. However, when the sign-in session is compromised in AITM attacks, only a password reset is not an efficient solution. Even if the victim's password is reset and sessions are revoked, the attacker can set up persistence methods to sign in a controlled manner by tampering with MFA. An attacker can add a new multi-factor authentication (MFA) policy to gain control over a victim's account. This can be achieved by signing in with a one-time password (OTP) sent to the attacker's mobile phone. Despite the victim's actions taken, the attacker will still have control over the account. Although AI-powered threat management systems attempt to avoid MFA, it remains crucial for ensuring identity security. MFA is highly effective in preventing most threats. MFA forces AITM attackers to develop session cookie theft techniques. Organizations need to work with their identity provider to ensure security controls like MFA. Microsoft customers can implement methods like using the Microsoft Authenticator, FIDO2 security keys, and certificate-based authentication (Microsoft, 2023).

6 CONCLUSION

The ways of using computers and networks are changing, the number of users is growing, but so is the number of malicious users who want something that does not naturally belong to them. In parallel with the development of new user software, programs for system protection and attacks on systems are also being developed. Each new software brings with it new risks. Both hackers and security experts are actively looking for potential vulnerabilities. The only question is who will be faster at a certain moment.

Based on the analysis, we saw that MITM attacks did not arise with the advent of computers and computer networks. They have existed since ancient times. Also, this analysis showed that they can cause extensive damage to users, service providers, and everyone who uses the Internet. Methods for performing MITM attacks change over time. Nowadays, more and more knowledge and often advanced technology is required. There are MITM attacks on individual users and large corporations.

Often, MITM attacks are combined with other types of attacks, so it is difficult to draw a line and classify an individual attack into a certain category. Many attacks included MITM attack elements.

[5] MSI – Verizon's 2022 Mobile Security Index

After analyzing various examples, we found that large MITM attacks still occur and have not yet been overcome. Therefore, we reject the null hypothesis and accept the alternative hypothesis that states "MITM attacks still exist and can cause harm to modern computer systems and their users".

WORKS CITED

Amato, F., & Kirschbaum, F. (2010). *evilgrade, "You still have pending upgrades!"*. Retrieved from Defcon: https://www.defcon.org/images/defcon-18/dc-18-presentations/Amato-Kirschabum/DEFCON-18-Amato-Kirschabum-Evilgrade.pdf

Antonioli, D. (2023). BLUFFS: Bluetooth Forward and Future Secrecy Attacks and Defenses. *Proceedings of the 2023 ACM SIGSAC Conference on Computer and Communications Security* (pp. 636-659). Copenhagen: ACM.

Arndt, J. (2023, May 09). *Man-in-the-Middle (MitM) attacks reaching inboxes increase 35% since 2022.* Retrieved from Cofense: https://cofense.com/blog/cofense-intelligence-strategic-analysis-2/?utm_source=bambu&utm_medium=social&utm_campaign=advocacy&blaid=4531672

Ashford, W. (2018, May 15). *No need to panic about Efail attacks*. Retrieved from ComputerWeekly: https://www.computerweekly.com/news/252441102/No-need-to-panic-about-Efail-attacks

Case No. 5:16-MD-02752-LHK, U. S. (2020, Mar 06). *Yahoo! Inc. Customer Data Security Breach Litigation Settlement. Case No. 5:16-MD-02752-LHK .* Retrieved from Yahoodatabreachsettlement: https://yahoodatabreachsettlement.com/

Cekerevac, Z., Dvorak, Z., Prigoda, L., & Cekerevac, P. (2017, 07 15). Internet of things and the man-in-the-middle attacks – Security and economic risks. (Z. Čekerevac, Ed.) *MEST Journal, 5*(2), 15-25. doi:10.12709/mest.05.05.02.03

CISA. (2016, Sep 30). *Lenovo Superfish Adware Vulnerable to HTTPS Spoofing.* Retrieved from Cybersecurity & Infrastructure Security Agency: https://www.cisa.gov/news-events/alerts/2015/02/20/lenovo-superfish-adware-vulnerable-https-spoofing

Ecuron. (2023). *Man In The Middle Attack (MITM) – A Primer*. Retrieved from Ecuron: https://www.ecuron.com/man-in-the-middle-attack-mitm-a-primer/

EFAIL. (2018, May 16). Retrieved from EFAIL: https://efail.de/

Evans, D. (2011, Apr). *The Internet of Things - How the Next Evolution of the Internet Is Changing Everything.* Retrieved from Cisco - White Paper: http://www.cisco.com/c/dam/en_us/about/ac79/docs/innov/IoT_IBSG_0411FINAL.pdf

Fortinet. (2020). *2020 State of Operational Technology and Cybersecurity Report.* Fortinet. Retrieved from https://www.arrow.com/ecs-media/10918/report-2020-ot-cybersecurity.pdf

Goldstein, P. (2023, Oct 13). *How To Detect and Prevent 'Man in the Middle' Attacks.* Retrieved from BizTech.

Goodin, D. (2015, Feb 19). *Lenovo PCs ship with man-in-the-middle adware that breaks HTTPS connections [Updated].* Retrieved from ars Technica: https://arstechnica.com/information-technology/2015/02/lenovo-pcs-ship-with-man-in-the-middle-adware-that-breaks-https-connections/

Gregg, M. (2015, 12 11). *Six ways you could become a victim of man-in-the-middle (MiTM) attacks this holiday season.* Retrieved from The Huffington Post: http://www.huffingtonpost.com/michael-gregg/six-ways-you-could-become_b_8545674.html

Gregg, M. (2015A). *How new technologies are reshaping MiTM attacks*. Retrieved from TechTarget: http://searchnetworking.techtarget.com/tip/How-new-technologies-are-reshaping-MiTM-attacks

Henriques, N. (2016, Dec 19). *1-Billion Yahoo Users' Database Reportedly Sold For $300,000 on Dark Web.* Retrieved from Linkedin: https://www.linkedin.com/pulse/1-billion-yahoo-users-database-reportedly-sold-300000-nuno-henriques

Hylender, C. D., Langlois, P., Pinto, A., & Widup, S. (2023). *2023 Data Breach Investigations Report.* Verizon. Retrieved from Verizon.

Hypr. (2023). *Adversary-in-the-Middle (AitM)*. Retrieved from HYPR: https://www.hypr.com/security-encyclopedia/adversary-in-the-middle

Irei, A., & Scarpati, J. (2022, Dec 06). *Wireless security: WEP, WPA, WPA2 and WPA3 differences.* Retrieved from TechTarget: https://www.techtarget.com/searchnetworking/feature/Wireless-encryption-basics-Understanding-WEP-WPA-and-WPA2

Jasek, S. (2016, Jul-Aug). GATTacking Bluetooth Smart Devices - Introducing a New BLE Proxy. *Black Hat USA 2016* (p. 49). Mandalay Bay, Las Vegas: Black hat. Retrieved from Black hat: https://www.blackhat.com/docs/us-16/materials/us-16-Jasek-GATTacking-Bluetooth-Smart-Devices-Introducing-a-New-BLE-Proxy-Tool.pdf

Khandelwal, S. (2016, Dec 15). *Yahoo Admits 1 Billion Accounts Compromised in Newly Discovered Data Breach.* Retrieved from The Hacker News: https://thehackernews.com/2016/12/yahoo-data-breach-billion.html

Kiprin, B. (2021, Apr 02). *What Is the Heartbleed Bug and How to Prevent It.* Retrieved from VeraCode: https://crashtest-security.com/prevent-heartbleed/

Martens, B. (2023, Jun 07). *What Is a Man-in-the-Middle Attack? [Full Guide 2023]*. Retrieved from Safety Detectives: https://www.safetydetectives.com/blog/avoiding-the-man-in-the-middle-preventing-a-common-cyberattack/

Microsoft. (2023, Jun 08). *Detecting and mitigating a multi-stage AiTM phishing and BEC campaign*. Retrieved from Microsoft: https://www.microsoft.com/en-us/security/blog/2023/06/08/detecting-and-mitigating-a-multi-stage-aitm-phishing-and-bec-campaign/

Ornaghi, A., & Valleri, M. (2015, Mar 14). *Ettercap project*. Retrieved from Ettercap: https://ettercap.github.io/ettercap/index.html

Perlroth, N. (2017, Oct 03). All 3 Billion Yahoo Accounts Were Affected by 2013 Attack. *The New York Times*. Retrieved from https://www.nytimes.com/2017/10/03/technology/yahoo-hack-3-billion-users.html

Poddebniak, D., Dresen, C., Mueller, J., Ising, F., Schinzel, S., Friedberger, S., . . . Schwenk, J. (2018). Efail: Breaking S/MIME and OpenPGP Email Encryption using Exfiltration Channels. *27th USENIX Security Symposium* (pp. 549-566). Baltimore: USENIX.

Poremba, S. (2022, Sep 08). *How to prevent man-in-the-middle attacks in healthcare.* Retrieved from Verizon: https://www.verizon.com/business/resources/articles/s/how-to-prevent-man-in-the-middle-attacks-in-healthcare/

Proofpoint. (2016, Dec 13). *Home Routers Under Attack via DNSChanger Malware on Windows, Android Devices.* Retrieved from Proofpoint: https://www.proofpoint.com/us/blog/threat-insight/home-routers-under-attack-dnschanger-malware-windows-android-devices#

Rocha, E. (2018, Oct 1). *GhostDNS: New DNS Changer Botnet Hijacked Over 100,000 Routers.* Retrieved from GlobalDots: https://www.globaldots.com/resources/blog/ghostdns-new-dns-changer-botnet-hijacked-over-100000-routers/

Rowe, B. (2023, Sep 14). *The Latest Phishing Trends and Predictions*. Retrieved from Securus Communications: https://securuscomms.co.uk/the-latest-phishing-trends-and-predictions/

Senouci, F. z. (2023, Jul 23). *Yahoo Data Breach: An In-Depth Analysis of One of the Most Significant Data Breaches in History.* Retrieved from Medium: https://shellmates.medium.com/yahoo-data-breach-an-in-depth-analysis-of-one-of-the-most-significant-data-breaches-in-history-ba5b46be560b

Song, D. (2001). *Dsniff.* Retrieved from monkey.org: https://www.monkey.org/~dugsong/dsniff/

Spring, T. (2016, Aug 11). *Bluetooth Hack Leaves Many Smart Locks, IoT Devices Vulnerable*. Retrieved from threatpost: https://threatpost.com/bluetooth-hack-leaves-many-smart-locks-iot-devices-vulnerable/119825/

Stockley, L. (2021, Nov 22). *MitM Attacks: How to Avoid the Mobile Piggy in the Middle.* Retrieved from Traced: https://traced.app/2021/11/22/mitm-attacks-how-to-avoid-the-mobile-piggy-in-the-middle/

Sullivan, N. (2021, Mar 27). *Heartbleed Revisited.* Retrieved from Cloudflare: https://blog.cloudflare.com/heartbleed-revisited/

Toulas, B. (2023, Nov 28). *New BLUFFS attack lets attackers hijack Bluetooth connections.* Retrieved from BleepingComputer: https://www.bleepingcomputer.com/news/security/new-bluffs-attack-lets-attackers-hijack-bluetooth-connections/

Tran, S. (2017, Feb 21). *Verizon and Yahoo amend terms of definitive agreement.* Retrieved from Verizon News Center: https://www.verizon.com/about/news/verizon-and-yahoo-amend-terms-definitive-agreement

Vailshery, L. S. (2023, Jul 27). *Number of Internet of Things (IoT) connected devices worldwide from 2019 to 2023, with forecasts from 2022 to 2030*. Retrieved from Statista: https://www.statista.com/statistics/1183457/iot-connected-devices-worldwide/

Vanhoef, M., & Piessens, F. (2017). *Key Reinstallation Attacks: Breaking WPA2 by forcing nonce reuse.* Retrieved from Krackattacks: https://www.krackattacks.com/

Vanhoef, M., & Ronen, E. (2019, Apr). Dragonblood: Analyzing the Dragonfly Handshake of WPA3 and EAP-pwd. *IEEE Symposium on Security and Privacy.* Oakland (San Francisco): IEEE. Retrieved from https://wpa3.mathyvanhoef.com/

Venter, S. (2023, Mar 22). *Why your servers can still suffer from (a) Heartbleed – and what to do.* Retrieved from TuxCare: https://tuxcare.com/blog/why-your-servers-can-still-suffer-from-a-heartbleed-and-what-to-do/

Verizon. (2021). *2021 Mobile Security Index.* Verizon. Retrieved from Verizon: https://www.verizon.com/business/resources/reports/mobile-security-index.html

Verizon. (2023). *2023 Mobile Security Index white paper.* Verizon. Retrieved from https://www.verizon.com/business/resources/reports/mobile-security-index-report.pdf

Vijayan, J. (2019, Apr 08). *'Exodus' iOS Surveillance Software Masqueraded as Legit Apps*. Retrieved from DarkReading: https://www.darkreading.com/cyberattacks-data-breaches/-exodus-ios-surveillance-software-masqueraded-as-legit-apps

W3Techs. (2023, Dec 11). *Usage statistics of HTTP Strict Transport Security for websites.* Retrieved from W3Techs Web Technology Surveys: https://w3techs.com/technologies/details/ce-hsts

Zadig, S. (2012-2013, Fall/Winter). Botnet Investigations: An Inspector General Perspective. *The Journal of Public Inquiry*, 38-42.

Received for publication: 21.01.2024
Revision received: 08.02.2024
Accepted for publication: 08.01.2025.

How to cite this article?

Style – **APA** *Sixth Edition:*

Cekerevac, Z., Cekerevac, P., Prigoda, L., & Naima, F. A. (2025, 01 15). Security Risks from the Modern Man-In-The-Middle Attacks. (Z. Cekerevac, Ed.) *MEST Journal, 13*(1), 34-51. doi:10.12709/mest.13.13.01.04

Style – **Chicago** *Sixteenth Edition:*

Cekerevac, Zoran, Petar Cekerevac, Lyudmila Prigoda, and Fawzi Al Naima. "Security Risks from the Modern Man-In-The-Middle Attacks." Edited by Zoran Cekerevac. *MEST Journal* (MESTE) 13, no. 1 (01 2025): 34-51.

Style – **GOST** *Name Sort:*

Cekerevac Zoran [et al.] Security Risks from the Modern Man-In-The-Middle Attacks [Journal] // MEST Journal / ed. Cekerevac Zoran. - Belgrade – Toronto : MESTE, 01 15, 2025. - 1 : Vol. 13. - pp. 34-51.

Style – **Harvard** *Anglia:*

Cekerevac, Z., Cekerevac, P., Prigoda, L. & Naima, F. A., 2025. Security Risks from the Modern Man-In-The-Middle Attacks. *MEST Journal,* 15 01, 13(1), pp. 34-51.

Style – **ISO 690** *Numerical Reference:*

Security Risks from the Modern Man-In-The-Middle Attacks. **Cekerevac, Zoran, et al.** [ed.] Zoran Cekerevac. 1, Belgrade – Toronto : MESTE, 01 15, 2025, MEST Journal, Vol. 13, pp. 34-51.

MEST Journal
DOI 10.12709/mest.13.13.01.05

CRYPTOGRAPHIC FOUNDATIONS FOR BLOCKCHAIN SECURITY IN DECENTRALIZED NETWORKS

Milan Feltovic
University of Žilina, Faculty of Security Engineering, Žilina, Slovakia
https://orcid.org/0009-0004-3057-2912

JEL Category: **C88**

Abstract

In the rapidly evolving digital technology landscape, blockchain emerges as a pivotal innovation with the potential to revolutionize industries far beyond its original application in cryptocurrencies like Bitcoin. This article explores the critical role of cryptography in decentralized information networks, emphasizing its importance in ensuring the integrity, confidentiality, and authenticity of digital transactions. It examines the mathematical foundations underlying cryptographic techniques, including elliptic curve cryptography and hash functions, and discusses their application in consensus protocols such as Proof-of-Work. Furthermore, the paper addresses the challenges and potential vulnerabilities posed by quantum computing to current cryptographic standards. By providing a comprehensive overview of both theoretical and practical aspects of cryptography in blockchain technology, this study aims to enlighten readers on the robust security measures essential for maintaining trust and security in decentralized systems. Moreover, the discussion extends to the implications of cryptographic advancements for various sectors such as healthcare, finance, and public administration, highlighting how blockchain enhances transparency and security in these fields. This article underscores the urgency of advancing cryptographic research to address emerging threats and ensure the resilience of blockchain systems against future technological developments. The findings emphasize the need for ongoing innovation in cryptographic methods to safeguard the integrity of decentralized networks in an era of increasing digital interconnectivity.

Keywords: *blockchain, cryptography, elliptic curve, hash functions, transaction integrity, Proof-of-Work, quantum computing, public key, digital signatures, encryption protocols.*

1 INTRODUCTION

In today's era of digital advancement and innovation, blockchain technology is transforming various industrial sectors and significantly altering the paradigm of information storage and sharing. Initially developed as the foundation for digital currencies like Bitcoin, its potential has expanded

Address of the author:
Milan Feltovic
milan@feltovic.com

far beyond, reaching areas such as healthcare, finance, and public administration, where it contributes to increased transparency and security. In healthcare, blockchain enables secure storage and sharing of medical records among various healthcare providers, improving care coordination and patient privacy protection (Nakamoto, 2009). In finance, blockchain provides efficient and transparent solutions for international payments, reducing transaction costs and eliminating the need for intermediaries (Buterin, 2014). In public administration, blockchain technology increases the transparency and trustworthiness of public records and elections, thereby enhancing public trust in these systems (Gallian, 2021).

One of the key aspects of blockchain is cryptography, which underpins the security and trust in these decentralized systems. Cryptography in blockchains ensures that transactions are not only secure but also immutable, which is critically important for maintaining integrity and trust in digital systems. Given the growing cybersecurity threats, the need for advanced cryptographic solutions has become even more pressing (Sipser, 2021). The development of robust cryptographic methods has been significantly influenced by the understanding of cryptographic codes, as described by Secret Bits, which outlines the evolution of unbreakable codes and their implications (Abelson, Ledeen, & Lewis, 2008).

This article aims to provide insight into how cryptography supports the security and functionality of decentralized information networks, with a particular emphasis on blockchain technology. I analyze the mathematical foundations on which cryptography is built and examine its various applications, from basic hashing functions to advanced elliptic curve algorithms. Additionally, I address the challenges posed by quantum computing to current cryptographic standards and discuss future research directions in the field of post-quantum cryptography.

2 METHODS

In this section, I provide a detailed description of the cryptographic techniques used in blockchain technology. Elliptic Curve Cryptography (ECC) and hashing functions (SHA-256) are crucial for ensuring the integrity and authenticity of transactions. I also focus on consensus protocols, such as Proof-of-Work, and their role in maintaining the consistency of the blockchain network. Additionally, I analyze the impact of quantum computing on current cryptographic standards and discuss post-quantum cryptographic solutions.

Blockchain technology, originally developed as an architecture for the cryptocurrency Bitcoin, has rapidly garnered interest not only in technological circles but also across a broad spectrum of industrial applications (Nakamoto, 2009). Today, blockchain is used in various sectors, including finance, healthcare, and logistics, providing a decentralized solution that enhances transparency and reduces the need for third-party verification of transactions.

A key factor enabling the secure and efficient operation of blockchain is cryptography. Gallian (2021) explains how mathematical principles, particularly number theory and abstract algebra, provide the foundation for cryptographic algorithms used in blockchain technologies (Gallian, 2021). For instance, elliptic curve cryptography (ECC), as described by Koblitz, Menezes, and Vanstone, is widely recognized for its ability to offer strong encryption with relatively small key sizes, which reduces computational requirements and improves system performance (Koblitz, Menezes, & Vanstone, 2000). Understanding the underlying principles of trapdoor functions is also crucial, as they form the basis for many cryptographic algorithms (Wikipedia, Trapdoor function, 2013).

In the area of consensus protocols, such as Proof-of-Work, detailed by Nakamoto and Buterin, hash functions like SHA-256 are used to ensure the integrity of the blockchain. These methods help protect the network from unauthorized changes and ensure that all copies of the distributed ledger remain consistent and unaltered (Buterin, 2014).

Recently, concerns have emerged regarding potential threats from quantum computing, which could disrupt current cryptographic standards. Shor's research shows that quantum algorithms could efficiently solve problems like factorization and discrete logarithms, which underpin many

existing encryption systems. This paradigm shift necessitates new approaches to security in the era of quantum technologies, as indicated by the latest studies in post-quantum cryptography (Shor, 1999).

This literature review underscores the importance of ongoing research and development in cryptography to ensure the security of decentralized networks. As blockchain technology grows and evolves, it will be crucial to ensure that cryptographic methods stay ahead of potential threats to maintain the trust and integrity of these systems (Briggs, 1998).

3 MATHEMATICS AND THEORY OF CRYPTOGRAPHIC TECHNIQUES

At the core of cryptographic techniques used in blockchain technology are mathematical and theoretical principles that provide security and trust in digital systems. These principles include number theory, abstract algebra, complexity theory, and algorithms based on these principles.

3.1 Number Theory

Number theory is a fundamental aspect of cryptography and involves the study of the properties of numbers, particularly integers. In cryptography, number theory is utilized in:

- **Factorization of Numbers**: Crucial in RSA cryptography, where security relies on the difficulty of factoring large composite numbers into prime numbers.
- **Exponential and Modular Arithmetic**: These operations form the basis for algorithms such as RSA (modular exponentiation) and algorithms based on discrete logarithms used in ECC (Koblitz, Menezes, & Vanstone, 2000).

The RSA algorithm, based on the difficulty of factoring large numbers, is widely used to secure communications and digital signatures. On the other hand, elliptic curve cryptography (ECC) leverages the complexity of the elliptic curve discrete logarithm problem and offers higher security with smaller key sizes, making it ideal for devices with limited computational power (Anon., The cryptographic hash function SHA-256, 2023).

3.2 Abstract Algebra: Groups

Abstract algebra deals with structures such as groups, rings, and fields, which are essential for understanding cryptographic algorithms.

A group is mathematically defined as a pair (G, +), where G is a finite set of elements and "+" is a binary operation. A group must have the following properties:

- **Closure under +**: $\forall x, y \in G, x + y \in G$
- **Associativity**: $\forall x, y, z \in G, (x + y) + z = x + (y + z)$
- **Identity element e ∈ G**: $\forall x \in G, e + x = x$
- Inverse elements: $\forall x \in G, -x \in G$ and $x + (-x) = e$

An Abelian group (commutative group) additionally has the property of commutativity:

- **Commutativity**: $\forall x, y \in G, x + y = y + x$

Non-zero integers modulo p $(Z/pZ-\{0\}=Zp^*)$, where p is a prime number, form a multiplicative group, which is very useful in cryptography, such as in the Diffie-Hellman key exchange and elliptic curve cryptography (ECC) (Koblitz, Menezes, & Vanstone, 2000).

3.3 Complexity Theory

Complexity theory analyzes the time and space requirements of algorithms. Understanding Big-O notation is crucial for analyzing the efficiency of these algorithms (Macedo, 2018).

- **P vs NP Problem**: The security of many cryptographic systems assumes that certain problems are "hard," meaning that there is no quick (polynomial-time) algorithm to solve them. The security of RSA relies on the assumption that factorization is hard (Aamir, 2019).
- **Quantum Computing**: Quantum computers can efficiently solve problems like integer factorization and discrete logarithms, which would jeopardize algorithms like RSA and ECC, motivating research in the field of post-quantum cryptography (Shor, 1999).

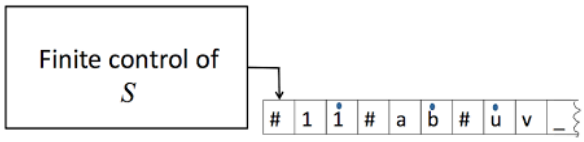


Fig. 1: Illustrated Turing Machine
Source: (Anon., 2011)

The image illustrates the concept of a Turing machine, a fundamental element in computational complexity theory. A Turing machine is a model of computation that consists of an infinite tape and a read-write head that can change states based on predefined rules. This model is crucial for understanding how computational problems are solved and the limits of computational capacity.

3.4 Cryptographic Protocols and Algorithms

Hash Functions: Hash functions, such as SHA-256 used in Bitcoin, transform input data into a fixed-length output and are designed to be fast and collision-resistant (i.e., to ensure that two different inputs do not produce the same output) (Anon., The cryptographic hash function SHA-256, 2023).

Hash functions can be categorized into cryptographic and non-cryptographic. Non-cryptographic hash functions are used, for example, in hash tables or for error detection (CRC), and do not protect against intentional collisions. Cryptographic hash functions, like SHA-256, are used in blockchain consensus protocols (e.g., Proof-of-Work), digital signatures, and encryption algorithms. For a cryptographic hash function to be considered secure, it must meet the following criteria:

- **Pre-image resistance**: Given a hash value h(m), it should be computationally infeasible to determine the original input m that maps to h(m).
- **Second pre-image resistance**: Given an input m1 and its hash value h(m1), it should be computationally infeasible to find a different input m2 such that h(m2) = h(m1).
- **Collision resistance**: It should be computationally infeasible to find two distinct inputs m1 and m2 such that h(m1) = h(m2).

A hash function cannot be inverted, even assuming an attacker with unlimited computational power. For example, there are $\mathbf{2^{256}}$ possible values for a 256-bit hash. Even if an attacker managed to find all possible pre-images for a specific hash (which would require, on average, $\mathbf{2^{256}}$ attempts), there are $\mathbf{2^{2048}}$ possible combinations of bits for a 2048-bit pre-image. According to the pigeonhole principle, if there are n pigeons and m pigeonholes, and n > m, then at least one pigeonhole must contain more than one pigeon. Therefore, for $\mathbf{2^{2048}}$ possible pre-images and $\mathbf{2^{256}}$ possible hash values, each hash value will, on average, correspond to $\mathbf{2^{1792}}$ different 2048-bit pre-images. Since all pre-images have the same probability, a specific pre-image m can never be uniquely determined (Anon., The cryptographic hash function SHA-256, 2023).

Digital Signatures: Digital signatures, such as ECDSA used in blockchain, provide a way to verify the identity of the sender and the integrity of the message. ECDSA uses elliptic curve cryptography (ECC), known for its high security and efficiency. Elliptic curves are mathematically represented by equations such as $\mathbf{y^2 = x^3 + Ax + B}$, allowing for secure and rapid key exchange. ECC is computationally more efficient than traditional methods, such as RSA, in achieving the same level of security. In the ECDSA system, a private key is used to create a signature, which can be verified by a public key. This process ensures that the message has not been altered and is authentic. Digital signatures are crucial for securing transactions in decentralized networks like blockchain (Sipser, 2021).

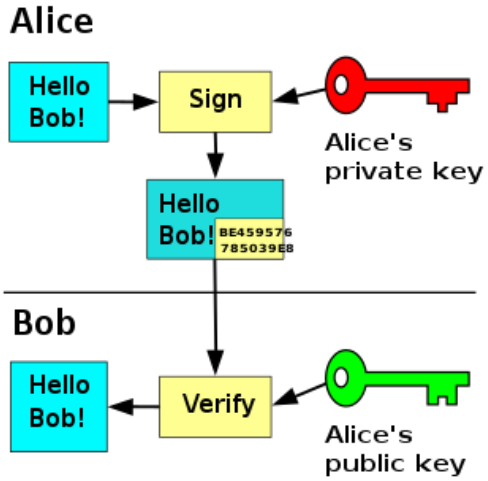


Fig. 2: Public Key Digital Signature
Author: (Wikipedia, 2024)

The illustration demonstrates the process of a digital signature using a public key. In public key cryptography, a pair of keys - a private key and a public key - is used to ensure the confidentiality and authenticity of messages. The private key is used to create a digital signature, which can be verified using the associated public key, thereby confirming the sender's identity and the integrity of the message.

3.5 Application in Blockchain Technology: Elliptic Curve Cryptography (ECC)

ECC leverages the properties of elliptic curves over finite fields. The security of ECC lies in the elliptic curve discrete logarithm problem (ECDLP), which exploits the commutative properties of the additive group of points on the curve.

Elliptic curves are mathematically described by the equation $\mathbf{y^2 = x^3 + Ax + B}$ (Anon., The cryptographic hash function SHA-256, 2023).

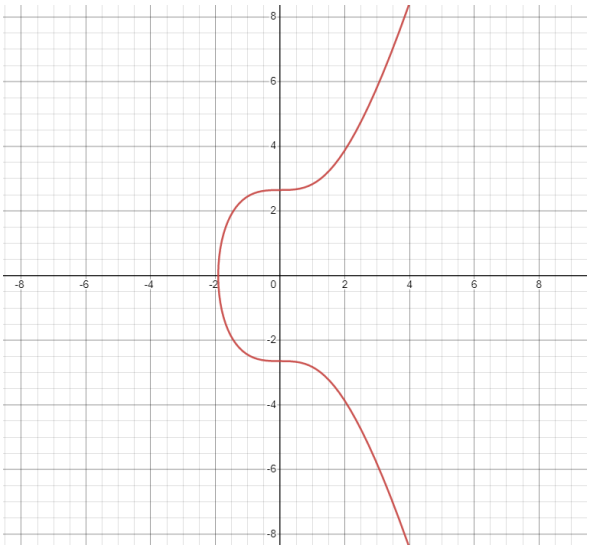


Fig. 3: Continuous graph of the elliptic curve $y^2 = x^3 + 7$ *, so that* $x,y \subseteq Rx, y$
Source: Author

The image shown in Fig. 3 depicts the graph of an elliptic curve, mathematically described by the equation

$$y^2 = x^3 + Ax + B \qquad \text{(Anon., 2019).}$$

This graph is important for understanding elliptic curves, which are used in elliptic curve cryptography (ECC). This type of cryptography is both efficient and secure, making it ideal for use in blockchain technologies.

- **Point Addition**: Adding two points, P and Q, on an elliptic curve can be visualized by drawing a line through these points. If this line intersects the elliptic curve at another point, the point directly below this intersection represents the sum P + Q.

The illustration shown in Fig. 4 depicts the process of adding two points, P and Q, on an elliptic curve. This operation is fundamental in elliptic curve cryptography (ECC), where point addition is used for encryption and decryption of information. Adding points on an elliptic curve is visualized by drawing a line through the two points, with the resulting point below the intersection representing the sum P + Q.

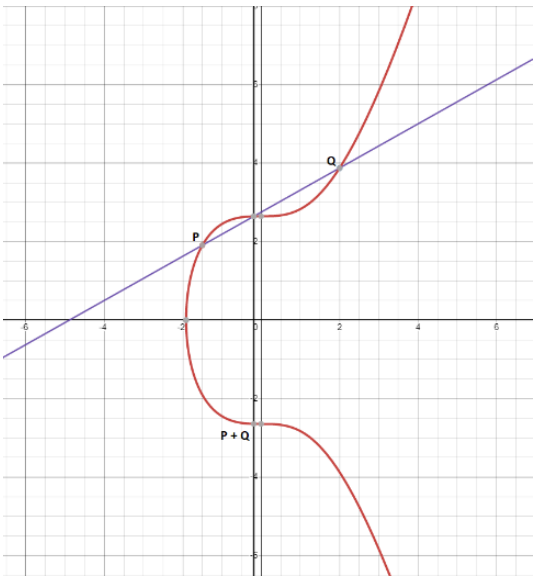


Fig. 4: Addition of Points P + Q on an Elliptic Curve
Source: Author

- **Inverse Points**: Adding a point and its inverse results in a virtual point O, known as the "point at infinity." This is represented as:

$$P + (-P) = O.$$

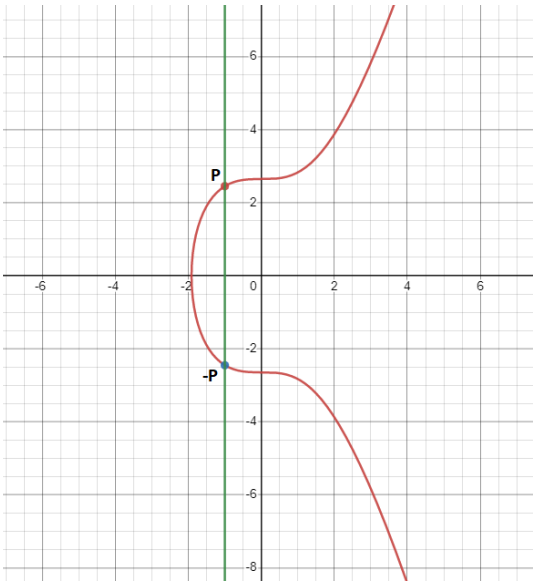


Fig. 5: Addition of Inverse Points on an Elliptic Curve: P + (-P) = O
Source: Author

Figure 5 illustrates the addition of point P and its inverse point -P on an elliptic curve, resulting in the virtual point O, known as the "point at infinity." The line connecting point P and its inverse -P does not intersect the elliptic curve but extends to infinity, representing the equation P + (-P) = O.

- **Point Doubling**: Doubling a point, P + P = 2P, is crucial for point multiplication, which is key to cryptographic applications of elliptic curves (Koblitz, Menezes, & Vanstone, 2000).

The illustration in Fig. 6 depicts the process of doubling a point P on an elliptic curve, which is a crucial operation in elliptic curve cryptography (ECC). This process involves finding the tangent at point P, determining the intersection of this tangent with the curve, and then reflecting the intersection point over the x-axis to get the resulting point 2P.

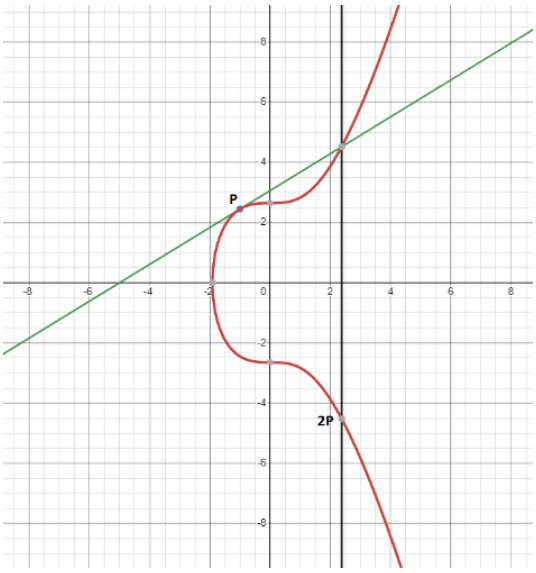


Fig. 6: Doubling a Point: P+P=2P
Source: Author

ECC employs the elliptic curve discrete logarithm problem (ECDLP), a variation of the discrete logarithm problem (DLP). In the ECDSA digital signature, the private key k is used to create a signature, while point Q serves as the public key (Koblitz, Menezes, & Vanstone, 2000).

3.6 Cryptography in Blockchain

In the blockchain context, cryptographic algorithms primarily focus on integrity and authenticity rather than privacy protection. The blockchains mainly use digital signatures to verify identity and secure messages. One of the most popular algorithms is the Elliptic Curve Digital Signature Algorithm (ECDSA), which is based on Elliptic Curve Cryptography (ECC) (Koblitz, Menezes, & Vanstone, 2000).

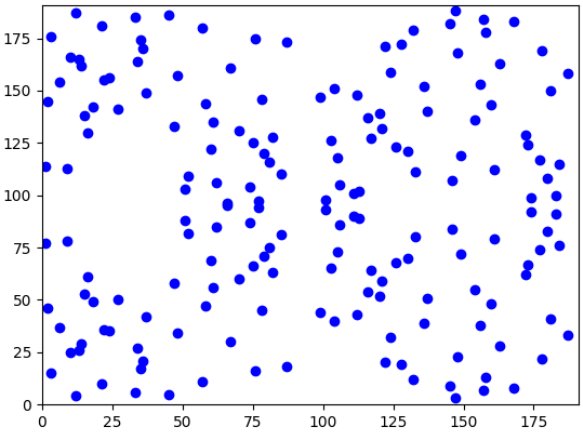


Fig. 7: (x,y) where $x,y \subseteq Z_{191}$ a $y^2=x^3+7$
Source: Author

The illustration shows a discrete graph of the elliptic curve $y^2 = x^3 + 7$ over the finite field Z_{191}, where x and y are integers within this range. This graph illustrates the use of the elliptic curve discrete logarithm problem (ECDLP) in elliptic curve cryptography (ECC), which underpins the ECDSA digital signature algorithm.

ECDSA is widely recognized for its security and efficiency, making it ideal for use in blockchain technologies. The advantage of ECDSA over RSA is that it requires a smaller key size to achieve the same level of security. For example, a 512-bit ECDSA key is computationally more efficient than a 4096-bit RSA key, leading to its increasing use in modern cryptography. These mathematical and theoretical concepts provide a key framework for understanding and developing secure cryptographic solutions. They are essential for the design and analysis of secure digital systems. ECDSA ensures that transactions in the blockchain network are authentic and immutable. These features make blockchain technology robust and reliable for decentralized applications (Koblitz, Menezes, & Vanstone, 2000).

3.7 Quantum Computing

Quantum computing has the potential to significantly weaken current cryptographic standards, such as RSA and ECC, which secure most blockchain technologies. Traditionally, it is

assumed that computational models for breaking ciphers are comparable to deterministic universal Turing machines or random access models (RAM). However, quantum computers introduce a new dimension to this field. Algorithms like Shor's algorithm leverage quantum computational models to enable polynomial-time computation of problems considered difficult in classical cryptography, such as integer factorization or the discrete logarithm problem (DLP). Shor's algorithm can efficiently factor large numbers and solve DLP, threatening the security of many cryptosystems that rely on these problems, such as RSA and ECC (Shor, 1999).

Quantum computers, although still in the development stage, have already achieved significant breakthroughs. For instance, companies like Google and IBM have developed quantum processors capable of performing complex computations that are beyond the reach of classical computers. This progress underscores the urgency of research in post-quantum cryptography, which includes algorithms resistant to quantum attacks, such as lattice-based cryptography and multivariate polynomial cryptography (Shor, 1999).

As a result, the security of blockchain transactions and digital signatures could be compromised. Quantum computing has the potential to dramatically increase efficiency in solving these problems, meaning that current cryptographic techniques could become ineffective in the future. Therefore, new cryptographic methods resistant to quantum attacks, known as post-quantum cryptography, are being developed. These methods include algorithms based on problems that are difficult for quantum computers, such as lattice-based cryptography or multivariate polynomial cryptography (Briggs, 1998).

While quantum computers are still not widely available and are in the research and development stage, blockchain and cryptographic system developers need to be prepared for this future technological leap. Implementing and testing post-quantum algorithms is essential to ensure the long-term security of blockchain technologies and cryptographic systems. This transition to new cryptographic standards will be crucial for maintaining security and trust in decentralized systems in the era of quantum computing. For developers and organizations, it is crucial to begin implementing and testing post-quantum cryptographic algorithms today to be prepared for future threats. Investment in the research and development of these technologies is essential for the long-term security and trustworthiness of blockchain systems (Briggs, 1998).

4 RESULTS

The results of my research demonstrate the effectiveness and security of cryptographic techniques used in blockchain technology. Here are the key findings:

4.1 Effectiveness of Elliptic Curve Cryptography (ECC)

Elliptic Curve Cryptography (ECC) is a vital component in blockchain security. ECC provides strong encryption with relatively small key sizes compared to traditional cryptographic methods like RSA. This efficiency makes ECC particularly suitable for blockchain applications, which require high security without compromising performance. ECC can achieve comparable security levels with significantly smaller keys, leading to faster computations and reduced storage requirements. The use of ECC in blockchain enhances transaction processing speed and reduces the computational load on network nodes.

4.2 Robustness of Hash Functions (SHA-256)

Hash functions, specifically SHA-256, play a crucial role in ensuring the integrity of blockchain transactions. SHA-256 is highly resilient to collision attacks, meaning it is extremely difficult for two different inputs to produce the same hash output. The probability of finding a collision in SHA-256 is negligible, reinforcing the trust in the blockchain's immutability. SHA-256 is computationally efficient, enabling quick verification of transaction data and blocks within the blockchain.

4.3 Role of Consensus Protocols (Proof-of-Work)

Consensus protocols, such as Proof-of-Work (PoW), are essential for maintaining the

consistency and security of blockchain networks. PoW is effective in preventing double-spending and ensuring that all nodes agree on the blockchain's current state. The computational effort required for PoW (e.g., solving cryptographic puzzles) acts as a deterrent against malicious attacks, making the network more secure. However, PoW is resource-intensive, leading to high energy consumption. This highlights the need for more sustainable alternatives or optimizations.

4.4 Impact of Quantum Computing

Quantum computing poses a potential threat to current cryptographic standards, including those used in blockchain technology. The study examines the vulnerabilities introduced by quantum algorithms, such as Shor's algorithm, which can efficiently solve problems that are difficult for classical computers (e.g., factoring large integers and calculating discrete logarithms). If quantum computers become practical, they could break the cryptographic algorithms (RSA, ECC) that underlie blockchain security. This necessitates the development and adoption of post-quantum cryptographic algorithms that are resistant to quantum attacks.

4.5 Post-Quantum Cryptography Solutions

In response to the threat of quantum computing, the study explores post-quantum cryptographic solutions that can be integrated into blockchain technology. These solutions are designed to be secure against quantum attacks. Key findings include lattice-based cryptography and multivariate polynomial cryptography, which are promising candidates for post-quantum security. Implementing these post-quantum solutions in blockchain will require careful consideration of computational efficiency and integration with existing blockchain protocols.

4.6 Conclusions of the Results

The research confirms that current cryptographic techniques are effective in securing blockchain technology. However, the threat of quantum computing necessitates a proactive approach to adopting post-quantum cryptographic solutions. Continuous research and development are crucial to maintaining the security and efficiency of blockchain networks in the face of evolving technological challenges.

5 CONCLUSIONS

In the rapidly evolving landscape of decentralized information networks, particularly within blockchain technology, cryptography plays a crucial role. As the backbone of cryptographic security, it ensures the confidentiality, integrity, and authentication of data within these networks.

Today, decentralized networks often employ sophisticated encryption methods such as RSA, ECC (Elliptic Curve Cryptography), and AES (Advanced Encryption Standard) to secure data transmission. Public key cryptography is widely used in blockchain to secure transactions and create digital signatures, ensuring that only authorized parties can process the data.

Blockchain networks, whether private or public, are increasingly adopting these advanced encryption methods. Private networks focus on internal security and data privacy, while public networks emphasize transparency and broad accessibility.

As networks expand, maintaining the efficiency of cryptographic operations becomes challenging, especially in large-scale public sector applications. The advent of quantum computing poses a significant threat to current cryptographic standards, as quantum algorithms could potentially break many of the encryption methods in use today.

Ensuring interoperability between private and public blockchain networks while maintaining robust cryptographic standards is a significant challenge. Different networks may use various encryption methods, complicating secure communication between platforms. Adhering to diverse data protection laws and regulations, particularly in public sector applications, requires a delicate balance while maintaining stringent encryption standards.

Effective management of cryptographic keys is essential, as their loss or theft can lead to severe security breaches, particularly in private

blockchain networks where access control is critical.

With the growing influence of decentralized networks in both the private and public sectors, the role of encryption in ensuring their security and trust is indispensable. While the current state reflects strong foundations in cryptography, the industry must proactively address challenges related to scalability, quantum threats, interoperability, regulatory compliance, and key management to maintain robust, secure, and efficient networks. The future of these networks depends on their ability to adapt and evolve in response to these emerging challenges.

My study emphasizes the importance of advanced cryptographic techniques for ensuring the confidentiality, integrity, and authenticity of data. Quantum computing poses a potential threat, making it crucial to continue research in post-quantum cryptography. The future of blockchain technology depends on the ability to adapt to these new challenges and maintain a high level of security.

WORKS CITED

Aamir, B. (2019). *P Vs NP Problem In A Nutshell.* Retrieved from https://medium.com/@bilalaamir/p-vs-np-problem-in-a-nutshell-dbf08133bec5

Abelson, H., Ledeen, K., & Lewis, H. (2008, Jun 3). *Secret Bits: How Codes Became Unbreakable*. Retrieved from informIT: https://www.informit.com/articles/article.aspx?p=1218422

Anon. (2019, Apr 24). *Secp256k1*. Retrieved from Bitcoin.it: https://en.bitcoin.it/wiki/Secp256k1

Anon. (2023). *The cryptographic hash function SHA-256*. Retrieved from https://helix.stormhub.org/papers/SHA-256.pdf

Anon. (n.d.). *TURING MACHINES*. Retrieved from andrew.cmu.edu: https://www.andrew.cmu.edu/user/ko/pdfs/lecture-13.pdf

Briggs, M. E. (1998, Apr 17). *An Introduction to the General Number Field Sieve.* Retrieved from Virginia Tech.: https://vtechworks.lib.vt.edu/items/3b866f8e-d533-48ae-a671-b88e4cb0a7bc

Buterin, V. (2014). *Ethereum Whitepaper.* Retrieved from https://ethereum.org/en/whitepaper/

Contributors. (2013, Jul). *Trapdoor function*. Retrieved from Wikipedia: https://en.wikipedia.org/wiki/Trapdoor_function

Contributors. (2024, Jan). *Public-key cryptography*. Retrieved from Wikipedia: https://en.wikipedia.org/wiki/Public-key_cryptography

Gallian. (2021). *Contemporary abstract algebra.* CRC Taylor & Francis Group.

Koblitz, N., Menezes, A., & Vanstone, S. (2000, Mar). The State of Elliptic Curve Cryptography. *Designs, Codes and Cryptography, 19*, 173-193. doi:10.1023/A:1008354106356

Macedo, C. (2018). *www.Dev4Devs.com*. Retrieved from What is the Big-O?: https://dev4devs.com/2018/01/19/understanding-the-big-o-how-to-think-to-develop-good-and-fast-and-performatic-solutions/

Nakamoto, S. (2009). *Bitcoin: A Peer-to-Peer Electronic Cash System.* Retrieved from https://bitcoin.org/bitcoin.pdf

Shor, P. W. (1999). *Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer.* Retrieved from https://epubs.siam.org/doi/10.1137/S0036144598347011

Sipser. (2021). *Introduction to the theory of computation.* Cengage Learning.

Received for publication: 01.07.2024
Revision received: 08.07.2024
Accepted for publication: 08.01.2025.

How to cite this article?

Style – **APA** *Sixth Edition:*

Feltovic, M. (2025, 01 15). Cryptographic Foundations for Blockchain Security in Decentralized Networks. (Z. Cekerevac, Ed.) *MEST Journal, 13*(1), 52-61. doi:10.12709/mest.13.13.01.05

Style – **Chicago** *Sixteenth Edition:*

Feltovic, Milan. "Cryptographic Foundations for Blockchain Security in Decentralized Networks." Edited by Zoran Cekerevac. *MEST Journal* (MESTE) 13, no. 1 (01 2025): 52-61.

Style – **GOST** *Name Sort:*

Feltovic Milan Cryptographic Foundations for Blockchain Security in Decentralized Networks [Journal] // MEST Journal / ed. Cekerevac Zoran. - Belgrade – Toronto : MESTE , 01 15, 2025. - 1 : Vol. 13. - pp. 52-61.

Style – **Harvard** *Anglia:*

Feltovic, M., 2025. Cryptographic Foundations for Blockchain Security in Decentralized Networks. *MEST Journal,* 15 01, 13(1), pp. 52-61.

Style – **ISO 690** *Numerical Reference:*

Cryptographic Foundations for Blockchain Security in Decentralized Networks. **Feltovic, Milan.** [ed.] Zoran Cekerevac. 1, Belgrade – Toronto : MESTE , 01 15, 2025, MEST Journal, Vol. 13, pp. 52-61.

MEST Journal
DOI 10.12709/mest.13.13.01.06

FORENSIC ANALYSIS OF PRIVATE BLOCKCHAINS IN THE PUBLIC SECTOR: CHALLENGES, TECHNIQUES, AND FUTURE

Milan Feltovic
University of Žilina, Faculty of Security Engineering, Žilina, Slovakia
https://orcid.org/0009-0004-3057-2912

JEL Category: **C88**

Abstract

This article explores the forensic analysis of private blockchains in the public sector, focusing on identifying challenges, describing techniques, and predicting future trends. Unlike public blockchains, private blockchains provide a higher level of access control and data protection, making them attractive for various public applications such as digital land registries, citizen identity management systems, supply chain tracking, and healthcare record management. Forensic analysis of private blockchains is a specialized discipline that combines traditional digital forensic principles with a deep understanding of blockchain technology and cryptography. The main components of this discipline are the identification, collection, preservation, analysis, and presentation of evidence. The article also examines specific aspects such as the analysis of cryptographic evidence, the examination of block structures, and data integrity verification. The importance of forensic analysis of private blockchains grows with their increasing use in the public sector. This article highlights the need for specialized tools and methodologies development, continuous education of forensic experts, and international cooperation in standardization and knowledge exchange. Future trends include the integration of artificial intelligence, the improvement of methods for preserving evidence integrity, and addressing legal and ethical challenges associated with forensic analysis in an international context. The goal of this article is to provide a comprehensive overview of the forensic analysis of private blockchains and to emphasize its key role in ensuring the integrity, transparency, and trustworthiness of digital systems in the public sector.

Keywords: *Private blockchains, digital forensics, cryptography, smart contracts, data security, identity management, transaction analysis, artificial intelligence.*

1 INTRODUCTION

Blockchain technology has become a significant element of digital transformation adopted by organizations worldwide in recent years. Public blockchains, such as Bitcoin and Ethereum, are widely known for their openness and transparency

Address of the author:
Milan Feltovic
milan@feltovic.com

(Nakamoto, 2009). On the other hand, private blockchains are gaining increasing attention, particularly in the public sector, where their closed systems provide higher levels of access control and data protection (Anon, 2023).
Although private blockchains offer significant advantages in enhanced security and privacy protection, their complex structure and closed nature pose challenges for forensic analysis. With the growing deployment of private blockchains in the public sector, such as in healthcare records and identification systems, there is an increasing need for effective forensic methods to ensure their integrity and trustworthiness.

Forensic analysis of private blockchains is a specialized area of digital forensics that deals with investigating and analyzing data in these closed networks. It aims to ensure the integrity and trustworthiness of systems, identify potential security issues, and provide evidence for legal and administrative purposes. This article focuses on the challenges, techniques, and future of forensic analysis of private blockchains, providing an overview of how this field contributes to the security and efficiency of public systems (Bonet, 2023, Jun 23).

Existing research predominantly focuses on the technical aspects of blockchain technologies, but detailed forensic analysis of private blockchains, which would also encompass legal and ethical aspects, remains insufficiently explored. This research aims to fill this gap by providing a comprehensive perspective on the methods and tools necessary for legal evidence and compliance assurance.

2 METHODS

This study builds on my several years of experience as an expert in forensic operations, where I have developed a particular interest in blockchain technology and its applications in forensic analysis. To establish a theoretical foundation and overview of existing knowledge, I conducted a comprehensive literature review, analyzing academic articles, studies, and white papers available in digital libraries. In my research, I used keywords such as "forensic analysis," "private blockchain," "security strategies," and "public sector."

As part of my research, I also gathered practical insights, utilizing information from Chainalysis, a leader in blockchain analysis. This information provided valuable insights into current trends and tools used in the industry for monitoring and analyzing transactions on private blockchains. Additionally, I obtained technical details on the deployment of blockchain technologies such as Hyperledger Fabric and Ethereum through online documentation and resources available on GitHub.

Integrating theoretical knowledge from the literature review with practical information enabled a deeper understanding of the challenges and possibilities of forensic analysis of private blockchains. In the study, I critically evaluated sources, compared various opinions and techniques, and formulated conclusions based on a combination of personal experiences, and theoretical and practical knowledge.

Private blockchains are being utilized in various areas of the public sector, including:

- *Digital land registry*: For example, a project in Georgia uses blockchain to manage property rights and real estate records (Shang & Price, 2019).
- *Citizen identity management systems*: For instance, e-Estonia, where blockchain is used to manage identities and ensure the integrity of personal data (PWC, 2019).
- *Supply chain tracking*: For example, FDA projects in the USA use blockchain to track the movement of drugs and ensure their authenticity (Anon., 2020).
- *Healthcare record management*: For example, initiatives in Estonia use blockchain to manage and protect patient healthcare records (Einaste, 2018).

2.1 Definition of Forensic Analysis of Private Blockchains

Forensic analysis of private blockchains is a specialized area of digital forensics that involves the investigation and analysis of data in closed blockchain networks. The goal is to identify, collect, preserve, analyze, and present evidence that can be used for legal and administrative purposes (Xu, 2021). This discipline combines traditional digital forensic principles with a deep

understanding of blockchain technology, cryptography, and distributed systems.

2.1.1 Key Components of Forensic Analysis of Private Blockchains

Evidence identification: This process involves locating relevant data within the blockchain network, including transaction records, smart contracts, and metadata. It is crucial to accurately determine which data is relevant to the investigation (Zheng, 2020).

Evidence collection: Evidence collection requires specialized tools and techniques to extract data from blockchain nodes. It is essential to ensure the integrity and authenticity of the information obtained (NIST, 2023).

Evidence preservation: This includes creating forensic copies of blockchain data and securely storing them in a way that maintains their evidential value. It is important to keep the data unchanged and available for further analysis.

Evidence analysis: This step involves a detailed examination of the collected data using specialized tools and techniques. Analysis may include examining transactions, smart contracts, and network activity to identify suspicious or unusual behavior (Bonneau, J., et al., 2015).

Evidence presentation: Forensic analysis results must be presented clearly and understandably for legal and administrative purposes. This includes creating a report that clearly describes the findings and provides evidence to support conclusions.

2.1.2 Specific Aspects of Forensic Analysis of Private Blockchains

Cryptographic evidence analysis: This involves verifying digital signatures, checking the integrity of hashes, and analyzing cryptographic protocols used in the network (ENISA, 2023). These procedures ensure that the data has not been altered and is authentic.

Block structure examination: This requires a detailed understanding of block formats, their linkages, and the consensus mechanisms used in the blockchain network.

Data integrity verification: This involves checking the integrity of the blockchain chain and detecting any attempts to tamper with historical data. Ensuring data integrity is crucial for the trustworthiness of the entire system.

Access control analysis: In private blockchains, examining access control mechanisms and identity management is key. These mechanisms, which are not present in public blockchains, ensure that only authorized users have access to certain information (Günther, M., Liebkind, J., & Nyberg, T., 2020).

2.1.3 Difference from Forensic Analysis of Public Blockchains

Verification of access rights: Unlike public blockchains, where anonymity is the main challenge, forensic analysis of private blockchains focuses on verifying whether all actions in the network were performed by authorized users (Santos, C., Almeida, F., & Oliveira, L., 2021).

Identification of unauthorized changes: In private blockchains, it is important to detect any attempts to manipulate data or network configuration. These changes can have serious consequences for the security and trustworthiness of the system.

Audit log analysis: Detailed examination of logs and audit records, often more accessible in private networks, allows for identifying and tracking the actions of individual users and nodes in the network (Xu, 2021).

Analysis of specific consensus mechanisms: Private blockchains often use different consensus mechanisms than public networks. These mechanisms can be proprietary and require specialized knowledge and tools for their analysis (NIST, 2023).

2.1.4 Legal and Ethical Aspects

Compliance with data protection laws: Forensic analysis of private blockchains must consider data protection regulations, such as GDPR in the EU. It is essential to ensure that personal data is protected and processed following regulations (Zheng, 2020).

Confidentiality of sensitive business information: During forensic analysis, it is important to protect the confidentiality of business information to prevent its unauthorized disclosure or misuse (Risius, M. & Spohrer, K., 2017).

Respect for jurisdictional limitations: Especially in the case of international blockchain networks, it is necessary to comply with the legal regulations and restrictions of different jurisdictions. This may

involve cooperation with regulatory authorities and adherence to local laws.

2.2 Importance of Forensic Analysis of Private Blockchains

The forensic analysis of private blockchains is becoming increasingly important, especially with the growing adoption of blockchain technology in the public sector. This discipline plays a key role in ensuring the integrity, security, and trustworthiness of blockchain systems. Here are the main reasons why the forensic analysis of private blockchains is so crucial:

2.2.1 Key Factors Increasing the Importance of Forensic Analysis of Private Blockchains

Protection of critical infrastructure: Many government institutions implement blockchain technologies for managing critical data and processes, such as land registries, healthcare records, or identity management systems. Forensic analysis of private blockchains is crucial for identifying and investigating potential security incidents in these systems (Zyskind, G., Nathan, O., & Pentland, A., 2015).

Combating financial crime: Private blockchains are increasingly used in the financial sector. Forensic tools are essential for detecting fraud, money laundering, and other financial crimes in these systems. They help ensure that transactions are legitimate and that financial flows are transparent.

Ensuring the integrity of public records: Many countries implement blockchain technologies for managing public registries, such as land records or citizen registries. Forensic analysis is crucial for verifying the integrity of these records and investigating possible manipulations (ENISA, 2023). This helps maintain the credibility and accuracy of public information.

Supporting regulatory oversight: With the growing use of blockchain technologies, regulatory authorities need effective tools for monitoring and oversight. Forensic techniques enable regulators to monitor compliance with regulations, identify potential violations, and ensure that organizations adhere to applicable laws and standards (Santos, C., Almeida, F., & Oliveira, L., 2021).

2.2.2 Specific Benefits of Forensic Analysis of Private Blockchains

Increased transparency: Forensic tools enable detailed analysis of transactions and activities on the blockchain, contributing to higher transparency. This increases citizens' trust in public institutions and helps prevent corruption and fraud (Wuest & Gervais, 2018).

Improved auditability: Forensic analysis provides robust methods for auditing blockchain systems. This is key for ensuring accountability and integrity in public institutions. Regular audits can uncover inconsistencies and ensure that systems operate correctly (Günther, M., Liebkind, J., & Nyberg, T., 2020).

Faster detection and response to incidents: Forensic tools enable rapid identification of anomalies and potential security threats. This allows for quicker and more effective responses to incidents, minimizing damage and ensuring the rapid restoration of normal system operations (Bonneau, J., et al., 2015).

Supporting the legal system: Forensic analysis of private blockchains provides reliable evidence for legal proceedings. This is crucial for resolving disputes and enforcing laws in the digital environment. Evidence obtained from the blockchain can be used in court to support claims and charges.

2.2.3 Economic Aspects

Reducing financial losses: Effective forensic analysis can help quickly detect and stop fraudulent activities, leading to significant savings for the public sector. Rapid detection and remediation of issues minimize financial damages and increase confidence in blockchain technologies (Shang & Price, 2019).

Optimizing compliance costs: Forensic tools can automate many aspects of regulatory oversight, reducing compliance costs for public sector organizations. Automation reduces the need for manual checks and increases efficiency (NIST, 2023).

2.2.4 Future Trends Increasing Importance

Integration with artificial intelligence: Forensic tools are expected to increasingly use artificial intelligence for advanced data analysis. AI will enable more efficient detection of complex

patterns and anomalies, increasing the accuracy and speed of forensic analyses (Zheng, 2020).

International cooperation: With the increasing number of global blockchain projects, the need for cross-border forensic collaboration grows. This will require the development of new protocols and tools for international forensic analysis, improving the ability to address global issues (Zyskind, G., Nathan, O., & Pentland, A., 2015).

Response to new types of threats: As blockchain technologies evolve, new types of security threats will emerge. Forensic analysis will need to continuously innovate to address these threats and ensure the integrity of blockchain systems (Xu, 2021).

2.3 Techniques for Forensic Analysis of Private Blockchains

Forensic analysis of private blockchains employs various specialized techniques to analyze and investigate activities in closed blockchain networks. These techniques are continuously evolving with advancements in blockchain technologies. Here are the main categories of techniques with detailed descriptions:

2.3.1 Transaction Analysis

Tracking asset movement: This technique uses graph algorithms to map the flow of assets between addresses in the blockchain network. It helps identify transfer patterns that may indicate suspicious activities (Zheng, 2020).

Pattern analysis: This technique applies statistical methods to identify unusual frequencies or volumes of transactions. Machine learning is also used to detect anomalies in transaction data. Metadata analysis of transactions provides additional information about the nature of transfers.

Clustering analysis: This technique group addresses based on their transactions, helping identify potentially linked entities. Heuristic algorithms are used to uncover hidden relationships between participants in the blockchain network.

2.3.2 Smart Contract Analysis

Static code analysis: Examines the source code of smart contracts to identify potential vulnerabilities. Automated tools detect known patterns of risky code and analyze the contract logic to identify unexpected behaviors.

Dynamic analysis: This technique simulates the execution of smart contracts in a controlled environment, monitoring contract behavior under different input conditions and identifying potentially exploitable states or unexpected interactions (Zyskind, G., Nathan, O., & Pentland, A., 2015).

Symbolic execution: Uses formal methods to model mathematically all possible execution paths of a contract. Identifies conditions under which undesirable behavior may occur.

2.3.3 Network Architecture Analysis

Topological analysis: Maps the structure of the blockchain network, identifying key nodes and their interconnections. Analyzes the distribution of computational power in the network, helping understand how the network is organized and where potential weaknesses lie.

Consensus mechanism analysis: Examines the implementation and behavior of consensus algorithms. Identifies potential weaknesses in the consensus process, which is crucial for ensuring the integrity and trustworthiness of the blockchain network (NIST, 2023).

Network communication analysis: Monitors and analyzes communication patterns between nodes. Identifies anomalies in network traffic that may indicate an attack or other security issues.

2.3.4 Access Control and Identity Analysis

Audit of access rights: Examines the identity management and access control system in the blockchain network. Verifies whether all actions were performed by authorized users, ensuring no unauthorized accesses occurred.

Change analysis in rights: Tracks the history of changes in access rights and identifies potentially unauthorized or suspicious changes. This technique helps identify attempts to misuse access rights (Santos, C., Almeida, F., & Oliveira, L., 2021).

Behavioral analysis: Monitors and analyzes user behavior patterns in the network. Identifies

deviations from normal behavior that may indicate account compromise or other security threats.

2.3.5 Cryptographic Analysis

Signature verification: Verifies the integrity of digital signatures used in transactions and smart contracts. Identifies potentially forged or compromised signatures, which is crucial for ensuring the trustworthiness of data (Bonneau, J., et al., 2015).

Hash function analysis: Verifies the correctness of hash function implementation and usage. It looks for potential collisions or weaknesses in hash algorithms that could be exploited for data manipulation.

Cryptographic protocol analysis: Examines the implementation and usage of cryptographic protocols in the network. Identifies potential vulnerabilities in cryptographic schemes that could be used for attacks (Risius, M. & Spohrer, K., 2017).

2.3.6 Off-Chain Data Analysis

Correlation of on-chain and off-chain data: Connects blockchain transactions and events with external data. It uses external information sources to contextualize blockchain activities, helping better understand the broader context.

Metadata analysis: Examines additional information associated with blockchain transactions. Extracts and analyzes data stored in OP_RETURN fields or similar structures, providing supplementary information about transactions and their participants (NIST, 2023).

2.3.7 Temporal Analysis

Event timeline: Reconstructs the chronological sequence of events in the blockchain network. It identifies causal relationships between various activities, helping understand how individual events developed over time (ENISA, 2023).

Temporal pattern analysis: Examines the distribution of activities over time to identify unusual patterns. It uses anomaly detection techniques to identify non-standard temporal sequences that may indicate suspicious activities.

These techniques are often combined and applied iteratively during a forensic investigation. Their effective use requires a deep understanding of blockchain technology, cryptography, network protocols, and forensic principles. With the evolution of blockchain technologies, forensic techniques are expected to develop further to meet new challenges and threats.

2.4 Challenges of Forensic Analysis of Private Blockchains

Forensic analysis of private blockchains faces numerous technical, legal, and ethical challenges. These challenges can complicate investigating and analyzing data in closed blockchain networks. Here are the main challenges this field encounters:

2.4.1 Technical Challenges

Restricted access to network nodes: In private blockchains, it is not possible to freely access all nodes in the network. This limited access can hinder data collection and comprehensive network analysis, as not all nodes may be available for inspection and monitoring (Risius, M. & Spohrer, K., 2017).

Variety of implementations: Private blockchains can be implemented in various ways, meaning there is no single approach to accessing and analyzing them. Each implementation may require specific tools and techniques, increasing the complexity of forensic analysis.

Complexity of smart contracts: Smart contracts can be very complex and contain intricate logic and interactions. Analyzing these contracts requires advanced tools and expertise to identify potential vulnerabilities and inconsistencies (Zyskind, G., Nathan, O., & Pentland, A., 2015).

Proprietary consensus mechanisms: Private blockchains often use proprietary consensus mechanisms that are not commonly known and documented. Analyzing these mechanisms can be challenging and requires specialized knowledge and tools (Günther, M., Liebkind, J., & Nyberg, T., 2020).

2.4.2 Legal and Ethical Challenges

Uncertainties regarding jurisdiction: In the case of international private blockchains, it may be unclear which legal regulations and jurisdictions are relevant. This can complicate investigations, especially if network participants are from different countries with different laws and regulations (ENISA, 2023).

Data protection and privacy laws: Forensic analysis must be conducted in compliance with data protection regulations, such as GDPR in the EU. It must be ensured that sensitive personal data is protected and processed responsibly to avoid privacy violations (Zheng, 2020).

Ethical considerations: There are moral questions regarding the scope and methods of conducting forensic analysis in closed systems. It is important to balance the need for investigation and the protection of individual rights. Forensic analysts must work with a high degree of integrity and responsibility (Bonneau, J., et al., 2015).

Preserving the integrity of evidence: During forensic analysis, it is crucial to ensure that evidence remains unchanged and reliable. This includes creating forensic copies of data and securely storing them. It is also necessary to ensure the confidentiality of sensitive information to prevent unauthorized disclosure (Santos, C., Almeida, F., & Oliveira, L., 2021).

These technical, legal, and ethical challenges represent significant obstacles that need to be overcome for forensic analysis of private blockchains to be effective and reliable. Advanced tools, expert education, and international cooperation are key to addressing these challenges and ensuring the security and integrity of blockchain systems.

2.5 Technical Details of Forensic Analysis of Private Blockchains

These technical details provide an overview of specific methods and tools used in the forensic analysis of private blockchains. It is important to note that actual forensic analysis often requires a combination of various advanced techniques as well as a deep understanding of specific blockchain platforms and the context of the investigation.

2.5.1 Data Extraction from Blockchain Nodes

The data extraction from blockchain nodes is a crucial step in forensic analysis. Figure 1 shows an example of a Python script for extracting data from a Hyperledger Fabric node (Hyperledger, 2024).

```
from hfc.fabric import Client
# Initialize the client
client = Client(net_profile="connection-
profile.json")
# Connect to the network
client.new_channel('mychannel')
# Extract data from a specific block
block_number = 1000
block = client.query_block(block_number,
'mychannel')
# Analyze transactions in the block
for tx in block.get('data').get('data'):
    transaction =
tx.get('payload').get('data').get('actio
ns')[0].get('payload').get('action')
    print(f"Transaction: {transaction}")
```

Fig. 1 Extracting data from the Hyperledger Fabric node
Source: GitHub (2024)

This code (GitHub, 2024) serves to interact with the blockchain network on the Hyperledger Fabric platform using the hfc.fabric library. The code demonstrates how one can connect to the network, query blocks in the blockchain, and analyze transactions within them.

2.5.2 Transaction Analysis

After data extraction, the next step is transaction analysis. Figure 2 shows an example of a function for detecting unusual patterns in transactions.

```
import pandas as pd
from scipy import stats
def detect_anomalies(transactions):
    df = pd.DataFrame(transactions)
    df['z_score'] = stats.zscore(df['value'])
    anomalies = df[abs(df['z_score']) > 3]
    return anomalies
# Using the function
transactions = [{'value': 10}, {'value': 100},
{'value': -5}]
anomalies = detect_anomalies(transactions)
print(f"Detected anomalies: {anomalies}")
```

Fig.2 Transaction Analysis
Source: GitHub (2024)

This code (GitHub, 2024) serves to detect anomalous transactions in the dataset using a statistical method known as Z-score. It uses the pandas' library (Pandas, 2024) for data manipulation and SciPy for computing statistics. The code focuses on identifying transactions with extreme values compared to the rest of the dataset.

2.5.3 Smart Contract Analysis

Smart contract analysis is critical for uncovering potential vulnerabilities. Figure 3 shows an example of using the Mythril tool (Mythril, 2019) to analyze a Solidity smart contract:

```
from mythril.mythril import Mythril
from mythril.exceptions import
CriticalError
def analyze_contract(contract_file):
    myth = Mythril()
    try:

myth.load_from_solidity(contract_file)
        issues =
myth.fire_lasers(modules=["ether_thief",
"arbitrary_write"])
        for issue in issues:
            print(f"Issue:
{issue.description}")
    except CriticalError as ce:
        print(f"Critical error
encountered: {ce}")
# Using the function
analyze_contract("MyContract.sol")
```

Fig.3 Smart Contract Analysis
Source: Mythril (2019)

This code (GitHub, 2024) is a tool for static analysis of smart contracts written in Solidity, intended for the Ethereum blockchain. It uses the Mythril library, known for its capabilities to identify security vulnerabilities and issues in smart contracts.

2.5.4 Event Timeline Reconstruction

Event timeline reconstruction is important for understanding the sequence of activities. Figure 4 shows an example of a function to create a timeline.

This code (GitHub, 2024) is a tool for visualizing the timeline of events. It uses the pandas' library for data manipulation and Matplotlib (Hunter, J. D., 2007) for plotting the graph. It allows converting a list of events into a timeline with labels, where each event is displayed on the graph according to its timestamp.

```
        import pandas as pd
    import matplotlib.pyplot as plt
     def create_timeline(events):
       df = pd.DataFrame(events,
    columns=['timestamp', 'event'])
           df['timestamp'] =
    pd.to_datetime(df['timestamp'])
    df = df.sort_values('timestamp')
fig, ax = plt.subplots(figsize=(12, 6))
ax.plot(df['timestamp'], range(len(df)),
                'o-')
 for i, txt in enumerate(df['event']):
           ax.annotate(txt,
     (df['timestamp'].iloc[i], i),
  xytext=(10, 0), textcoords='offset
              points')
    plt.title('Timeline of Events')
          plt.xlabel('Time')
     plt.ylabel('Event Sequence')
          plt.tight_layout()
              plt.show()
        # Using the function
              events = [
   ('2023-01-01 10:00:00', 'Contract
            Deployment'),
    ('2023-01-02 15:30:00', 'Unusual
             Transaction'),
('2023-01-03 09:45:00', 'Access Pattern
              Change')
                ]
        create_timeline(events)
```

Fig.4 Timeline Reconstruction
Source: (GitHub, 2024)

2.5.5 Network Communication Analysis

Analyzing network communication between blockchain network nodes can reveal potential security issues. Figure 5 is an example of using the Scapy library (Scapy, 2024) to analyze network traffic:

```
from scapy.all import *
def analyze_network_traffic(pcap_file):
    packets = rdpcap(pcap_file)
    for packet in packets:
        if TCP in packet and
packet[TCP].dport == 7051:  # The Port
used by Hyperledger Fabric
            print(f"Blockchain
communication detected:
{packet.summary()}")
            if Raw in packet:
                payload =
packet[Raw].load
                # Analýza payload-u
# Using the function
analyze_network_traffic("blockchain_traf
fic.pcap")
```

Fig.5 Network Analysis
Source: (GitHub, 2024)

This code (GitHub, 2024) is a tool for analyzing network traffic, specifically focused on the captured communication of the Hyperledger Fabric blockchain, using the Scapy library. Scapy is a powerful Python library for packet manipulation, capturing, and analyzing network traffic.

2.6 Future of Forensic Analysis of Private Blockchains

The forensic analysis of private blockchains will continuously evolve and adapt to new challenges and technological advancements. It is full of challenges but also opportunities for improvement and innovation. Investments in new technology development, education of experts, and international cooperation will be crucial for ensuring the integrity and trustworthiness of blockchain systems in the public sector. Several key areas will significantly impact this discipline:

- *Development of standards*: International organizations, such as ISO (International Organization for Standardization) and NIST (National Institute of Standards and Technology), are working on creating standards and guidelines for blockchain technologies, including forensic analysis. ISO/TC 307 deals with the standardization of blockchain technologies, and NIST is developing guidelines for blockchain cybersecurity (NIST, 2023). These initiatives will help create unified procedures and improve the efficiency of forensic analyses.
- *Potential regulatory changes*: In the coming years, new regulations specific to blockchain technologies are expected to be adopted. In the European Union, legislation is being planned that will require forensically auditable records for blockchains used in the public sector. Similar legislation is being considered in the United States to increase transparency and accountability (Zheng, 2020). These regulatory changes will improve forensic investigation capabilities and increase confidence in blockchain technologies.
- *Integration with artificial intelligence*: Forensic tools are expected to increasingly utilize artificial intelligence (AI) for advanced data analysis. AI can help more quickly and accurately identify anomalies and suspicious patterns in blockchain data. This integration will enable more efficient and automated forensic analyses, increasing their accuracy and reliability (Risius, M. & Spohrer, K., 2017).
- *International cooperation*: With the growing number of international blockchain projects, the need for cross-border forensic cooperation increases. Organizations like Interpol and Europol emphasize international cooperation in the field of blockchain forensic analysis. This cooperation will include the development of new protocols and tools for sharing information and coordinating investigations between different countries (Günther, M., Liebkind, J., & Nyberg, T., 2020). International cooperation is essential for effectively addressing global blockchain-related issues.
- *Response to new types of threats*: As blockchain technologies evolve, new types of security threats will emerge. Forensic analysis must continuously innovate to address these new threats. Research and development of new techniques and tools will be crucial for ensuring that forensic analyses can identify and address new security challenges (Xu, 2021).

2.7 Artifacts and Their Analysis

Forensic analysis of private blockchains involves examining various types of data referred to as artifacts. These artifacts provide key information for the investigation and can include transaction data, smart contract data, logs and audit records, blockchain structure data, and configuration data. Each type of artifact is important for understanding and analyzing the blockchain network.

2.7.1 Transaction Data

Timestamps: These marks indicate the exact time and date of each transaction in the blockchain. They help reconstruct the chronology of events and identify transaction patterns (Bonneau, J., et al., 2015).

Participant identifiers: Public keys or other identifiers allow the identification of individual transaction participants. These identifiers are important for tracking the origin and destination of assets.

Transaction metadata: Includes the type of operation (such as asset transfer, smart contract signing), the amount of assets transferred, and additional information that can provide context for each transaction.

2.7.2 Smart Contract Data

Bytecode: The compiled code of the contract deployed on the blockchain. This code determines how the contract behaves and what operations it can perform (Santos, C., Almeida, F., & Oliveira, L., 2021).

Application Binary Interface (ABI): The definition of the contract's functions and parameters, allowing interaction with the smart contract. ABI is essential for understanding how the smart contract can be called and what data it expects.

Contract state: Current values of the variables in the contract. These data reflect the current state of the smart contract and can provide information about its historical and current operations (Zyskind, G., Nathan, O., & Pentland, A., 2015).

2.7.3 Logs and Audit Records

System logs: Records of operations at the blockchain platform level, which may include node activities, transactions, and consensus events (Zheng, 2020).

Application logs: Records generated by specific applications running on the blockchain. These logs can provide detailed information about the activities of individual applications and smart contracts (Risius, M. & Spohrer, K., 2017).

Audit records: Detailed information about user accesses and actions. These records are crucial for tracking who performed which operations and when.

2.7.4 Blockchain Structure Data

Block headers: Information about each block, including the hash of the previous block. Block headers provide data about the chain of blocks and allow the verification of blockchain integrity (Bonneau, J., et al., 2015).

Merkle tree: A structure used for efficient transaction verification. The Merkle tree allows quick and reliable verification that a transaction is part of a specific block without searching the entire block.

2.7.5 Configuration Data

Network settings: Information about the topology and rules of the network, such as consensus rules, the number of nodes, and their roles in the network. These data are crucial for understanding the functioning and behavior of the blockchain network (Santos, C., Almeida, F., & Oliveira, L., 2021).

Consensus rules: Details on how consensus is reached in the network. These rules determine how nodes cooperate to verify and add new blocks to the blockchain.

Why are these artifacts significant?

Timestamps and participant identifiers: Help forensic experts track when and who performed specific transactions, which is essential for reconstructing events and identifying suspicious activities.

Smart contract data: Provide a detailed view of the logic and execution of smart contracts, which is necessary for analyzing their security and correctness.

Logs and audit records: These are crucial for tracking operations and activities in the network, enabling the identification of unauthorized access and potential security incidents.

Blockchain structure data: It allows verification of the integrity and continuity of the blockchain, which is important for the trustworthiness and security of the entire network.

Configuration data: It provides context for the functioning of the network and allows the understanding of how the network is organized and how it reaches consensus (Zheng, 2020).

2.8 Analysis Tools

Several specialized tools have been developed specifically for the forensic analysis of private blockchains. These tools help ensure that data and operations in the blockchain network can be thoroughly analyzed to identify potential security issues, fraud, and other anomalies. The following tools are crucial for the effective management and analysis of private blockchain networks, as they help ensure their security, performance, and regulatory compliance:

- *Hyperledger Caliper* is a tool for benchmarking and performance analysis of private blockchains. It allows testing different blockchain implementations and measuring their performance using various indicators such as latency, throughput, and transactions per second (TPS). This tool helps developers and administrators understand the performance characteristics of their blockchain networks and identify areas where optimization is needed (NIST, 2023).
- *Accenture Blockchain Forensic Suite* is a comprehensive tool designed for forensic analysis of blockchain platforms such as

Hyperledger Fabric and R3 Corda. It includes tools for collecting, analyzing, and visualizing blockchain data, enabling the identification and tracking of transactions, verification of smart contract integrity, and analysis of network activity. This tool provides forensic analysts with robust means for investigating suspicious activities and ensuring regulatory compliance (Risius, M. & Spohrer, K., 2017).

- *Quorum Explorer* is a specialized tool designed for network analysis based on Quorum, an enterprise version of Ethereum. This tool allows monitoring and analysis of transactions, smart contracts, and network activity in the Quorum blockchain network. It provides visualizations and detailed overviews of the state of the network and its participants, helping organizations maintain oversight of their blockchain network, identify anomalies, and ensure optimal operation (Santos, C., Almeida, F., & Oliveira, L., 2021).

2.9 Case Studies

Given the sensitive nature of forensic investigations, many case details remain confidential. The following case studies are based on publicly available information and anonymized examples that illustrate the use of forensic analysis of private blockchains in the public sector.

2.9.1 Case No. 1: Uncovering fraud in the public procurement system (anonymized European country, 2022)

A government agency implemented a private blockchain system to manage public procurement to increase transparency and efficiency. Anomalies in contract awards were recorded, suggesting possible manipulation of the supplier selection process. Forensic experts reviewed the transaction history in the blockchain, focusing on patterns in contract awards. A detailed analysis of the smart contract code controlling the procurement process was conducted. They created a chronological reconstruction of key events in the system. The result was the discovery of unauthorized changes in the smart contract code that allowed the manipulation of selection criteria. A series of suspicious transactions linked to a specific administrator account were identified. The investigation led to the uncovering of a corruption scheme, legal consequences for those involved, and significant changes in the public procurement system.

2.9.2 Case No. 2: Protecting the integrity of the digital real estate registry (anonymized Asian country, 2023)

A government body implemented a private blockchain to manage the real estate registry to increase security and efficiency. Cases of unauthorized changes to property rights were reported. Experts examined the access records and permissions in the system. They analyzed in detail the metadata associated with transactions related to changes in property rights. They verified the integrity of digital signatures and hashes linked to the relevant transactions. The result was the identification of a series of unauthorized accesses to the system through compromised employee accounts and the detection of sophisticated malware that allowed the circumvention of security controls.

2.9.3 Case No. 3: Analyzing anomalies in the healthcare records system (anonymized North American country, 2024).

A regional healthcare system implemented a private blockchain to manage patient health records. Unusual patterns in access to health records were recorded, indicating a potential leak of sensitive data. Experts analyzed the access patterns to the records, identifying anomalies in the timing and frequency of access. They thoroughly examined the audit logs of the blockchain system and conducted a forensic analysis of network communication between the blockchain nodes. The result was the discovery of unauthorized access to the records through a poorly configured API.

These case studies illustrate the diversity and complexity of challenges faced by forensic analysis of private blockchains in the public sector. They also emphasize the importance of advanced forensic techniques and tools to preserve the integrity and security of these systems.

3 RESULTS

This study has yielded important findings regarding the forensic analysis of private blockchains in the public sector, reflecting the current state and identifying the main challenges and risks. Through the literature and sources

review, I discovered that the forensic challenges of private blockchains often relate to limited data access, high levels of encryption, and the lack of standardized tools for effective analysis. These factors make the acquisition and verification of forensic evidence complicated and require special techniques and approaches.

In addition to technical challenges, I identified security risks that include vulnerabilities in the implementation of smart contracts and potential data leakage through network interfaces. These security weaknesses demand increased attention and the development of new forensic methods to address them adequately.

From a legal and ethical perspective, the study highlighted significant dilemmas related to personal data protection and compliance with jurisdictional constraints. These findings underscore the need for a better regulatory framework and international agreements to help address issues associated with the use of forensic techniques in private blockchains.

Overall, my findings emphasize the complexity of forensic analysis of private blockchains and highlight the need for continuous research and development in this area to effectively face the challenges that these technologies bring.

4 CONCLUSIONS

Forensic analysis of private blockchains is an integral part of ensuring the integrity and trustworthiness of blockchain systems in the public sector. As this technology is increasingly adopted by various government and public institutions, the need for advanced forensic techniques and tools that enable effective investigation and analysis also grows. It is important to invest in the development and improvement of tools specifically designed for the analysis of private blockchains to address the specific challenges associated with closed systems, such as identifying unauthorized access and tracking transactions.

In this study, I emphasized the importance of continuous education and training for forensic experts who must keep pace with rapidly evolving technologies. These experts need not only technical skills but also an understanding of the legal and ethical aspects of forensic analysis. International collaboration in developing standards and sharing knowledge is crucial, as blockchain technology is a global phenomenon.

Regulatory authorities and international organizations should work together to create unified rules and procedures for blockchain forensic analysis. It is essential to find a balance between effective investigation and privacy protection to ensure that forensic analysis respects individual rights and complies with legal regulations concerning data protection.

Future research should focus on developing advanced techniques for analyzing complex smart contracts, which are becoming increasingly sophisticated and require new methods for identifying vulnerabilities and verifying their correct execution. This research should also improve methods for preserving the integrity of evidence in distributed systems, including the creation of forensic copies and the secure storage of data. Finally, research should address the legal and ethical challenges associated with forensic analysis in an international context to ensure that such analysis complies with global legal regulations and ethical standards.

In conclusion, forensic analysis of private blockchains is a critical tool for maintaining the security and trustworthiness of digital systems in the public sector. Investments in tool development, expert education, and international collaboration are key to the future success and effectiveness of forensic analysis in this dynamically evolving field.

WORKS CITED

Anon. (2023, Jun 28). *Introducing Splice, a New Hyperledger Lab for Canton Network interoperability.* Retrieved from Hyperledger Foundation: https://www.lfdecentralizedtrust.org/blog/introducing-splice-a-new-hyperledger-lab-that-supports-canton-network-interoperability

Anon. (2020). Retrieved from FDA DSCSA Blockchain Interoperability: https://www.fda.gov/media/169883/download

Bonet, J. (2023, Jun 23, June). *Consolidated Annual Activity Report 2022.* EUROPOL. Retrieved from https://www.europol.europa.eu/cms/sites/default/files/documents/Consolidated%20Annual%20Activity%20Report%202022.PDF

Bonneau, J., Miller, A., Clark, J., Narayanan, A., Kroll, J. A., & Felten, E. W. (2015). Research Perspectives and Challenges for Bitcoin and Cryptocurrencies. *2015 IEEE Symposium on Security and Privacy*, 104-121.

Einaste, T. (2018, Feb 26). *Blockchain and healthcare: the Estonian experience.* Retrieved from e-estonia.com: https://e-estonia.com/blockchain-healthcare-estonian-experience/

ENISA. (2023, Oct 19). *ENISA Threat Landscape 2023.* (I. Lella, E. Tsekmezoglou, M. Theocharidou, E. Magonara, A. Malatras, R. S. Naydenov, & C. Ciobanu, Eds.) doi:10.2824/782573

GitHub. (2024). *Fabric-sdk-py.* Retrieved from GitHub: https://github.com/hyperledger/fabric-sdk-py

Günther, M., Liebkind, J., & Nyberg, T. (2020). Digital Forensics in Blockchain Environments: Distinctive Features and Forensic Process. *Forensic Science International: Digital Investigation. 2020, 33*, 200-219.

Hunter, J. D. (2007). Retrieved from Matplotlib: A 2D Graphics Environment. Computing in Science & Engineering, vol. 9, no. 3, 2007: https://matplotlib.org/

Hyperledger. (2024). Retrieved from Hyperledger Fabric: https://www.hyperledger.org/

Mythril. (2019). *Mythril*. Retrieved from Github.com: https://mythril-classic.readthedocs.io/en/develop/about.html

Nakamoto, S. (2009). *Bitcoin: A Peer-to-Peer Electronic Cash System.* Retrieved from https://bitcoin.org/bitcoin.pdf

NIST. (2023). Guidelines for Blockchain Cybersecurity. *NIST Special Publication 800-204*.

Pandas. (2024). *Pandas*. Retrieved from The Pandas Development Team: https://pandas.pydata.org/

PWC. (2019). Retrieved from Estonia – the Digital Republic Secured by Blockchain: https://www.pwc.com/gx/en/services/legal/tech/assets/estonia-the-digital-republic-secured-by-blockchain.pdf

Risius, M., & Spohrer, K. (2017). A Blockchain Research Framework: What We (don't) Know, Where We Go from Here, and How We Will Get There. *Business & Information Systems Engineering. 2017, 59(6)*, 385-409.

Santos, C., Almeida, F., & Oliveira, L. (2021). Blockchain: A Literature Review on Forensic Methods and Challenges. *IEEE Access. 2021, 9*, 312-330.

Scapy. (2024). *Scapy*. Retrieved from Scapy: https://scapy.net/

Shang, Q., & Price, A. (2019). A Blockchain-Based Land Titling Project in the Republic of Georgia. *Innovations: Technology, Governance, Globalization, 12*(3-4), 72-78.

Wuest, K., & Gervais, A. (2018). Do you need a Blockchain? *2018 Crypto Valley Conference on Blockchain Technology (CVCBT)* (pp. 45-54). Zug, Switzerland: IEEE. doi:10.1109/CVCBT.2018.00011

Xu, J. (2021). Forensic Analysis of Private Blockchain Networks. *Journal of Digital Forensics, Security and Law. 2021, 16(2)*, 45-62.

Zheng, Z. e. (2020). An Overview of Blockchain Technology: Architecture, Consensus, and Future Trends. *International Congress on Big Data*, 557-564.

Zyskind, G., Nathan, O., & Pentland, A. (2015). Decentralizing Privacy: Using Blockchain to Protect Personal Data. *IEEE Security and Privacy Workshops*, 180-184.

Received for publication: 01.07.2024
Revision received: 08.07.2024
Accepted for publication: 08.01.2025.

How to cite this article?

Style – **APA** *Sixth Edition:*

Feltovic, M. (2025, 01 15). Forensic Analysis of Private Blockchains in the Public Sector: Challenges, Techniques, and Future. (Z. Cekerevac, Ed.) *MEST Journal, 13*(1), 62-75. doi:10.12709/mest.13.13.01.06

Style – **Chicago** *Sixteenth Edition:*

Feltovic, Milan. "Forensic Analysis of Private Blockchains in the Public Sector: Challenges, Techniques, and Future." Edited by Zoran Cekerevac. MEST Journal (MESTE) 13, no. 1 (01 2025): 62-75.

Style – **GOST** *Name Sort:*

Feltovic Milan Forensic Analysis of Private Blockchains in the Public Sector: Challenges, Techniques, and Future [Journal] // MEST Journal / ed. Cekerevac Zoran. - Belgrade – Toronto : MESTE, 01 15, 2025. - 1 : Vol. 13. - pp. 62-75.

Style – **Harvard** *Anglia:*

Feltovic, M., 2025. Forensic Analysis of Private Blockchains in the Public Sector: Challenges, Techniques, and Future. *MEST Journal,* 15 01, 13(1), pp. 62-75.

Style – **ISO 690** *Numerical Reference:*

Forensic Analysis of Private Blockchains in the Public Sector: Challenges, Techniques, and Future. **Feltovic, Milan.** [ed.] Zoran Cekerevac. 1, Belgrade – Toronto : MESTE, 01 15, 2025, MEST Journal, Vol. 13, pp. 62-75.

MEST Journal
DOI 10.12709/mest.13.13.01.07

IIA CYBERSECURITY TOPICAL REQUIREMENT AND ISO/IEC 27001

Haris Hamidovic
MKF/MKD EKI Sarajevo, Sarajevo, Bosnia and Herzegovina
https://orcid.org/0000-0002-1296-5008

JEL Category: **K22, M15**

Abstract

Cyber security protects an organization's information assets from unauthorized users, disruption, alteration, or destruction and strengthens the overall control environment to reduce risk. Cyber attacks can lead to direct and indirect effects that are often significant, as computers, networks, programs, data, and sensitive information are critical components of most organizations. Because organizations rely heavily on information technology resources, a clearly defined cybersecurity plan, objectives, inherent risks, and effective controls should be a priority for management. The IIA Cybersecurity Topical Requirement provides a consistent, comprehensive approach to assessing the design and implementation of cybersecurity governance, risk management, and control processes. The IIA's activities on the Cybersecurity Topical Requirement development will certainly contribute to increasing the cyber security level in business organizations. Given that it is possible to map the requirements from the IIA Cybersecurity Topical Requirement with the requirements from the ISO/IEC 27001 standard, it would be more than useful to use the existing good practices and experience related to the use of ISO/IEC 27001 and related standards in terms of practical implementation and assessment of compliance with IIA requirements. In this paper, we present one of the possible ways how the good practices of the international standard ISO/IEC 27001 can be used to assess the level of compliance with the IIA Cybersecurity Topical Requirement.

Keywords: *computers, information, corporate security, management of technology, auditing.*

1 INTRODUCTION

The Institute of Internal Auditors - The IIA after the research conducted at the global level indicates the risk of cyber security as the greatest risk for modern business organizations. A similar situation is expected in the next three years. (IIA, 2024 a)

Address of the author:
Haris Hamidović
haris.hamidovic@eki.ba

Therefore, the IIA launched in 2024 a pilot project for the development of topical audit requirements in the domain of cyber security. Topical requirements provide audit requirements for specific areas and clarify the audit methodology. (IIA, 2024 b)

In the middle of 2024, a draft of topical requirements in the field of cyber security was submitted to the association members for review and comments. For organizations that already use

the ISO/IEC 27001 information security management framework, we find possible appropriate mappings between IIA topical requirements and ISO/IEC 27001 requirements and controls, so we propose a more granular assessment of the degree of compliance for each of the IIA requirements than one stated in the IIA document Appendix B – Tool to Document Conformance with Topical Requirement where conformance level is expressed only as Yes / No / Partial.

2 CHALLENGES OF INFORMATION SECURITY MANAGEMENT

Failure to protect information can be seen mainly as a management failure and cannot be solved by technology alone. ISACA – the International Association of Experts for Auditing and Control of Information Systems – emphasizes that it is necessary to raise consideration of the need for adequate protection of information resources to the level of the highest management bodies of every business organization, as is done for other critical management functions. To achieve a significant improvement in information security, senior management and boards of directors must be responsible for information security management. They must provide the necessary leadership, organizational structure, oversight, resources, and processes to ensure that information security management is an integral and transparent part of governing the organization's business operations. Since information security risk is a business risk and has a direct impact on business goals, the responsibility for establishing an appropriate information security program must be balanced between security professionals and business leaders. (ISACA, 2022)

Those who understand the scope and depth of information risks increasingly say that information, as a critical resource, must be treated with the same care, caution, and prudence as any other for the business organization's survival critical asset.

Previously, the focus of protection was often on the IT systems that process and store the vast majority of information, and not on the information itself. However, today this approach is considered too narrow to achieve the level of integration, process assurance, and overall security that is really needed. Information security takes the broader view that content information and knowledge based on it must be adequately protected, regardless of how it is handled, processed, transmitted, or stored. This protection increasingly includes the need to consider security issues associated with technologies based on cloud computing and other virtual technology platforms. Business organizations exist to create value for their stakeholders. Therefore, every organization - commercial or not - has value creation as a management objective. Creating value means realizing benefits with optimal use of resources and risk optimization. Benefits can take many forms, such as: financial for commercial enterprises and high-quality public service for state entities. (ISACA, 2022)

The increasing dependence on information and supporting systems and the growing risk of numerous threats force management to make difficult and often expensive decisions about effectively solving the information security problem. In addition, numerous new and existing laws and regulations increasingly require compliance and a higher level of accountability due to governments' efforts to address sophisticated attacks and growing losses that pose an increasing threat to the nation's critical infrastructure. (ISACA, 2022)

3 AREA OF APPLICATION OF INFORMATION SECURITY

Information security deals with all aspects of information in any medium (eg, written, spoken, electronic), regardless of whether the information is created, viewed, transmitted, stored, or destroyed. It differs from IT security, which deals with information security within the boundaries of a technology domain, usually in a custodial capacity. It is significant to pay attention to this difference. The IT department usually does not own most of the information in its systems; instead usually, it just owns devices that process information. Information is under the supervision, control, and custody of the IT, and the IT functions as the custodian of the data owner. (ISACA, 2021)

Professional literature mentions cyber security as a particular topic and concept and as an area of specific concern, significant for the management of overall information security. Although definitions

vary widely, it is commonly believed that cybersecurity is a sub-discipline of information security. Specific areas covered by cyber security include Advanced Persistent Threats (APT), malware, ransomware, identity theft in all its forms, and several other cyber-related threats. It should be remembered that in many areas in recent years there has been a convergence of cyber security and information security. (ISACA, 2021)

In the context of information security management, it is important that the scope and responsibilities of information security are clearly stated in the information security strategy and reflected in the policies. It is also essential that information security is fully supported by senior management and various organizational units. Without clearly defined responsibilities for information security, it is impossible to assign responsibility. (ISACA, 2021)

4 ASSESSMENT AND EVALUATION OF CYBER SECURITY MANAGEMENT

When performing an internal audit engagement that includes cybersecurity objectives in their scope, internal auditors must assess whether the organization's management processes adequately address cybersecurity.

According to the IIA Cybersecurity, Topical Requirements are structured to guide performing internal audit services in three areas: governance, risk management, and control processes. Each area includes (IIA, 2024 b):

- Requirements, which are mandatory and cover essential organizational objectives.
- Considerations, which are not mandatory but serve as best practices for evaluating the design and implementation of organizational objectives.

For example, in the Evaluating and Assessing Cybersecurity Governance domain, it is stated that auditors must assess whether Policies and procedures related to cybersecurity risk management processes are established and periodically updated, including the promotion of practices that strengthen the control environment based on widely adopted frameworks (NIST, COBIT, and others).

Considerations for this Governance Requirement are: To assess how the essential governance processes are applied to cybersecurity objectives, internal auditors may review:

Policies, procedures, and other relevant documentation used by the organization to oversee daily cybersecurity duties including:

1. Documents that are clear, concise, consistent, and regularly updated, particularly as new cybersecurity risks emerge and no less than annually.
2. Procedures concerning the identification, analysis, resolution, and reporting of breaches or other instances of sensitive data loss.
3. Documentation detailing how management ensures those policies and procedures are adequate to uphold cybersecurity operations. (IIA, 2024-b)

In Evaluating and Assessing Cybersecurity Risk Management, we find Requirement: A process is established to identify and manage cybersecurity risks related to third parties. Vendors, suppliers, and other providers of outsourced processes and/or services are contractually required to implement effective cybersecurity controls that adequately protect the confidentiality, integrity, and availability of the organization's systems and data to which third parties have access.

The appropriate considerations are (IIA, 2024 b):

- To assess the required aspects of cybersecurity risk management, internal auditors may review the organization's process for managing third-party cybersecurity risks.
- To verify that vendor cybersecurity controls are applied before starting a business relationship and that contracts build in the right to periodic reviews throughout the relationship.
- To include obtaining and analyzing the third party's service organization controls report and verifying the organization has documented its SOC report review, which should include ensuring user control considerations have been implemented.
- Gain an understanding of management's approach to determining if third parties have an appropriate control environment that is

commensurate with the organization's controls.

When it comes to the area of Evaluating and Assessing Cybersecurity Control Processes, as an example we will cite Requirements: Adequately integrates cybersecurity into the system development life cycle for business applications, including software and acquired or custom-developed applications.

The appropriate considerations are: How the organization addresses cybersecurity within its system development life cycle, including the following control aspects:

1. Planning: Cybersecurity has been identified as a key component when assessing risks and analyzing potential vulnerabilities. The scope and objectives of the software implementation should be included as the organization evaluates cybersecurity controls during the planning phase.
2. Gathering requirements: Cybersecurity requirements are a component when defining functional requirements, which should also include complying with all applicable legal and regulatory requirements.
3. Design: Cybersecurity considerations are included as an integral part of the detailed processing requirements. Controls should be identified in all design aspects as the organization more formally defines the needs of the system architecture design (such as platforms, user interfaces, databases, and others).
4. Development: The organization has established a secure environment and formally defined a development process that minimizes cyber vulnerabilities (for example, limited user access to development code, appropriate segregation from the production environment, the use of approved tools, the existence of audit trails to track development activities, specific cybersecurity requirements for vendor-developed software, and others).
5. Testing: The organization includes the review and assessment of cybersecurity during the testing phase (for example, automated testing, penetration testing, and vulnerability assessment). The organization should be able to quickly be alerted to and address any cyber vulnerabilities identified through testing, which includes a detailed description of the vulnerability and what code changes or mitigating controls were established in response.
6. Deployment: As new software is moved into production, the organization should carefully monitor potential cybersecurity threats, including ensuring end-users have been trained to use the software in a way that minimizes cybersecurity risks. The organization should ensure that events and errors are logged and analyzed related to potential cybersecurity events.
7. Maintenance: The organization should ensure that all security-related software releases are applied promptly and should have open communication with software vendors to ensure emerging risks and threats are properly controlled and that end-users are informed of any known vulnerabilities. (IIA, 2024 b)

5 MAPPING WITH REQUIREMENTS FROM ISO/IEC 27001

By analyzing each of the IIA Cybersecurity Topical Requirements, we find a corresponding mapping to one or more controls and processes from the international standard ISO/IEC 27001. (ISO/IEC, 2022 a)

For example, for the IIA Cybersecurity Topical Requirement:

“Internal auditors must assess if the organization has implemented appropriate physical security controls to protect high-risk information centers (such as data centers, network operations centers, and security operations centers) from attacks”

we find the following possible mappings with ISO/IEC 27001 controls:

7.1. Physical controls
7.2. Physical security perimeters
7.3. Physical entry
7.4. Securing offices, rooms, and facilities
7.5. Physical security monitoring
7.6. Protecting against physical and environmental threats

For each of the controls in the international standard ISO/IEC 27002, we can find

recommendations regarding their implementation. (ISO/IEC, 2022 b)

So, for example, for 7.6 Protecting against physical and environmental threats, the control description is stated: Protection against physical and environmental threats, such as natural disasters and other intentional or unintentional physical threats to the infrastructure should be designed and implemented. The purpose of control is to prevent or reduce the consequences of events originating from physical and environmental threats. The guidance for implementation is risk assessment to identify the potential consequences of physical and environmental threats. It should be performed at a physical site before beginning critical operations and at regular intervals. Necessary safeguards should be implemented and changes to threats should be monitored. Specialist's advice should be obtained on how to manage risks arising from physical and environmental threats such as fire, flood, earthquake, explosion, civil unrest, toxic waste, environmental emissions, and other forms of natural disasters or disasters caused by human beings…(ISO/IEC, 2022 b)

When it comes to assessing the level of implementation, the following scale, which can be found in professional literature, can be useful (ISO27k Forum, 2022):

1. Nonexistent - Complete lack of recognizable policy, procedure, control, etc.
2. Initial - Development has barely started and will require significant work to fulfill the requirements
3. Limited - Progressing nicely but not yet complete
4. Defined - Development is more or less complete although detail is lacking and/or it is not yet implemented, enforced, and actively supported by top management
5. Managed - Development is complete, the process/control has been implemented, and recently started operating
6. Optimized - The requirement is fully satisfied, is operating fully as expected, is being actively monitored and improved, and there is substantial evidence to prove all that to the auditors

The levels of implementation can further be expressed in the form of a scale from 0 to 5, and the level of implementation could be more clearly displayed on a scale from 0 to 1 - for example in Figure 1.

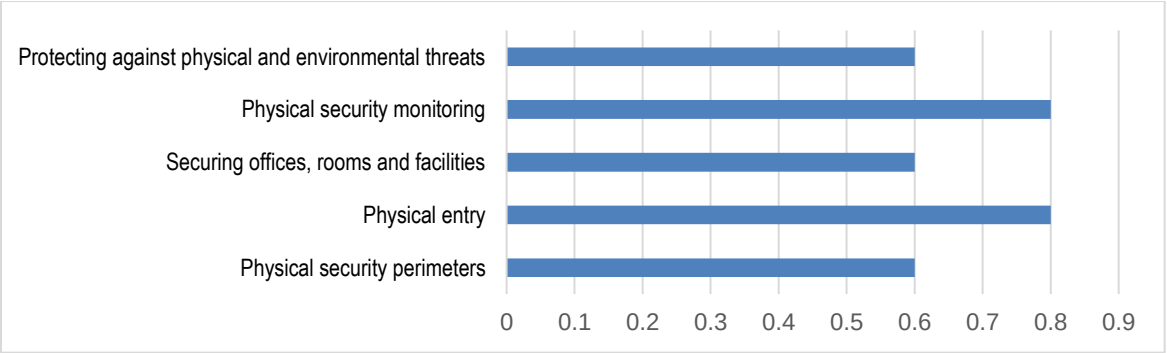


Fig. 1 An example of the achieved level of implementation

6 CONCLUSIONS

IIA's activities on the Cybersecurity Topical Requirement development will certainly contribute to increasing the cyber security level in business organizations. Given that it is possible to map the requirements from the IIA Cybersecurity Topical Requirement with the requirements from the ISO/IEC 27001 standard, we think that it is necessary to use the existing good practices related to the use of this and related standards in terms of compliance with the IIA requirements. The example of the level of compliance presented in the paper, which consists of 5 levels, can give auditors and security managers a more realistic picture of the level of compliance achieved, and areas where more efforts need to be made to overcome the discrepancy between the existing and the desired state.

WORKS CITED

ISACA. (2021, Mar 31). *Cybersecurity Fundamentals Study Guide*, 3rd Edition. ISBN 978-1604207514. Isaca

ISACA. (2022, Feb 28). *CISM Review Manual, 16th Edition*. ISBN 978-1604209013. Isaca

IIA. (2024a). *Risk in Focus 2024 Global Summary*. Retrieved from The Institute of Internal Auditors, https://www.theiia.org/en/internal-audit-foundation/latest-research-and-products/risk-in-focus/

IIA. (2024b). *Cybersecurity Topical Requirement.* Retrieved from The Institute of Internal Auditors, https://www.theiia.org/globalassets/site/standards/editable-versions/cybersecurity-topical-requirement-english.pdf

ISO/IEC. (2022a). ISO/IEC 27001:2022, Information security, cybersecurity and privacy protection — Information security management systems — Requirements. Retrieved from ISO, https://www.iso.org/standard/27001

ISO/IEC. (2022b). ISO/IEC 27002:2022, Information security, cybersecurity, and privacy protection — Information security controls. Retrieved from ISO, https://www.iso.org/standard/75652.html

ISO27k Forum. (2022). ISO/IEC 27001:2022 ISMS Status, Statement of Applicability (SoA), and Controls Status (gap analysis) workbook. Retrieved from ISO, https://www.iso27001security.com/ISO27k_ISMS_6.1_SoA_2022.xlsx

Received for publication: 05.08.2024
Revision received: 17.08.2024
Accepted for publication: 08.01.2025.

How to cite this article?

Style – **APA** *Sixth Edition:*

Hamidovic, H. (2025, 01 15). IIA Cybersecurity Topical Requirement and ISO/IEC 27001. (Z. Cekerevac, Ed.) *MEST Journal, 13*(1), 76-81. doi:10.12709/mest.13.13.01.07

Style – **Chicago** *Sixteenth Edition:*

Hamidovic, Haris. "IIA Cybersecurity Topical Requirement and ISO/IEC 27001." Edited by Zoran Cekerevac. *MEST Journal* (MESTE) 13, no. 1 (01 2025): 76-81.

Style – **GOST** *Name Sort:*

Hamidovic Haris IIA Cybersecurity Topical Requirement and ISO/IEC 27001 [Journal] // MEST Journal / ed. Cekerevac Zoran. - Belgrade – Toronto : MESTE, 01 15, 2025. - 1 : Vol. 13. - pp. 76-81.

Style – **Harvard** *Anglia:*

Hamidovic, H., 2025. IIA Cybersecurity Topical Requirement and ISO/IEC 27001. *MEST Journal,* 15 01, 13(1), pp. 76-81.

Style – **ISO 690** *Numerical Reference:*

IIA Cybersecurity Topical Requirement and ISO/IEC 27001. **Hamidovic, Haris.** [ed.] Zoran Cekerevac. 1, Belgrade – Toronto : MESTE, 01 15, 2025, MEST Journal, Vol. 13, pp. 76-81.

MEST Journal
DOI 10.12709/mest.13.13.01.08

ENHANCING IT MATURITY THROUGH IT GENERAL CONTROLS (ITGC) AUDITS

Haris Hamidovic
MKF/MKD EKI Sarajevo, Sarajevo, Bosnia and Herzegovina
https://orcid.org/0000-0002-1296-5008

JEL Category: **K22, M15**

Abstract

IT General Controls (ITGC) audits are vital for organizations that rely on information technology, as they offer independent assurance regarding the effectiveness of internal controls, governance, and risk management. This process enables management to understand the strengths and weaknesses of their IT controls and receive practical recommendations for improvement. Using best practice frameworks from IIA and ISACA, ITGC audits align with industry standards, helping organizations meet legal and regulatory requirements while supporting secure and efficient IT operations. Competent auditors, equipped with formal education, experience, and certifications like CISA, CISM, CRISC, and CISSP play a critical role in these audits. They ensure that IT systems and processes comply with governance criteria, protect data integrity, confidentiality, and availability, and align IT operations with organizational objectives. Through ITGC audits, auditors can identify risks in areas such as change management, logical access, business continuity, and physical security, helping organizations enhance their IT maturity and resilience.

Keywords: IT General Controls, ITGC, GITC, IT audit, Risk Management, Information Security.

1 INTRODUCTION

The purpose of the audit function is to provide management and senior leadership with independent assurance concerning internal controls, governance, and the organization's risk management activities. While the board and stakeholders define the mission and strategy of the enterprise, management is responsible for executing them. Auditors play a crucial role in independently and objectively ensuring that management activities are aligned with corporate objectives.

Different types of audits include (ISACA, 2022):

- IT Audit: Assessment of IT systems and security controls.
- Financial Audit: Verification of financial data accuracy.
- Operational Audit: Evaluation of efficiency and effectiveness.
- Integrated Audit: A combination of financial, operational, and IT audits.

Each type of audit helps an organization maintain comprehensive control over business operations and ensure compliance with laws and standards.

Address of the corresponding author:
Haris Hamidović
haris.hamidovic@eki.ba

An IT audit is a formal examination and/or testing of information systems aimed at determining whether (ISACA, 2022):

- IT systems meet applicable laws, regulations, contracts, and/or industry guidelines.
- IT systems and processes comply with governance criteria and relevant policies and procedures.
- Data has appropriate levels of confidentiality, integrity, and availability.
- IT operations are conducted efficiently and aligned with objectives.

The IT audit also assesses whether the internal controls implemented by management provide reasonable assurance that business objectives will be met and that undesired events are either prevented or promptly detected and corrected.

Examples of audits that may fall under IT audit evaluations include (ISACA, 2022):

- IT General Controls (ITGC) audits
- Application audits
- IT process audits
- Cybersecurity audits
- IT governance audits
- IT infrastructure audits
- Physical security audits
- IT compliance audits
- Business continuity and disaster recovery audits

This paper provides an overview of the concept and components of IT General Controls (ITGC) auditing.

2 IT GENERAL CONTROLS (ITGC)

The Institute of Internal Auditors (IIA), a leading global authority in internal auditing, emphasizes in its Global Technology Audit Guide (GTAG) 1 that “internal auditor must understand the range of controls available for mitigating IT risks. Controls may be classified to clarify their purposes and where they fit within the overall system of internal controls. By understanding these classifications, control analysts and auditors are better equipped to position them within the control framework and address key questions, such as: Are detective controls adequate for identifying errors that might bypass preventive controls? Are corrective controls sufficient for addressing errors once detected?” Figure 1 presents one of the control classifications, as illustrated in the IIA's GTAG 1 document. (IIA, 2012)

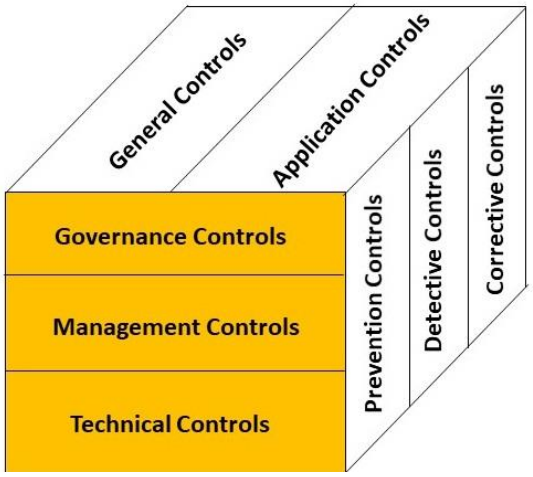


Figure 1. Control classifications according to IIA’s GTAG 1

Source: (IIA, 2012)

A common classification of IT controls is between general and application controls. (IIA, 2012)

ISACA defines IT General Controls (ITGC) in its IT Audit Fundamentals Study Guide as follows: “A general computer (IT) control is a control, other than an application control, that relates to the environment within which computer-based application systems are developed, maintained, and operated, and is therefore applicable to all applications. The objectives of general controls are to ensure the proper development and implementation of applications, as well as the integrity of program and data files and/or computer operations. Like application controls, general controls may be either manual or programmed. General controls support the entire enterprise in a centralized manner as part of the IT infrastructure. Since the infrastructure is often shared among different departments within the same organization, the term "general controls" is also used to describe all controls in the infrastructure, including those that support operating systems, networks, or facilities. These controls typically include centralized user administration policies, standards and procedures, and technical elements such as access controls, firewalls, and intrusion detection systems.” (ISACA, 2022)

In the field of IT audit, "IT General Controls" (ITGC) and "General IT Controls" (GITC) are used interchangeably, but for this paper, we will use the abbreviation ITGC.

According to ISACA guidelines, common IT general controls (ITGC) include the following (ISACA, 2022):

- Logical access controls
- Change, patch, release, and configuration management controls
- Data backup, storage, and recovery controls
- Business continuity and disaster recovery controls
- IT operations controls
- Physical access and environmental controls
- System development life cycle (SDLC) controls

On the other hand, ISACA defines application controls as the policies, procedures, and activities designed to provide reasonable assurance that objectives relevant to a given automated solution (application) are achieved. As such, application controls are controls over input, processing, and output functions. They include methods for ensuring that (ISACA, 2022):

- Only complete, accurate, and valid data are entered and updated in a computer system.
- Processing accomplishes the correct task.
- Processing results meet expectations.
- Data are maintained completely and accurately and are available for reporting.

3 BASIC PHASES OF ITGC AUDIT

IT audit consists of three basic phases (ISACA, 2022):

1. Planning: The scope and methodology of the audit are defined, including resource allocation and a timeline.
2. Fieldwork: Evidence is gathered and analyzed through control testing and system assessment.
3. Reporting: In this phase, the auditor presents findings and makes recommendations to key stakeholders.

The goal of each phase is to ensure that the audit process is comprehensive and focused on achieving relevant business objectives.

During the preparation of IT auditors for an ITGC audit, the recommendations provided in guidelines for IT auditors, published by professional auditing associations such as the IIA and ISACA, can be of great assistance. For example, the IIA, in its handbook Fundamentals of IT Audit for Operational Auditors, lists example documents or sources of information that may be collected by the internal auditor during an ITGC audit. For example, during the SLDC audit, the IT auditor should pay attention to the following records (IIA, 2022):

- The project framework contains scope, objectives, team composition, timeline, consideration of changes, etc., with evidence of review/approval from the project owner and project sponsor.
- The project schedule (and related documents) outlining key tasks, dependencies, effort, resource assignments, and dates.
- Evidence of initial budget approval and any changes to the budget since the initial approval.
- Evidence of current budget monitoring tools used to manage/track the budget, ensuring all resource expenses are up to date.
- The business case for the project.
- A benefits realization strategy that includes a detailed plan to achieve the project/business goals, with timelines and milestones.
- Approved business, technical, and functional documentation, etc.

These guidelines can be of great practical use to new and experienced IT auditors as a foundation for preparation.

The ISACA CISA Review Manual is also an excellent practical tool for preparing IT auditors to conduct ITGC audits. Based on practical experience, it contains sets of questions designed to help auditors prepare for conducting audits. (ISACA, 2024).

An IT auditor should provide a balanced report, describing not only negative issues in terms of findings, but also giving positive, constructive comments regarding improved processes, controls, or the efficiency of existing controls. (ISACA, 2022) Unfortunately, in practice, auditors often highlight what is wrong, making it difficult for business stakeholders reading the report to understand the positive aspects of the ITGC environment within the organization. Given this, it could be beneficial to use a maturity model based on the ISACA COBIT framework during ITGC audits (ISACA, 2019), which would highlight the current maturity level of various ITGC components and could serve as a basis for developing an

improvement plan towards the desired state. Figure 2 provides a simplified graphical representation from ISACA COBIT 4.1, showing the current maturity level, the industry average (if known), and the desired maturity level. (ISACA, 2007)

Fig. 2 Example of the current maturity level, the industry average, and the desired maturity level
Source: (ISACA, 2007)

4 EXPECTATIONS OF AN IT AUDITOR

An IT auditor is expected to maintain a high level of professionalism and expertise, adhering to a code of ethics, ensuring impartiality, and applying due professional care. According to the IT audit code of ethics, the auditor must act with integrity, safeguard data confidentiality, and continually develop their skills. The auditor must remain objective, avoid conflicts of interest, and protect the autonomy of the IT audit function to ensure the quality and credibility of the entire audit process.

IT audit is expected to provide objective assessments that assist management in making informed decisions. Management is responsible for:

- Ensuring adequate IT resources,
- Implementing security measures and regulatory compliance,
- Defining internal policies to regulate employee behavior.

IT auditor evaluates these aspects, tests their application, and identifies areas that need improvement.

According to the IT Audit Framework, IT audit and assurance practitioners should (ISACA, 2020):

- Demonstrate sufficient professional competencies—such as relevant skills, knowledge, and experience—before commencing the planned engagement.
- Evaluate alternative methods for acquiring the necessary skills to perform the engagement. This may involve subcontracting, outsourcing certain tasks, postponing the assignment until the skills are available, or otherwise ensuring the availability of appropriate expertise.
- Ensure that team members involved in the IT audit and assurance engagement possess either a CISA certification or another relevant professional designation, along with adequate formal education, training, and work experience.
- Provide reasonable assurance, when leading an IT audit or assurance engagement, that all team members have the requisite professional competency to carry out their assigned tasks.
- Possess sufficient knowledge of key areas necessary to effectively and efficiently conduct the IT audit or assurance engagement, in collaboration with other team members and any involved specialists.
- Meet the continuing professional education or development requirements associated with CISA or other relevant professional designations.
- Regularly update professional knowledge through educational courses, seminars, conferences, webcasts, and on-the-job training, ensuring a level of professional

service appropriate to the IT audit or assurance role.
- Consider utilizing external resources if the required competencies are unlikely to be available within the necessary timeframe.

For specialized audits, such as those focused on cybersecurity, additional respected certifications include ISACA's CISM and CRISC, as well as ISC2's CISSP. (IIA, 2015)

The Institute of Internal Auditors has developed a specialized program for internal auditors related to ITGC, which covers the following areas:

- Recognize the importance of the governance of enterprise IT.
- Associate project delivery with effective and efficient technology-driven processes.
- Realize the impact technology has on business processes.
- Identify and assess basic IT general controls related to:
- IT Change Management,
- Business Resilience,
- Logical Security,
- Physical Security,
- Environmental Controls,
- IT Operations and Services Management,
- System Development Life Cycle.

This program is designed to enhance the internal auditors' skills in assessing critical areas of ITGC, helping them support organizational governance and security.

5 CASE STUDY: ITGC AUDIT IN A PUBLIC HEALTHCARE INSTITUTION

A public healthcare institution struggled with outdated IT systems and insufficient data management controls, especially concerning patient data security. The lack of a centralized IT governance strategy increased the risk of data breaches and non-compliance with regulations like GDPR and national healthcare standards.

ITGC Audit Implementation:

The audit focused on addressing vulnerabilities in three critical areas:

1. *Access Controls*: Assessing who has access to sensitive data and how access is granted and monitored.
2. *Change Management*: Evaluating the procedures for updating and maintaining IT systems.
3. *Operational Resilience*: Ensuring reliable data backups and testing disaster recovery plans.

Findings:

- Unauthorized access was identified due to poorly defined access control policies.
- Software updates were managed informally, leading to unplanned system downtimes.
- Backup systems were unreliable and did not cover all critical data repositories.

Actions Taken:

- A centralized access control system was implemented, incorporating multi-factor authentication and regular audits.
- Standardized procedures for approving and testing IT system changes were introduced.
- Automated backup processes were established, with regular disaster recovery testing.

Outcomes:

- Compliance with regulatory requirements significantly improved, reducing the risk of data breaches.
- Operational resilience was enhanced, ensuring faster recovery from potential incidents.
- Trust from patients and regulatory authorities in the institution's data management practices increased.

This example demonstrates how ITGC audits can help public institutions strengthen IT governance, improve data protection, and achieve regulatory compliance.

In the article "Six ITGC audit controls to improve business continuity" on TechTarget, the author provides a sample checklist that can serve as a starting point for planning, scheduling, and conducting an ITGC audit. These six critical ITGC controls include essential areas such as access management, change management, and disaster recovery, among others. These controls form a comprehensive framework that helps organizations ensure effective IT governance, mitigate risks, and improve business continuity strategies. The checklist offers actionable steps for conducting a thorough ITGC audit and is a

practical guide for auditors and IT managers. (TechTarget, n.d.).

6 CONCLUSIONS

The audit of IT General Controls (ITGC) is crucial for all business organizations that rely on information technology, as it ensures the reliability, security, and integrity of their IT systems. By following established best practice frameworks developed by the Institute of Internal Auditors (IIA) and ISACA, organizations can standardize their ITGC audits, enhancing both their effectiveness and alignment with industry standards. Competent auditors, with formal education, practical experience, and recognized IT audit and security certifications, are essential for conducting these audits effectively. This expertise enables auditors to provide management with objective assurance on the current state of ITGC controls. Additionally, auditors can offer practical recommendations to improve the maturity level of these controls, helping organizations mitigate risks and strengthen their IT infrastructure in line with evolving industry demands.

WORKS CITED

IIA. (2012). Global Technology Audit Guide (GTAG) 1 Information Technology Risk and Controls, 2nd Edition

IIA. (2015). Lifelong learning for internal auditors

IIA. (2022). Fundamentals of IT Audit for Operational Auditors

ISACA. (2007). COBIT 4.1: Framework for IT Governance and Control

ISACA. (2019). COBIT 2019 Framework: Governance and Management Objectives

ISACA. (2020). IT Audit Framework (ITAF): A Professional Practices Framework for IT Audit, 4th Edition

ISACA. (2022). IT Audit Fundamentals Study Guide

ISACA. (2024). CISA Review Manual

TechTarget. (n.d.). Six ITGC audit controls to improve business continuity. Retrieved December 10, 2024, from https://www.techtarget.com/searchdisasterrecovery/tip/Six-ITGC-audit-controls-to-improve-business-continuity

Received for publication: 05.08.2024
Revision received: 17.08.2024
Accepted for publication: 08.01.2025.

How to cite this article?

Style – **APA** *Sixth Edition:*

Hamidovic, H. (2025, 01 15). Enhancing IT Maturity through IT General Controls (ITGC) Audits. (Z. Cekerevac, Ed.) *MEST Journal, 13*(1), 82-88. doi:10.12709/mest.13.13.01.08

Style – **Chicago** *Sixteenth Edition:*

Hamidovic, Haris. "Enhancing IT Maturity through IT General Controls (ITGC) Audits." Edited by Zoran Cekerevac. *MEST Journal* (MESTE) 13, no. 1 (01 2025): 82-88.

Style – **GOST** *Name Sort:*

Hamidovic Haris Enhancing IT Maturity through IT General Controls (ITGC) Audits [Journal] // MEST Journal / ed. Cekerevac Zoran. - Belgrade – Toronto : MESTE, 01 15, 2025. - 1 : Vol. 13. - pp. 82-88.

Style – **Harvard** *Anglia:*

Hamidovic, H., 2025. Enhancing IT Maturity through IT General Controls (ITGC) Audits. *MEST Journal,* 15 01, 13(1), pp. 82-88.

Style – **ISO 690** *Numerical Reference:*

Enhancing IT Maturity through IT General Controls (ITGC) Audits. **Hamidovic, Haris.** [ed.] Zoran Cekerevac. 1, Belgrade – Toronto : MESTE, 01 15, 2025, MEST Journal, Vol. 13, pp. 82-88.

MEST Journal
DOI 10.12709/mest.13.13.01.09

THE EVOLUTION OF REINSURANCE SUPPLY IN ALGERIA: AN ANALYTICAL STUDY

Aboubaker Khoualed
Badji Mokhtar University, Annaba, Algeria
https://orcid.org/0009-0004-0042-0184

Khayreddine Bouzerb
Mohamed Seddik Benyahia, Jijel, Algeria
https://orcid.org/0000-0003-4096-7497

Hassiba Almi
Badji Mokhtar University, Annaba, Algeria
https://orcid.org/0009-0001-7560-754X

JEL Category: **G22**

Abstract

This study aims to analyze the development of the reinsurance offering in Algeria by examining the evolution of national acceptances, primarily represented by the premiums accepted by the Central Reinsurance Company (CCR), and international acceptances by foreign reinsurance companies during the period (2010-2023). The study mainly employs a qualitative descriptive approach. The research concluded that, since the implementation of Executive Decree No. 10-207, the mandatory cession rate to the CCR has increased to 50%, leading to a rise in the volume of premiums accepted locally to over 90% of the CCR's total activity. In contrast, international premiums did not exceed an average of 10%. Although national acceptances constitute the bulk of the CCR's business, the company has achieved notable progress in the international market in recent years thanks to policies aimed at expanding its external activities. The dominance of the local market is attributed to the CCR's monopoly over national acceptances, enhancing its capacity to absorb major risks in the local market, particularly in the IARDT (Fire, Accidents, Miscellaneous Risks, and Transport) branch and natural disasters. However, the company faces challenges in the international market, including intense competition in Europe. In conclusion, the research highlights the importance of developing the Algerian reinsurance market by updating the legislative framework and creating a competitive environment, which would enhance the ability of Algeria to manage risks more effectively locally and internationally.

Keywords: *Reinsurance; Reinsurance Premiums; National Acceptances; International Acceptances; Retained Premiums; Ceded Premiums; Central Reinsurance Company.*

Address of the corresponding author:
Aboubaker Khoualed
aboubaker.khoualed@univ-annaba.dz

1 INTRODUCTION

Despite its importance in insurance and financial markets, reinsurance has received little attention in economic and financial literature (Berger, Cummins, & Tennyson, 1992). It becomes evident that research in the field of reinsurance is quite recent. Even by the early 1990s, specialized studies were scarce and limited to works such as (Mayers & Smith, 1990), (Hoerger, Sloan, & Hassan, 1990), and (Doherty & Fine, 1981).

The first question that comes to mind when addressing this topic is: How did the concept of reinsurance originate? Generally, the answer lies in the fact that insurance companies issue policies and collect premiums in exchange for the promise to pay claims when accidents occur. For many types of insurance, the gap between the occurrence of an accident and its settlement can span several years. If an insurance company defaults during this period, policyholders may lose part of their claims. Therefore, the ultimate concern of any policyholder is the continued financial viability of the insurance company. This scenario presents several challenges, most notably (Cummins, Dionne, Gagné, & Nouira, 2021) (Weiss, 2007):

1. Policyholders cannot diversify their risks by using multiple insurance companies.
2. Policyholders cannot monitor insurance companies due to the high costs and expertise required.
3. The cyclical nature of the insurance business and the inherent risks in its operations.

From this context, the idea of reinsurance emerged, where an insurance company, called a reinsurer, accepts all or part of the loss risks covered by another insurance company, known as the ceding company (Graven & Tennant, 2003) (Crisafulli, 2023). In other words, reinsurance is a legal insurance contract whereby the reinsurer agrees to compensate the ceding insurance company for a specified share of certain insurance claims paid by the ceding company for a single policy or a defined group of policies (Patrik, 2006).

To put it simply, reinsurance is "insurance for insurance companies." (Gbenro, Duramany-Lakkoh, & Kamara, 2023). Reinsurance is a way for insurance companies to manage risks and protect themselves from big financial losses. Using this tool, catastrophic risks such as climate risks, which are typically difficult to insure, become insurable by transferring the risks to reinsurance companies (Xiong, Peng, & Nadarajah, 2023).

Because the concepts of reinsurance and co-insurance are often confused, it is significant to distinguish between them. Co-insurance is a process in which several insurers (insurance companies) cover the same risk under a single insurance contract, with risks distributed in equal or unequal shares as agreed upon. The management responsibility, from the beginning of the contract to its termination or cancellation, is assigned to the principal insurer, who receives a commission for this role (Driessen, Fragnelli, Katsev, & Khmelnitskaya, 2015) (Olubajo, 2003). This type of insurance is typically used for major risks, such as environmental pollution (Driessen, Fragnelli, Katsev, & Khmelnitskaya, 2015).

The following diagram illustrates the difference between reinsurance and co-insurance in a simplified manner:

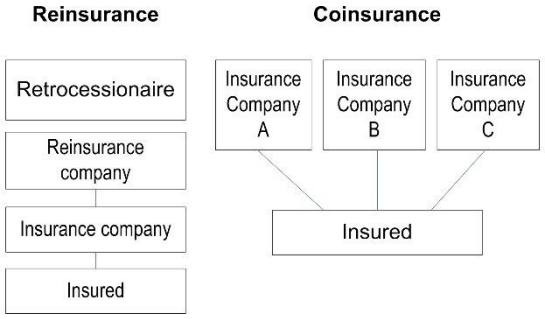


Fig. 1 The difference between reinsurance and co-insurance (Wehrhahn, 2009)

The reinsurance plays a significant role in absorbing the risks inherent in the direct insurance industry. It serves two main purposes:

- Reinsurance capital allows direct insurance companies to underwrite more business.
- Reinsurance capital protects insurance companies from budgetary fluctuations caused by large and unexpected losses (Haueter, 2020).

It is observed that the risks borne by insurance companies are not highly diversified, as these companies tend to specialize geographically and technically to make their distribution structures profitable and leverage their underwriting expertise. This highlights the importance of reinsurance in enabling insurance companies to

mitigate the surges in risk levels. Reinsurance companies use actuarial models more intensively because they bear the most hazardous and least diversified portion of the claims (Deelstra & Plantin, 2014).

Therefore, reinsurance helps reduce insolvency risk, enhances the financial viability of insurance companies, mitigates losses, smooths the insurance cycle, and reduces agency costs (Bernard, 2013). Overall, reinsurance serves the following functions: increasing underwriting capacity, reducing equity capital constraints, decreasing the variability of technical results, lowering unearned premium reserves, providing protection against catastrophic loss (Crisafulli, 2023), reducing expected taxes by exploiting specific tax structures, and gaining comparative advantages in delivering real services (Cummins, Dionne, Gagné, & Nouira, 2021). It also opens new horizons and greater business opportunities in consulting services through partnerships between reinsurers and insurance companies (Witthoff, 2020).

While reinsurance may be a relatively recent concept for the global economy, in Algeria, it is even more nascent, with the market still in its early stages in terms of legislative and institutional frameworks, activity volume, coverage, risk types, acceptances, and all other indicators of the reinsurance industry. Algeria has only one reinsurer, the Central Reinsurance Company (CCR). Additionally, even in terms of academic research on reinsurance in Algeria, the reality shows a very limited number of specialized studies in this field.

1.1 Study Problem

Like all other sectors, the interaction between supply and demand for reinsurance operations is subject to market forces and mechanisms. Algerian insurance companies, representing the demand side, seek coverage for part or all the risks that exceed their capacity. On the other hand, reinsurance companies in general, and the Central Reinsurance Company (CCR) in particular, representing the supply side, agree to provide coverage. This research paper will analyze the development of reinsurance supply in the Algerian market by studying the evolution of both national and international acceptances following the issuance of Executive Decree No. 10-207 on September 9, 2010. This decree mandates that at least 50% of all reinsurance business must be ceded to the national reinsurer (CCR), compelling Algerian insurance companies and CCR to adhere to this regulation, thereby affecting the supply of reinsurance in the Algerian market.

Given the context, the research phenomenon can be framed through the following main question:

> *What is the status of the development of national and international acceptances in the Algerian reinsurance market after the issuance of Executive Decree No. 10-207?*

1.2 Study objectives

The primary purpose of this study is to analyze the development of the reinsurance supply in Algeria by tracking the evolution of national acceptances, represented by the premiums accepted by the Central Reinsurance Company (CCR), and international acceptances by global reinsurance companies during the study period of 2010-2023.

This analysis will provide insights into the current state of the reinsurance market in Algeria, including its various indicators, strengths, and weaknesses. Such understanding will be highly valuable in formulating significant recommendations to help develop the Algerian reinsurance market and enhance its competitive capacities both locally and internationally.

Additionally, this research aims to bridge the local research gap in this field. Previous Algerian studies addressing the topic of reinsurance in Algeria are very rare, and most available studies are written in French and Arabic, while studies in English are extremely limited.

2 LITERATURE REVIEW

The Algerian insurance and reinsurance market has undergone significant transformations in recent decades, with numerous studies addressing various aspects of the sector to support economic growth and market development.

The study by Bouzaher & Necira (2017) provided a fundamental analysis of the development of the reinsurance market in Algeria, highlighting the

factors that could boost demand in the national reinsurance market. It also examined the economic contributions of reinsurance and its interaction with the broader insurance market, offering a deeper understanding of the critical role reinsurance plays in Algeria.

Improving retention levels in reinsurance has been a key aspect of the Algerian insurance market development. The study by Cheraitia and Medjden (2020) explored this aspect by examining convex optimization techniques, offering insights into how these methods can be used to enhance risk management and pricing accuracy. This study is particularly relevant to the Algerian reinsurance market, where effective risk management practices through reinsurance cessions are essential for the stability and growth of the insurance sector.

Technological advancements have also played a significant role in shaping the Algerian insurance market, particularly in auto insurance, which accounts for more than 50% of the sector's total production. Oucherif and Touche (2023) developed advanced pricing systems using machine learning algorithms, which have the potential to revolutionize the way risks are assessed and priced. These innovations are crucial for improving the efficiency and accuracy of pricing models in the Algerian insurance market, contributing to better risk management, and enhancing the market's competitiveness.

Social and cultural factors have also been identified as key determinants of consumer behavior towards insurance products in Algeria. The study by Mahdjour and Benhabib (2017) found that religious beliefs negatively impact Algerian consumers' attitudes toward insurance, particularly in cases where insurance products conflict with religious values. This social and cultural dimension underscores the need for the insurance market to develop culturally sensitive products that align with the values and beliefs of Algerian consumers, presenting a challenge with significant implications for market penetration and acceptance.

In addition to technological, social, and cultural factors, the profitability of insurance companies in Algeria has been closely linked to risk management practices through reinsurance arrangements, as identified in a study by (Lazli & Bouakkaz (2024). Components such as disaster indicators and underwriting practices were identified as critical factors influencing profitability. The study's findings indicated that effective risk management is not only necessary for insurance and/or reinsurance companies but also contributes to the stability and growth of the entire market.

The regulatory environment has also played a significant role in shaping Algeria's reinsurance market. Despite efforts to liberalize the insurance sector, the reinsurance market remains dominated by the national reinsurer "CCR" (Caisse Centrale de Réassurance, formerly the Algerian Reinsurance Fund), resulting in limited competition in the reinsurance field. Several studies, including those by Altuntas, Garven, and Rauch (2018) and Cole and McCullough (2006), acknowledged the ineffectiveness of regulatory changes and highlighted the potential for market failure and insufficient coverage for catastrophic risks.

Demand for reinsurance in Algeria is also influenced by economic conditions, including trade openness and economic growth. Studies by Eling and Jia (2017), and Eling and Luhnen (2010) emphasized the impact of economic fluctuations, such as changes in oil prices, on the financial stability of insurance companies and their demand for reinsurance coverage. These studies underscore the interconnection between the economic environment and the stability of insurance and reinsurance markets.

Growth opportunities in Algeria's reinsurance market are emerging, driven by increased awareness of risk management and the importance of insurance among businesses and individuals. Cole, Lee, and McCullough (2007) discussed the potential for developing specialized reinsurance products, such as catastrophe bonds, which could enhance the market's capacity to handle large-scale risks.

(Kajwang, 2022) suggested that by adopting advanced analytics, artificial intelligence, and digital platforms, reinsurance companies could improve their competitiveness and better meet the needs of direct insurance companies.

3 METHODOLOGY

To address the research problem and contribute effectively to achieving its objectives, the descriptive methodology was adopted, which is considered one of the most suitable approaches for studying various social phenomena in general (Nassaji, 2015) (Creswell & Creswell, 2018) and economic and financial natural phenomena in particular.

Descriptive research aims to describe the studied phenomenon and its various characteristics (Gall, Gall, & Borg, 2007). Thus, descriptive research works to make precise and detailed observations and document phenomena of significance (Bhattacherjee, 2012). In other words, it aims to shed light on current issues and problems through an organized data collection process that enables a more detailed description of the situation, as compared to not using this method (Manjunatha, 2019).

There are several reasons why researchers propose using a qualitative descriptive method, most notably: when it is challenging to define a specific problem or research objectives clearly; when the research goals require a more detailed and in-depth understanding; when the objective is to study the occurrence of natural phenomena; when the researcher wishes to study several interconnected research policies; or when a more modern approach is needed (Furidha, 2013).

Regarding the sources of information, the study relied on various secondary sources, including books, journals, conferences, working papers, international reports, and specialized websites. Additionally, the study utilized a series of annual reports issued by the Central Reinsurance Company during the study period. It is important to note that all reports were in French, as it is the official language used in Algeria's financial and banking sector and its administration. These reports were translated and used for analysis and conclusion.

4 CENTRAL REINSURANCE COMPANY (CCR) ACTIVITY

Reinsurance offerings in Algeria are primarily represented by the acceptances of the Central Reinsurance Company (CCR). Therefore, we will first provide an overview of CCR as the national reinsurer, followed by an examination of the development of reinsurance offerings through the study of both international and national acceptances in the Algerian market.

4.1 Overview of the Central Reinsurance Company (CCR)

The Central Reinsurance Company (CCR) was established by Ordinance 54/73, dated October 1, 1973. It is a joint-stock company with a capital of 40 million DZD as of 1975, fully owned by the Algerian state, with its headquarters located in Ouled Fayet, Algiers. The company began its actual operations in 1975 by reinsuring risks ceded from national insurance companies. During this period, CCR benefited from a monopoly in the Algerian insurance market until 1995, when the market was liberalized. Despite this, CCR continues to hold a dominant position in the Algerian reinsurance sector, offering services across various branches of reinsurance to its clients both domestically and internationally. Moreover, CCR reinsures natural disasters under state guarantees, in addition to insuring all the insurance companies in the Algerian market.

CCR maintains commercial relationships with all Algerian insurance companies and numerous reinsurers and brokers worldwide. These professional relationships with the international reinsurance market are crucial nationally and internationally. They have enabled CCR to gain commercial expertise and reputation, while also allowing it to collaborate with foreign entities such as MED RE, AFRICA RE, and ARAB RE AWRIS, in which it is an active member of reinsurance syndicates. Thanks to its importance and the quality of its relationships, CCR currently competes with reinsurance companies in the Arab world, Africa, and Asia, participating in risk coverage in those regions. It is also an active member of the executive committee of FAIR and participates in the technical committees of reinsurance pools, owing to its extensive experience in reinsurance, such as the Arab Pool for Marine and Non-Marine, the African Pool for Aviation and Fire, and the Asian Pools for Non-Marine and Aviation.

In 2023, the CCR's capital reached 30 billion DZD, equivalent to 227 million USD. It has been rated B+ for financial strength by the American agency AM Best and carries a credit rating of BBB- (Issuer

Credit Rating, ICR). Additionally, CCR enjoys state guarantees for covering natural disaster risks. The mandatory cession rate in favor of CCR was raised to 50%, which significantly boosted its capital and business volume, reducing its reliance on agreements with the international reinsurance market in its favor. Consequently, CCR now controls a substantial market share, as reflected since the enforcement of Decree 10-207 in 2011. According to data provided by AM Best Rating, CCR has had the best technical performance among all reinsurers in the Middle East and North Africa (MENA) region over the past five years. One of the CCR's key strengths lies in the quality of its qualified and multidisciplinary human resources. Executives are carefully selected and undergo specialized reinsurance training, both nationally and internationally, with advanced training provided by the world's leading reinsurance companies, enabling CCR to serve its clients domestically and abroad.

4.2 Evolution of the Capital of the Central Reinsurance Company

Since its establishment, CCR has experienced capital growth, which we will outline as follows.

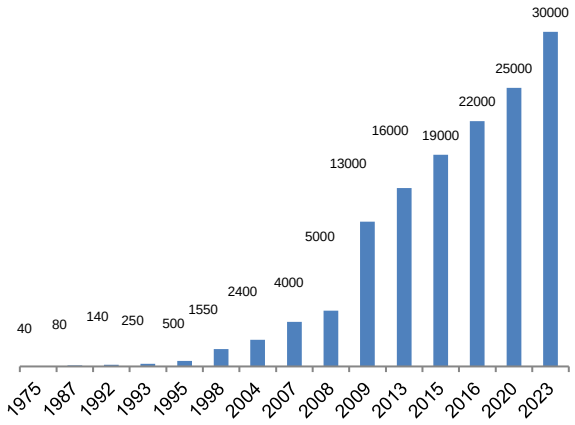


Fig. 2 Evolution of the CCR's Capital (1975-2023)

As observed from the figure above, the CCR's capital has shown continuous growth since its establishment. The highest growth rate was recorded in 1998, with an increase of 210%, as the capital grew from 500 million DZD in 1995 to 1.55 billion DZD in 1998. This significant increase resulted from the liberalization of the insurance and/or reinsurance market during that period and the CCR's entry into the international reinsurance market. Consequently, this step was essential for enhancing the CCR's competitiveness and its ability to offer attractive proposals to Algerian insurance companies.

Following this, the next notable growth occurred in 2009, with a capital increase of 160%, driven by the company's efforts to obtain ratings from global rating agencies. In recent years, from 2013 to 2020, the growth rates have been declining, recorded at (23%, 19%, 16%, 14%) for the years 2013, 2015, 2016, and 2020, respectively. However, in 2023, the capital rose significantly to 30 billion DZD, reflecting the company's financial strength.

Given the CCR's substantial connection to the international reinsurance market, it is essential to study the evolution of its capital in US dollars, which is detailed in:

Table. 1 Evolution of the CCR's Capital in USD during the period (1987-2023) (Compagnie centrale de réassurance, 2023).

Year	Capital (Million DZD)	Exchange Rate (USD)	Capital in USD (Million USD)
1987	80	87.91	0.9
1992	140	87.91	1.6
1993	250	87.91	2.8
1995	500	87.91	5.7
1998	1550	87.91	17.6
2004	2400	87.91	27.3
2007	4000	87.91	45.5
2008	5000	87.91	56.9
2009	13000	87.91	147.9
2013	16000	87.91	182
2015	19000	107.76	177.4
2016	22000	110.76	198.6
2017	22000	114.8	191.6
2018	22000	117.93	186.59
2019	22000	119.25	184.48
2020	25000	131.23	190.5
2023	30000	135.84	220,84

We observe that, despite the continuous growth of the CCR's capital in Algerian dinars, its growth in US dollars has been less significant. This discrepancy is due to changes in the exchange rate, which has seen a decline in recent years, beginning in 2017. This can be further illustrated in Figure 3.

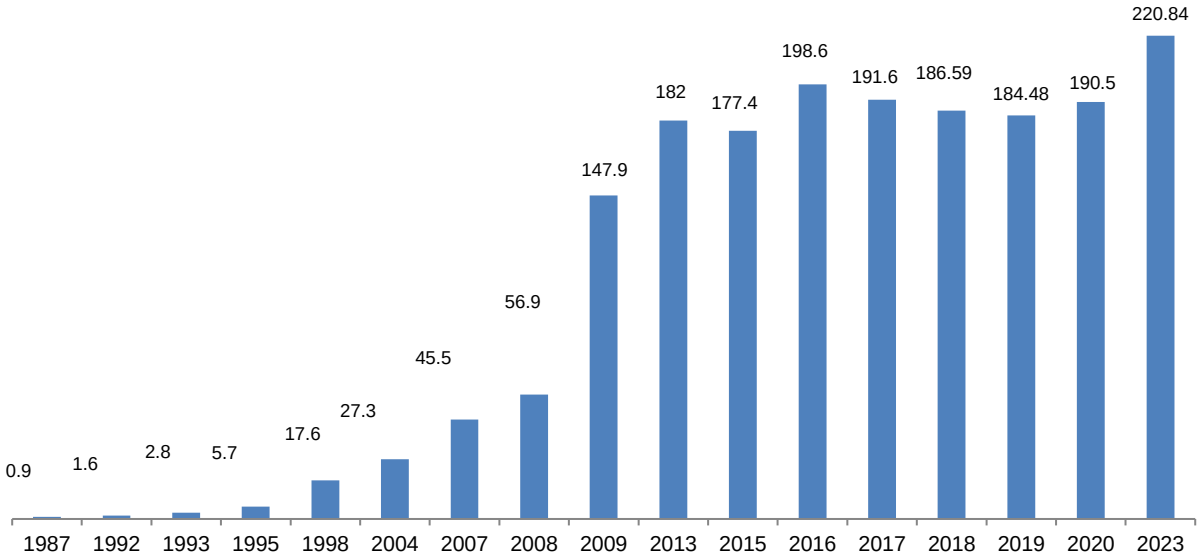


Fig.3 Evolution of the CCR's Capital in USD (in millions) from 1987 to 2023

Wwe observe that the growth rates were very similar during the early years, from 1987 to 2013, due to the stability of the exchange rate during this period. However, from 2015 onwards, there was volatility in the evolution of the CCR's capital values in US dollars. Despite the capital growth denominated in Algerian dinars, there was a decrease when evaluated in US dollars during 2015, 2017, 2018, and 2019, with the following respective rates: (-3%, -4%, -3%, -1%).

4.3 Branches in which the Central Reinsurance Company (CCR) operates

As CCR is a multi-branch reinsurance company, it provides coverage in all forms of reinsurance, whether in life reinsurance or non-life reinsurance. Furthermore, except for financial reinsurance (through capital markets), which the company does not engage in, CCR possesses the expertise and capabilities to handle all forms of proportional and non-proportional reinsurance. This can be differentiated between the domestic market and the international market:

4.3.1 Domestic Market

CCR offers its services to cedents in Algeria, covering their reinsurance needs across almost all branches of property and casualty insurance and life insurance. As the sole national reinsurance company specializing in reinsurance since its inception in Algeria, CCR responds to any coverage requests from its domestic clients in the following branches:

A. Non-marine branches:

These include fire and related risks, including business interruption, engineering risks, machinery breakdown, drilling equipment, natural disasters, motor, political risks, all forms of civil liability, decennial liability, agricultural risks, etc. For life insurance, the guarantees offered include assistance and travel, credit insurance, accidents, health insurance, etc., and all other insurance products previously mentioned, which are provided by property and casualty insurance companies as well as life insurance companies.

B. Marine branches:

These cover hull insurance for ships and aircraft, transported goods, including anticipated business interruption losses, civil liability for carriers (land, sea, and air), railway goods transport, war risks, and transport-related risks, etc.

4.3.2 International Reinsurance Market

CCR offers its capabilities to its partners in various regions (Africa, the Arab world, Asia, and Europe) within the international reinsurance market, covering major branches of activity: marine, non-marine, and energy. CCR has been operating in

the international market since its inception and, as a result, favors long-term commercial relationships with its partners. The proposed branches include treaty reinsurance in areas such as fire, engineering risks, transportation, motor, life, agricultural risks, etc. In facultative reinsurance, the branches include fire and related risks, land/marine risks, engineering risks (TRC/TRM/BDM), ship hulls, etc.

5 DEVELOPMENT OF DOMESTIC AND INTERNATIONAL ACCEPTANCES IN THE ALGERIAN REINSURANCE MARKET

Reinsurance offerings are represented by the volume of acceptances achieved by CCR, whether domestic or international. These acceptances reflect the turnover of the Central Reinsurance Company and are particularly important in terms of international acceptances, as they contribute to the company's overall turnover in foreign currency and are considered services exported abroad.

5.1 Evolution of the Total Turnover of CCR

The turnover of CCR represents the volume of premiums accepted, whether national or international. This is governed by the following relationship:

Total Turnover of CCR = Nationally Accepted Premiums + Internationally Accepted Premiums. Referring to the CCR's annual financial reports, the evolution of total turnover can be observed in the graph in Fig. 4.

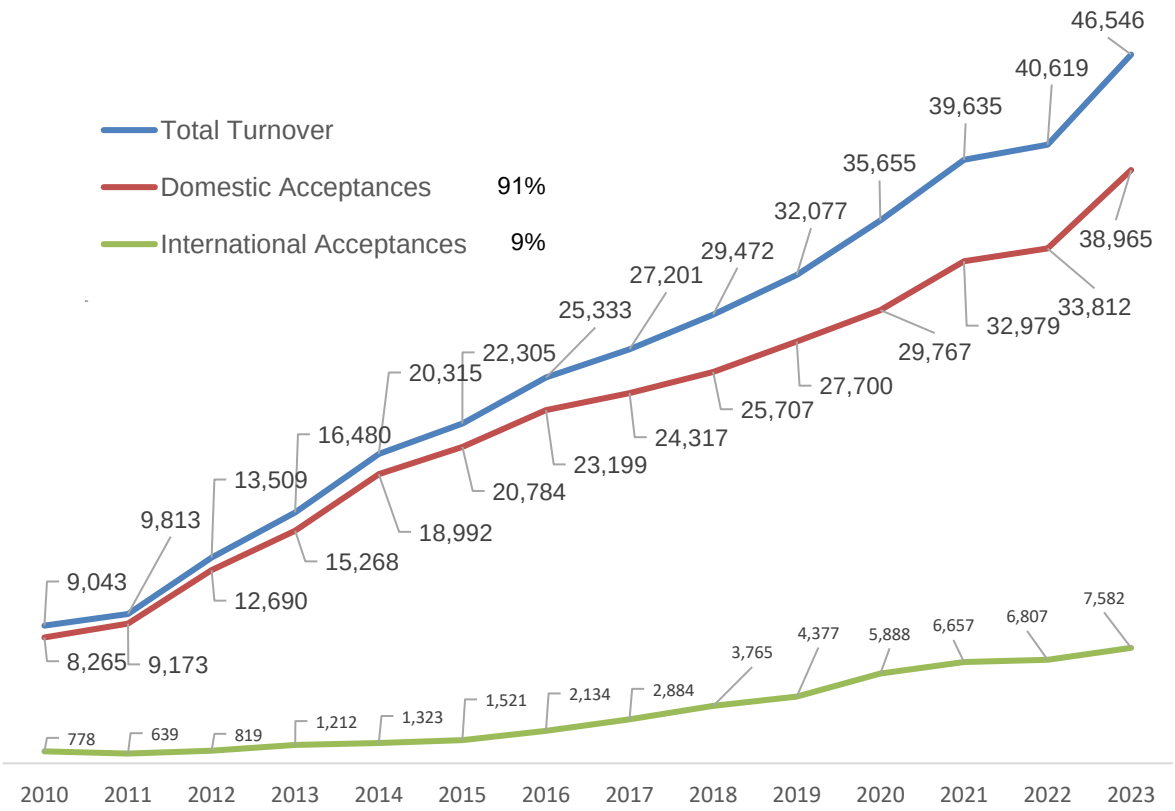


Fig.4 Evolution of the CCR's Turnover (2010-2023) – Units: Million DZD.

The majority share of the CCR's turnover over the years is attributed to national acceptances rather than international ones. This is primarily the result of compulsory cessions from all insurance companies in Algeria, which are required to cede at least half of the business designated for reinsurance to the national reinsurer, CCR. Despite the decree being implemented in 2011,

national acceptances were already high in 2010 due to the demand from public damage insurance companies, which in turn deal with CCR.

We observe that the growth rates of the CCR's turnover are closely aligned with the growth rates of national acceptances, in contrast to international acceptances, which have grown at approximately double the rate of the overall turnover or national acceptances since 2010. However, 2009 saw a decline of 18%. The average share of national acceptances during the studied period represents 91% of acceptances, while international acceptances averaged only 9% of the CCR's total turnover. Despite this, there has been notable growth in international acceptances in recent years, attributed to the CCR's policy of targeting the international market. These acceptances are divided according to geographic regions as illustrated in the graph in Fig. 5.

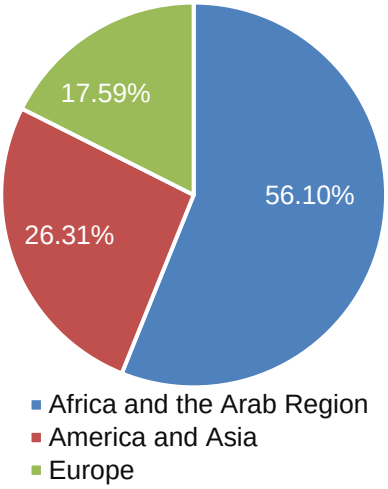


Fig.5 Distribution of International Acceptances by Geographical Region

This distribution reflects the CCR's strong position in Africa and the Arab region, where it is considered a significant competitor. The relatively low percentage in Europe is primarily because major reinsurers are concentrated there, making the competition much more intense. The IARDT branch holds the largest share of acceptances, whether overall, national, or international, due to the nature and severity of the risks involved in this branch. The branches can be observed in the Fig. 6.

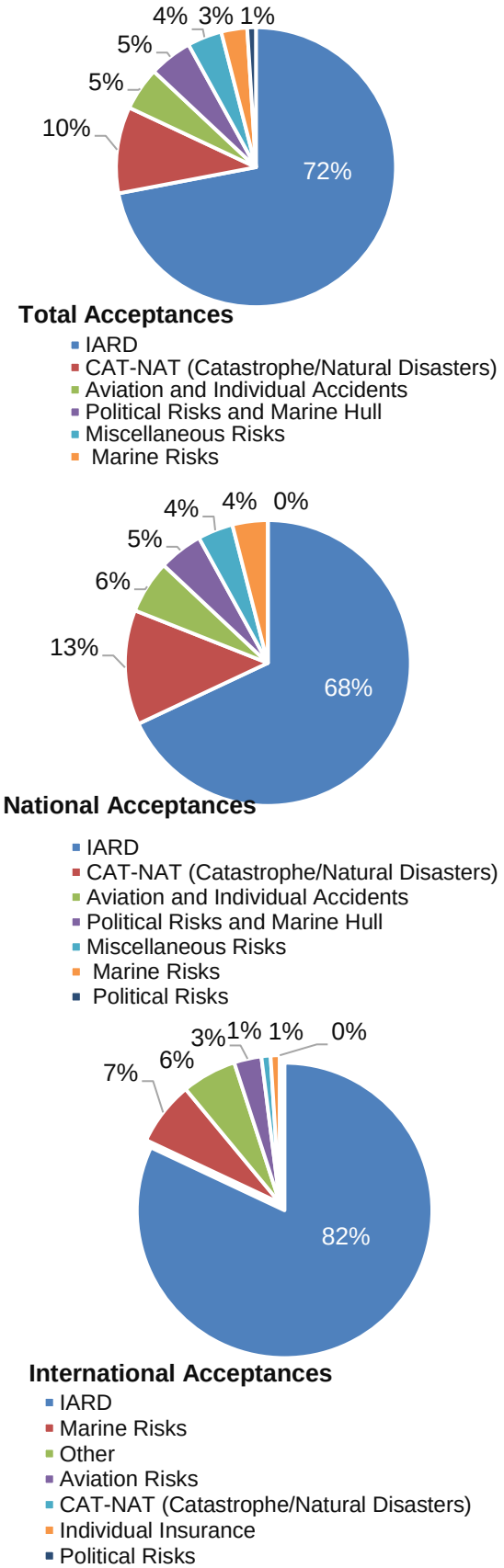


Figure. 6 Structure of Branches in the Acceptances Achieved by CCR (%)

The IARDT branch takes the largest share of acceptances, followed by the natural disaster branch, considering that CCR manages the latter. Despite its mandatory nature, the figures do not reach the desired level. The overall acceptance rates closely align with national acceptance rates, representing over 90%.

5.2 The Position of International Acceptances in the Algerian Reinsurance Market

The turnover in the insurance market is calculated by aggregating the premiums issued in direct insurance by all damage and life insurance companies, including both public and private cooperatives, as well as the premiums issued by the specialized insurance companies SGCI and CAGEX, and the international acceptances within the framework of reinsurance operations conducted by CCR. International acceptances constitute only 3% of the total turnover of the Algerian insurance and/or reinsurance market, as illustrated by:

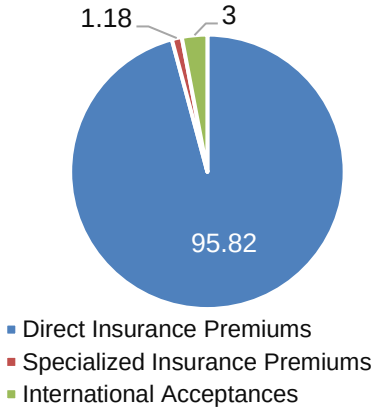


Fig. 7 The position of international acceptances in the Algerian insurance and/or reinsurance market

From the above figure, we observe that the largest share of production, 95.82%, is attributed to direct insurance, which refers to the total premiums issued, net of cancellations, by damage and life insurance companies, cooperatives, whether public, private, or mixed, operating within Algeria. These amounts represent the gross value, including reinsurance amounts (ceded premiums), whether to the Central Reinsurance Company (CCR) or international reinsurance companies, as they are merely transfers of premiums from the accounts of cedents to the accounts of reinsurers.

Therefore, we focus solely on international acceptances, which refer to premiums ceded by insurance companies operating outside Algeria to the benefit of the Central Reinsurance Company, to cover specific risks, whether through agreements or facultative reinsurance. These premiums are in foreign currency and are considered part of the export of services abroad; they constitute only 3% of the total turnover achieved in the market. The remaining percentage, 1.18%, pertains to the premiums issued by the specialized companies SGCI and CAGEX.

5.3 Retention and Retrocession in CCR

The total accepted premiums may be partially retained by CCR, with the portion exceeding its capacity being retroceded to reinsurers in the international market. Here, we refer to:

Net CCR Turnover (retained premiums) = Gross Turnover (total accepted premiums) - Assigned premiums (retroceded).

The development of retention and retrocession rates can be observed in Table 2.

Table. 2 Development of the CCR's net turnover (2010-2023) (Units: million DZD).

Year	Total Turnover (Accepted Premiums)	Net Turnover (Retained Premiums)	Retention Rate (%)	Assigned Premiums (Retroceded)	Retrocession Rate (%)
2010	9,043	5,219	59	3,824	41
2011	9,813	5,903	60	3,910	40
2012	13,509	7,534	56	5,975	44
2013	16,480	9,063	55	7,417	45
2014	20,315	12,798	63	7,516	37
2015	22,305	13,471	60	8,834	40
2016	25,333	14,660	58	10,673	42
2017	27,201	16,423	60	10,778	40
2018	29,472	17,904	60.7	11,568	39.3
2019	32,077	19,871	62	12,206	38
2020	35,655	22,304	63	13,351	37
2021	39,635	22,240	56	17,395	44
2022	40,619	23,588	58	17,031	42
2023	46,546	26,826	57	19,720	43

The table shows that the retention rate at CCR ranges between 55% and 63% during the period from 2010 to 2023, while the retrocession rate ranges between 37% and 45%. This indicates that the company follows a relatively conservative policy, retaining approximately 60% of the accepted premiums, while redistributing around 40% to international reinsurers.

Retrocession is a strategy employed by CCR to alleviate the burden of large risks that may impact its financial capacity. This process helps protect the company from significant market fluctuations or catastrophic losses. The greater the company's ability to retain more premiums without needing to retrocede, the more financially stable and profitable it becomes, provided that it can effectively absorb those risks.

The high retention rates, averaging around 59.7%, reflect the CCR's ability to absorb a substantial proportion of risks without heavily relying on retrocession. This bolsters the trust of both the local and international markets in the company and demonstrates its financial strength. However, this financial strength is not absolute; CCR still relies on retrocession for approximately 40% to mitigate high risks.

We observe variations in the retention rate across different years, with the highest retention rate

recorded in 2014 and 2020 at 63%, and the lowest in 2013 at 55%. This variation is due to financial pressures and changes in the type and size of risks the company faced during this period. This leads us to examine the retained and ceded branches at CCR over the study period, as illustrated in Fig. 8.

The IARDT branch, which includes industrial and commercial insurance as well as natural disasters, represents the largest portion of retained premiums and ceded premiums. This is expected due to the significant risks in this branch. For instance, natural disasters are high-impact risks requiring substantial financial capacity to manage. Therefore, the company resorts to ceding a significant portion of these risks.

The distribution between retention and ceding across the different branches reflects the CCR's specialization in handling a diverse range of risks. Branches that involve high risks, such as natural disasters and marine insurance, often experience a relatively larger degree of ceding, given the potential size of the losses.

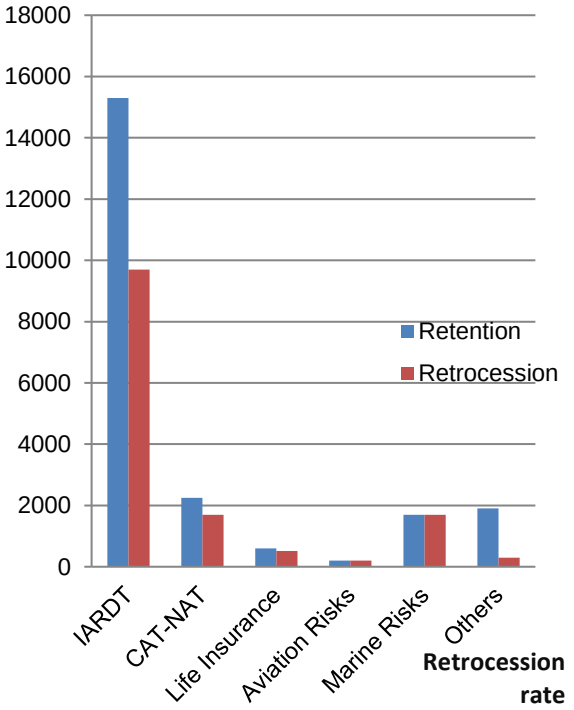


Fig.8 Retained and ceded branch shares at CCR

Looking at previous data, we can observe that the retention rate has remained relatively stable in recent years, with some slight improvement in its average. This reflects the company's ability to improve risk management over time, leveraging its accumulated experience to increase retention rates while maintaining a reasonable balance between retention and ceding.

The continuous improvement in the retention rate is a result of the CCR's enhanced ability to manage risks, thanks to growth in capital and the strengthening of specialized human resources. This improvement has helped CCR gain more control over operations within both the local and international markets, reducing reliance on ceding.

Although ceding reduces the financial risks associated with directly bearing premiums, it also affects the company's profitability, as CCR forfeits part of the revenues to reinsurers in foreign currency. The stability of the retention rate around 60% indicates the company's desire to balance risk reduction with profitability increase. A ceding rate of approximately 40% suggests that the company still requires the support of reinsurers, especially for large or international risks.

The analysis of retention and ceding at CCR shows that the company relies on a balanced strategy, blending the retention of a significant portion of premiums with ceding part of the risks to the international market. This policy supports the company's financial stability, with the potential to enhance this strategy to increase profitability and reduce reliance on ceding, by strengthening capital and developing internal risk management capabilities.

6. CONCLUSIONS

The study demonstrated that the implementation of Executive Decree No. 10-207, which imposes a mandatory cession of at least 50% in favor of CCR, has reinforced the company's dominance in the Algerian reinsurance market. This decree has led to a significant increase in the volume of national acceptances, accounting for 91% of total accepted premiums, which illustrates the local market's heavy reliance on CCR. In contrast, international acceptances remain relatively limited at just 9%, highlighting the need for the company to expand its activities on international markets.

On the other hand, the data showed that the IARDT branch represents the largest portion of total accepted premiums, followed by natural disasters. However, the figures for natural disasters have not reached the expected levels despite their mandatory nature, raising questions about the effectiveness of the current management of this branch.

Regarding retention and ceding rates, the retention rate hovers around 60%, indicating the CCR's ability to handle a significant portion of the risks internally while redistributing the remainder to international reinsurers. This is a positive indicator, as the company demonstrates the capacity to retain a large portion of its business, strengthening its financial position. However, the relative reliance on ceding suggests the need to enhance the company's internal capabilities to increase retention rates and achieve greater independence.

Study Findings:

The study's findings can be summarized in the following points:

- Increased dominance of CCR in the local market: The mandatory cession rate increase has bolstered the company's dominance over national acceptances, enhancing its financial stability but reducing competition in the market.
- Limited international acceptances: Despite noticeable expansion, international acceptances remain limited compared to national ones, necessitating the development of more effective strategies for international market expansion.
- High retention with reliance on ceding: High retention rates reflect the company's strength in absorbing risks but continued reliance on ceding indicates the need to strengthen the company's capabilities to reduce external dependence.
- Weak management of natural disasters: Despite being mandatory, natural disaster figures remain below the required level, highlighting the need to improve management policies in this branch to increase its effectiveness.

These findings open the door for a reassessment of the current reinsurance policies in Algeria, with a focus on enhancing competition and expanding international operations to improve market efficiency.

Lastly, this study recommends reconsidering the mandatory cession rate, currently set at a minimum of 50% for the Central Reinsurance Company. The study also recommends the development of the Algerian reinsurance market through several measures, the most notable being:

- Encouraging competition in the local market: There should be a reconsideration of the mandatory cession rate in favor of CCR to encourage competition from other reinsurers in the local market. This could stimulate innovation and improve the quality of insurance services provided to insurance companies, ultimately enhancing overall market efficiency.
- Strengthening collaboration with regional and international reinsurers: CCR can enhance its partnerships with reinsurers in Africa, the Arab region, and Asia by developing new agreements and capitalizing on opportunities in these markets. This would increase the CCR's share in the international market and

reduce its reliance on European reinsurers, who pose strong competition.

- Improving risk management: the CCR's risk management system should be enhanced by adopting artificial intelligence technologies and big data analytics to predict future disasters and risks more accurately. Additionally, improving governance within the company will ensure transparency and efficiency in decision-making related to the cession and retention of premiums.
- Investing in education and professional training: To ensure CCR is capable of meeting international market challenges and improving its performance, continuous education, and specialized training for employees must be prioritized. Advanced training in underwriting models and risk management will enhance the company's ability to make better-informed decisions.
- Diversifying reinsurance products: Expanding CCR's products into areas such as agricultural, health, and environmental reinsurance will help diversify risks and increase growth opportunities, especially given the rising demand for such insurance products.
- Increasing digitization and technological innovation: CCR should invest in advanced digital systems to improve operational efficiency, from evaluation and underwriting to risk management. This could include advanced analytics for pricing, claims management, and customer service, contributing to enhanced competitiveness and improved overall performance.
- Developing cession strategies: Cession strategies can be improved by establishing precise risk assessment mechanisms for high-impact risks. This will enable CCR to determine when it is necessary to cede part of the risks and identify the best global markets to manage them, thus improving returns on investments related to the cession.
- Adopting a smart retention policy: A "smart retention" policy should be implemented, where more premiums are retained in cases where the company is better equipped to absorb the risks while reducing premium cession in higher-risk scenarios. This approach will increase the company's ability to control returns from retained premiums.
- Developing advanced underwriting models: The use of advanced actuarial and analytical models for risk assessment will allow the company to retain more premiums without increasing financial risk.

By following these recommendations, CCR can improve its performance and competitiveness locally and internationally, contributing to the more efficient and sustainable development of the Algerian reinsurance market.

WORKS CITED

Altuntas, M., Garven, J. R., & Rauch, J. (2018). On the corporate demand for insurance: evidence from the global reinsurance market. *Risk Management and Insurance Review, 21*(2), 211-242. doi:https://doi.org/10.1111/rmir.12107

Berger, L. A., Cummins, J. D., & Tennyson, S. (1992). Reinsurance and the liability insurance crisis. *Journal of Risk and Uncertainty, 5*(3), 253-272. doi:https://doi.org/10.1007/BF00057882

Bernard, C. (2013). Risk sharing and pricing in reinsurance market. In G. (. Dionne, *Handbook of insurance* (pp. 603-626). Springer.

Bhattacherjee, A. (2012). *Social science research: principles, methods, and practices* (2nd ed.). Create Space Independent Publishing Platform. doi:https://digitalcommons.usf.edu/cgi/viewcontent.cgi?article=1002&context=oa_textbooks

Bouzaher, N., & Necira, O. (2017). Analytical approach to reinsurance in Algeria as an emerging market. *Journal of Economic and Financial Studies*, 264. doi:https://doi.org/10.37488/2057-010-003-021

Cheraitia, Z., & Medjden, H. K. (2020). Application of Convex Optimization Results of DE FINETTI's Problem for Proportional Reinsurance (A Case Study of CAARAMA Insurance Company in Algiers). *Management & Economics Research Journal, 2*(4), 86-100.

Cole, C. R., & McCullough, K. A. (2006). A reexamination of the corporate demand for reinsurance. *Journal of Risk and Insurance, 73*(1), 169-192. doi:https://doi.org/10.1111/j.1539-6975.2006.00170.x

Cole, C. R., Lee, R. B., & McCullough, K. A. (2007). A test of the eclectic paradigm: evidence from the U. S. reinsurance market. *Journal of Risk and Insurance, 74*(1), 493-522. doi:https://doi.org/10.1111/j.1539-6975.2007.00222.x

Creswell, J. W., & Creswell, J. D. (2018). *Research design: qualitative, quantitative, and mixed methods approaches.* California: SAGE.

Crisafulli, M. (2023). *Efficient reinsurance strategies considering counterparty default risk.* Italy: University of Roma.

Cummins, J. D., Dionne, G., Gagné, R., & Nouira, A. (2021). The costs and benefits of reinsurance. *Geneva Papers on Risk and Insurance – Issues and Practice*, 177-199. doi:http://dx.doi.org/10.2139/ssrn.1142954

Deelstra, G., & Plantin, E. (2014). *Risk theory and reinsurance.* Springer. doi:https://doi.org/10.1007/978-1-4471-5568-3

Doherty, N., & Fine, S. (1981). Reinsurance under conditions of capital market equilibrium: a note. *Journal of Finance, 36*(4), 949-953.

Driessen, T. S., Fragnelli, V., Katsev, I. V., & Khmelnitskaya, A. B. (2015). On 1-convexity and nucleolus of co-insurance games. *Insurance: Mathematics and Economics, 48*(2), 217-225. doi:https://doi.org/10.1016/j.insmatheco.2010.10.009

Eling, M., & Jia, R. (2017). Recent research developments affecting nonlife insurance : the CAS risk premium project 2014 update. *Risk Management and Insurance Review, 20*(1), 63-77. doi:https://doi.org/10.1111/rmir.12072

Eling, M., & Luhnen, M. (2010). Efficiency in the international insurance industry: a cross-country comparison. *Journal of Banking & Finance, 34*(7), 1497-1509. doi:https://doi.org/10.1016/j.jbankfin.2009.08.026

Furidha, B. W. (2013). Comprehension of the descriptive qualitative research method: a critical assessment of the literature. *ACITYA WISESA, 2*(4), 1-8. doi:https://doi.org/10.56943/jmr.v2i4.443

Gall, M. D., Gall, J. P., & Borg, W. R. (2007). *Educational research: an introduction.* Boston: Pearson.

Gbenro, O. B., Duramany-Lakkoh, E. K., & Kamara, S. (2023). An Assessment of the Stakeholders' Perception of Reinsurance and Insurance Products and Services on the Performance of Insurance Companies. *International Journal of Development and Economic Sustainability, 11*(2), 1-37. doi:https://doi.org/10.37745/ijdes.13

Graven, J. R., & Tennant, J. L. (2003). The demand for reinsurance: theory and empirical tests. *Assurances et gestion des risques, 71*(2), 217-237. doi:https://ssrn.com/abstract=6717

Haueter, N. V. (2020). *Reinsurance function and markets*. Retrieved from Oxford Research Encyclopedia of Business and Management: https://oxfordre.com/business/view/10.1093/acrefore/9780190224851.001.0001/acrefore-9780190224851-e-268

Hoerger, T., Sloan, F., & Hassan, M. (1990). Loss volatility, bankruptcy, and the demand for reinsurance. *Journal of Risk and Uncertainty, 3*(3), 421-245. doi:https://doi.org/10.1007/BF00116782

Kajwang, B. (2022). Contribution of reinsurance business to the economy. *International Journal of Economic Policy, 2*(2), 20-30. doi:https://doi.org/10.47941/ijecop.963

Lazli, K., & Bouakkaz, N. (2024). The Risk-Profitability Nexus: Evidence from Algerian Insurance Companies. *SocioEconomic Challenges (SEC), 8*(2).

Mahdjour, M., & Benhabib, A. (2017). A Study of the Socio-Cultural Factors That Influence Algerian Consumer Attitude towards Insurance Products. *Journal of Account & Marketing, 6*(1), 242-253. doi:10.4172/2168-9601.1000242

Manjunatha, N. (2019). Descriptive research. *Journal of Emerging Technologies and Innovative Research, 6*(6), 863-867. Retrieved from https://www.jetir.org/papers/JETIR1908597.pdf

Mayers, D., & Smith, C. (1990). On the corporate demand for insurance: evidence from the reinsurance market. *Journal of Business, 63*(1), 19-40. doi:https://doi.org/10.2307/253678

Nassaji, H. (2015). Qualitative and descriptive research: data type versus data analyses. *Language Teaching Research, 9*(2), 129-132. doi:https://doi.org/10.1177/1362168815572747

Olubajo, A. T. (2003). *The law of co-insurance policies.* University of Southampton.

Oucherif, W., & Touche, N. (2023). Modeling claims frequency in the Algerian automobile insurance market using machine learning. *The Notebooks of Cread, 39*(3), 217-234.

Patrik, G. (2006). Reinsurance, Functions and values. In *Encyclopedia of Actuarial Science.* New York: John Wiley & Sons, Ltd.

Wehrhahn, R. (2009). *Introduction to reinsurance.* Washington: The World Bank.

Weiss, M. A. (2007). Underwriting cycles: a synthesis and further directions. *Journal of Insurance, 30*(1), 31-45. Retrieved from http://www.jstor.org/stable/41946268

Witthoff, E. (2020). Principles of reinsurance contract law? The reinsurer's perspective. *Uniform Law Review, 25*(1), 57-66. doi:https://doi.org/10.1093/ulr/unaa004

Xiong, Q., Peng, Z., & Nadarajah, S. (2023). Optimal reinsurance under the linear combination of risk measures in the presence of reinsurance loss limit. *Risks, 13*(7), 1-26. doi:https://doi.org/10.3390/risks11070125

Received for publication: 13.10.2024
Revision received: 31.10.2024
Accepted for publication: 08.01.2025.

How to cite this article?

Style – **APA** *Sixth Edition:*

Khoualed, A., Bouzerb, K., & Almi, H. (2025, 01 15). The Evolution of Reinsurance Supply in Algeria: An Analytical Study. (Z. Cekerevac, Ed.) *MEST Journal, 13*(1), 89-104. doi:10.12709/mest.13.13.01.09

Style – **Chicago** *Sixteenth Edition:*

Khoualed, Aboubaker, Khayreddine Bouzerb, and Hassiba Almi. "The Evolution of Reinsurance Supply in Algeria: An Analytical Study." Edited by Zoran Cekerevac. *MEST Journal* (MESTE) 13, no. 1 (01 2025): 89-104.

Style – **GOST** *Name Sort:*

Khoualed Aboubaker, Bouzerb Khayreddine and Almi Hassiba The Evolution of Reinsurance Supply in Algeria: An Analytical Study [Journal] // MEST Journal / ed. Cekerevac Zoran. - Belgrade – Toronto : MESTE, 01 15, 2025. - 1 : Vol. 13. - pp. 89-104.

Style – **Harvard** *Anglia:*

Khoualed, A., Bouzerb, K. & Almi, H., 2025. The Evolution of Reinsurance Supply in Algeria: An Analytical Study. *MEST Journal,* 15 01, 13(1), pp. 89-104.

Style – **ISO 690** *Numerical Reference:*

The Evolution of Reinsurance Supply in Algeria: An Analytical Study. **Khoualed, Aboubaker, Bouzerb, Khayreddine and Almi, Hassiba.** [ed.] Zoran Cekerevac. 1, Belgrade – Toronto : MESTE, 01 15, 2025, MEST Journal, Vol. 13, pp. 89-104.

MEST Journal
DOI 10.12709/mest.13.13.01.10

CRISIS MANAGEMENT IN IT COMPANIES: THE CASE OF SKOPJE

Kiril Postolov
University SS. Cyril and Methodius, Faculty of Economics, Skopje, Republic of North Macedonia
https://orcid.org/0000-0002-1551-9898

Boris Postolov
Renewable Energy Supply DOOEL, Skopje, Republic of North Macedonia

JEL Category: **G22**

Abstract

Crisis management presents a significant challenge for IT companies, yet its effective implementation is crucial for ensuring the organization's continued success and operational efficiency. Crisis management is a multifaceted process that integrates knowledge and theories from various fields. Research on crisis management within the IT sector is extensive, with scholars aiming to identify key issues and best practices for managing crises in this domain. This paper seeks to explore how crisis management is applied within IT companies, with a particular focus on those operating in Skopje. To achieve this, a narrative approach was employed, utilizing secondary sources of information. Additionally, empirical research the authors conducted through a survey questionnaire distributed to 30 IT companies in Skopje. The data collected were analyzed and visualized through tables and graphs, leading to conclusions and actionable recommendations. The findings suggest that crisis management in the IT sector in Skopje is still in its nascent stages. There is a lack of established, effective crisis management models to address emerging challenges, leaving companies vulnerable to unexpected crises. This paper highlights the need to develop robust crisis management strategies tailored to the specific needs of the IT sector.

Keywords: *Crisis, Crisis Management, Symptoms, Sources, Activities of Crisis Management, Bearers of Crisis Management.*

1 INTRODUCTION

The significance of managing organizational crises lies in the timely identification and resolution of potential threats, as failure to do so can lead to organizational decline and, ultimately, the failure of the enterprise. Crises are an inherent part of organizational life, and while they can disrupt a business's functioning, they also affect employees, often leading to psychosomatic disorders and stress-related health issues.

Address of the corresponding author:
Kiril Postolov
kirilp@eccf.ukim.edu.mk

Crisis phenomena have been studied across various academic disciplines, including economics, medicine, psychology, history, and politics. For instance, in psychology, a crisis may refer to a personal or identity crisis, while in medicine, it may relate to a health crisis, and in politics, a national crisis. This interdisciplinary interest underscores the complex nature of crises and their far-reaching impacts.

The organizational crises study has provided valuable insights essential for navigating such challenges. Scholars have approached the subject from diverse perspectives, leading to a variety of theoretical frameworks and understandings. However, synthesizing these varied viewpoints into a unified theory remains a challenge, as the causes and impacts of crises differ depending on the context and nature of the organization.

A key concept related to organizational crises is crisis management—a critical organizational function aimed at navigating and mitigating the impact of crises. In modern business environments, the inevitability of crises has become widely recognized, and organizations are increasingly focusing on developing crisis management strategies to address them when they arise. The role of crisis management is to steer the organization through periods of instability, ensuring both short-term recovery and long-term resilience.

For managers, effective crisis management requires identifying the root causes of crises and also implementing strategies that minimize their negative consequences. Proactive crisis management is essential for preserving the organization's stability, protecting its reputation, and ensuring its long-term viability.

2 MANAGING A MODERN CRISIS

Managing a modern crisis is a highly complex and time-consuming operation that involves multiple stakeholders, ranging from political figures to business leaders, and individuals directly impacted by the crisis. The primary objective of crisis management is to prevent the crisis from escalating and, ideally, to restore the organization to its pre-crisis state with minimal lasting consequences.

This goal is at the core of crisis management, which seeks to implement operational strategies aimed at achieving this outcome.

Academic literature offers many definitions and interpretations of what defines a crisis. Below, we focus on a selection of definitions that most effectively capture the essence of a crisis.

Sapriel (2003, p. 348) defines a crisis as "an event, revelation, allegation, or set of circumstances which threatens the integrity, reputation, or survival of an individual or organization".

Cater and Beal (2014, p. 65) describe a crisis as "a low-probability situation with significant consequences for the organization, a high degree of uncertainty, and a sense of decision-making urgency".

Shrivastava, Mitroff, Miller, and Miglani (1988, p. 285) offer a more in-depth definition: "An organizationally based disaster, which causes extensive damage and social disruption, involves multiple stakeholders, and unfolds through complex technological, organizational, and social processes".

Crisis, as a phenomenon, is intrinsically linked to the functioning of the organization. It is difficult to discuss the operational dynamics of any modern enterprise without considering the potential for crises. While some crises are inevitable regardless of the company's preparedness, recognizing and addressing early warning signs can significantly reduce their impact.

The definitions of crisis management also vary, reflecting different perspectives on how to address and mitigate crises. Here are several notable definitions that outline its essence.

Thomas and McNair-Connolly (2017) define crisis management as "the planning for, and management of a perceived risk, an unexpected disaster, or a business disruption."

Coombs (2007, p. 5) asserts that crisis management is the collective sum of activities aimed at preventing and minimizing real damage because of a crisis.

Bigley and Roberts (2001) describe it as involving "coordinating complex technical systems and designing an organizational structure to prevent, mitigate impact, and learn from crises."

Blythe (2002) outlines a crisis management process that includes: identifying potential weak points, assessing existing procedures, recognizing new procedures needed to eliminate these weaknesses, organizing a crisis management plan, utilizing the plan when needed, and continuously monitoring processes for new vulnerabilities.

Millar and Heath (2004) identify three essential elements for good crisis management: a clear plan of action, an early warning system to signal a potential crisis, and a trained crisis management team capable of effectively addressing the situation.

Crisis management encompasses activities designed to identify, plan for, respond to, and resolve crises. From a managerial perspective, crisis management involves actively engaging in processes to navigate situations that threaten the organization's survival. It requires managers to detect emerging threats in the external environment and act swiftly to mitigate risks.

In essence, crisis management can be viewed as a specialized form of enterprise management aimed at mastering all processes that could jeopardize the organization's survival. Mitroff (1994, pp. 101-102) notes, it is no longer a question of whether a crisis will occur, but when.

Crisis management is thus the highest priority for any enterprise aiming to prevent or overcome processes that might significantly disrupt operations or threaten the organization’s continued existence. If the goal of crisis management is to ensure the organization continues to meet its objectives, it may also involve restructuring, reengineering, or reorganization.

3 SYMPTOMS OF CRISIS

Identifying the early symptoms of a potential crisis is crucial for companies to avert more severe consequences. These symptoms are often not immediately visible and may manifest as subtle, underlying issues. Typically, the first signs include a decline in market share and orders. They are followed by a drop in sales and solvency. However, it is important to note that these signs do not always indicate an impending crisis; they can represent temporary challenges that may be resolved shortly. No company remains at the peak of success indefinitely, and such fluctuations are common in the business cycle. Nevertheless, they can serve as valuable signals for companies to initiate necessary changes, whether in human resources, organizational culture, or the technology and equipment used in production.

Some symptoms may be more pronounced than others, and this variance makes it particularly challenging for managers to distinguish between minor setbacks and genuine signs of an impending crisis. The most difficult task for managers is recognizing when these symptoms cross the threshold into a crisis. Early identification is crucial for implementing timely corrective actions and preventing the problem from worsening.

Sometimes, the signs of an impending crisis are not immediately visible in an organization's financial or operational results. While there may not always be clear indicators pointing to a crisis, it is essential to recognize the symptoms that suggest a crisis could be on the horizon. These symptoms can manifest in several ways, and different authors have identified a range of warning signs. Some key symptoms include:

- *Decreasing liquidity and an inability to meet financial obligations, especially to suppliers.*
- *Declining profitability, as indicated by a reduced rate of return on investments.*
- *Falling sales, shrinking market share, delays in product deliveries, and reduced incoming orders.*
- *Employee dissatisfaction, expressed through strikes, high turnover rates, or low morale.*
- *Rising production errors, increased waste, and declining capacity utilization.*
- *Reduction in investment for research and development, and growing inefficiency in business processes.*
- *Restrictive dividend policies.*
- *Delays in reinvestment, and a failure to update or improve business strategies.*
- *Resistance to external ideas or innovation, hindering progress and adaptability.*

Recognizing these symptoms is critical, but it is important to remember that some signs may reflect temporary setbacks rather than the onset of a crisis. Nonetheless, they provide valuable

opportunities for companies to reassess their strategies, processes, and operations.

4 TYPES OF CRISIS MANAGEMENT

While there are various classifications of crisis management, in theory, two primary types are commonly recognized:

- *Active Crisis Management*
- *Reactive Crisis Management (Muller, p. 38)*

4.1 Active Crisis Management

Active crisis management refers to proactive measures taken to identify and mitigate potential crises before they occur. It involves early detection and the implementation of strategies that prevent crises from escalating. Active crisis management aims to address problems before they become significant, reducing the likelihood of a crisis unfolding.

Anticipatory Crisis Management: Involves preparing countermeasures in advance by creating contingency plans and scenarios to ensure a timely response if a crisis arises.

Preventive Crisis Management: It focuses on the planning, implementation, and control of strategies, based on early warning indicators, to prevent a crisis from developing.

4.2 Reactive Crisis Management

In contrast, reactive crisis management involves responding to crises after they have occurred. This situation demands swift and effective measures to mitigate damage and promptly restore normal operations. Reactive crisis management is focused on managing disruptions that have already affected the organization.

Responsive Crisis Management: a company applies it when a crisis has already occurred. The management leads the company through the crisis and acts towards a resolution.

Liquidation Crisis Management: This occurs when the organization faces a situation where recovery is no longer possible, and the focus shifts to minimizing losses and protecting stakeholders during the planned liquidation of the company.

Each type of crisis management requires different strategies and tools, depending on whether the crisis is imminent, ongoing, or irreversible.

5 CRISIS MANAGERS

The success of crisis management depends largely on the individuals or groups responsible for executing the strategies. These individuals, often called "crisis managers," play a critical role in planning, implementing, and monitoring the crisis management process.

5.1 Internal Crisis Management

Top management within the company often takes the lead in managing crises. However, the question arises: Can the same management team that led the company into a crisis also be responsible for navigating it? There is no single answer to this, but two main schools of thought exist:

- *Top Management Should Not Be Responsible:* Some argue that the same team responsible for the crisis cannot effectively lead the recovery, as their actions or decisions may have contributed to the situation.
- *Top Management Can Lead the Recovery:* Others believe that top management, being familiar with the company's internal workings, is best positioned to steer the organization out of the crisis, provided they take immediate and effective action.
- *Whether top management is suitable for crisis management depends on their actions.* If they are proactive, implement sound strategies, and take decisive measures, they may continue to lead the crisis management efforts. However, if their actions are passive or ineffective, they may lose credibility, and the company may need external assistance.

5.2 Tasks of Crisis Management Leaders

Top management, as crisis managers, must undertake the following tasks:

- *Initiating, preventing, or managing the crisis: Proactively addressing potential threats.*
- *Selecting and approving crisis management measures: Deciding on the appropriate actions to address the crisis.*
- *Human resource management: Ensuring the workforce is properly managed during a crisis.*

5.3 External Crisis Management Resources

In some cases, a company may require external help. That could involve hiring external advisors or crisis managers to provide an objective perspective or expertise in managing the crisis.

External Advisors: These consultants bring objectivity and independence to the crisis management process. They can provide valuable insights and help implement strategies that might be difficult for internal management due to emotional or organizational biases. However, external consultants face challenges, such as unfamiliarity with the company's internal culture, potential resistance from employees, and high costs. In some cases, these factors may hinder their effectiveness.

Crisis Managers: Often freelance professionals or former executives with expertise in crisis management, crisis managers are typically brought in when existing management is unable to resolve the crisis. They bring a fresh perspective, but their role can be contentious, as they may face resistance from employees and management. Crisis managers must be able to make tough decisions, analyze the situation objectively, and implement change rapidly.

When selecting a crisis manager, organizations should prioritize the following criteria:

- *Experience in crisis management: Proven track record in leading organizations through crises.*
- *Toughness and resilience: Ability to withstand pressure and make difficult decisions.*
- *Authority: The crisis manager must hold a certain level of influence within the organization.*
- *Analytical thinking: Strong problem-solving skills to understand the crisis and develop effective solutions.*
- *Confidence and assertiveness: A crisis manager must have the self-assurance to take charge and lead decisively.*

It is not necessary to find all these qualities in a single individual. Sometimes, a team of crisis managers can be assembled, with each member contributing different skills and expertise to form a balanced and effective leadership team.

6 RESEARCH METHODOLOGY

To collect data for this research, most surveys we conducted online. This method allowed the authors to distribute the questionnaires to a larger number of respondents in a shorter time frame and at a lower cost. Additionally, conducting the survey online ensured anonymity, which is known to increase the likelihood of receiving more honest and accurate responses. However, some questionnaires were also distributed in person to ensure a variety of responses.

Within the research, the following rules were accepted:

- *The survey was conducted among people born between 1975 and 2000.*
- *Only individuals with an academic education were included, regarding the level of education.*
- *To obtain relevant data and results, the authors determined that the sample size was above 30 respondents.*

The questionnaire consisted of two sections with a total of 10 questions:

- *Section 1* contained 3 demographic questions about the respondents' age group, gender, and level of education.
- *Section 2* included questions related to the functioning of IT enterprises in the Municipality of Skopje, particularly in relation to their ability to continue operations during a crisis.

The questionnaire utilized a Likert scale (1=Strongly disagree, 2=Disagree, 3=Neutral, 4=Agree, 5=Strongly agree) to measure the respondents' opinions on various aspects of crisis management in IT enterprises.

The first table we constructed is related to the demographic characteristics of the respondents, in terms of gender, level of education, and age. Its content is presented in Table 1.

Table 1. Demographic characteristics of respondents

SEX	
Male	22
Female	12
LEVEL OF EDUCATION	
Graduated	30
Master	3
Ph.D.	1

AGE	
Under 25 years old	15
Between 25 and 30	12
Between 31-36	3
Between 37-41	2
Up 41	2

Source: Authors' original research

We constructed Table 2 based on the answers received and obtained a mean score.

The data from these demographic categories were used to better understand the respondents' backgrounds and their potential influence on perceptions of crisis management in IT enterprises.

When we collected the survey data, we analyzed the responses using descriptive statistics. We calculated the mean score for each question in Section 2, which provided insights into the respondents' overall views on the state of crisis management in IT enterprises in Skopje. This statistical approach helped us to identify trends, patterns, and significant differences in responses, which will be discussed in the following sections of the paper.

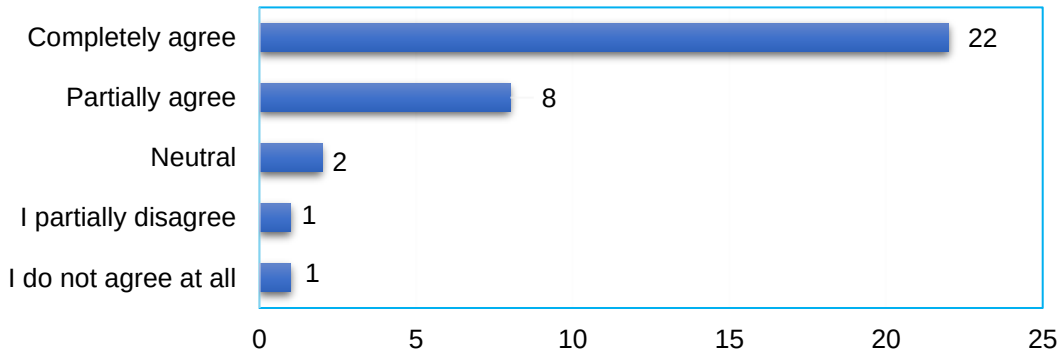
The last two questions are related to whether they have problems with AI and political issues, like war, political change, etc., in these sectors.

We can see the answers from graphs 1 and 2.

Table 2. Organizational questions related to the crisis

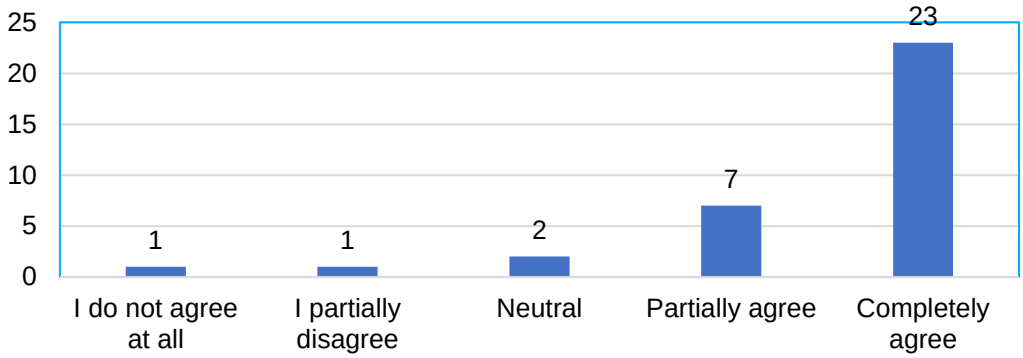
No.	Finding	Strongly Disagree **1**	Disagree **2**	Neutral **3**	Agree **4**	Strongly Agree **5**	Results
1.	We have not felt a crisis so far	0	0	3	10	21	4.53
2.	Do you anticipate the possibility of a crisis?	0	0	4	12	18	4.41
3.	Do you think that if there is a crisis in your business, it will be quickly overcome?	0	0	0	5	29	4.85
4.	Are you able to recognize the symptoms of a crisis in your company?	0	0	10	14	10	4.00
5.	There will be no hiding information if there is a crisis	1	3	4	18	8	3.85
6.	Do you think there are managers and leaders in your company who are ready to handle any crisis?	1	1	2	20	10	4.09
7.	Do you think outside experts should be hired if you get into a crisis?	18	16	0	0	0	1.47

Source: Authors' original research



Graph 1. Do you think the application of artificial intelligence will affect the emergence of a crisis in this sector?

Source: Authors' original research



Graph 2. Do world political and military changes contribute to a crisis in this sector?
Source: Authors' original research

7 FINDINGS AND CONCLUSIONS

The survey results reveal several key insights into how employees in the IT sector perceive crises and the sector's ability to handle potential crises:

- *Perception of Crisis in the Workplace:* Employees generally did not perceive an ongoing crisis in their work environment (average score: 4.53), but they felt confident in their ability to anticipate a potential crisis before it occurred (average score: 4.41).
- *Crisis Management Confidence:* There is strong agreement (score: 4.85) that, in the event of a crisis, the organization would swiftly address and overcome it. Employees also expressed confidence in recognizing the early symptoms of a crisis, which would enable them to respond appropriately.
- *Transparency in Crisis Communication:* Employees indicated a moderate level of trust (score: 3.85) that in the event of a crisis management would not conceal critical information. Instead, it would be shared with all employees, ensuring transparency and collective awareness.
- *Internal vs. External Crisis Management:* Most respondents (score: 4.09) believed that internal resources should be utilized to address crises, rather than hiring external crisis managers (score: 1.47). This suggests a preference for internal knowledge and problem-solving capabilities in managing crises.
- *Impact of Artificial Intelligence:* A notable concern among employees was the increasing use of artificial intelligence (AI), with 30 out of 34 respondents agreeing (either fully or partially) that AI poses a threat to their jobs. This reflects a broader apprehension within the sector regarding the evolving role of AI and its potential impact on employment.

External Factors Contributing to Crisis Risk: Political and military events were also identified as significant factors that could destabilize the sector. Such events may lead to the relocation of IT firms or the loss of contracts, resulting in job displacement and further economic uncertainty.

Based on the survey results, it is evident that the IT sector, while contributing significantly to the country's GDP and offering competitive salaries, is not immune to crises. The dynamic nature of the sector, driven by rapid technological advancements and external factors like political instability, requires a well-structured crisis management approach.

Employees in the sector are aware of the potential threats to their work, especially regarding AI and external geopolitical events. However, they also demonstrate a strong belief in their ability to detect early signs of crises and respond effectively, provided they are equipped with the right tools and knowledge.

A critical takeaway is the importance of timely crisis detection, not only for managers but also for employees. Both need to be capable of identifying symptoms of a crisis and taking proactive measures to mitigate its impact. Additionally, choosing the right crisis management strategy—anticipatory or reactive—is vital to prevent or minimize potential damage.

Furthermore, the selection of a crisis manager should not be rigidly confined to either internal or

external candidates. The ideal crisis manager is a person who possesses the necessary expertise and qualities to resolve the situation at hand, regardless of their affiliation with the organization.

In conclusion, while the IT sector enjoys certain advantages, including a relatively high standard of living for its employees, it must remain vigilant. Crisis management, in theory and practice, must be an integral part of the sector's operational strategy to ensure its resilience and continued success in the face of unforeseen challenges.

WORKS CITED

Bigley, G. A. & Roberts, K. H. (2001) The Incident Command System: High Reliability Organizing for Complex and Volatile Task Environments. *The Academy of Management Journal*, *44*(6), 1281-1299. doi: 10.2307/3069401

Blythe, B. T. (2002). *Blindsided. New York:* Portfolio Penguin Putnam

Cater, J. J. III, & Beal, B. (2014). Ripple effects on family firms from an externally induced crisis. *Journal of Management Family Business, 4*(1), 62-78.

Coombs, W. T. (2007). *Ongoing Crisis Communication: Planning, Management, and Responding* (Second edition). Sage Publications

Millar, D. P., & Heath, R. L. (2004). *Responding to the crisis: A Rhetorical Approach to Crisis Communication.* Lawrence Erlbaum Associates Inc., New Jersey: Mahwah.

Mitroff, I. I. (1994, Winter). Crisis Management and Environmentalism: A Natural Fit. *California Management Review,* 36(2), pp. 101-113. doi: 10.2307/41165747

Mueller, R. *(1985, October).* Corporate management with crises. *Long Range Planning,* 18(5), 38-48.

Postolov, K. (2011). Teorija na organizacija. Univerzitet „Sv. Kiril i Metodij", Skopje.

Sapriel, C. (2003). Effective crisis Management: Tools and best practice for the new millennium. *Journal of Communication Management,* 7(4), 348-355.

Shrivastava, P., Mitroff, I. I., Miller, D., & Miglani, A. (1988, Jul). Understanding Industrial Crises. *Journal of Management Studies, 25*(4), 285-303.

Thomas, C. R., & McNair-Connolly, C. J. (2017, Dec). An Effective Response: Smoldering Crisis and Capacity Cost Management. *Cost management, 31*(6), 6-29.

Received for publication: 10.12.2024
Revision submission: 20.12.2024
Accepted for publication: 08.01.2025

How to cite this article?

Style – **APA** *Sixth edition:*

Postolov, K., & Postolov, B. (2025, 01 15). Crisis Management in IT Sector Companies: The Case of the City of Skopje. (Z. Čekerevac, Ed.) *MEST Journal, 13* (1), 105-113. doi:10.12709/mest.13.13.01.10

Style - **Chicago** *Sixteenth edition:*

Postolov, Kiril and Boris Postolov. "Crisis Management in IT Sector Companies: The Case of the City of Skopje". Edited by Zoran Čekerevac. *Vesnik MEST* (MESTE) 13, no. 1 (01 2025): 105-113.

Style - **GOST** *Sort by name:*

Postolov Kiril and Postolov Boris Crisis Management in Companies from the IT Sector: The Case of the City of Skopje [Journal] // MEST Journal / ed. Cekerevac Zoran. - Belgrade – Toronto: MESTE, 01 15, 2025. - 1: Vol. 13. - pp. 105-113

Style – **Harvard** *Anglia:*

Postolov, K. & Postolov, B., 2025. Crisis Management in Companies from the IT Sector: The Case of the City of Skopje. *MEST Journal,* 15 01, 13(1), pp. 105-113.

Style – **ISO 690** *Numerical Reference:*

Crisis Management in Companies from the IT Sector: The Case of the City of Skopje. **Postolov, Kiril and Postolov, Boris.** [ed.] Zoran Cekerevac. 1, Belgrade – Toronto: MESTE, 01 15, 2025, MEST Journal, Vol. 13, pp. 105-113

MEST Journal
DOI 10.12709/mest.13.13.01.11

CHINA - CENTRAL AND EASTERN EUROPEAN COUNTRIES (CEEC) COLLABORATION ON ELECTRIC VEHICLE MARKET DEVELOPMENT

Goran Pavel Santek
China-CEEC Innovation Cooperation Research Center, Ningbo University of Technology, University of Zagreb, Croatia
https://orcid.org/0000-0003-1232-5454

Marko Vidnjevic
China-CEEC Innovation Cooperation Research Center, Ningbo University of Technology, Alma Mater Europaea - ECM, Slovenia
https://orcid.org/0009-0004-1107-1186

JEL Category: **F2**

Abstract

This paper explores China's collaboration with Central and Eastern European Countries (CEEC), specifically focusing on the partnership with Croatia in higher education, renewable energy, and electric vehicles (EVs). The analysis underscores China's dominance in the global EV market with more than half of worldwide EV sales and charging station installations. On the contrary, despite Croatia's lower overall EV sales, the country is still recognized in the EV market, particularly through the presence of Rimac. The electric vehicle industry in China is witnessing an accelerated growth trajectory, outpacing developments in Western countries. The China-CEEC collaboration could serve as a potential stepping-stone for the Chinese EV companies to enter the EU market and cooperation could play a substantial role in the global EV market's future dynamics, acting as a bridge for Chinese companies to successfully navigate the European landscape. In the context of the article, it should be mentioned that it is predicted that China will also look for ways of cooperating with Croatia in the fields of green power, smart grids, and technologies for collecting solar energy.

Keywords: *China-CEEC, Electric vehicles, Innovation, International Trade, EV market, automotive industry*

Address of the corresponding author:
Marko Vidnjevič
marko.cceec@gmail.com

1 INTRODUCTION

On April 26, 2012, the China-Central and Eastern European Countries (CEEC) Cooperation was inaugurated, establishing a cross-regional

collaborative platform rooted in longstanding friendship. Driven by a collective aspiration for mutually beneficial cooperation and shared development, the initiative has witnessed dynamic growth. Encompassing diverse domains such as economy, trade, culture, education, youth exchange, agriculture, tourism, science, technology, health, and think-tank exchange, the collaboration has proven fruitful. Beyond its multifaceted impact, the China-CEEC Cooperation has played a pivotal role in fortifying bilateral ties between China and Central and Eastern European nations, contributing significantly to the broader enrichment of China-Europe relations (China-CEEC, 2021).

Official diplomatic relations between the People's Republic of China and the Republic of Croatia were inaugurated in May 1992. Over three decades, this relationship has evolved into a remarkable collaboration, extending beyond diplomatic spheres to encompass higher education and renewable energy initiatives. Notably, the partnership between Beijing Sport University and the University of Zagreb has expanded from sports to the academic realm, marking the first agreement between the universities of China and Croatia. Furthermore, in the field of higher education, the Zagreb School of Economics and Management has fostered collaboration with eight Chinese universities. This robust academic engagement complements the growing presence of Chinese companies in Croatia, particularly evident in the completion of landmark projects such as the Peljesac Bridge. Noteworthy is the collaboration in the renewable energy sector, exemplified by the 156-megawatt Senj wind farm, a testament to the largest Chinese investment in Croatia to date. This multifaceted collaboration underscores a thriving relationship built on mutual respect, appreciation, and exemplary cooperation despite differences in size, geography, or economic strength (China-CEEC, 2022).

Prime Minister Plenkovic's endorsement of the China-CEEC Cooperation as "an excellent tool for all of us in Central and Eastern Europe" highlights its instrumental role, fostering numerous signed contracts, regular dialogue, and mutual understanding. Importantly, Plenkovic underscores the need for heightened cooperation and dialogue between China and the European Union, particularly concerning global challenges such as security, peace, and climate change, with a specific emphasis on the energy sector. He notes, "We have witnessed the spike of energy prices, and I think in that respect, the global dialogue on energy issues and energy supplies is where the EU and China should cooperate, and that, of course, includes Croatia" (China-CEEC, 2022b).

Building upon the foundation of the China-CEEC Cooperation and the multifaceted collaboration between China and Croatia, it becomes imperative to explore the dimensions of sustainability within this partnership. As we delve into the various sectors encompassed by this collaboration, a particular spotlight turns toward sustainable practices, notably in the realm of electric vehicles.

Rimac Automobili, a prominent player in the electric vehicle industry, closed a significant 30 million EUR investment deal with Camel Group Ltd., Asia's largest battery manufacturer based in China, in 2017. This substantial investment marks the single largest foreign direct investment in a Croatian technology company and aligns with Rimac's mission to redefine electric-powered vehicles. The funds will not only benefit Rimac's sister company, Greyp Bikes, but also support the launch of new products, expansion of production capacity, and global outreach. The strategic partnership underscores Rimac's position as a go-to technology provider for global automotive manufacturers and highlights its profitable trajectory since 2012. Camel Group's CEO, Liu Changlai, emphasizes the synergies between Rimac and Camel Group in delivering world-class EV components and technologies, further catalyzing the transition to a fully electric fleet. This investment adds another layer to the multifaceted collaboration narrative, showcasing the evolving landscape of sustainable practices, particularly in the electric vehicle sector, within the broader

context of international cooperation and innovation (Rimac, 2017).

Continuing the narrative of development and the collaborative efforts between China and Europe in the electric vehicle sector, the momentum continued to grow with a notable development in July 2022. When Hungary's Minister of Foreign Affairs and Economic Affairs, Peter Sialto, and Zhang Hui, Vice President of NIO Europe, jointly announced a significant initiative in Budapest—the establishment of the NIO Energy European Factory (He, Huang, Yao, Chen, & Chen, 2023).

2 ELECTRIC VEHICLE MARKET ANALYSIS

China's Electric Vehicles market is projected to achieve a revenue of US$292.1 billion in 2023. With a projected steady annual growth rate of 6.38% from 2023 to 2028, the market is forecasted to achieve a volume of US$398 billion by the conclusion of this period. Fueled by increasing demand, an estimated 8.77 million EV units are expected to be sold in China by 2028, reflecting a rising trend in consumer acceptance. The volume-weighted average price of EVs in China is forecasted to be US$46.9k in 2023. Notably, China is set to lead the global EV market in 2023, emphasizing its dominant role, driven by government subsidies and robust infrastructure supporting swift adoption (Statista, 2023a).

The electric vehicle industry in China is witnessing an accelerated growth trajectory, outpacing developments in Western countries. A notable aspect of this evolution is the proactive engagement of many Chinese automobile manufacturers in high-value activities. Driven by a desire to internationalize their presence, these manufacturers are strategically positioning themselves to introduce their cutting-edge electric vehicles into the global market. This shift underscores a decisive effort by Chinese automotive entities to position themselves at the forefront of innovation and market leadership in the rapidly evolving domain of electric vehicles (Wang, Chen, Wang, Ning, & Vanhaverbeke, 2014). Numerous Chinese electric vehicle firms, including SAIC, BYD, and Great Wall Motors, have demonstrated a notable proficiency in electric vehicle technology, surpassing that of traditional leaders in the automotive industry (Wang & Kimble, 2013).

Chinese electric vehicle firms currently hold relatively modest market shares in European markets. An illustrative example is BYD, a prominent Chinese EV leader, which delivered a mere 1500 units of passenger EVs to Norway in 2021. This limited market expansion may be attributed to unforeseen challenges that Chinese firms are encountering. Consequently, the present scenario prompts an inquiry into the adequacy of ownership advantages possessed by Chinese EV firms for achieving success in the European market and competing effectively with local rivals. Furthermore, an examination of the potential disadvantages that these Chinese firms might confront becomes a focal point of interest in understanding their position in the European EV market (Gu, Belussi, & Narula, 2023).

Chinese electric vehicle firms have surpassed their European counterparts in large-scale EV manufacturing. In 2021, Great Wall Motor, BYD, and NIO collectively produced 1,265,269, 737,502, and 92,921 EV units respectively. This contrasts with European leaders like Volkswagen, whose EVs accounted for only 20% of the total production of 1,734,973 cars. Notably, Audi produced 781,612 units with EVs constituting just 10%. The superior production capacity of Chinese firms is attributed to an established industrial cluster, particularly in the east and south of China, streamlining operations across multiple provinces. This cluster approach allows firms like SAIC to seamlessly integrate research, purchasing, and manufacturing, optimizing efficiency and reducing costs associated with transportation and communication (Gu, Belussi, & Narula, 2023).

Figure 1 outlines total battery electric vehicle (BEV) and plug-in hybrid electric vehicle (PHEV) sales in million units for both China and the global market from 2020 to 2023, along with projected sales extending to 2028. In 2020, China constituted 41.20% of the worldwide total, recording 1.31 million vehicle sales. This share increased to 50.61% in 2022, with China's sales reaching 6.09 million units. Projections indicate a continued upward trend, with an anticipated 51.53% of the global total in 2028, representing 8.77 million vehicle sales.

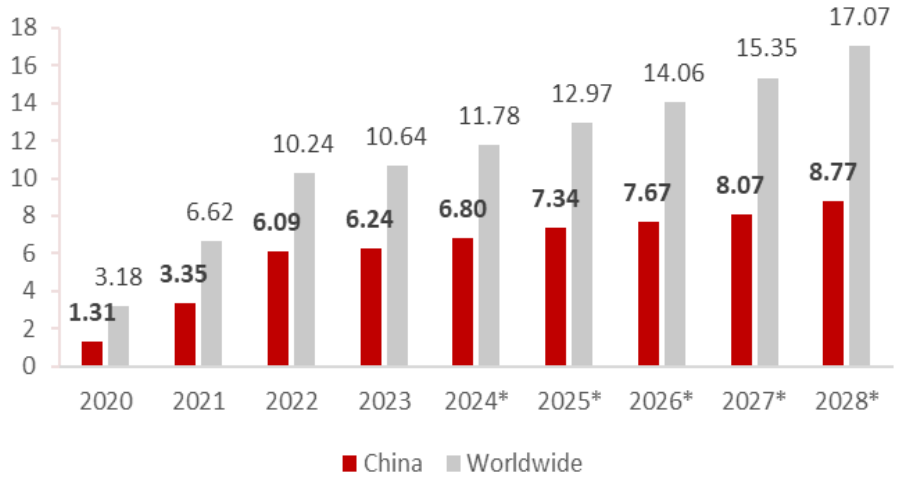


Fig. 1 Global and Chinese vehicle sales in million vehicles

Source: (Statista, 2023a)

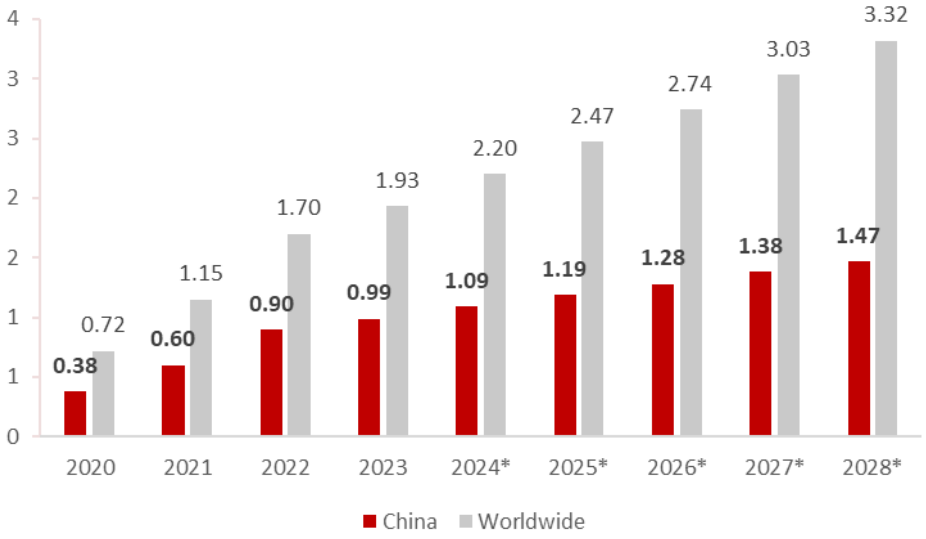


Fig. 2 Global and Chinese charging stations installed in million charges

Source: (Statista, 2023a)

China has been at the forefront of supporting the electric vehicle sector by offering subsidies since 2009. The government's sustained commitment to subsidizing EV producers engaged in public transport, taxis, and the consumer market has been instrumental in fostering the growth of the EV industry. Over the period spanning from 2009 to 2022, China allocated more than 200 billion yuan (US$28 billion) towards EV subsidies and tax incentives, solidifying its position as a global leader in the adoption and promotion of electric vehicles. Additionally, China's commitment is further underscored by a comprehensive policy framework that includes exemptions from consumption tax and vehicle & vessel tax for carmakers involved in EV production, subcontracted processing, and importation. Until the end of 2022, substantial purchase subsidies incentivize various vehicle types, including a maximum subsidy of 12,600 yuan for battery electric vehicle (BEV) passenger cars and 4,800 yuan for plug-in hybrid (PHEV) passenger cars. Furthermore, the subsidies extend to non-fast-charging BEV buses (50,400 yuan), fast-charging BEV buses (36,400 yuan), PHEV buses (21,300 yuan), BEV trucks (28,000 yuan), and PHEV trucks (17,600 yuan). The purchase tax exemption, in effect until the end of 2027, exempts new EVs purchased by December 31, 2025, and reduces the purchase tax by half for those bought between January 1, 2026, and December 31, 2027. (Yu, 2023).

The Electric Vehicles market in Croatia is projected to achieve a revenue of US$144 million in 2023. With an anticipated robust annual growth rate of 24.51% from 2023 to 2028, the market is poised to reach a projected volume of US$430.9 million by the end of this period. Fueled by growing demand, the market foresees the sale of 7,853 EV units in Croatia by 2028, indicating a positive trajectory in consumer acceptance. In 2023, the volume-weighted average price of Electric Vehicles in Croatia is forecasted to be US$ 54.4k, providing insight into the pricing dynamics within the market (Statista, 2023b).

Croatia has implemented a comprehensive set of incentives to propel the adoption of electric vehicles. These encompass registration tax benefits, exempting electric vehicles from excise duties, and ownership tax benefits, relieving owners from special environmental taxes. Notably, the government offers substantial purchase subsidies, with co-financing of up to €9,291 for BEVs and hydrogen cars, €5,309 for low-emission plug-in hybrids, and €2,640 for electric ATVs, motorcycles, and mopeds. The Ministry of Environmental Protection and Energy allocated €11.9 million in 2021, extending into 2022, to incentivize private and business purchases of BEVs. Furthermore, Croatia actively supports EV infrastructure, allocating €1.32 million in 2020 for the co-financing of charging stations. These measures collectively create a favorable environment, encouraging both individuals and businesses to embrace electric vehicles and contribute to sustainable transportation solutions (European Commission, 2023).

3 CONCLUSIONS

This paper exported the intricate collaboration between China and Central and Eastern European Countries (CEEC), focusing on the partnership with Croatia across higher education, renewable energy, and electric vehicles (EVs). The China-CEEC Cooperation, initiated in 2012, has proven to be a dynamic platform fostering fruitful collaborations in various domains. Despite China's overwhelming dominance in the global EV market, Croatia, notably through Rimac Automobili, has carved a niche, showcasing the potential for unique contributions from smaller nations.

The collaboration has strengthened bilateral ties and positioned itself as a potential steppingstone for Chinese EV companies to enter the European Union market. The endorsement of the China-CEEC Cooperation by Prime Minister Plenkovic highlights its instrumental role in fostering dialogue, understanding, and mutually beneficial contracts, especially in addressing global challenges like energy security and climate change.

As we navigate the sustainable dimensions of this partnership, the strategic investment in Rimac Automobili by China's Camel Group and the establishment of the "NIO Energy European Factory" in Hungary underscore the evolving landscape of sustainable practices in the EV sector. The continued growth of the EV market in China, supported by government subsidies and infrastructure, contrasts with the emerging market in Croatia, driven by comprehensive incentives and a positive consumer outlook.

The China-Central and Eastern European Countries (CEEC) Cooperation has the potential to significantly influence the future dynamics of the global electric vehicle (EV) market, serving as a conduit for Chinese companies to effectively navigate the European market. This partnership not only signifies a strategic convergence of economic interests but also highlights the potential for meaningful international collaboration and innovation in advancing sustainable transportation solutions.

WORKS CITED

China-CEEC. (2021). *About Us*. Retrieved from Cooperation between China and Central and Eastern European Countries: http://www.china-ceec.org/eng/jj/zyjz/202112/t20211228_10476286.htm

China-CEEC. (2022). *China-Croatia ties have rapidly flourished*. Retrieved from Cooperation between China and Central and Eastern European Countries: http://www.china-ceec.org/eng/zzwl/202203/t20220304_10647986.htm

China-CEEC. (2022b). *Croatia looks forward to deepening ties with China: Croatian PM*. Retrieved from Cooperation between China and Central and Eastern European Countries: http://www.china-ceec.org/eng/zzwl/202205/t20220527_10693471.htm

European Commission. (2023). *European Commission*. Retrieved from European Alternative Fuels Observatory: https://alternative-fuels-observatory.ec.europa.eu/transport-mode/road/croatia/incentives-legislations

Gu, Y., Belussi, F., & Narula, R. (2023). Entering European countries: advantages and difficulties for Chinese electric vehicle firms. *Marco Fanno Working Papers*, 1-30. doi:https://www.economia.unipd.it/sites/economia.unipd.it/files/20230302.pdf

He, B., Huang, X., Yao, S., Chen, G., & Chen, Y. (2023). Analysis of Internationalization Strategy Problems and Countermeasures of NIO Automobile. *World Journal of Information Technology, 1*(1), 35-50.

Rimac. (2017). *Rimac Closes 30M EUR Investment With*. Retrieved from Rimac: https://www.rimac-automobili.com/media/press-releases/rimac-closes-30m-eur-investment-with-camel-group/

Statista. (2023a). *Electric Vehicles - China Statista*. Retrieved from Statista: https://www.statista.com/outlook/mmo/electric-vehicles/china

Statista. (2023b). *Electric Vehicles - Croatia*. Retrieved from Statista: https://www.statista.com/outlook/mmo/electric-vehicles/croatia

Wang, F., Chen, J., Wang, Y., Ning, L., & Vanhaverbeke, W. (2014). The effect of R&D novelty and openness decision on firms' catch-up performance: Empirical evidence from China. *Technovation, 34*(1), 21-30. doi:https://www.researchgate.net/publication/259117753_The_effect_of_RD_novelty_and_openness_decision_on_firms'_catch-up_performance_Empirical_evidence_from_China

Wang, H., & Kimble, C. (2013). Innovation and Leapfrogging in the Chinese Automobile Industry: Examples From Geely, BYD, and Shifeng. *Global Business and Organizational, 32*(6), 6-17.

Yu, B. (2023). *China Dialogue*. Retrieved from Life after subsidies for China's EVs: https://chinadialogue.net/en/business/life-after-subsidies-for-chinas-evs/#:~:text=More+than+200+billion+yuan,support+and+subsidies+have+declined

Received for publication: 23.02.2024
Revision received: 29.03.2024
Accepted for publication: 08.01.2025.

How to cite this article?

Style – **APA** *Sixth Edition:*

Santek, G. P., & Vidnjevic, M. (2025, 01 15). China - Central and Eastern European Countries (CEEC) Collaboration on Electric Vehicle Market Development. (Z. Cekerevac, Ed.) *MEST Journal, 13*(1), 114-120. doi:10.12709/mest.13.13.01.11

Style – **Chicago** *Sixteenth Edition:*

Santek, Goran Pavel, and Marko Vidnjevic. "China - Central and Eastern European Countries (CEEC) Collaboration on Electric Vehicle Market Development." Edited by Zoran Cekerevac. *MEST Journal* (MESTE) 13, no. 1 (01 2025): 114-120.

Style – **GOST** *Name Sort:*

Santek Goran Pavel and Vidnjevic Marko China - Central and Eastern European Countries (CEEC) Collaboration on Electric Vehicle Market Development [Journal] // MEST Journal / ed. Cekerevac Zoran. - Belgrade – Toronto : MESTE, 01 15, 2025. - 1 : Vol. 13. - pp. 114-120.

Style – **Harvard** *Anglia:*

Santek, G. P. & Vidnjevic, M., 2025. China - Central and Eastern European Countries (CEEC) Collaboration on Electric Vehicle Market Development. *MEST Journal,* 15 01, 13(1), pp. 114-120.

Style – **ISO 690** *Numerical Reference:*

China - Central and Eastern European Countries (CEEC) Collaboration on Electric Vehicle Market Development. **Santek, Goran Pavel and Vidnjevic, Marko.** [ed.] Zoran Cekerevac. 1, Belgrade – Toronto : MESTE, 01 15, 2025, MEST Journal, Vol. 13, pp. 114-120.

MEST Journal
DOI 10.12709/mest.13.13.01.12

LEARNING INTERNATIONAL ECONOMICS AND TRADE IN A TRANSNATIONAL PROGRAM: A PHENOMENOLOGICAL STUDY

Xiantong Zhao
Faculty of Education, Southwest University, Chongqing, China
https://orcid.org/0000-0002-9599-0689

Qian Lai
Faculty of Education, Southwest University, Chongqing, China

Hang Yi
Faculty of Education, Southwest University, Chongqing, China

Renying Xu
Faculty of Education, Southwest University, Chongqing, China

JEL Category: **A22, I21**

Abstract

This phenomenological study delves into the learning experiences of Chinese undergraduate students enrolled in a transnational International Economics and Trade program, which is collaboratively run by Chinese and Australian universities. Through in-depth semi-structured interviews with 23 students from various years of study, the research aims to uncover how these students navigate and derive meaning from their experiences within a cross-cultural educational setting. Data analysis reveals three prominent themes: the differences in course design for state-planned versus non-state-planned students, the challenges posed by intensive academic demands and diverse assessment methods, and the necessity of adapting to distinct teaching methodologies prevalent in the two educational systems. The findings underscore the urgent need for improved administrative coordination, enhanced collaboration among Chinese and Australian teaching staff, and better preparation for students entering transnational programs. This study significantly contributes to the understanding of the complexities inherent in cross-border higher education, providing valuable insights that can inform strategies to enhance teaching quality and enrich student experiences in similar international programs.

Keywords: *Transitional program; Chinese undergraduates; Learning experience; Cross-cultural educational environment; Phenomenology*

Address of the corresponding author:
Xiantong Zhao
zxt1981@swu.edu.cn

1 INTRODUCTION

The internationalization of higher education is an ongoing process that incorporates cross-cultural and global factors into the goals and operations of universities (Knight, 2003). In the field of higher education in China, internationalization is embodied in various forms and strategies, which are prominently reflected in the mobility of students and scholars, academic cooperation, and collaborative research projects (Huang, 2007). A key aspect of this process is the integration of international partnerships and educational models that bridge diverse educational systems, which are essential for enhancing the global competitiveness of Chinese universities.

In China, TNHE is widely called Chinese Foreign Cooperation in Running Schools (CFCRS) (Hou et al., 2014). CFCRS encompasses joint institutions and programs (Yang, 2014) and plays a pivotal role in the internationalization of Chinese universities (Huang, 2007). The CFCRS program, also known as Zhongwai Hezuo Banxue Xiangmu, represents collaborative ventures between local Chinese universities and foreign or overseas higher education institutions aimed exclusively at educating Chinese students (Hou et al., 2014). These partnerships also facilitate the exchange of best practices in management, teaching methodologies, and technology integration, which are crucial for adapting to the demands of the global educational landscape. For the convenience of international readers, the term ‘transnational programs’ is used throughout this paper instead of ‘CFCRS programs’, although these terms are interchangeable within the context of Chinese higher education.

These programs employ teaching staff from both foreign partner universities and Chinese institutions, offering courses that combine language learning with specialized subject instruction in a foreign language. Key educational resources, such as curricula, instructional outlines, textbooks, and teaching technologies, are sourced from partner foreign universities. The diverse teaching and learning methods include group discussions, presentations, role-plays, and business simulation games. Additionally, foreign partner universities’ assessment methods have been incorporated to enrich the traditionally exam-focused Chinese evaluation system. This blend of resources and methodologies creates a cross-cultural educational environment. Such collaborations also serve as a model for innovative educational practices, contributing to the transformation of educational management in China.

While many studies have been conducted on different aspects of TNHE in China, including its historical development, policy framework, and challenges (Huang, 2008; Wang, 2016; Yang, 2008), studies that have specifically concentrated on Chinese students' actual learning experiences in cross-system educational settings remain very limited (Qin & Te, 2016). As Dai, Lingard, and Musofer (2019) point out, learning in the CFCRS means learning between two education systems (Chinese system vs. foreign system) and the disparities between educational systems can be double-edged - they might serve as valuable learning experiences, but could also pose adjustment difficulties for students (Dai, Matthews & Renshawc 2019). According to Cook-Sather (2006), students' voices are essential for educators and institutions aiming to gain insight into the realities of specific educational programs and environments. In the context of global education systems, understanding the lived experiences of students within transnational programs is crucial for improving the management and quality of these transnational collaborations. Dai and Garcia (2019) further argue that understanding students’ authentic learning experiences helps to examine the quality of TNHE from a micro perspective. Therefore, this research aims to enrich the body of knowledge by exploring the students’ lived experiences of learning in a transnational program jointly run by a Chinese university and an Australian university.

2 METHODOLOGY

2.1 Research setting and participants

The transnational program of interest for this study is an International Economics and Trade (IET) program, jointly developed by a Chinese university and an Australian university in 2004 and later accredited by the Chinese MOE (Ministry of Education). Extensive educational resources provided by the Australian partner university were integrated into the transnational program at the Chinese higher education institution,

encompassing the curriculum, instructional frameworks, teaching materials (such as textbooks), pedagogical methodologies, and academic personnel.

Students completing the IET program are required to develop comprehensive skills in economic theory, analytical thinking, and global financial concepts. The curriculum emphasizes proficiency in English across all communication modes, along with a strong mathematical and statistical foundation. Graduates must demonstrate expertise in market analysis, business administration, and quantitative research methods. The program also emphasizes personal qualities such as flexibility, collaborative skills, creative thinking, and ethical awareness.

The curriculum combines diverse business-related subjects, delivered through a unique bilateral teaching approach. While some courses are conducted by Chinese faculty members, many are jointly taught by Chinese and Australian instructors in both languages. Additionally, certain language-focused courses are exclusively led by international faculty. Students face significant academic demands, including adapting to Australian teaching methods and improving their English proficiency early in the program. The intensive curriculum requires students to complete approximately 200 credits over four years, often resulting in extended daily schedules from morning until evening.

The research participant selection followed specific guidelines. Eligible students needed to be transnational IET program learners with experience in internationally-taught courses. The study aimed to include students from all year levels while maintaining gender balance. The final participant group comprised 23 students (7 males, 16 females) distributed across different academic years: 8 first-year, 11 second-year, 2 third-year, and 2 fourth-year students. This sample size aligns with Creswell and Poth's (2018) guidelines for phenomenological research, which suggest that 1-30 participants are appropriate.

Before the start of the interview, all participants were informed about the overall objectives of the research and their rights related to the interview process. Each participant completed a student information sheet that collected personal details such as age, gender, year of study, and major courses. It is important to note that all participants, regardless of whether they were first-year or fourth-year students, were enrolled in the Chinese university exclusively to pursue the transnational program. This program is essentially a '4+0' model, where the number before the '+' indicates the years spent at local Chinese universities, and the number after the '+' represents the years spent at partner universities abroad.

2.2 Data collection and analysis

Phenomenology is particularly well-suited for understanding the subjective, lived experiences of individuals (Creswell & Poth, 2018). Van Manen (1990) identified phenomenology as the study of the essence of experiences, which can be best understood in detail within a context. The present research concerns a group of undergraduates' lived learning experience in a transnational IET program, making it ideal for a phenomenological approach. Moreover, transnational programs are complex, multilevel learning experiences determined by institutional, cultural, and personal factors. Phenomenology allows the researcher to delve deeply into participants' perspectives, uncovering nuances that might otherwise have gone undetected when using other research approaches. Furthermore, the phenomenological method has been working well in exploring learning and adaptation in transnational contexts, as existing phenomenological studies have revealed subtle processes such as skill acquisition, acculturation, and self-development (Ruddock & Turner, 2007). We, therefore, believed that applying phenomenology would help us gain in-depth insight into the way students of transnational programs constructed meaning from their academic and cultural experiences and offer a deeper understanding of their learning journey in a cross-cultural environment.

This research adopted the interpretive phenomenological approach since interpretive phenomenology fundamentally focuses on the process of meaning-making, which helps the researchers uncover how students made sense of their experiences in this transnational program. The way that students interpret their experiences and give meaning to these experiences is of great concern since it can strongly influence their learning outcomes and satisfaction with the

program. Realizing that the aim of this study is not to reveal the essence of learning in a transnational program (Moustakas, 1994), we abandoned transcendental phenomenology in favor of interpretive phenomenology.

We employed semi-structured interviews as the primary means to collect data. The main interview questions included: Can you describe specific moments or activities that were particularly memorable, impactful, or meaningful in your learning? What did these experiences mean to you? What did you learn from them? Meanwhile, we also collected textual materials such as student handbooks and teaching syllabi as supplementary materials. It was expected that the use of diverse data sources would help alleviate the limitations and biases associated with relying on a single method, thereby enhancing the credibility and robustness of the research and improving the validity and reliability of the findings (Patton, 1999).

In analyzing the data, we followed the procedures proposed by Smith, Flowers, and Larkin (2009). We began by reading the transcripts multiple times and listening to the audio recordings to engage with the content and ensure a comprehensive understanding. Following this, an initial noting phase was completed where we produced detailed annotations, focusing on semantic content, language use, and explicit meanings that were conveyed by participants. Interpretative insights were also included to show how and why participants said what they did in the context of any emerging patterns of meaning. In the developing emergent themes phase, these annotations were used to generate concise themes that reflected key features of the participants' accounts. This involved the synthesis of descriptive comments with interpretative insights, with irrelevant data points being discarded to maintain focus on the research aims. Mapping of emergent themes was undertaken to explore relationships across these so that the emergent and super-ordinate themes were organized into a structured presentation for each participant. Data from each participant was analyzed separately. During this process, themes from prior cases were bracketed to allow each analysis to remain firmly embedded in the participant's distinctive account. Afterward, the themes were identified across cases by grouping similar themes and identifying links between them. Finally, themes were further refined, named, and integrated into super-ordinate themes, which captured shared experiences while honoring individual nuances.

3 FINDINGS & DISCUSSION

The interpretive phenomenological analysis of the interview data led to the identification of three themes that reflect the Chinese undergraduates' learning experience in the transnational IET program.

3.1 Subtle differences in course design: state-planned vs. non-state-planned students

This study revealed two distinct categories of undergraduate enrollment: state-planned and non-state-planned students. According to Mok and Ong (2014), students who complete the Gao Kao (College Entrance Examination) and receive university placement through the national quota system are classified as state-planned students. In contrast, non-state-planned students encompass those who enter universities through alternative pathways, such as self-funded students or adult learners who did not gain admission through the traditional Gao Kao.

Based on an analysis of the student handbook and syllabi we collected, there were slight variations in the curricula that students were required to complete. Specifically, over the four years, state-planned undergraduates needed to complete 51 mandatory courses and 31 elective courses, while non-state-planned undergraduates were expected to take 44 mandatory courses and 22 electives. Among these courses, 22 differed between the two groups, indicating that state-planned and non-state-planned students shared the majority of their courses.

Examining the courses offered in this transnational IET program highlights the discipline's comprehensive nature. The curriculum draws extensively from various business-related fields and includes both 'hard' and 'soft' knowledge components. The 'hard' components typically involve technical aspects with universal rules, which Corder (1990) describes as subject-dependent, such as accounting. In contrast, the

'soft' components are more contextually dependent, reflecting environmental influences, as noted by Corder (1990), such as marketing.

3.2 Struggling to cope: course taking and exams

This transnational IET program mandates that undergraduates take courses hosted by both Chinese and Australian lecturers, which results in a demanding academic schedule. According to the student handbook, all Chinese students must earn approximately 200 credit points across various courses to fulfill both Chinese and Australian degree requirements. This intensive workload helps explain why students frequently mention feeling overwhelmed by the number of classes and academic pressure.

Another source of pressure comes from the exams and quizzes. Similar to what Dai and colleagues (2019; 2020) have found, both Chinese and Australian lecturers had their preferred way of examining. The Chinese teachers frequently assessed students based on a single final exam taken at the end of the semester. This closed-book exam remained a predominant and high-stakes method of evaluation. As S19 summarized: "Chinese teachers have large exams, with the university organizing the time and location, and everyone attends to take the exam." Such a finding is in line with Dai, Matthews, and Renshaw (2020) and Dai, Matthews, and Reyes (2019) who discovered that the main method of assessment in China centered on textbook examinations. S17 expressed dissatisfaction with this assessment approach:

> *I don't like the way Chinese teachers test, because it's so concentrated, and there are so many predetermined key points you have to memorize. You need to retain all that information, and then the following two weeks are especially exhausting.*

This experience sharply contrasts with what Dai, Lingard, and Musofer (2019) and Dai, Matthews, and Reyes (2019) found in their studies, where Chinese participants felt it was easier and less pressured to pass exams in Chinese universities. While Dai, Matthews, and Renshaw (2020) did not further explore the reasons for the dominance of the textbook-focused exam, we found that it could be attributed to the university's policy. The university mandated that certain courses, particularly required ones, must have a final closed-book exam. As S20 noted, "The university's regulations require that all mandatory courses hosted by Chinese lecturers have a final exam, and this exam must be closed book." This policy limits teachers' ability to adopt alternative assessment methods like those used in primary and secondary education for evaluating college students.

However, some Chinese lecturers have begun to adopt evaluation methods from Western countries, gradually transitioning toward a more process-oriented approach. This method prioritizes students' actual performance and engagement throughout the learning process, offering timely assessments of their learning quality, recognizing achievements, and identifying areas for improvement. S6 shared:

> *For example, in our class, one part of the grade is based on the final exam score, and the other part comes from regular assignments, such as homework, essays, and group discussions. Attendance also contributes to the regular grade. The final exam score is weighted, and then, both components are combined to determine the final grade.*

This unique finding has seldom been made in prior studies (e.g. Dai, Matthews, & Reyes, 2019).

Australian lecturers prioritized ongoing assessment of academic performance throughout the learning process. As S1 observed, "The foreign teachers pay more attention to the regular grades and individual performance. We have exams now and then." Similarly, S10 remarked that Australian teachers "definitely emphasize the assessment during the regular classes, which is different from Chinese teachers." Furthermore, the assessment formats in Australian classrooms are notably diverse. S14 commented, "The foreign teachers have an exam every one-and-a-half month or so. Sometimes it is a speech, sometimes it is writing." These findings align with what Dai, Matthews, and Reyes (2019) revealed. While Dai, Matthews, and Reyes (2019) focus research on Chinese students who experience examinations at Australian universities, our study examines Chinese undergraduate students who undergo Australian-style examinations within the

transnational IET program in mainland China. In other words, the Chinese students in our research can engage with and experience the assessment methods of Australian higher education without the need to travel abroad.

Another distinguishing feature of Australian assessments is the use of clear scoring points, with evaluations following well-defined standards and criteria. For instance, S15 illustrated this with a recent exam, stating:

> *There are scoring points for content, as well as eye contact, body language, and being able to speak without notes during the speech. And then there is grammar, with different tenses and sentence structures.*

Most interviewed students expressed satisfaction with the assessment methods used by Australian teachers. They highlighted the process-oriented nature of these assessments, which provided ongoing supervision and encouraged learners to focus on consistent effort and participation. S2 explained:

> *The foreign teacher's evaluation method provides ongoing monitoring. Regular exams mean you will not feel as stressed as you would in classes where the review only starts at the end of the term. They constantly remind you to study hard and take class seriously.*

Other students, however, expressed that they did not favor the Australian way of assessment. S19 mentioned:

> *... for an exam like this with a foreign teacher, I must constantly prepare for it. I am very anxious, and the exam can only be taken in English, whether it is spoken, written, or performed.*

This negative opinion contrasts with existing findings (e.g., Dai, Matthews, and Reyes, 2019), in which Chinese learners generally hold a positive view of the exam methods employed by foreign universities and tend to evaluate these methods quite favorably.

Within this transnational IET program, all students must undertake both Chinese and Australian curricula, resulting in a substantial assessment burden. The academic evaluation framework encompasses conventional Chinese assessment methodologies and novel Australian evaluation protocols, collectively contributing to an intensified academic workload. Chinese learners consistently experience significant challenges in meeting these diverse assessment requirements. Moreover, these students must demonstrate considerable cognitive flexibility in alternating between Chinese and Western academic assessment paradigms to achieve satisfactory academic outcomes and maintain passing grades across all course components.

3.3 Facing different teaching: learning between the familiar and unfamiliar

All undergraduates in this transnational IET program were exposed to a diverse array of teaching styles and methodologies. While they were accustomed to the Chinese educational approach, the Australian pedagogical methods were unfamiliar to them. As a result, their learning experience was shaped by navigating the interplay between the familiar and the unfamiliar.

Most participants were impressed by the novel instructional approaches used by the Australian lecturers, such as cooperative learning, which represents an innovative pedagogical approach emphasizing mutual assistance among group members. This teaching method assigns clearly defined roles to participants, fostering collaboration to achieve a common goal. By engaging in cooperative learning, students are encouraged to balance their interests with the collective needs of the group (Johnson & Johnson, 1987). The Australian teaching staff adeptly employed this instructional strategy, with students demonstrating approval and enthusiasm for such activities. For instance, S19 vividly recalled a classroom activity:

> *Last semester, we had a debate between groups. Each group presented their respective arguments, followed by an inter-group debate conducted entirely in English. The highlight was a decisive group at the end, which determined the winners and awarded prizes.*

Such activities exemplify how cooperative learning can combine academic rigor with student engagement, particularly in language and debate-focused settings. Moreover, the Australian lecturers facilitated the organization of Chinese

learners into diverse groups, enabling them to engage in presentations and role-playing activities.

Although the teaching methods employed by Australian lecturers effectively captured the attention of Chinese learners and enhanced their engagement, they also led to some misunderstandings and confusion. That was particularly evident when the Australian instructors provided students with significant freedom. For instance, S23 recalled, "In our economics class, the teacher asked us to prepare an activity, come up with our ideas, choose or create a brand, and express the characteristics of the service ourselves." Some students felt quite perplexed when first encountering this approach.

> *The foreign teacher would not tell us how to proceed in the middle; they just told us what needed to be completed in the end. It was quite confusing because we did not know what the specific requirements were. (S23)*

However, students eventually realized that:

> *… all those things were in the book. When I looked at it again, I felt that the teacher did not need to explain it in class, and I understood the lecturer better. (S17)*

It was found that the traditional lecture-based teaching method remained predominant in many Chinese classrooms and was often delivered in a rigid and didactic manner. That echoed Dai, Matthews, and Renshaw (2020), who observed that Chinese lecturers tended to position themselves at the center of the classroom and directly impart detailed knowledge in transnational programs.

However, some educators are pioneering innovative strategies to enhance student participation and accountability. The Chinese instructors implemented a variety of interactive strategies, including group activities, presentations, and role-playing exercises in the classroom. For example, S19 recounted a specific activity arrangement conducted in a course led by a Chinese teacher:

> *The teacher split us into a few groups at the start of the semester. And then, in each class, one group would come up to do a news report. You could pick your way, like record a video or be a host or something and talk about the companies that you think are popular at the moment, like their marketing strategies and stuff.*

Moreover, S2 detailed the procedures for a role-play activity:

> *If it is a role-play, it is a group of roughly two to three people. You will be given a topic to make up your own story. You will have about 5 minutes to get ready. After 5 minutes, one group will be randomly chosen to go up and act it out.*

It is noteworthy that, although many students are captivated by the teaching methods of foreign instructors, a cohort of students still prefers the traditional Chinese classroom approach. For instance, student S6 expressed this preference.

> *It is just a habit from my school days before. I am still more used to the way Chinese teachers do it. They give us more exercises to do. Foreign teachers are more likely to have class discussions or do activities they think are fun, like group discussions and such.* I am still more used to having the teacher in class and giving us some questions to complete.

This participant appeared unable to differentiate between middle school and university education, as he continued to adopt a learning style more suited to middle school, preferring to improve his academic performance through repetitive exercises. Additionally, when discussing why she preferred courses taught by Chinese instructors, S2's response revealed another reason: a sense of fulfillment or the richness and compactness of the course content. This packed and fast-paced learning experience gave S2 a feeling of productivity and a strong sense of achievement in her studies.

> *It makes our classes feel quite fulfilling; the entire lesson is packed with content. It makes the classes more interesting, and I think the arrangement is good. I enjoy these fulfilling and busy classes. After finishing a lesson, I feel really happy, like, 'Oh, I learned a lot!'*

According to Dai, Matthews, and Renshaw (2020) and Dai, Lingard, and Musofer (2019), the divergent instructional methodologies employed by foreign and Chinese faculty yielded contrasting learning orientations: foreign educators' student-centered approach facilitated independent

learning practices, while Chinese instructors' teacher-dominated pedagogical style fostered student dependence on detailed scope transmission. We contend that the differences between these two teaching approaches cannot be fully equated with the distinction between foreign and local faculty members. In other words, it cannot be assumed that Australian teachers inherently favor student-centered teaching methods, while Chinese teachers invariably adhere to teacher-centered approaches. As our findings suggest, some Chinese teachers in the transnational IET program also employ diverse teaching methods to create more dynamic classrooms, effectively fostering student engagement, initiative, and creativity. It is also noteworthy that Chinese undergraduates have their preferred styles and approaches to teaching, and they might not highly evaluate or even get used to the Western lecturers' ways of instruction easily.

4 CONCLUSIONS & IMPLICATIONS

Using an interpretive phenomenological approach this research explores Chinese undergraduate students' learning experience in a transnational IET program through three main themes. This study contributes to the existing body of knowledge by offering valuable insights into the complexities and nuances of implementing transnational IET programs in Chinese higher education institutions.

The research provides some empirical data for improving the teaching quality of transnational IET programs in the higher education internationalization context. Some suggestions and implications regarding the teaching and learning practice can be:

1. First, it is recommended that at the institutional level, the university should improve the administrative system to provide better services for transnational IET programs. Cross-border joint ventures may be more demanding in terms of institution-level support and management. For example, the student assessment and workload found in this study are much related to the teaching-learning administrative system. The rigid assessment method demonstrates the institution's inflexibility in managing transnational programs. These inflexible regulations potentially and negatively influence Chinese teachers' enthusiasm to reform teaching and assessment through transnational programs. Taking courses taught by teaching staff from two different cultures can be both exciting and exhausting, which is why the students are so overworked. Managers and educators should realize that good learning outcomes are not necessarily related to the amount of workload. In other words, superabundant curricula and tasks would not lead to better learning outcomes. Therefore, it is recommended that both Chinese and Australian administrators should work together to find a sound approach to help learners achieve better results using appropriate learning tasks and workload.
2. Second, both Chinese and Australian teachers should increase opportunities for promoting communication and cooperation in teaching. It is found in the present research that many Chinese teachers have studied abroad, particularly in some English-speaking countries. They are thus expected to have few linguistic and cultural barriers while communicating with their foreign counterparts. Given that many Australian teachers have very limited time in China, it is suggested that Chinese teachers proactively communicate thoughts and ideas about teaching with the Australians. Both groups should learn from the students' feedback to improve their teaching.
3. Third, the learners themselves are advised to cherish their educational opportunities to learn in the transnational programs. The tuition fee for such a cross-border joint program was found to be very high, about four times higher than that of normal domestic programs. However, their money can be well spent, since all of them experience a cross-cultural learning and teaching environment, which is impossible for other domestic programs. Given that foreign teachers often provide much freedom in learning, the students are expected to be enthusiastic and change their role from passive to active. It is found that most foreign teachers are friendly and tolerant and welcome the Chinese learners' willingness to communicate with them.

WORKS CITED

Ashton-Hay, S., Wignell, P., & Evans, K. (2016). International student transitioning experiences: Student voice. *Journal of Academic Language and Learning*, (10), A1–A19.

Corder, C. (1990). *Teaching hard, teaching soft: A structured approach to planning and running effective training courses*. Gower.

Cook-Sather, A. (2006). Sound, presence, and power: "Student voice" in educational research and reform. *Curriculum Inquiry, 36*(4), 359–390.

Creswell, J. W., & Poth, C. N. (2018). *Qualitative inquiry and research design: Choosing among five approaches* (4th ed.). SAGE.

Dai, K., Garcia, J. (2019). Intercultural learning in transnational articulation programs: The hidden agenda of Chinese students' experiences. *Journal of International Students, 9*(2), 362–383.

Dai, K., Lingard, B., & Musofer, R. P. (2019). Mobile Chinese students navigating between fields: (Trans)forming habitus in transnational articulation programmes? *Educational Philosophy and Theory, 52*(12), 1329–1340.

Dai, K., Matthews, K. E., & Reyes, V. (2019). Chinese students' assessment and learning experiences in a transnational higher education programme. *Assessment & Evaluation in Higher Education, 45*(1), 70–81.

Dai, K., Matthews, K. E., & Renshaw, P. (2020). Crossing the 'bridges' and navigating the 'learning gaps': Chinese students learning across two systems in a transnational higher education programme. *Higher Education Research & Development, 39*(6), 1140–1154.

Hou, J., Montgomery, C., & McDowell, L. (2014). Exploring the diverse motivations of transnational higher education in China: Complexities and contradictions. *Journal of Education for Teaching, 40*(3), 300–318.

Huang, F. (2007). Internationalization of higher education in the developing and emerging countries: A focus on transnational higher education in Asia. *Journal of Studies in International Education, 11*(3–4), 421–432.

Huang, F. (2008). Regulation and practice of transnational higher education in China. In L. Dunn & M. Wallace (Eds.), *Teaching in transnational higher education: Enhancing learning for offshore international students* (pp. 23–33). Routledge.

Johnson, D. W., & Johnson, R. T. (1987). *Learning together and alone: Cooperative, competitive, and individualistic learning*. Prentice-Hall, Inc.

Knight, J. (2003). Updated internationalization definition. *International Higher Education*, (33), 2–3.

Mok, K. H., & Ong, K. C. (2014). Transforming from "Economic Power" to "Soft Power": Transnationalisation and internationalization of higher education in China. In Q. Li & C. Gerstl-Pepin (Eds.), *Survival of the fittest: The shifting contours of higher education and the United States* (pp. 171–188). Springer.

Moustakas, C. (1994). *Phenomenological research methods*. Sage Publications

Patton, M. Q. (1999). Enhancing the quality and credibility of qualitative analysis. *Health Services Research, 34*(5), Part II, 1189–1208.

Qin, Y., & Te, A. Y. C. (2016). Cross-border higher education in China: How the field of research has developed. *Chinese Education & Society, 49*(4–5), 303–323.

Ruddock, H. C., & Turner, D. S. (2007). Developing cultural sensitivity: Nursing students' experiences of a study abroad programme. *Journal of Advanced Nursing, 59*(4), 361–369.

Smith, J. A., Flowers, P., & Larkin, M. (2009). *Interpretative phenomenological analysis: Theory, method, and research*. Sage Publications.

van Manen, M. (1990). *Researching lived experience: Human science for an action sensitive pedagogy*. Althouse Press.

Wang, T. (2016). Intercultural dialogue framework for transnational teaching and learning. In K. Bista & F. Charlotte (Eds.), *Campus support services, programs, and policies for international students* (pp. 223–242). IGI Global.

Yang, R. (2008). Transnational higher education in China: Contexts, characteristics and concerns. *Australian Journal of Education, 52*(3), 272–286.

Yang, R. (2014). China's strategy for the internationalization of higher education: An overview. *Frontiers of Education in China, 9*(2), 151–162.

Received for publication: 03.12.2024
Revision received: 11.12.2024
Accepted for publication: 08.01.2025.

How to cite this article?

Style – **APA** *Sixth Edition:*

Zhao, X., Lai, Q., Yi, H., & Xu, R. (2025, 01 15). Learning International Economics and Trade in a Transnational Program: A Phenomenological Study. (Z. Cekerevac, Ed.) *MEST Journal, 13*(1), 121-130. doi:10.12709/mest.13.13.01.12

Style – **Chicago** *Sixteenth Edition:*

Zhao, Xiantong, Qian Lai, Hang Yi, and Renying Xu. "Learning International Economics and Trade in a Transnational Program: A Phenomenological Study." Edited by Zoran Cekerevac. *MEST Journal* (MESTE) 13, no. 1 (01 2025): 121-130.

Style – **GOST** *Name Sort:*

Zhao Xiantong [et al.] Learning International Economics and Trade in a Transnational Program: A Phenomenological Study [Journal] // MEST Journal / ed. Cekerevac Zoran. - Belgrade – Toronto : MESTE, 01 15, 2025. - 1 : Vol. 13. - pp. 121-130.

Style – **Harvard** *Anglia:*

Zhao, X., Lai, Q., Yi, H. & Xu, R., 2025. Learning International Economics and Trade in a Transnational Program: A Phenomenological Study. *MEST Journal,* 15 01, 13(1), pp. 121-130.

Style – **ISO 690** *Numerical Reference:*

Learning International Economics and Trade in a Transnational Program: A Phenomenological Study. **Zhao, Xiantong, et al.** [ed.] Zoran Cekerevac. 1, Belgrade – Toronto : MESTE, 01 15, 2025, MEST Journal, Vol. 13, pp. 121-130.

Reviewers of the MEST Journal – alphabetically

1. Dr. **Ahmed Jabbar Abid**, Asst. Prof., Middle Technical University, Baghdad, Iraq
2. Dr. **Svetlana Anđelić**, Prof., Information Technology School - ITS, Belgrade, Serbia
3. **Dragan Anucojić**, Mgr., Independent researcher, Belgrade, Serbia
4. Dr. **Dragutin Ž. Arsić**, Assoc. Prof., Faculty of Business and Law of the "MB" University Belgrade, Belgrade, Serbia
5. Dr. **Suat Askin**, Asst. Prof., Adiyaman University, Adıyaman Merkez/Adıyaman, Turkey
6. **Olga Artemenko**, PhD, Bukovinian University, Faculty of Computer Sciences and Technologies, Chernivtsi, Ukraine
7. Dr. **Daniel Badulescu**, Prof., Faculty of Economic Sciences, University of Oradea, Romania
8. Prof. Dr. **Milan Beslać**, Faculty of Business Economy and Entrepreneurship in Belgrade, Belgrade, Serbia
9. Dr. sc. **Mario Bogdanović**, Prof., Istrian University of Applied Sciences Pula, Croatia
10. Dr. **Nikola Bračika**, Assoc. Prof., Business School Čačak, Belgrade, Serbia
11. Mr **Nemanja Budimir**, Agency for Bookkeeping "Budimir", Banja Luka, Bosnia and Herzegovina
12. CSc. **Anastasia Bugaenko**, "Ukrgasbank", Kyiv, Ukraine
13. Prof. **Justyna M. Bugaj**, Jagiellonian University, Krakow, Poland
14. Prof. Dr. **Ana Čekerevac**, University Belgrade Faculty of Political Sciences, Belgrade, Serbia
15. Prof. Dr. **Zoran Čekerevac**, Independent researcher, Belgrade, Serbia
16. **Sanja Čukić**, MA, Faculty of Business and Law, "MB" University, Belgrade, Serbia
17. Dr. **Dražen Ćućić**, Assistant Professor, Faculty of Economics in Osijek, Osijek, Croatia
18. Dr. **Radmila Ćurčić**, Ass. Prof., Faculty of Business and Law, "MB" University, Belgrade, Serbia
19. Prof. Dr. **Sreten Ćuzović**, Faculty of Economics, University of Niš, Niš, Serbia
20. Prof. Dr. **Predrag Damnjanović**, Business School Čačak, Belgrade, Serbia
21. Prof. Dr. **Branko Davidović**, Technical College, Kragujevac, Serbia
22. Dr. **Derya Dispinar**, Asst. Prof., Istanbul University, Metallurgical and Materials Engineering, Avcilar, Istanbul, Turkey
23. Prof. Ing. **Zdenek Dvorak**, PhD, Faculty of Special Engineering University of Žilina, Žilina, Slovakia
24. **Bela Yu. Dzhamirze**, PhD, Assoc. Prof., Maikop State Technological University, Maikop, Russia
25. Prof. Dr. **Branislav Đorđević,** Emeritus, Belgrade, Serbia
26. Prof. Dr. **Branko Đurović**, Medical Faculty, University of Belgrade, Belgrade, Serbia
27. **Ljupčo Eftimov**, PhD, Asst. Prof., Faculty of Economics - Skopje, Skopje, R. Macedonia
28. Prof. **Valeriy Eudokymenko**, DrSc, Bukovinian State Finance and Economics University, Chernivtsi, Ukraine
29. Ing. **Stanislav Filip**, PhD, Assoc. Prof., School of Economics and Management in Public Administration in Bratislava, Slovakia
30. **Jelena Fišić**, MA, "Pro-elektro" doo, Belgrade, Serbia
31. **Milena Gajic-Stevanovic**, DMD, MSc.SM, PhD, Institute of Public Health of Serbia, Belgrade, Serbia
32. **Bogdan Gats**, Chernivtsy Trade and Economics Institute of the Kyiv National Trade and Economics University, Chernivtsy, Ukraine
33. Ph.D. **Darie Gavrilut**, University of Oradea, Faculty of Economic Sciences, Oradea, Romania
34. Prof. Dr. **Sonja T. Gegovska-Zajkova**, Ss Cyril and Methodius University, Faculty of Electrical Engineering and Information Technologies, Skopje, Macedonia
35. **Mariya P. Hristova**, PhD, Assoc. Prof., "Todor Kableshkov" University of Transport, Sofia, Bulgaria
36. Dr. **Miroljub Ivanović**, Prof.v.s., Higher School of Vocational Studies in Education of Tutors in Sremska Mitrovica, Sremska Mitrovica, Serbia
37. Dr. **Aleksandra M. Izgarjan**, Assoc. Prof., Faculty of Philosophy, University of Novi Sad, Novi Sad, Serbia
38. Dr. **Miloje Jelić**, Preduzeće za proizvodnju “Klanica“d.o.o. Kraljevo
39. Prof. Dr. **Zoran Jerotijević**, Faculty of Business and Law of the "MB" University in Belgrade, Belgrade, Serbia
40. Dr. **Bisera S. Jevtić**, Assoc. Prof., University of Niš - Faculty of Philosophy, Niš, Serbia
41. Prof. Dr. **Natalija Jolić**, Faculty of Transport and Traffic Sciences, University of Zagreb, Zagreb, Croatia

42. Prof. Dr. **Svetlana Kamberdieva**, North Caucasian Institute of Mining and Metallurgy (State Technological University), NCIMM (STU), Vladikavkaz, Republic of North Ossetia – Alania, Russia
43. Prof. Dr. **Zvonko Kavran**, Faculty of Transport and Traffic Sciences, University of Zagreb, Zagreb, Croatia
44. Prof. **Antoaneta Kirova**, PhD, "Todor Kableshkov" University of Transport, Sofia, Bulgaria
45. Ing. **Jozef Klučka**, PhD, Assoc. Prof., Faculty of special engineering University of Žilina, Žilina, Slovakia
46. Prof. **Petar Kolev**, Dr, "Todor Kableshkov" University of Transport, Sofia, Bulgaria
47. **Oksana Koshulko**, PhD, Assoc. Prof., Polotsk State University, Novopolotsk, Republic of Belarus
48. Prof. Dr. **Boris Krivokapić**, Faculty of Business and Law of the "MB" University Belgrade, Belgrade, Serbia
49. Dr. **Evelin Krmac**, Asst. Prof., University of Ljubljana, Faculty of Maritime Studies, and Transportation, Portorož, Slovenia
50. Prof. Dr. **Adil Kurtić**, University of Tuzla - Faculty of Economics, Tuzla, Bosnia and Herzegovina
51. Dr. **Aleksandar Lebl**, Iritel AD, Beograd, Serbia
52. Prof. Dr. **Branko Ž. Ljutić**, certified auditor, University Business Academy, Novi Sad, Serbia
53. Ing. **Maria Luskova**, PhD, Faculty of special engineering University of Žilina, Žilina, Slovakia
54. CSc. **Elena S. Maltseva**, Assoc. Prof., Maykop State Technological University, Maykop, Russia
55. Dr. **Dubravka Mandušić**, University of Zagreb - Faculty of Agriculture, Zagreb, Croatia
56. **Milorad Markagić**, University of Defense - Military Academy, Belgrade, Serbia
57. **Željko Mateljak**, PhD, University of Split, Faculty of Economics, Split, Croatia
58. Prof. Dr. **Dobrivoje Mihailović**, University of Belgrade, Faculty of Organizational Sciences, Belgrade, Serbia
59. Prof. Dr. **Božidar Mihajlović**, College of Business Economics and Entrepreneurship in Belgrade, Belgrade, Serbia
60. Dr. **Ivo Mijoč**, Assistant Professor, Faculty of Economics in Osijek, Osijek, Croatia
61. Dr. **Živanka Miladinović Bogavac**, Asst. Prof., Faculty of Business and Law of the "MB" University Belgrade, Belgrade, Serbia
62. Dr. **Zoran Milenković**, Prof.v.s., College of Tourism, Belgrade, Serbia
63. Dr. **Živorad Milić**, Prizma, Kragujevac, Srbija
64. Dr. **Milorad Milošević**, Prof.v.s., Business School Čačak, Belgrade, Serbia
65. Dr. **Aleksandar Miljković**, Assoc. Prof., Faculty of Business and Law of the "MB" University Belgrade, Belgrade, Serbia, and FORKUP, Novi Sad, Srbija
66. **Piotr Misztal**, PhD, Assoc. Prof., Jan Kochanowski University in Kielce, Kielce, Poland
67. Prof. Dr. **Dragan M Momirović**, Faculty of Business and Law of the "MB" University Belgrade, Belgrade, Serbia
68. Dr. **Saša Muminović**, Julon d.d. Ljubljana, Slovenia
69. Dr. **Musaria Karim Mahmood**, Department of Energy systems Engineering, Ankara Yildirim Beyazıt Üniversitesi, Ankara, Turkey
70. Prof. Dr. **Predrag M. Nemec**, Faculty of Management in Sport, "Alfa" University, Belgrade, Serbia
71. Prof. Dr. **Nevenka Nićin**, Faculty of Business and Law of the "MB" University Belgrade, Belgrade, Serbia
72. Ing. **Ladislav Novak**, PhD, Assoc. Prof., Faculty of special engineering University of Žilina, Žilina, Slovakia
73. Dr. **Srećko Novaković**, Assistant Prof., High Business and Technical School Doboj, Bosnia and Herzegovina and College of Vocational Studies for Education of Tutors and Coaches, Subotica, Serbia
74. Prof. Dr. **Saša Obradović**, Fakultet za ekonomiju i inženjerski menadžment, Novi Sad, Serbia
75. Dr. **Milorad Opsenica**, Assistant Prof., Traffic Engineering Faculty of the International University, Brcko District, Bosnia and Herzegovina
76. CSc. **Tatiana Paladova**, Assoc.Prof., Maikop State Technological University, Maikop, Russia
77. Prof. Dr. **Yurij Vasylyovych Pasichnyk**, Cherkassy State Technological University, Cherkassy, Ukraine
78. Prof. **Dinara Peskova**, PhD, Bashkir Academy of Public Administration and Management under the Auspices of the Republic of Bashkortostan, Ufa, Russia
79. Prof. Dr. **Šemsudin Plojović**, University of Novi Pazar, Novi Pazar, Serbia
80. Prof. Dr. **Lyudmila Prigoda**, Maikop State Technological University, Maikop, Russia

81. Prof. Dr. **Vlado N. Radić**, Faculty of Business Economics and Entrepreneurship, Belgrade, Serbia
82. Dr. **Dragan Radović**, Assoc. Prof., Faculty of entrepreneurial business and management of the real estate of the "Union – Nikola Tesla" University, Belgrade, Serbia
83. Prof. Dr. **Dušan Regodić**, Faculty of Business and Law, "MB" University, Belgrade, Serbia
84. Dr. **Bojan Ristić**, Prof., Information Technology School, Belgrade, Serbia
85. Dr. **Slobodan Ristić**, University Belgrade, Faculty of Organizational Sciences, Belgrade, Serbia
86. **Muzafer Saračević**, PhD, Assistant Prof., University in Novi Pazar, Novi Pazar, Serbia
87. Dr. **Drago Soldat**, Prof.v.s., Technical College, Zrenjanin, Serbia
88. Prof. Dr. **Dragan Dj. Soleša**, Faculty of Economics and Engineering Management, University Business Academy, Novi Sad, Serbia
89. Ing. **Katarina Stachova**, PhD, School of Economics and Management in Public Administration in Bratislava, Slovakia
90. **Jasmina Starc**, PhD, Assistant Prof., School of Business and Management Novo Mesto na Loko, Novo Mesto, Slovenia
91. **Bohdana Stepanenko-Lypovyk**, MA, Institute for Economics and Forecasting of the Ukrainian National Academy of Sciences, Kyiv, Ukraine
92. Ing. **Eva Sventekova**, PhD, Assoc. Prof., Faculty of Special Engineering, University of Žilina, Žilina, Slovak Republic
93. Prof. Dr. **Radomir Šalić**, "Metropolitan" University in Belgrade, Belgrade, Serbia, and "Synergy" University in Bijeljina, Bijeljina, Bosnia and Herzegovina
94. Prof. Dr. **Dubravka Škunca**, Faculty of Business and Law, "MB" University, Belgrade, Serbia
95. **Daniela Todorova**, PhD, Assoc. Prof., "Todor Kableshkov" University of Transport, Sofia, Bulgaria
96. Prof. Dr. **Miomir Todorović**, Faculty of Business and Law, "MB" University, Belgrade, Serbia
97. Prof. Dr. **Zoran Todorović**, "Mediteran" University Podgorica – MTS "Montenegro Tourism School", Bar, Montenegro
98. Dr. **Janusz Tomaszewski**, Assoc. Prof., Eugeniusz Kwiatkowski University of administration and business, Gdynia, Poland
99. **David Ramiro Troitino**, Assoc. Prof., Tallinn University of Technology, Tallinn, Estonia
100. Dr. **Kristian Ujvary**, Ministry of Interior of the Slovak Republic, Bratislava, Slovak Republic
101. Dr. **Detelin Vasilev**, Assoc. Prof., "Todor Kableshkov" University of Transport, Sofia, Bulgaria
102. Prof. Dr. **Dragan Vučinić**, Higher school of modern business, Belgrade, Serbia
103. Prof. Dr. **Slavoljub Vujović**, Institute of Economics, Belgrade, Serbia
104. **Branko Vujatović**, Center for Applied Mathematics and Electronics - Belgrade, Serbia
105. Prof. **Yaroslav Vyklyuk**, DSc, Lviv Polytechnic National University, Lviv, Ukraine
106. Dr. hab. Eng. **Zenon Zamiar**, Assoc. Prof., Wroclaw University of Environmental and Life Sciences, Wroclaw, Poland
107. Prof. Dr. **Nada Živanović**, Faculty of Business and Law, "MB" University, Belgrade, Serbia
108. Prof. Dr. **Dragan R. Životić**, Faculty of Management in Sport, "Alfa" University, Belgrade
109. ***You? . . . . . To apply, fill-up the form, and return it to*** meste@meste.org
Form can be downloaded from https://www.meste.org/documents/Reviewers_declaration.docx

Editorial procedure

https://www.meste.org/ojs/index.php/mest/about/submissions#authorGuidelines

Peer review

All manuscripts submitted to MEST Journal will be reviewed by up to three experienced reviewers. At least two reviewers must recommend the article for publication. The selection of reviewers for each of the submitted works will be carried out by the editor-in-chief. In cases where the editor-in-chief is the author or coauthor, for submitted work reviewers will be selected by the deputy chief editor or one of the members of the Scientific Committee. The names of the reviewers will be published in the journal in the special list without specifying the titles of the papers that they reviewed. For the reviewing, authors are requested to submit all documents at once at the time of their submission with the following structure:

- A title page, which includes:
  - The title of the article
  - The name(s) of the author(s) with the concise and informative title(s)
  - The ORCID identifier(s) of the author(s)
  - The affiliation(s) and address(es), and e-mail address of the author(s)
  - The e-mail address, and telephone and fax numbers of the corresponding author
  - Abstract (The abstract should be in the range of 150 to 250 words and should not contain any undefined abbreviations or unspecified references.
  - Keywords (4 to 6 keywords which can be used for indexing purposes)
- A blind manuscript without any author names and affiliations in the text or on the title page. Self-identifying citations and references in the article text should either be avoided or left blank.

Authors must honor peer review comments in order to the manuscript improvement. All changes must be elaborated, and an improved manuscript should be submitted to the Editor-In-Chief. Of course, authors can argue peer review comments by giving reasons/references to counter peer review comments. After receiving of resubmitted manuscript Editor-in-Chief will choose whether the manuscript will be published or sent to the old/new reviewers.

Manuscript submission

MEST accepts the only manuscripts that use the template MEST_Template.docx from the web address: https://meste.org/documents/MEST_Template.docx with un-modified format only.

Submission of a manuscript implies that the corresponding author responsible declares:

- that the submitted article is an original work and has not been published before.
- that it is not under consideration for publication anywhere else.
- that its publication has been approved by all co-authors if any; and
- that there are not any legal obstacles for the article publishing.

The publisher will not be held legally responsible should there be any compensation claims.

Permissions

Authors, who wish to insert figures, tables, or passages of text that have previously been published elsewhere, are required to obtain permission from the copyright owner(s), and to attach the evidence that such permission has been granted when submitting their papers. Any material received without such evidence will be considered as author's.

Submission

Authors should submit their manuscripts by e-mail to the address: mest.submissions@meste.org .

E-mail should contain the following items:

1. **Declaration and copyright transfer**, which should include that:
   - the submitted article is an original work and has not been published before.
   - the submitted article is not under consideration for publication anywhere else.
   - the submitted article publication has been approved by all co-authors if any; and
   - there are no legal obstacles to article publishing.
2. **Title Page**, which should include:
   - Full title of the article (no more than 12 words)
   - The name(s) of the author(s)
   - The affiliation(s), email address(es), and address(es) of the author(s)
   - The short title (a concise and informative title, no more than 50 characters with spaces)
   - The e-mail address, and telephone and fax numbers of the corresponding author
   - ***Abstract*** (The abstract, paper summary, should be in the range of 150 to 250 words, and should not contain any undefined abbreviations or unspecified references. The Summary needs to hold all essential facts of the work, as the purpose of work, used methods, basic facts, and specific data if necessary. It must contain a review of underlined data, ideas, and conclusions from text, as well as recommendations for a group of readers that might be interested in the subject matter. The Summary must not have quoted references.
   - ***Keywords*** (4 to 10 keywords which can be used for indexing purposes need to be placed below the text). A list of recommended keywords can be found at: https://www.meste.org/Keywords.html .
3. **Manuscript,** which should be prepared as a camera ready, but without any data that can make a connection between author and the submitted article, such as author(s) name(s) and affiliation(s). Author(s) should avoid self-identifying citations and references. Manuscripts should be submitted in MS Word, following the template MEST_Template.docx, which can be downloaded from:
   https://meste.org/documents/MEST_Template.docx
   Manuscripts are not limited in length, but precise and concise writing should result with an article length of 8 to 14 pages, prepared according to the proposed MEST template.

   Authors must:
   - use a normal, plain 10-point Arial font for text.
   - Italics for emphasis.
   - use the automatic page numbering function to number the pages.
   - use tab stops or other commands for indents, not the space bar.
   - use the table function, not spreadsheets, to make tables.
   - use the equation editor or MathType for equations.
   - save their manuscript in .docx format (Word 2007 or higher).
   - use the decimal system of headings with no more than three levels.
   - define abbreviations at their first mention and use them consistently thereafter.
   - avoid footnotes, but, if necessary, footnotes can be used to give additional information about some term(s). Footnotes should not be used to referee citations, and they should never include the bibliographic details of a reference. Footnotes have not contained figures or tables. Footnotes to the text are numbered consecutively, automatically by the text editor. Endnotes are not intended for use in the article.
   - avoid the use of "the above table" or "the figure below";
   - use the SI system of units as preferable.

References – Works Cited (New up-to-date information should be used and referenced. References should be cited in the text by name and year in parentheses, according to the APA Sixth Edition.

The citation should be made using *References --> Citations & Bibliography* in MS Word®©, and we strongly recommend that the ***Work Cited*** list should be made automatically using MS Word®© option: *References --> Citations & Bibliography --> Bibliography --> Works Cited*. A more detailed explanation can be found in the tutorial at:
Create a bibliography, citations, and references - Word (microsoft.com)
https://support.microsoft.com/en-us/office/create-a-bibliography-citations-and-references-17686589-4824-4940-9c69-342c289fa2a5 .

4. **Acknowledgments** (All acknowledgments, if exist, should be placed on a separate page after the **Works Cited** list. The names of funding organizations or people should be written in full, unambiguously.)
5. **Tables** (All tables should be sent as separate files in .docx or .xlsx format.)
   - All table files must be named with "Table" and the table number, e.g., Table 1.
   - All attached tables must be numbered using Arabic numerals, and for each table, a table caption (title explaining the components of the table) should be provided.
   - Tables should always be lined in text in consecutive numerical order.
   - Previously published material should be identified by giving a reference to the source. The reference should be placed at the end of the table caption.
   - Footnotes to tables (for significance values and other statistical data) should be indicated by asterisks and placed beneath the table body.
6. **Photographs, pictures, clip arts, charts, and diagrams** should be numbered and sent as separate files in the .JPEG, .GIF, .TIFF or .PNG format in the highest quality. MS Office files are also acceptable, but font sizes and the size of the figure must suit the size in the published article. The quality of submitted material directly influences the quality of published work, so the MEST may require authors to submit figures of higher quality. All figure files must be named with "Fig" and the figure number, e.g., Fig. 1

   Remarks:
   - All figures can be made as colored and will be published free of charge as colored in the online publication.
   - Paper version of the document will be published as the grayscale document (black-white) so authors are kindly asked to check how their contributions look printed on black-white printers.
   - All lines should be at least 0.1 mm (0.3 pts) tick.
   - Scanned figure should be scanned with a minimum resolution of 1200 dpi.
   - For lettering, it is best to use sans serif fonts Helvetica or Arial.
   - Variance of font size within an illustration should be minimal (the sizes of characters should be 2–3 mm or 8-12 pts).
   - To increase clarity author(s) should avoid effects such as shading, outline letters, etc.
   - Titles and captions should not be included within illustrations.

MESTE does not provide English language support.

Manuscripts that are accepted for publication will be checked by MESTE lectors for spelling and formal style. This may not be sufficient if English is not the authors' native language. In most cases, these situations require substantial editing. MEST suggests that all manuscripts are edited by a native speaker before submission. A clear and concise language will help editors and reviewers to concentrate on the scientific content of the submitted paper. Correct language may allow a faster and smoother review process.

Authors are not obliged to use a professional editing service. Also, the use of such a service is not a guarantee of acceptance for publication.

Copyright Notice

Authors who publish with the MEST Journal agree to the following terms:

a. Authors retain copyright and grant the journal the right of first publication with the work simultaneously licensed under a Creative Commons Attribution License[1] that allows others to share the work with an acknowledgment of the work's authorship and initial publication in this journal.
b. Authors can enter separate, additional contractual arrangements for the non-exclusive distribution of the journal's published version of the work (e.g., post it to an institutional repository or publish it in a book), with an acknowledgment of its initial publication in this journal.
c. Authors are permitted and encouraged to post their work, with a note that the article is under consideration by MEST Journal, online (e.g., in institutional repositories or on their website) during the submission process, as it can lead to productive exchanges, as well as earlier and greater citation of published work (See The Effect of Open Access[2]).

Privacy Statement

The names and authors' affiliations, and the corresponding author's email address MEST Journal publishes within the published articles. The editors will use the other authors' addresses only in cases where identification of co-authors or communication with them is required.

The names and email addresses received in the MEST Journal will use exclusively for the stated purposes of this journal. That data will not be made available for any other purpose or to any other party except for the author's identification.

By entering data in the Title page form, the author in charge of the correspondence claims that the author and co-authors agree to the stated terms of use of personal data.

Proofreading

After the decision that the paper will be published, the processed article will be returned to the author for approval. The aim of the approval is that the author checks if some incorrectness appeared during the processing. Also, the author checks the completeness and accuracy of the text, tables, and figures. Any change must be noted and returned to MEST. After online publication, further changes can be made only in the form of an Erratum, which will be hyperlinked to the article. All changes must be specified and returned to MEST. Any substantial change can be done only with the approval of the Editor.

[1] https://creativecommons.org/licenses/by/4.0/
[2] http://opcit.eprints.org/oacitation-biblio.html

Submission Checklist

Before submitting your manuscript, please, check if you prepared all your attachments.

Submission Checklist:

☐ **The declaration** that:

- the submitted article is an original work and has not been published before;
- the submitted article is not under consideration for publication anywhere else;
- the submitted article publication has been approved by all co-authors if any; and
- there are no legal obstacles to article publishing.

☐ **Title Page**, which should include:

- The full title of the article (no more than 12 words)
- The name(s) of the author(s)
- The ORCID identifier(s) of the author(s)
- The affiliation(s), email address(es), and address(es) of the author(s)
- The e-mail address of the corresponding author
- The short title (a concise and informative title, no more than 50 characters with spaces)
- Abstract
- Keywords (no more than 10 words)

☐ **A manuscript** prepared as a camera ready, but without any data that can make a connection between author and the submitted article.

☐ **Acknowledgments** (if any)

☐ **All tables** – Each table has to be saved as a separated .docx file and attached to the e-mail. All table files must be named with "Table_" and the table number, e.g., Table_1, Table_2, etc.

☐ **All figures** – Each figure has to be saved as a separated .jpg, .gif, .tif, or .png file and attached to the e-mail. All graphic files must be named with "Figure_" and the table number, e.g., Figure_1, Figure_2, etc.

If everything is checked you can send your article to us to the address:

mest.submissions@meste.org

You can also use the online submission through

https://www.meste.org/ojs/index.php/mest/about/submissions#onlineSubmissions

Review MEST- M___

PART A:

SECTION I

Name and surname of the reviewer	
Reviewer's ORCID (optional)	
E-Mail	
Phone (optional)	
Manuscript No.	**M_...**
Title	
Author / Authors	----
Sent to reviewer	
The expected date of receipt of reviews	

PART B: *Reviewer only*

SECTION II: Comments of manuscript

General comment	
Introduction	
Methodology	
Results	
Discussion	
Findings	

SECTION II (continuation) (Click on the box next to the appropriate answer and check in one of the categories, or delete unnecessary if you are unable to check the desired box)

Bibliography / References	**Literature is relevant** **Citation is following the requirements**	**Yes** ☐ **Yes** ☐	**No** ☐ **No** ☐
Figures	**Figures are appropriate**	**Yes** ☐	**No** ☐
Tables:	**Tables are appropriate**	**Yes** ☐	**No** ☐

SECTION III

Please rate it from one of: *(1 = Excellent) (2 = Good) (3 = Correct) (4 = Poor)*

Originality	
Scientific contribution	
Technical quality of the article	
Clarity of presentation	
Depth of study	

SECTION IV – Recommendations for publication:
(Please select one of the options with an *X*)

Accept the article "as it is"	
The work requires minor repairs	
The work requires small-scale changes	
The work requires large-scale changes	
The work is good but it is not for publishing in the MEST Journal. It could be published in another journal, for example (propose)	
Work has to be rejected because (please specify the particular reason)	

SECTION V: Additional comments

This part of the review is confidential and will be available only to editors of the MEST Journal. If you have any special comment to the editors, you can enter it here.

Templates

The template for the MEST Journal articles preparing and submission can be found at the web address:

https://www.meste.org/mest/documents/MEST_Template.docx

The MEST Journal policies

https://www.meste.org/ojs/index.php/mest/about/editorialPolicies#sectionPolicies

4D414E4147454D454E54

454455434154494F4E

534349454E4345

544543484E4F4C4F47

45434F4E4F4D494353

ISSN 2334-7058 (Online)
DOI 10.12709/issn.2334-7058