ENSURING THE STATE FINANCIAL SECURITY AMIDST HYBRID THREATS: INSIGHTS FROM THE RUSSIAN-UKRAINIAN WAR

This article aims to analyze the multifaceted nature of hybrid financial security threats, particularly in the context of Russian aggression against Ukraine. It addresses the scientific problem of safeguarding state financial security amidst hybrid warfare, focusing on identifying key threats, evaluating their impact on financial stability, and proposing comprehensive measures to enhance resilience and protect financial infrastructure.

Analytical techniques such as thematic analysis and comparative analysis are utilized to examine the nature and impact of hybrid threats on financial security. The study focuses on the Russian-Ukrainian war as a case study to illustrate these threats’ real-world implications.

The research reveals that hybrid threats, which combine conventional military tactics with cyberattacks, misinformation, and economic pressures, pose significant challenges to financial stability. The ongoing Russian-Ukrainian war exemplifies these threats, with Ukraine facing severe economic destabilization. The study highlights the critical nature of cyber-attacks, misinformation campaigns, and economic espionage, which have undermined Ukraine’s financial infrastructure and public trust.
The findings offer practical insights for policymakers and financial institutions. Building resilience against hybrid threats requires dynamic strategies, including advanced cybersecurity measures, public awareness campaigns, and stronger international cooperation. Policymakers should enhance detection and response capabilities, foster public-private sector collaboration, and invest in innovative technologies to protect financial systems.

This study contributes to the understanding of contemporary security challenges by highlighting the novel and complex nature of hybrid threats. It provides a strategic framework for enhancing financial security, distinguishing itself from previous research by focusing on the specific context of the Russian-Ukrainian war and offering adaptive measures to address evolving threats. Limited access to certain classified information restricted the scope of the research. Future studies could benefit from real-time data to provide more dynamic insights.
ANALYSIS OF RECENT STUDIES AND PUBLICATIONS

The literature on financial security in the context of hybrid threats is vast and varied, offering numerous perspectives and analytical frameworks. Hybrid threats, as Lupulescu describes, have become a persistent feature in contemporary geopolitical dynamics, leveraging unconventional tactics by state and non-state actors to gain strategic advantages [1, p. 621]. These threats introduce new challenges in assessing societal impacts during ostensibly peaceful periods, encompassing physical, material, psychological, and emotional consequences. Lupulescu’s study highlights the importance of understanding these multifaceted threats and their impact on populations, especially in neighboring European countries. However, the study does not delve deeply into the financial security implications, necessitating further research to bridge this gap.

Varnalii and Bondarenko focus on the critical security concerns for Ukraine, exacerbated by both external and internal factors such as military conflicts, cyberterrorism, and economic instability [2, p. 111—112]. Their research underscores the paramount importance of financial security management for enterprises, particularly during wartime and post-war recovery. They emphasize the need for robust financial management systems to counteract threats and ensure the continuity of business operations. Despite acknowledging the war’s impact, the study lacks specific empirical evidence linking financial security of Ukrainian enterprises to hybrid threats from the Russian-Ukrainian conflict.

Kovalenko, Slatvinska, Sheludko, Makukha, and Valihuра explore the influence of monetary components on Ukraine’s financial security amidst political and socio-economic imbalances [3, p. 19-20]. Their research assesses monetary policy effectiveness and its impact on state financial security, highlighting the critical role of monetary policy in stabilizing macroeconomic processes during martial law. While the study identifies key threats and emphasizes the need for enhanced policy coordination, it falls short in providing actionable recommendations tailored to Ukraine’s specific context and the ongoing hybrid threats.

Nimani and Spahija analyze the direct impact of Russian aggression on the European financial market, comparing financial policies across European countries and the Balkan Peninsula [4, p. 142-143]. They highlight the exacerbation of existing socio-economic and financial trends due to the conflict, proposing an economic stabilization forecast model. However, the study lacks precise data or forecasts, and specific policy recommendations tailored to mitigating financial security risks amidst hybrid threats are also absent.

Hanzik and Drai emphasize the importance of continuous monitoring and analysis of key financial security indicators amidst escalating financial instability and heightened security threats [5, p. 33]. Their study identifies critical threats to national financial security, such as state budget debt burden, inflation, and banking system reliance on foreign capital. While providing forecasts and highlighting the need for transformative measures, the study does not adequately contextualize these impacts within the broader geopolitical and economic context of the Russian-Ukrainian war.

Blikhar, Vaolevskа, Ortynska, Vinichuk, and Kashchuk examine the economic and legal mechanisms for forming and implementing financial policy amidst the Russian-Ukrainian war [6, p. 301]. Their research reveals significant destabilizing factors, such as heightened inflation and exchange rate instability, impacting Ukraine’s financial policy. While they propose solutions for enhancing the economic and legal framework, the study lacks specific, actionable policy recommendations or strategies tailored to hybrid threats.

Wyrbek discusses the erosion of public trust due to hybrid threats like misinformation and manipulation of information, undermining state legitimacy [7, p. 328]. The article emphasizes the broad impact of these threats on societal functioning but lacks practical examples or empirical evidence related to financial security. Specific strategies or mechanisms for enhancing financial resilience against hybrid threats are not explored, limiting its relevance to practical policy discussions.

Korobtsova focuses on legislative foundations and strategies for safeguarding Ukraine’s financial security during wartime [8, p. 144-145]. The study identifies current threats and evaluates the state’s capacity to protect financial interests. While proposing improvements in economic and legal mechanisms, the text does not outline concrete, actionable policy recommendations or strategies tailored to address hybrid threats.

Chakalov and Nosan discuss the adaptation of traditional methods of managing financial and economic security to project management during wartime [9, p. 108]. They highlight the importance of modern security systems enabling remote control and functioning in digital environments. However, the study lacks emphasis on the unique challenges posed by hybrid threats, such as cyber warfare and information operations.

Varnali emphasizes the critical urgency of national security in the face of Russia’s military aggression [10, p. 92—93]. The study aims to deepen theoretical foundations and define mechanisms for security across various domains. Despite mentioning hybrid warfare, the text does not provide detailed analysis or practical recommendations for enhancing financial security amidst hybrid threats.

Yastrubetska, Krupka, Kovalenko, Zhmurko, and Mykulak propose a financial security management mechanism for Ukrainian companies operating amidst hybrid conflicts [11, p. 122]. Their study highlights the lack of sufficient research in this area and the inadequate government regulations governing financial security. While proposing development directions for financial security management, the study does not sufficiently discuss practical challenges or feasibility of these strategies.

Klymenko and Savostianenko review current approaches to assessing the impacts of Russian military aggression on Ukraine’s economic losses and post-war recovery plans [12, p. 71]. They emphasize the need for legislative measures to establish diverse financial support sources for Ukraine’s reconstruction. However, the study lacks a clear differentiation between traditional military
aggression and hybrid warfare tactics, limiting the depth of analysis required for understanding financial security implications.

Busol argues that modern national security hinges significantly on human capital and the comprehensive public administration encompassing all dimensions of national security [13, p. 10—12]. The article highlights the importance of addressing hybrid warfare but lacks detailed analysis or specific case studies related to hybrid threats faced by Ukraine. The list of high-priority steps to strengthen Ukraine’s protection against hybrid threats lacks detailed rationale or evidence of feasibility.

Varnalii and Tomashevskyi identify and address challenges in ensuring Ukraine’s financial security amidst hybrid warfare [14, p. 176; 15, p. 11—12]. They emphasize the importance of comprehensive data integration across all security domains. While comparative methods are mentioned, there is little explicit comparison with other countries facing similar hybrid threats, limiting the studies’ generalizability.

Zachosova and Babina analyze trends in bank and non-bank financial institutions in Ukraine, identifying traditional and hybrid threats to financial market participants [16, p. 87]. Their study highlights the necessity for financial institutions to adapt to these challenges. However, the text offers limited practical recommendations or strategies for government structures to mitigate these threats effectively.

Yordanova discusses the dynamic security landscape influenced by hybrid threats and the strategic role of sovereign debt in shaping national security strategies [17, p. 192—194]. The article emphasizes the evolving role of sovereign debt but does not provide a balanced analysis of potential counterarguments or alternative viewpoints, limiting its depth and persuasiveness in academic discourse.

Despite the wealth of insights into various aspects of financial security and hybrid threats, the literature reveals a notable gap in research on the peculiarities of ensuring state financial security amidst hybrid threats specifically caused by warfare.

### FORMULATION OF THE OBJECTIVES OF THE ARTICLE (TASK STATEMENT)

The article aims to analyze the multifaceted nature of hybrid financial security threats, particularly in the context of Russian aggression against Ukraine. It seeks to identify key threats, evaluate their impact on financial stability, and propose comprehensive, adaptive measures for enhancing resilience and safeguarding financial infrastructure.

### SUMMARY OF THE MAIN RESEARCH MATERIAL

Financial security threats refer to any actions or events that jeopardize the financial stability of a state. These threats can undermine the economic foundation, disrupt financial markets, and erode public confidence in the financial system. Traditional threats to financial security typically involve direct and overt actions by nation-states or organized criminal groups. These threats often manifest through economic sanctions, military actions, or blockades. For instance, a country might impose sanctions to cripple another nation’s economy, leading to a direct and immediate impact on financial stability. Traditional threats are generally easier to detect and respond to due to their overt nature and established legal frameworks.

Hybrid threats represent a blend of conventional and unconventional tactics aimed at destabilizing a state’s financial security. These threats often involve non-state actors, cyber attackers, and misinformation campaigns. Unlike traditional threats, hybrid threats are covert, multifaceted, and harder to detect. For example, cyber-attacks on financial institutions can disrupt services, steal sensitive data, and undermine public trust. The spread of false economic news through social media can also create panic and volatility in financial markets. The motivation behind hybrid threats is often to cause disruption and destabilization rather than direct dominance.

Table 1 highlights significant differences between traditional and hybrid threats across various criteria. Traditional threats, with their overt and direct nature, contrast...
include incidents of data theft and breach reports. Ukraine’s security level is unsatisfactory due to numerous reported data to gain competitive or strategic advantages. Indicators significant downtime. Indicators include instances of operations, such as destroying infrastructure, can cause incidents. Sabotage, physical disruption of financial information designed to create panic and instability. Russia’s attacks. Misinformation is the spread of false economic sentiment. Ukraine’s security level is dangerous as Indicators include the volume of false news and shifts in public sentiment. Ukraine is critical due to the high frequency and severity of attacks and the financial losses incurred. The security level in and steal sensitive data. Indicators include the frequency of institutions and infrastructure, aiming to disrupt operations and steal sensitive data. Indicators include the frequency of attacks and the financial losses incurred. The security level in Ukraine is critical due to the high frequency and severity of these attacks. Misinformation is the spread of false economic information designed to create panic and instability. Indicators include the volume of false news and shifts in public sentiment. Ukraine’s security level is dangerous as misinformation campaigns are rampant and difficult to counter. Economic espionage involves stealing sensitive financial data to gain competitive or strategic advantages. Indicators include incidents of data theft and breach reports. Ukraine’s security level is unsatisfactory due to numerous reported incidents. Sabotage, physical disruption of financial operations, such as destroying infrastructure, can cause significant downtime. Indicators include instances of sabotage and operational downtime. The security level is critical due to the severe impact of these actions. Circumventing international sanctions undermines the economic pressure to curb aggression. Indicators include the number of evasion incidents and their economic impact. Ukraine’s security level is unsatisfactory as evasion tactics are sophisticated and prevalent. Promoting corrupt practices to weaken financial stability is a common tactic. Indicators include the corruption index and financial irregularities. The security level is dangerous due to the high prevalence of corruption. Covert actions to influence financial markets cause volatility and instability. Indicators include market volatility and unexplained fluctuations. Ukraine’s security level is unsatisfactory due to frequent manipulation attempts. Illegal extraction of resources deprives the state of revenue and destabilizes the country (Table 2). Cyber-attacks involve targeted attacks on financial institutions and infrastructure, aiming to disrupt operations and steal sensitive data. Indicators include the frequency of attacks and the financial losses incurred. The security level in Ukraine is critical due to the high frequency and severity of these attacks. Misinformation is the spread of false economic information designed to create panic and instability. Indicators include the volume of false news and shifts in public sentiment. Ukraine’s security level is dangerous as misinformation campaigns are rampant and difficult to counter. Economic espionage involves stealing sensitive financial data to gain competitive or strategic advantages. Indicators include incidents of data theft and breach reports. Ukraine’s security level is unsatisfactory due to numerous reported incidents. Sabotage, physical disruption of financial operations, such as destroying infrastructure, can cause significant downtime. Indicators include instances of sabotage and operational downtime. The security level is critical due to the severe impact of these actions. Circumventing international sanctions undermines the economic pressure to curb aggression. Indicators include the number of evasion incidents and their economic impact. Ukraine’s security level is unsatisfactory as evasion tactics are sophisticated and prevalent. Promoting corrupt practices to weaken financial stability is a common tactic. Indicators include the corruption index and financial irregularities. The security level is dangerous due to the high prevalence of corruption. Covert actions to influence financial markets cause volatility and instability. Indicators include market volatility and unexplained fluctuations. Ukraine’s security level is unsatisfactory due to frequent manipulation attempts. Illegal extraction of resources deprives the state of revenue and destabilizes the economy. Indicators include reports of illegal activities and economic losses. The security level is dangerous given the ongoing illegal extraction activities. Infiltrating institutions with hostile insiders can lead to breaches and operational disruptions. Indicators include incidents of insider actions and their impacts. The security level is critical due to the difficulty in detecting and preventing insider threats. Using political means to influence financial policies can destabilize the economy. Indicators include changes in policies and economic indicators. The security level is satisfactory, reflecting effective but not foolproof countermeasures.

**CONCLUSIONS AND PROSPECTS FOR FURTHER RESEARCH IN THIS AREA**

The study on state financial security amidst hybrid threats, with a focus on the Russian-Ukrainian war, highlights the

<table>
<thead>
<tr>
<th>Threat category</th>
<th>Essence</th>
<th>Indicators</th>
<th>Level of security in Ukraine</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cyber attacks</td>
<td>Attacks on financial institutions and infrastructure</td>
<td>Frequency of attacks, financial losses</td>
<td>Critical</td>
</tr>
<tr>
<td>Misinformation</td>
<td>Spreading false economic information to cause panic</td>
<td>Volume of false news, public sentiment shifts</td>
<td>Dangerous</td>
</tr>
<tr>
<td>Economic espionage</td>
<td>Stealing sensitive financial data</td>
<td>Incidents of data theft, breach reports</td>
<td>Unsatisfactory</td>
</tr>
<tr>
<td>Sabotage</td>
<td>Disrupting financial operations through physical means</td>
<td>Instances of sabotage, operational downtime</td>
<td>Critical</td>
</tr>
<tr>
<td>Sanctions evasion</td>
<td>Circumventing international sanctions</td>
<td>Number of evasion incidents, economic impact</td>
<td>Unsatisfactory</td>
</tr>
<tr>
<td>Corruption</td>
<td>Promoting corrupt practices to undermine financial stability</td>
<td>Corruption index, financial irregularities</td>
<td>Dangerous</td>
</tr>
<tr>
<td>Market manipulation</td>
<td>Influencing financial markets through covert actions</td>
<td>Market volatility, unexplained fluctuations</td>
<td>Unsatisfactory</td>
</tr>
<tr>
<td>Resource theft</td>
<td>Illegal extraction of resources</td>
<td>Reports of illegal activities, economic losses</td>
<td>Dangerous</td>
</tr>
<tr>
<td>Insider threats</td>
<td>Infiltrating institutions with hostile insiders</td>
<td>Incidents of insider actions, breach impacts</td>
<td>Critical</td>
</tr>
<tr>
<td>Political pressure</td>
<td>Using political means to influence financial policies</td>
<td>Changes in policies, economic indicators</td>
<td>Satisfactory</td>
</tr>
</tbody>
</table>

Source: elaborated by authors.
complex and evolving nature of modern threats to financial stability. Key findings underscore that hybrid threats, blending conventional and unconventional tactics, pose significant challenges due to their covert, multifaceted, and rapidly changing characteristics. Unlike traditional threats, which are often overt and governed by established legal frameworks, hybrid threats such as cyber-attacks, misinformation, and economic espionage are harder to detect and mitigate.

The case of Ukraine illustrates how these hybrid threats can critically undermine financial security. Cyber-attacks on financial institutions and infrastructure, along with misinformation campaigns, have created a precarious financial environment. The spread of false economic news has destabilized markets, while economic espionage and sanctions evasion further complicate the financial landscape. The prevalence of corruption and insider threats exacerbates the situation, highlighting the need for robust, adaptive security measures.

For policymakers, the study suggests several practical implications. Building resilience against hybrid threats requires a dynamic approach, including advanced cybersecurity measures, comprehensive public awareness campaigns, and stronger international cooperation to enforce sanctions and combat corruption. Policymakers should focus on enhancing the detection and response capabilities of financial institutions, fostering collaboration between the public and private sectors, and investing in innovative technologies to safeguard financial infrastructure.

Further research is recommended in areas such as the integration of artificial intelligence and machine learning for threat detection, the development of more sophisticated misinformation countermeasures, and the exploration of new regulatory frameworks to address the legal ambiguities surrounding hybrid threats. As hybrid warfare continues to evolve, ongoing research and adaptive policy strategies will be crucial in maintaining financial security amidst contemporary geopolitical challenges.

Acknowledgements. The study was carried out as part of the grant "EU ECONOMIC SECURITY" (project number: 101083446, project acronym: EUCOSEC, call: ERASMUS-JMO-2022-HEI-TCH-RSCH, topic: ERASMUS-JMO-2022-CHAIR) supported by the European Education and Culture Executive Agency.

Literature:
15. Варналій, З. С., Томашевський, Т. Т. (2019). Заагрози фінансової безпеки України в умовах гібридної...
References:


