https://doi.org/10.26565/2786-4995-2026-1-13
UDC: 336.7:004.056:351.86

Maciejewski Jan
Professor, D.Sc. in Sociology
University College of Professional Education
1 Powstańców Śląskich Square
53-329 Wrocław, Poland
e-mail: jan.maciejewski@wskz.pl
ORCID ID: 0000-0002-0743-099X
Krivtsova Tetiana
Assistant Professor, PhD in Economics
University College of Professional Education
1 Powstańców Śląskich Square
53-329 Wrocław, Poland
e-mail: etiana.krivstova@wskz.pl
ORCID ID: 0000-0002-1693-6781

Threats to state financial security in the digital age: challenges for dispositional groups

Abstract. State financial security has become a crucial component of national security in the context of rapid digital transformation, geopolitical instability, and the expansion of hybrid threats. The increasing digitalization of financial systems enhances efficiency but simultaneously generates new systemic vulnerabilities related to cyber risks, algorithmic governance, and financial data centralization.

Problem statement. Modern financial infrastructures are increasingly exposed to hybrid operations, cyberattacks, and systemic shocks that may undermine institutional stability, public trust, and the operational capacity of dispositional groups responsible for maintaining public order and state resilience.

Unresolved aspects of the problem. Existing research predominantly examines financial security from an economic perspective, while the socio-institutional implications for dispositional groups and the relational dimension of financial security remain insufficiently explored, especially under conditions of digital financial governance and prolonged crisis environments.

Purpose of the article. The aim of this study is to identify and conceptualize key threats to state financial security in the digital era and to determine their impact on dispositional groups within a security-studies framework.

Presentation of the main material. The research applies a socio-systemic and interdisciplinary approach combining qualitative analysis of institutional reports (IMF, World Bank, BIS, World Economic Forum), selected statistical sources, and contemporary security-studies literature. The findings demonstrate that financial security in the digital age consists of two interrelated dimensions — financial stability and financial resilience. Digital transformation, CBDCs, cyber threats, and hybrid financial warfare reshape the architecture of state security and influence the functioning, morale, and institutional loyalty of dispositional groups.

Conclusions. The study confirms that financial security has evolved into a strategic pillar of national security. Strengthening state resilience requires integrating financial governance, cybersecurity, and social-institutional factors while ensuring transparency and trust in digital financial systems.

Keywords: *state financial security, digital transformation, hybrid threats, central bank digital currency, state resilience, cyber risks.*

JEL Classification: G28; H56; O33; G18.

Formulas: -; fig.: -, tabl.: , bibl.: 47;

For citation: Maciejewski Jan, Krivtsova Tetiana. Threats to state financial security in the digital age: challenges for dispositional groups. Financial and Credit Systems: Prospects for Development. №1(20) 2026. P. 173-191. https://doi.org/10.26565/2786-4995-2026-1-13

Introduction. Contemporary state security can increasingly be examined only with difficulty through a purely military lens. Accelerating globalization, rapid digital transformation of the economy, and profound socio-economic restructuring have shifted the analytical focus within security studies. Economic and financial security now occupies a central position - not merely as a question of macroeconomic stability, but as a prerequisite for political system endurance, social cohesion, and the state's capacity for effective crisis response (Cieślarczyk, 2021; Maciejewski, 2025).

A growing body of academic research demonstrates that the digitalization of finance is transforming not only monetary systems but also the broader architecture of global governance and economic security. Scholars emphasize that digital currencies, algorithmic financial infrastructures, and decentralized financial markets introduce new systemic risks while simultaneously expanding the strategic capacity of states to manage crises (Brunnermeier et al., 2021; Rogoff, 2021; Schär, 2021). These transformations blur the traditional boundaries between economic policy, cybersecurity, and national security, making financial stability an increasingly political and societal issue rather than a purely macroeconomic concern.

The relevance of this security dimension was explicitly underscored during the 56th World Economic Forum Annual Meeting in Davos (19–23 January 2026), held under the theme *A Spirit of Dialogue*. The meeting's conclusions emphasized that financial stability in an environment of digitalization, geopolitical confrontation, and intensifying technological risks has become one of the key pillars of global security. It was also noted that financial crises, cyber threats, and geopolitical pressure increasingly function as instruments of strategic influence, producing effects comparable to those of traditional military tools (World Economic Forum, 2026).

These dynamics are further intensified by the escalation of destabilizing phenomena: irregular migration, deepening social polarization, armed conflicts and hybrid warfare, rising cyberattacks, and the protracted wartime conditions in Ukraine. A common denominator across these processes is their direct or indirect impact on the state's financial system - both in fiscal terms and through institutional disruption. As highlighted in analyses by the International Monetary Fund and the World Bank, financial stability is now among the primary determinants of a state's resilience to multidimensional crises that simultaneously affect economic, social, and security domains (International Monetary Fund, 2024; World Bank, 2024).

Particular importance in this context attaches to what may be described as *new wartime habitualization* - a long-term societal adaptation to functioning under conditions of persistent threat. This adaptation is associated with gradual erosion of social capital, declining trust in public institutions, and the normalization of extraordinary instruments of economic and financial control (Beck, 2002; World Economic Forum, 2025). Consequently, financial security can no longer be treated as a strictly economic category; instead, it becomes an integral component of national security architecture, shaping administrative effectiveness and the operational capacity of dispositional groups (Maciejewski, 2025).

In this context, recent studies in international political economy highlight the growing importance of financial governance as a domain of strategic competition, where hybrid threats, cyber operations, and economic instruments increasingly intersect (Moschella & Tsingou, 2022; Buchanan et al., 2022). The integration of digital financial technologies into state governance structures therefore requires a multidisciplinary analytical approach combining security studies, sociology, and financial economics.

Building on these considerations, the article advances a conceptual perspective that integrates financial security, digital governance, and the sociological analysis of dispositional groups within a single analytical framework. By bridging security studies with contemporary debates on digital financial transformation, the study contributes to expanding the understanding of financial security as a relational and multidimensional phenomenon rather than a purely economic variable.

Against this background, a systematic analysis of threats to state financial security and their implications for dispositional groups becomes both theoretically and practically necessary.

Purpose, objectives and research methods. The purpose of this article is to identify and conceptualize the main threats to state financial security in the digital era and to explain their implications for dispositional groups from the perspective of security studies. The study adopts a socio-systemic approach and draws on recent reports by international institutions (World Bank, International Monetary Fund, Bank for International Settlements, World Economic Forum), selected statistical sources (Eurostat, Statistics Poland), and the work of Polish and international scholars examining financial and national security.

Literature review. The relationship between state financial security and dispositional groups has been addressed across multiple social science disciplines, notably economics, security studies, and sociology. Economic research has predominantly concentrated on macroeconomic stability, systemic robustness, and risks driven by financial globalization, including crisis and regulatory threats (International Monetary Fund, 2024; World Bank, 2023). While these studies provide an essential macroeconomic perspective, recent academic debates increasingly emphasize that financial security cannot be fully understood without considering digital infrastructures, decentralized financial systems, and evolving forms of economic governance. Research in international political economy and financial economics highlights the growing role of digital currencies, algorithmic markets, and cyber-financial risks as structural elements shaping contemporary financial stability (Brunnermeier et al., 2021; Moschella & Tsingou, 2022). Within security studies, a substantial body of work has focused on national security, economic security, and state resilience to hybrid and asymmetric risks (Cieślarczyk, 2021; Pieczywok, 2018).

In Polish scholarship, researchers such as Jan Maciejewski, Marian Cieślarczyk, Andrzej Pieczywok, and Janusz Gierszewski have explored the systemic character of state security, security culture, societal resilience, and the role of dispositional groups in maintaining state stability (Gierszewski, 2018; Maciejewski, 2025). These contributions have helped consolidate an understanding of security as multidimensional and relational, extending beyond classical military interpretations. However, despite the strong sociological and security-oriented tradition within Polish scholarship, the intersection between financial digitization and the functioning of dispositional groups remains relatively underdeveloped. Existing analyses rarely integrate technological transformation with questions of institutional legitimacy, morale, and operational readiness under conditions of digital financial governance. At the same time, financial security within this stream has usually been treated as a component of broader economic security, with limited reflection on its transformation under conditions of digitalization. This gap indicates the need for an interdisciplinary analytical framework capable of connecting financial digitization with institutional and sociological dimensions of security.

International literature - especially reports produced by the International Monetary Fund, the World Bank, the Bank for International Settlements, and the World Economic Forum - has increasingly emphasized the growing significance of digital, cyber, and financial risks for state stability (Bank for International Settlements, 2023; World Economic Forum, 2024). Recent academic studies emphasize that digital currencies and decentralized finance reshape financial governance and systemic stability (Brunnermeier et al., 2021; Schär, 2021; Moschella & Tsingou, 2022). These publications provide valuable empirical evidence and diagnoses of global trends; however, they rarely offer a deeper analysis of how these developments affect dispositional groups in social and institutional terms.

Accordingly, a comparatively underexplored area remains the linkage between state financial security in the digital age and the functioning of dispositional groups - particularly in the context of hybrid threats, digital financial control, and prolonged multidimensional crises. There is a clear shortage of integrative analyses that combine financial, digital, and sociological perspectives within a coherent security-studies framework.

Moreover, contemporary journal-based research increasingly frames financial security as a multidimensional process combining economic resilience, cyber governance, and socio-political stability. Studies on decentralized finance, digital money, and financial cybersecurity suggest that the future architecture of state security will depend on the ability to integrate financial, technological, and social dimensions within a coherent governance framework (Schär, 2021; Kshetri, 2023; Buchanan et al., 2022).

This identified research gap justifies the present inquiry. The article frames financial security as a crucial, yet insufficiently examined, element of contemporary state security architecture and highlights its relevance for the stability, morale, and operational readiness of dispositional groups under mounting digital and crisis pressures.

Research results. In the Polish research tradition of security studies, financial security is increasingly conceptualized as one of the key subsystems of national security. Jan Maciejewski argues that state security should be understood as a dynamic configuration of interdependent components - military, political, social, economic, and informational (Maciejewski, 2014; Maciejewski, 2025). Within such a framework, disruption in one subsystem may generate cascading effects that weaken the performance of the entire security system.

Marian Cieślarczyk stresses that economic security, including its financial dimension, plays a stabilizing role for the social system by conditioning the state's capacity to adapt under crisis conditions (Cieślarczyk, 2021). Andrzej Pieczywok and Janusz Gierszewski, in turn, underline the importance of institutional resilience of the financial system in the face of asymmetric and hybrid threats, pointing to the growing significance of non-military factors within contemporary security architecture (Gierszewski, 2018; Pieczywok, 2018).

State financial security may therefore be defined as the ability of the financial system to ensure macroeconomic stability, continuity of financing public functions, and resilience to internal and external disruptions - including those of digital and hybrid origin (International Monetary Fund, 2024; World Bank, 2023). Under conditions of a digital economy, this stability increasingly depends not on material resources, but on governance over financial flows, data, and the informational infrastructure that enables them (Bank for International Settlements, 2023).

Contemporary approaches to security in the social sciences progressively move away from treating it as a static condition, emphasizing instead its relational and processual nature. As Ulrich Beck notes, late-modern societies operate amid the continual production of risk - no longer a marginal phenomenon, but a constitutive feature of civilizational development (Beck, 2002). Security thus becomes less a simple function of protection against threats and more a dynamic relationship among social actors, state institutions, and structures of economic power.

From this standpoint, state financial security should not be analyzed as an autonomous segment of public policy; rather, it constitutes a relational dimension of social-system stability. Zdzisław Ścibiorek highlights that state security is multidimensional and depends on the quality of relations between public authority, society, and the international environment (Ścibiorek, 2013). As finance becomes digital, these relationships grow more complex because the interface between state and citizen is increasingly mediated by algorithms, digital platforms, and centralized information systems (World Economic Forum, 2024).

The relational character of financial security becomes especially visible in crisis situations. Public trust in financial institutions, central banks, and fiscal authorities then turns into a strategic resource that conditions the effectiveness of stabilization measures. Sociological research conducted after the global financial crisis and during the COVID-19 pandemic indicates that declining trust in financial institutions may rapidly undermine state legitimacy, escalate social tensions, and weaken the state apparatus's ability to implement decisions (World Bank, 2023).

In the digital era, the relational nature of financial security is further intensified by the automation and algorithmization of economic decision-making. Citizens interact less frequently with institutions through direct human contact and more often with impersonal digital systems. From the perspective of security studies, this carries significant consequences: responsibility for

financial decisions becomes dispersed, and mechanisms of social control may appear less transparent while simultaneously becoming more effective (International Monetary Fund, 2023).

This relational dimension directly affects dispositional groups. Their social standing, levels of public trust, and crisis-response capacity depend on the state's financial stability and the quality of relations between authority and society. When financial security erodes, dispositional groups may face loyalty dilemmas - between implementing state tasks and responding to public dissatisfaction driven by deteriorating economic conditions (Maciejewski, 2025).

Viewing financial security as relational therefore provides a more precise understanding of its relevance under contemporary hybrid and digital threats. It is not limited to balance sheets, macroeconomic indicators, or currency stability; rather, it forms part of a broader security architecture in which public trust, political legitimacy, and the state's capacity to sustain social cohesion play decisive roles. This assessment is echoed in the conclusions of the World Economic Forum Annual Meeting in Davos in 2026 (World Economic Forum, 2026).

The digitization of finance is among the most consequential megatrends shaping the contemporary global economy, with direct implications for the architecture of state financial security. This transformation spans both public finance (digital tax administration, e-government services, digitally mediated social transfers) and private finance (online banking, cashless payments, and the platformization of financial services). From a security-studies perspective, digitization is not a neutral modernization process: it reconfigures the nature of vulnerabilities by shifting risk from material resources toward informational, infrastructural, and algorithmic layers.

Recent assessments by the International Monetary Fund and the World Bank emphasize that macroeconomic stability is increasingly conditioned by the digital resilience of financial systems (International Monetary Fund, 2024; World Bank, 2024). Disruptions to data flows, ransomware incidents, or failures of settlement and clearing infrastructures can now produce effects comparable to those of a traditional banking crisis. In this sense, financial security is no longer the exclusive domain of fiscal and monetary policy; it becomes tightly coupled with the state's cybersecurity capacity and the protection of critical financial infrastructure (Bank for International Settlements, 2023).

Digitization also contributes to the concentration of decision-making power among a relatively narrow set of institutional actors. The algorithmization of credit, investment, and fiscal processes means that capital allocation decisions are increasingly executed automatically, using statistical models and machine-learning tools. The Bank for International Settlements has noted that heightened dependence on automated financial systems may amplify the risk of cascading failures and hard-to-anticipate domino effects (Bank for International Settlements, 2023). For state security, this implies growing exposure to systemic shocks whose triggers may be technical (e.g., software defects, infrastructure outages) as well as political (e.g., coercive interference, targeted disruption, regulatory capture).

Within a digital economy, a particularly sensitive issue is the sovereignty of financial data. Transaction data, consumer-behavior information, and citizens' risk profiles become strategic assets comparable to energy resources or other categories of critical infrastructure. The World Economic Forum has consistently argued that control over financial data is a key element of "new geopolitics," in which advantage accrues to states and entities capable of aggregating and analyzing such information in real time (World Economic Forum, 2024). The Davos 2026 discussions further reinforced that digital, financial, and geopolitical risks are increasingly intertwined and that resilient financial systems are now recognized as a pillar of global security (World Economic Forum, 2026). In practical terms, this signifies a durable fusion of financial security with informational and technological security.

While the digitization of public finance can increase the efficiency of budget management and reduce certain forms of abuse, it also creates new social risks. Automated welfare and fiscal systems may marginalize groups with limited digital competences, thereby intensifying financial

exclusion. From the standpoint of internal security, this constitutes a destabilizing factor that can fuel social frustration and weaken trust in public institutions (World Bank, 2023).

Polish security-studies scholarship stresses that state financial security in the digital era must be examined through the lens of systemic resilience. Marian Cieślarczyk argues that resilience encompasses not only the ability to absorb economic shocks but also the institutional capacity to adapt to changing technological and social conditions (Cieślarczyk, 2021). Digitization therefore confronts the state with the challenge of building systems that are simultaneously flexible and resistant to external interference, including hybrid operations.

Accordingly, the digital transformation of finance should be interpreted not merely as an administrative upgrade but as a process with deep national-security implications. Responding effectively requires policy integration across finance, cybersecurity, and internal security governance - while explicitly recognizing the stabilizing role of dispositional groups during crisis escalation (Maciejewski, 2025).

In light of the above, digitization should be understood not only as an improvement in financial flows or institutional efficiency, but as a shift in the logic of security-from classical macroeconomic instruments toward the design and governance of digital architectures. If data, settlement infrastructure, and decision-making algorithms become the crucial resources, then the future form of money - and the actors able to define the rules governing access to financial resources - turns into a strategic question (Bank for International Settlements, 2023; World Economic Forum, 2024). In this context, central bank digital currencies (CBDCs) represent not only an instrument of monetary policy but potentially a new “protocol” of state financial sovereignty, combining managerial advantages with novel systemic risks (International Monetary Fund, 2023). These developments align with recent economic research on CBDCs and digital monetary architectures (Auer et al., 2022; Rogoff, 2021).

One of the most far-reaching manifestations of the digital transformation of public and private finance is the development of central bank digital currencies (CBDCs). From the perspective of security studies, CBDCs cannot be treated solely as a technical innovation in payments or as a tool for improving monetary-policy transmission. Rather, they represent a qualitative shift in the architecture of money, reshaping the relationship among the state, financial markets, and citizens (Bank for International Settlements, 2023). Recent empirical research on digital financial instruments and stablecoin dynamics further suggests that the stability of digital monetary ecosystems depends on liquidity structures, governance design, and institutional credibility (Lyons & Viswanath-Natraj, 2023).

The Bank for International Settlements indicates that CBDCs are moving from pilot initiatives toward operational maturity, with the potential to enter routine economic circulation (Bank for International Settlements, 2023). This transition may bring benefits such as more efficient payment systems, lower transaction costs, and stronger levers for safeguarding financial stability. At the same time, it introduces a distinct category of systemic risk associated with an unprecedented centralization of financial information and decision-making capacity (International Monetary Fund, 2023).

A pivotal feature of this transformation is the programmability of money - understood as the ability to embed rules into monetary units, including conditional use, time limits, or purpose restrictions. Analyses by the Bank for International Settlements and the International Monetary Fund suggest that digital money may become a carrier of political and social rules rather than a purely neutral medium of exchange (Bank for International Settlements, 2023; International Monetary Fund, 2023). For state security, this implies a shifting boundary between fiscal and monetary policy and instruments of social control, raising questions about the scope of citizens’ financial autonomy and the durability of trust in public institutions (World Economic Forum, 2025).

The relational nature of financial security discussed above becomes even more salient in the CBDC context. Citizens no longer relate to money merely as an abstract market value but increasingly interact with a digital system whose operational logic is centrally designed and

enforced. Decisions about access to funds, transferability, or permitted uses may be executed automatically through algorithms and predefined criteria. As a result, decision-making responsibility becomes more diffuse, and democratic oversight mechanisms may become harder to grasp and contest (Beck, 2002; World Economic Forum, 2024).

These dilemmas were explicitly highlighted during the Davos 2026 discussions. The forum's concluding messages emphasized that CBDCs and digital payment systems can strengthen financial resilience, yet they may also generate political and social tensions if not embedded in transparent institutional and legal frameworks (World Economic Forum, 2026). In particular, the risk of trust erosion rises when digital financial instruments are perceived as tools of excessive control or selective access to resources (World Economic Forum, 2025).

From a national-security perspective, the cyber dimension of CBDCs is equally critical. Centralizing digital-money infrastructure can increase exposure to cyberattacks, technological sabotage, and hybrid operations conducted by state and non-state actors. Reports by the International Monetary Fund and the Bank for International Settlements warn that disruption of a CBDC system could produce cascading effects, including payment paralysis, liquidity stress, and a rapid loss of confidence in state institutions (Bank for International Settlements, 2023; International Monetary Fund, 2024). In this respect, digital money becomes part of critical infrastructure, requiring protection comparable to that of energy grids or telecommunications networks.

The implications for dispositional groups are indirect yet strategic. A state's financial stability-its ability to fund uniformed services on time and maintain continuity of salaries and public transfers - conditions their operational readiness (Maciejewski, 2025). Conversely, crises of confidence surrounding a digital-money regime may heighten social tensions, placing dispositional groups in the position of implementing decisions that carry substantial social costs (Cieślarczyk, 2021). CBDCs therefore function not only as instruments of financial policy but also as factors shaping state–society relations and the perceived legitimacy of the coercive apparatus.

In sum, central bank digital currencies constitute one of the key challenges to state financial security in the digital era. Their significance extends beyond economics into informational, social, and political security domains. Responsible CBDC implementation thus requires not only robust technological solutions but also a systemic reflection that anticipates long-term consequences for state stability and for the functioning of core security institutions (World Economic Forum, 2026).

Contemporary conflicts increasingly depart from the classical model of armed confrontation limited to the military domain. Hybrid warfare has become the dominant mode of strategic competition, combining coordinated actions across political, economic, informational, cyber, and social spheres. Within this paradigm, the financial system no longer serves merely as logistical support for conflict; instead, it emerges as a direct arena of strategic pressure.

From a security-studies perspective, hybrid warfare exploits structural vulnerabilities inherent in modern states, seeking to erode decision-making capacity without engaging regular armed forces. Analyses by the International Monetary Fund demonstrate that financial destabilization may generate effects comparable to kinetic military strikes, including paralysis of public functions, erosion of social trust, and institutional disorganization (International Monetary Fund, 2024). Consequently, financial security becomes a central component of state resilience against hybrid threats.

Hybrid financial warfare employs a diverse toolkit, encompassing economic sanctions, currency manipulation, market interference, and cyber operations targeting banking and fiscal infrastructure. The objective of these measures is not solely to weaken economic potential but, more critically, to undermine confidence in financial institutions and governance mechanisms. The World Bank emphasizes that a collapse of trust in the financial system produces cascading consequences, such as capital flight, inflationary pressures, and broader social instability (World Bank, 2023).

A particularly potent element of hybrid warfare is economic disinformation. Information campaigns aimed at discrediting central banks, tax systems, or social-support mechanisms amplify uncertainty and fear, often triggering irrational market behavior. In a digitally mediated economy,

such narratives disseminate rapidly, intensifying panic responses. Financial information thus becomes weaponized, while the media environment itself turns into a battlefield for systemic stability (World Economic Forum, 2024).

Cyber operations further reinforce the hybrid dimension of financial conflict. Attacks against payment systems, electronic banking platforms, and fiscal databases can temporarily deprive citizens and institutions of access to financial resources. In highly digitized monetary environments, even short-term disruptions may have severe consequences. The Bank for International Settlements notes that brief interruptions in financial-market infrastructure can generate disproportionate risks to overall state stability (Bank for International Settlements, 2023).

The expansion of central bank digital currencies and the increasing centralization of financial infrastructure add another layer to this threat landscape. Digital money, as part of critical infrastructure, becomes a strategic target for both technical attacks and political coercion. From a national-security standpoint, this necessitates reconceptualizing the financial system as a defensive asset rather than a neutral economic mechanism (International Monetary Fund, 2023).

Financial destabilization resulting from hybrid operations has direct repercussions for dispositional groups. Budgetary constraints, funding delays, inflation, and declining real wages negatively affect morale and operational effectiveness within uniformed services. Simultaneously, these groups are tasked with maintaining public order during crises, increasing both institutional and societal pressure on their actions.

Taken together, hybrid warfare reveals a fundamental shift in the understanding of state financial security. The financial system evolves from a background economic structure into an active domain of conflict, whose stability directly conditions the state's capacity to function under threat. Analyzing this dimension is therefore indispensable for understanding contemporary security challenges and assessing the role of dispositional groups within them (World Economic Forum, 2025).

The full-scale invasion of Ukraine by the Russian Federation in February 2022 created unprecedented conditions for state functioning under prolonged, high-intensity armed conflict. Beyond its military dimension, the war exposed the critical importance of financial security as a pillar of national endurance, enabling both sustained defense efforts and the continuity of essential administrative and social functions. In this sense, Ukraine has become a real-world laboratory of financial resilience under conditions of modern warfare.

One of the most urgent challenges at the outbreak of hostilities was maintaining the operational continuity of the banking and payment systems. Despite physical destruction, mass population displacement, and severe economic disruption, Ukraine's financial sector preserved basic functional stability. Assessments by the International Monetary Fund highlight the decisive role of rapid interventions by the National Bank of Ukraine, including capital controls, exchange-rate stabilization, and liquidity support for the banking sector (International Monetary Fund, 2024). These measures mitigated financial panic and prevented a collapse of public confidence during the initial phase of the war.

Equally significant was the scale of international financial assistance. Ukraine emerged as a major recipient of extraordinary support from the International Monetary Fund, the World Bank, the European Union, and G7 countries. These resources enabled the state to finance core public functions, including salaries for public servants and uniformed services, as well as social-benefit payments. According to the World Bank, preserving the continuity of financial transfers during wartime proved crucial for maintaining social stability and avoiding institutional breakdown (World Bank, 2024).

An important factor underpinning Ukraine's financial resilience was the advanced digitization of public and financial services achieved prior to 2022. Electronic banking systems, digital identification tools, and administrative platforms allowed many state services to operate despite physical infrastructure damage. From a security-studies standpoint, this experience confirms

that financial digitization can enhance state resilience, provided that adequate cybersecurity safeguards are in place (World Bank, 2023).

At the same time, the Ukrainian case underscores the ambivalent nature of digital financial resilience. Centralization of payment systems and growing reliance on digital infrastructure increased exposure to cyberattacks and hybrid interference. Ukrainian financial institutions and public administration were repeatedly targeted by coordinated cyber operations aimed at disrupting information flows and payment mechanisms. Reports by the World Economic Forum and cybersecurity agencies confirm that the war in Ukraine has transformed cyberspace into a fully integrated domain of conflict, tightly linking financial security with cyber defense (World Economic Forum, 2024).

From a sociological perspective, the societal implications of financial resilience are particularly salient. The uninterrupted payment of wages, pensions, and social benefits played a decisive role in sustaining a minimum level of public trust in the state under wartime conditions. For dispositional groups - armed forces, police, and emergency services - financial continuity was a fundamental prerequisite for maintaining morale, institutional loyalty, and operational readiness. Financial security thus functioned not merely as logistical support but as an integral element of military and internal-security capacity.

Ukraine's experience also illustrates that wartime financial resilience is inherently relational and processual. It emerges not solely from domestic economic decisions but from interactions among national institutions, international actors, and society at large. Analyses by the International Monetary Fund stress that sustaining this resilience over time requires not only external financial assistance but also social legitimacy and transparency in public-finance management (International Monetary Fund, 2024).

Ultimately, Ukraine provides an empirical example of a state operating under extreme threat, where financial security became a key determinant of survival and defensive capability. The lessons derived from this case are highly relevant for other states, including Poland, underscoring the need to construct financial systems capable of withstanding not only economic shocks but also prolonged armed conflict and hybrid aggression (World Bank, 2024; World Economic Forum, 2025).

The expansion of the digital economy and the accelerating digitization of financial systems have transformed cyberspace into a primary arena of hybrid conflict. Owing to its central role in state functioning and its deep dependence on information infrastructure, the financial sector ranks among the most vulnerable targets of destabilizing cyber operations. From a security-studies viewpoint, cyberattacks against finance should no longer be viewed as isolated incidents but as elements of deliberate non-military strategies (World Economic Forum, 2024).

Cyber operations targeting banks, payment systems, stock exchanges, and fiscal administrations may result in temporary paralysis of financial circulation, data loss, and disruption of public services. The Bank for International Settlements emphasizes that even brief outages in critical settlement infrastructures can produce disproportionate psychological and social effects, including financial panic and rapid erosion of institutional trust (Bank for International Settlements, 2023). In this respect, cyberattacks on finance constitute assaults on overall state stability rather than on individual institutions alone.

A defining feature of hybrid cyber warfare is attribution ambiguity. Anonymity and the use of proxy tools complicate responsibility assignment, limiting the applicability of traditional deterrence mechanisms. Analyses by the World Economic Forum indicate that cyber operations against financial infrastructure are characterized by low entry barriers, relatively modest costs, and high destabilization potential, making them attractive instruments for both state and non-state actors (World Economic Forum, 2024).

In increasingly digitized financial environments, electronic payment systems and centralized data registries represent particularly sensitive nodes. Ransomware attacks, transactional-data manipulation, and disruptions of digital-identity systems can generate not only economic losses but

also legitimacy crises for public institutions. From a sociological-security perspective, trust in the financial system is a fragile asset; once undermined, it is difficult to restore and may generate prolonged social tensions (World Bank, 2023).

The war in Ukraine confirms that cyberattacks on finance are an integral component of hybrid warfare. Ukrainian financial institutions and public authorities were repeatedly targeted by coordinated cyber campaigns designed to impair state functioning and amplify public uncertainty. Although defensive measures and international support mitigated their impact, the persistence of such attacks underscores the growing importance of financial-sector cybersecurity as a core element of national security (World Economic Forum, 2024).

The development of central bank digital currencies and the centralization of financial infrastructure further heighten cyber-related risks. CBDC systems, as components of critical infrastructure, may become targets of both technical attacks and disinformation campaigns aimed at undermining trust in digital money. Reports by the International Monetary Fund emphasize that cyber resilience must be treated as a prerequisite for any further digitization of finance (International Monetary Fund, 2023).

Cyber threats to finance also carry direct implications for dispositional groups. Payment disruptions, salary delays, or funding constraints may negatively affect morale and operational capacity. At the same time, these groups are tasked with managing the societal consequences of financial instability, intensifying institutional and public pressure on their performance (Maciejewski, 2025; Cieślarczyk, 2021).

In sum, cyberattacks against the financial sector represent one of the most effective instruments of contemporary hybrid warfare. Their impact derives not only from technical damage but from their ability to erode trust and destabilize state–society relations. In an era of deep financial digitization, safeguarding financial infrastructure against cyber threats becomes an indispensable element of state security strategy and a foundational challenge for institutions responsible for internal and external security (World Economic Forum, 2025). Cyber risks to financial infrastructure are increasingly analysed in interdisciplinary cybersecurity research (Kshetri, 2023).

Within security studies, dispositional groups occupy a distinctive position as a specialized segment of the state apparatus responsible for responding to threats to public order, internal security, and state stability. Their functioning presupposes institutional continuity, predictable financing, and social acceptance of coercive measures exercised in the name of the public good. Under stable conditions, these assumptions often remain implicit; they become critically visible, however, in periods of crisis marked by economic strain, financial instability, and technological disruption (Cieślarczyk, 2021; Maciejewski, 2025).

From a sociological perspective, dispositional groups are not merely instruments of state authority but actors embedded in social relations shaped by trust, legitimacy, and public evaluation. As Jan Maciejewski emphasizes, their effectiveness depends not only on formal competences or material resources but also on the stability of the institutional and economic environment in which they operate (Maciejewski, 2025). State financial security therefore constitutes a foundational condition for their operational capacity and long-term resilience (Cieślarczyk, 2020).

In the digital era, the challenges confronting dispositional groups intensify significantly. Financial digitization, the expansion of electronic money, escalating cyber threats, and the hybrid character of contemporary conflicts expose these formations to systemic uncertainty. These dynamics require a reconceptualization of their role and operating conditions - one that extends beyond traditional military or policing frameworks and incorporates financial and technological dimensions of security (World Economic Forum, 2025; International Monetary Fund, 2024).

In classical approaches, dispositional groups are defined as specialized state formations tasked with responding to threats to public and national security. The literature typically includes the armed forces, police, border guards, emergency services, and other uniformed formations

characterized by a high level of readiness, hierarchical organization, and subordination to public authority (Maciejewski, 2025).

From the standpoint of security studies, dispositional groups constitute a core element of state resilience, performing a stabilizing function during crises. Marian Cieślarczyk notes that a state's capacity to respond effectively to threats depends not only on institutional preparedness but also on the conditions under which security institutions are required to operate (Cieślarczyk, 2021). In this context, financial security - understood as continuity of funding, budgetary predictability, and resistance to economic shocks - emerges as a factor of fundamental importance (Cieślarczyk, 2021; Maciejewski, 2025).

To further clarify the position of dispositional groups within the system of state security, it is useful to refer to the sociological typology proposed by Jan Maciejewski. Maciejewski conceptualizes dispositional groups as a differentiated set of formations embedded in distinct sectors of state security, whose functions, modes of action, and sources of legitimacy vary according to the specific domain in which they operate (Maciejewski, 2025).

Within this framework, a key analytical distinction is made between military dispositional groups, uniformed coercive services, and civilian dispositional groups, the latter playing a particularly important role in the sphere of economic and financial security. Civilian dispositional groups in the system of state economic security include specialized administrative, regulatory, and supervisory bodies responsible for safeguarding the stability and continuity of financial processes. Their tasks encompass, inter alia, fiscal administration, public finance management, financial supervision, crisis coordination, and the implementation of extraordinary economic measures under conditions of heightened risk (Maciejewski, 2025).

Unlike classic uniformed formations, civilian dispositional groups operating in the financial sector do not rely on direct coercion as their primary instrument. Instead, their dispositional character manifests itself through institutional readiness, legal authority, and the capacity to rapidly implement binding financial decisions in situations of systemic threat. In periods of financial instability or crisis, these groups act as key intermediaries between political decision-makers and the operational functioning of the financial system, translating strategic directives into concrete regulatory and administrative actions (Maciejewski, 2025).

Maciejewski emphasizes that civilian dispositional groups in the domain of economic security acquire heightened strategic importance precisely in situations where financial security is challenged by external shocks, hybrid operations, or digital disruptions. Their effectiveness depends on procedural efficiency, access to reliable information, and the ability to operate under conditions of social pressure and political urgency. At the same time, their actions remain closely linked to public trust, as financial interventions directly affect citizens' economic conditions and perceptions of state legitimacy (Maciejewski, 2025; Cieślarczyk, 2020).

In this sense, civilian dispositional groups constitute a crucial - yet often underestimated - component of the broader architecture of state financial security. Their role complements that of uniformed services by ensuring the functional stability and resilience of the financial system, thereby creating the institutional preconditions for effective crisis response across the entire security sector (Cieślarczyk, 2021).

Financial pressure generated by economic crises, armed conflicts, or digital destabilization affects dispositional groups on multiple levels. It includes direct constraints on operational funding as well as indirect social effects such as declining real wages, erosion of professional prestige, and growing internal frustration. When financial strain persists over time, these factors may undermine morale, weaken cohesion, and erode institutional loyalty (Maciejewski, 2025).

Dispositional groups also function at the intersection of state authority and society, making them particularly sensitive to shifts in public sentiment triggered by financial instability. During crises, they frequently become the immediate recipients of social expectations - and, at times, public frustration - stemming from deteriorating living conditions. From a sociological-security

perspective, this situation heightens the risk of role conflict between fulfilling state-mandated tasks and preserving social legitimacy (Cieślarczyk, 2021).

Digital threats further complicate this environment. Disruptions to payment systems, cyberattacks on fiscal administration, or failures in digital infrastructure may directly affect the ability of dispositional groups to perform their duties. In such circumstances, financial stability ceases to be merely an organizational precondition and becomes a direct component of operational security.

From a system-level perspective, dispositional groups should thus be understood as integral components of state security whose effectiveness is closely linked to financial stability and institutional continuity. Examining the pressures they face under financial and digital threats allows for a more comprehensive understanding of state resilience and helps identify areas requiring reinforcement over the long term.

The progressive digitization of public finance and the expansion of financial-surveillance instruments significantly reshape the operating environment of dispositional groups. In an era of electronic money, automated settlement systems, and algorithmic public-finance management, the relationship between the state and its security apparatus undergoes a qualitative transformation. From a security-studies perspective, this shift is not neutral: it directly affects morale, institutional loyalty, and the social legitimacy of dispositional groups.

Digital financial control - understood as an integrated system for monitoring, conditioning, and automating financial flows - enhances the state's capacity to manage resources during crises. At the same time, it introduces new asymmetries of power, as decisions regarding funding, remuneration, and benefits are increasingly executed outside the direct influence of operational commanders or institutional leadership. Sociological analyses indicate that depersonalization of financial decision-making may generate a sense of diminished agency among officers and soldiers, weakening their identification with state institutions.

The morale of dispositional groups is closely linked to perceptions of economic stability and predictability of service conditions. In crisis environments characterized by inflationary pressure, budgetary constraints, or payment disruptions, even temporary delays in salaries or benefits can produce internal tensions. Under digitalized financial regimes, these risks are paradoxically amplified: while automated systems accelerate transfers under normal conditions, they also render institutions more dependent on technological infrastructure vulnerable to malfunction and cyber interference (International Monetary Fund, 2024; Bank for International Settlements, 2023).

Institutional loyalty represents another critical dimension affected by digital financial control. Loyalty is not purely normative but relational, grounded in reciprocity between the state and its security personnel. As Jan Maciejewski argues, sustaining this relationship requires not only formal discipline but also a shared conviction that state actions are rational, fair, and predictable (Maciejewski, 2025). Excessive centralization of financial decisions and opaque algorithmic allocation mechanisms may erode this conviction.

The broader social context further intensifies these dynamics. In crisis situations, dispositional groups often become executors of decisions that restrict access to financial resources or enforce economic controls. When such measures are perceived as outcomes of impersonal systems rather than accountable political choices, social responsibility tends to shift toward those implementing them. From the perspective of internal security, this constitutes a significant risk to the social legitimacy of security institutions.

The prospective deployment of central bank digital currencies and programmable financial instruments may exacerbate these tensions. The ability to condition or selectively restrict access to funds during emergencies raises fundamental questions about acceptable limits of state intervention. For dispositional groups, this environment increases exposure to ethical dilemmas and loyalty conflicts arising from the intersection of financial governance and coercive authority.

Overall, digital financial control functions as an ambivalent force. It strengthens the state's crisis-management capacity while simultaneously generating risks for morale, institutional loyalty, and public trust in dispositional groups.

Financial crises - particularly under conditions of economic digitization and hybrid threats - rarely remain confined to the economic domain. Their effects rapidly permeate the social sphere, generating tensions, protests, and declining trust in public institutions. In this context, dispositional groups become a central pillar of state security, responsible for maintaining public order and enforcing decisions adopted under crisis pressure.

From a security-studies perspective, financial crises function as catalysts for destabilization processes that may escalate into open social conflict. Inflation, declining real incomes, restricted access to public services, and disruptions to payment systems directly affect societal well-being. World Bank research indicates that economic crises significantly increase the likelihood of social unrest, particularly in states simultaneously exposed to armed conflict or mass displacement (World Bank, 2023).

Under such conditions, dispositional groups operate in environments characterized by elevated operational risk. They are tasked with enforcing order while simultaneously experiencing the same economic pressures as the broader population. This dual position amplifies internal strain and heightens vulnerability to organizational stress. From a sociological-security viewpoint, prolonged exposure to such conditions increases the risk of burnout, discipline erosion, and weakened internal cohesion.

Digitalization further accelerates the dynamics of crisis escalation. Economic disinformation disseminated through social media can rapidly intensify public emotions and provoke collective reactions. Dispositional groups are increasingly compelled to act under informational pressure, where operational decisions must be made amid incomplete or contradictory data. As emphasized by the World Economic Forum, the convergence of financial and informational crises constitutes one of the most serious challenges to contemporary internal security (World Economic Forum, 2025).

Another operational challenge concerns the legitimacy of coercive action. Enforcing measures related to economic restrictions, financial controls, or the protection of critical infrastructure may provoke social resistance. In contexts of diminished trust in public institutions, responsibility for crisis outcomes is often displaced onto implementing actors rather than policy designers. From a national-security perspective, erosion of social acceptance for dispositional groups undermines the effectiveness of crisis response.

Recent experiences - including the COVID-19 pandemic and the war in Ukraine - demonstrate that financial crises increasingly assume prolonged and overlapping forms. In such conditions, dispositional groups must function in a state of sustained mobilization, underscoring the importance of financial resilience as a factor sustaining long-term operational capacity. As Marian Cieślarczyk observes, state resilience depends not only on material resources but also on the endurance of security institutions over time (Cieślarczyk, 2021).

The analysis indicates that financial crises and associated social tensions represent one of the most demanding operational challenges for dispositional groups in the digital era. Effective performance under these conditions requires not only legal and organizational preparedness but also stable financial foundations and a high level of social trust.

The analysis of threats to state financial security in the digital era gains particular relevance in light of the adoption of the new National Security Strategy of the Republic of Poland on 25 July 2025, prepared by the Minister of National Defence in cooperation with the National Security Bureau (National security strategy of the Republic of Poland, 2025). Although the document does not define a formal time horizon explicitly framed as a "Strategy to 2030," it functions as a strategic guideline of a medium- and long-term character, outlining the foundations of state security policy for the coming decade.

The Strategy clearly states that Poland's national security can no longer be understood exclusively in military terms. Instead, it encompasses the security of citizens, the stability of state functioning, and balanced socio-economic development embedded in an increasingly adverse and dynamic international environment. Within this framework, state financial security emerges as a *sine qua non* condition for the achievement of strategic objectives such as territorial integrity, institutional resilience, and the capacity for sustained crisis response.

The 2025 Strategy further emphasizes the growing significance of hybrid threats, cyber risks, and geopolitical pressure, which increasingly employ economic and financial instruments as tools of strategic influence. In this context, financial security ceases to be confined to fiscal or monetary policy alone and becomes an integral component of the national security system, closely interlinked with informational, technological, and social security dimensions.

From the perspective of dispositional groups, the strategic provisions of the document are of particular importance. The Strategy explicitly highlights the necessity of maintaining the operational capacity of the state under conditions of prolonged crises, which presupposes stable and predictable financing of structures responsible for both internal and external security. Dispositional groups, operating at the intersection of the state and society, thus emerge not merely as executors of strategic decisions but as key carriers of state resilience in situations of escalating social and economic tension.

At the same time, the Polish National Security Strategy indirectly confirms conclusions drawn from the analyses of the World Economic Forum in 2026, according to which financial stability under conditions of digital transformation and hybrid conflict constitutes one of the pillars of global security. The convergence of these diagnoses suggests that the future of Poland's security will increasingly depend on the state's ability to integrate security policy, financial policy, and digital risk management within a coherent strategic framework.

Looking ahead to the coming years - corresponding *de facto* to a horizon around 2030 - the central challenge for Poland will be the construction of state financial resilience. This resilience should be understood not merely as macroeconomic stability, but as the system's capacity to absorb, adapt to, and recover from cumulative crises. Of particular importance is the ability to ensure continuity in the financing of public tasks and the effective functioning of dispositional groups under conditions of social pressure and informational disruption.

The overall findings of this study confirm that the provisions of the 2025 National Security Strategy place financial security at the core of contemporary thinking about state resilience. Strengthening this dimension requires a systemic approach that integrates economic, technological, and social instruments, while consciously recognizing the role of dispositional groups as a key stabilizing force for public order and state security in an era of growing uncertainty.

The strategic perspective presented above confirms that financial security has become a central organizing principle of contemporary state resilience. In the case of Poland, this dimension is explicitly embedded in the 2025 National Security Strategy, which recognizes the growing interdependence between financial stability, digital transformation, and the capacity to withstand hybrid threats. The analysis of systemic risks, institutional arrangements, and the role of dispositional groups demonstrates that financial security operates not as an isolated policy field, but as a cross-cutting factor shaping the effectiveness of the entire security architecture. Taken together, these findings provide a basis for synthesizing the study's key conclusions and outlining their theoretical and practical implications.

Discussion. The obtained results confirm that state financial security in the digital era should be interpreted not only through traditional macroeconomic indicators but also through the prism of institutional resilience and social relations between the state and society. The findings demonstrate that digital transformation fundamentally reshapes the architecture of financial governance by introducing new forms of systemic vulnerability associated with cyber threats, hybrid financial warfare, and algorithmic decision-making.

Compared with existing studies that primarily focus on financial stability as a macroeconomic category, the present research expands the analytical perspective by emphasizing the relational dimension of financial security. In particular, the results support the arguments of contemporary security-studies scholars who highlight the growing interdependence between financial systems, technological infrastructures, and societal trust. While institutional reports by international organizations underline the importance of cyber resilience and digital governance, this study contributes by demonstrating how these transformations directly affect dispositional groups operating within the security architecture of the state. These findings correspond with recent debates on digital financial governance and systemic stability in international political economy literature (Moschella & Tsingou, 2022; Buchanan et al., 2022).

The analysis shows that the introduction of digital financial instruments, including central bank digital currencies and automated financial control mechanisms, has an ambivalent impact. On the one hand, digitalization enhances crisis-management capacity, increases the efficiency of financial flows, and strengthens the ability of the state to respond to hybrid threats. On the other hand, excessive centralization of financial data and algorithmic governance may generate risks for institutional legitimacy, public trust, and the morale of dispositional groups responsible for maintaining public order during periods of financial instability.

In comparison with previous research focusing mainly on economic or technological aspects of digital finance, this article highlights the socio-institutional consequences of financial transformation. The findings suggest that predictable financing, transparency of financial governance, and institutional continuity play a decisive role in maintaining the operational effectiveness and loyalty of dispositional groups. These results are consistent with broader debates on resilience within security studies, which emphasize that financial security functions as a cross-sectoral element influencing political stability and social cohesion.

At the same time, several limitations of the study should be acknowledged. The research relies primarily on qualitative analysis of institutional reports and theoretical literature, which may limit the empirical generalization of conclusions. Future research could incorporate quantitative indicators of financial resilience, comparative case studies of digital financial governance across different countries, and empirical surveys examining the perceptions of dispositional groups toward digital financial control mechanisms.

Furthermore, the rapid evolution of digital financial technologies implies that the risks identified in this study remain dynamic and context-dependent. Additional interdisciplinary research combining finance, sociology, and cybersecurity studies is necessary to better understand long-term implications for state security and democratic accountability.

Overall, the discussion confirms that financial security in the digital era represents a multidimensional process integrating economic stability, technological resilience, and social legitimacy. Recognizing this complexity is essential for developing balanced security strategies capable of strengthening state resilience without undermining institutional trust or societal cohesion.

Conclusions. The results discussed above demonstrate that the transformation of financial systems in the digital era requires a rethinking of traditional approaches to national security analysis. Rather than viewing financial stability solely through macroeconomic indicators, this study highlights the need to interpret financial security as a multidimensional process shaped by technological change, hybrid threats, and evolving state–society relations. The analysis conducted in this article demonstrates that financial security has become one of the key determinants of state security in the digital era. Accelerated financial digitization, the expansion of cyber and hybrid threats, and the increasing use of economic instruments as tools of strategic influence have fundamentally transformed the role of financial systems within the architecture of national security. Financial security can no longer be treated solely as a component of economic policy; it must be understood as a strategic condition for institutional continuity, social stability, and effective crisis response.

The study shows that state financial security in the digital era is best captured through two interrelated dimensions: financial stability and financial resilience. Financial stability ensures the operational continuity of fiscal and monetary systems, while financial resilience determines the state's capacity to absorb shocks, adapt to prolonged crises, and recover under conditions of systemic pressure. Digital transformation intensifies both dimensions simultaneously, increasing efficiency while generating new vulnerabilities related to cyber risks, data centralization, and algorithmic governance.

A central finding concerns the growing importance of hybrid threats targeting financial systems. Financial destabilization, cyberattacks, and economic disinformation increasingly function as instruments of non-military coercion, capable of producing effects comparable to conventional armed actions. The empirical example of Ukraine illustrates that maintaining financial security is a prerequisite for sustaining defense efforts, preserving public trust, and preventing institutional collapse during long-term conflict.

The article also highlights the strategic role of dispositional groups as a key link between the state and society. Their operational effectiveness, morale, and institutional loyalty are closely dependent on the level of financial security maintained by the state. In this context, civilian dispositional groups operating within the system of economic and financial security emerge as a particularly important, yet often underestimated, component of state resilience. Digital financial control, including the prospective deployment of central bank digital currencies, represents an ambivalent factor: it strengthens crisis-management capacity while simultaneously posing risks to institutional trust and social legitimacy if implemented without transparency and accountability. From a theoretical perspective, the article contributes to expanding the analytical framework of security studies by integrating insights from financial economics, sociology, and international political economy. This interdisciplinary approach allows financial security to be conceptualized not only as an economic resource but also as a relational factor influencing institutional legitimacy, public trust, and crisis governance capacity.

From a strategic perspective, the case of Poland confirms that financial security occupies a central position in contemporary security thinking. The 2025 National Security Strategy explicitly situates financial stability and resilience among the foundations of state security in an environment characterized by digital transformation and hybrid pressure. Strengthening this dimension requires a systemic approach that integrates financial policy, cybersecurity, and security governance, while consciously accounting for the social and institutional conditions under which dispositional groups operate.

In conclusion, ensuring financial security in the digital era demands not only technological solutions and regulatory instruments, but also a comprehensive understanding of the social mechanisms that underpin state resilience. Further empirical research should explore the long-term implications of digital financial architectures for institutional trust, democratic accountability, and the functioning of core security institutions under conditions of sustained uncertainty.

In an environment characterized by accelerating digital transformation and persistent geopolitical uncertainty, strengthening financial security will increasingly depend on the ability of states to balance technological innovation with institutional transparency and social legitimacy. Future research should therefore focus on empirical analyses of digital financial governance and its long-term implications for state resilience and democratic accountability.

References

1. Auer, R., Cornelli, G., & Frost, J. (2022). Rise of the central bank digital currencies: Drivers, approaches and technologies. *Economic Policy*, *37*(112), 801–861. https://doi.org/10.1093/epolic/eiac004
2. Balan, O., Voitenko, M., & Pulcha, D. (2024). Ukraine's post-war recovery: key steps and experience of leading countries. *Economic Journal of Odesa Polytechnic*, (1). https://doi.org/10.15276/EJ.01.2024.3
3. Bank for International Settlements. (2023). *Annual economic report 2023*. https://www.bis.org/publ/arpdf/ar2023e.htm
4. Bank for International Settlements. (2023). *Central bank digital currencies: System design and interoperability*.
5. Bank for International Settlements. (2023). *Cyber resilience of financial market infrastructures*.
6. Bank for International Settlements. (2024). *Annual economic report 2024*.

7. Barro, R. J. (1997). *Determinants of economic growth*. MIT Press. https://ui.adsabs.harvard.edu/abs/1994nsf....9320504B/abstract
8. Beck, T., Levine, R., & Loayza, N. (2000). Finance and the sources of growth. *Journal of Financial Economics*, *58*(1-2), 261–300. https://pure.uvt.nl/ws/portalfiles/portal/1024769/sources.pdf
9. Beck, U. (2002). *Risk society: Towards a new modernity* (S. Cieśla, Trans.). Scholar.
10. Brunnermeier, M. K., James, H., & Landau, J.-P. (2021). The digitalization of money. *Journal of Economic Perspectives*, *35*(2), 85–108. https://doi.org/10.1257/jep.35.2.85
11. Buchanan, B., Naqvi, N., & Weinhardt, C. (2022). Digital currencies and financial stability: Implications for monetary policy. *Finance Research Letters*, *46*, Article 102332. https://doi.org/10.1016/j.frl.2021.102332
12. Cieślarczyk, M. (2020). *Security culture and societal resilience of the state*. Difin.
13. Cieślarczyk, M. (2021). *State resilience under hybrid threats*. Difin.
14. Collier, P. (2007). *The bottom billion: Why the poorest countries are failing*. Oxford University Press. https://treasury.gov.au/sites/default/files/2019-03/05_The_bottom_billion.pdf
15. Eurostat. (2023). *Digitalisation and social inclusion in the European Union*.
16. Gierszewski, J. (2018). *Internal security of the state*. Difin.
17. International Monetary Fund. (2023). *Cyber risk supervision for the financial sector*.
18. International Monetary Fund. (2023). *The rise of digital money*.
19. International Monetary Fund. (2023). *Ukraine: Recovery framework for economic stabilization and growth*. https://mof.gov.ua/storage/files/1UKREA2023003.pdf
20. International Monetary Fund. (2024). *Global financial stability report 2024*.
21. International Monetary Fund. (2024). *Ukraine: Staff report for the extended fund facility*.
22. Kshetri, N. (2023). Cybersecurity and cyberwar: What everyone needs to know about financial cyber risks. *Journal of Cybersecurity*, *9*(1), Article tyad012. https://doi.org/10.1093/cybsec/tyad012
23. Lyons, R. K., & Viswanath-Natraj, G. (2023). What keeps stablecoins stable? *Journal of International Money and Finance*, *131*, Article 102777. https://doi.org/10.1016/j.jimonfin.2022.102777
24. Maciejewski, J. (2014). *Dispositional groups: A sociological analysis*. Wydawnictwo Uniwersytetu Wrocławskiego.
25. Maciejewski, J. (2025). *Dispositional groups: A sociological analysis* (3rd expanded ed.). Wydawnictwo Uniwersytetu Wrocławskiego; Szermierz.
26. Moschella, M., & Tsingou, E. (2022). Regulating finance in the digital age: Global governance challenges. *Review of International Political Economy*, *29*(6), 1942–1965. https://doi.org/10.1080/09692290.2021.1903780
27. National Security Strategy of the Republic of Poland. (2025). *National security strategy of the Republic of Poland*.
28. OECD. (2025). *Mapping Ukraine's financial markets and corporate governance framework for a sustainable recovery*. OECD Publishing. https://www.oecd.org/en/publications/mapping-ukraine-s-financial-markets-and-corporate-governance-framework-for-a-sustainable-recovery_866c5c44-en.html
29. Pieczywok, A. (2018). *Social security under asymmetric threats*. Difin.
30. Redziuk, Y. (2024). Leading risks of geopolitical and geoeconomics for business activity in Ukraine during the war. *Actual Problems of International Relations*, *1*(159), 138–145. https://doi.org/10.17721/apmv.2024.159.1.138-145
31. Redziuk, Y. (2024). Mechanisms of external financing of the Ukrainian economy during war and approaches to their optimization. *Economy of Ukraine*, *68*(12), 51–66. https://doi.org/10.15407/economyukr.2024.12.051
32. Redziuk, Y. V. (2023). Formation of competitive clusters of Ukraine in the conditions of global challenges. *Strategy of Economic Development of Ukraine*, *53*, 63–77. https://doi.org/10.33111/sedu.2023.53.063.077
33. Rogoff, K. (2021). The digitalization of money. *Journal of Economic Perspectives*, *35*(2), 5–28.
34. Rybak, M. (2022). Assessment of efficiency and factors of business development in Ukraine. *Economy and Society*, *45*. https://doi.org/10.32782/2524-0072/2022-45-72
35. Schär, F. (2021). Decentralized finance: On blockchain- and smart contract-based financial markets. *Federal Reserve Bank of St. Louis Review*, *103*(2), 153–174.
36. Ścibiorek, Z. (2013). *State security: An outline of key issues*. Akademia Obrony Narodвої.
37. Stiglitz, J. E. (2003). *Globalization and its discontents*. Norton. https://doi.org/10.1002/jid.1134
38. World Bank. (2023). *Digital public infrastructure and resilience in conflict-affected states*.
39. World Bank. (2023). *Resilience of financial systems in fragile and conflict-affected states*.
40. World Bank. (2023). *Social impacts of economic crises and conflict*.
41. World Bank. (2024). *Cybersecurity and financial sector stability in conflict-affected states*.
42. World Bank. (2024). *Global economic prospects 2024*.
43. World Bank. (2024). *Ukraine rapid damage and needs assessment 2024*.
44. World Economic Forum. (2024). *Global cybersecurity outlook 2024*.
45. World Economic Forum. (2024). *Global risks report 2024*.
46. World Economic Forum. (2025). *Global risks report 2025*.
47. World Economic Forum. (2026). *Annual meeting 2026: A spirit of dialogue*.

Received: 06.11.2025 *Accepted:10.03.2026*
Received after review: 11.02.2026 *Published: 31.03.2026*

Authors Contribution: *All authors have contributed equally to this work*
Conflict of Interest: *The authors declare no conflict of interest*

Мацеєвський Ян
професор, доктор соціологічних наук
Коледж професійної освіти пл. Повстанців Шльонських,
1 53-329 Вроцлав, Польща
e-mail: jan.maciejewski@wskz.pl
ORCID ID: 0000-0002-0743-099X
Кривцова Тетяна
ад'юнкт, кандидат економічних наук
Коледж професійної освіти
пл. Повстанців Шльонських, 1 53-329 Вроцлав, Польща
e-mail: etiana.krivstova@wskz.pl
ORCID ID: 0000-0002-1693-6781

Загрози фінансовій безпеці держави в цифрову епоху: виклики для диспозиційних груп

Анотація. Фінансова безпека держави стала ключовим компонентом національної безпеки в умовах стрімкої цифрової трансформації, геополітичної нестабільності та розширення гібридних загроз. Посилення цифровізації фінансових систем підвищує ефективність, але одночасно створює нові системні вразливості, пов'язані з кіберризиками, алгоритмічним управлінням та централізацією фінансових даних.

Постановка проблеми. Сучасні фінансові інфраструктури все частіше піддаються впливу гібридних операцій, кібератак та системних шоків, що можуть підірвати інституційну стабільність, суспільну довіру та оперативну спроможність диспозиційних груп, відповідальних за підтримання громадського порядку та стійкість держави.

Невирішені аспекти проблеми. Існуючі дослідження переважно розглядають фінансову безпеку з економічної точки зору, тоді як соціально-інституційні наслідки для диспозиційних груп та реляційний вимір фінансової безпеки залишаються недостатньо вивченими, особливо в умовах цифрового фінансового управління та тривалого кризового середовища.

Мета статті. Метою даного дослідження є ідентифікація та концептуалізація ключових загроз фінансовій безпеці держави в цифрову еру, а також визначення їхнього впливу на диспозиційні групи в межах методології наук про безпеку.

Виклад основного матеріалу. У дослідженні застосовано соціосистемний та міждисциплінарний підходи, що поєднують якісний аналіз інституційних звітів (МВФ, Світового банку, БМР, Всесвітнього економічного форуму), окремих статистичних джерел та сучасної літератури з питань безпеки. Результати демонструють, що фінансова безпека в цифрову епоху складається з двох взаємопов'язаних вимірів — фінансової стабільності та фінансової стійкості. Цифрова трансформація, цифрові валюти центральних банків (CBDC), кіберзагрози та гібридні фінансові війни змінюють архітектуру державної безпеки та впливають на функціонування, моральний дух та інституційну лояльність диспозиційних груп.

Висновки. Дослідження підтверджує, що фінансова безпека еволюціонувала у стратегічну опору національної безпеки. Зміцнення державної стійкості потребує інтеграції фінансового управління, кібербезпеки та соціально-інституційних факторів при одночасному забезпеченні прозорості та довіри до цифрових фінансових систем.

Ключові слова: *фінансова безпека держави, цифрова трансформація, гібридні загрози, цифрова валюта центрального банку, стійкість держави, кіберризики.*

Формули: -; рис.: -; табл.: -; бібл.: 47.

Для цитування: Maciejewski Jan, Krivtsova Tetiana. Threats to state financial security in the digital age: challenges for dispositional groups. Фінансово-кредитні системи: перспективи розвитку. №1(20) 2026. С. 173-191. https://doi.org/10.26565/2786-4995-2026-1-13

Список літератури

1. Auer R., Cornelli G., Frost J. Rise of the central bank digital currencies: Drivers, approaches and technologies. *Economic Policy*. 2022. Vol. 37(112). P. 801–861. https://doi.org/10.1093/epolic/eiac004.
2. Balan O., Voitenko M., Pulcha D. Ukraine's post-war recovery: key steps and experience of leading countries. *Economic Journal of Odesa Polytechnic*. 2024. № 1. https://doi.org/10.15276/EJ.01.2024.3.
3. Annual economic report 2023 / Bank for International Settlements. Basel : BIS, 2023. URL: https://www.bis.org/publ/arpdf/ar2023e.htm.
4. Central bank digital currencies: System design and interoperability / Bank for International Settlements. Basel : BIS, 2023.
5. Cyber resilience of financial market infrastructures / Bank for International Settlements. Basel : BIS, 2023.
6. Annual economic report 2024 / Bank for International Settlements. Basel : BIS, 2024.
7. Barro R. J. Determinants of economic growth. Cambridge : MIT Press, 1997. URL: https://ui.adsabs.harvard.edu/abs/1994nsf....9320504B/abstract.
8. Beck T., Levine R., Loayza N. Finance and the sources of growth. *Journal of Financial Economics*. 2000. Vol. 58(1-2). P. 261–300. URL: https://pure.uvt.nl/ws/portalfiles/portal/1024769/sources.pdf.

9. Beck U. Risk society: Towards a new modernity / trans. S. Cieśla. Warsaw : Scholar, 2002.
10. Brunnermeier M. K., James H., Landau J.-P. The digitalization of money. *Journal of Economic Perspectives*. 2021. Vol. 35(2). P. 85–108. https://doi.org/10.1257/jep.35.2.85.
11. Buchanan B., Naqvi N., Weinhardt C. Digital currencies and financial stability: Implications for monetary policy. *Finance Research Letters*. 2022. Vol. 46. Art. 102332. https://doi.org/10.1016/j.frl.2021.102332.
12. Cieślarczyk M. Security culture and societal resilience of the state. Warsaw : Difin, 2020.
13. Cieślarczyk M. State resilience under hybrid threats. Warsaw : Difin, 2021.
14. Collier P. The bottom billion: Why the poorest countries are failing. Oxford : Oxford University Press, 2007. URL: https://treasury.gov.au/sites/default/files/2019-03/05_The_bottom_billion.pdf.
15. Digitalisation and social inclusion in the European Union / Eurostat. Luxembourg : Publications Office of the EU, 2023.
16. Gierszewski J. Internal security of the state. Warsaw : Difin, 2018.
17. Cyber risk supervision for the financial sector / International Monetary Fund. Washington, D.C. : IMF, 2023.
18. The rise of digital money / International Monetary Fund. Washington, D.C. : IMF, 2023.
19. Ukraine: Recovery framework for economic stabilization and growth / International Monetary Fund. 2023. URL: https://mof.gov.ua/storage/files/1UKREA2023003.pdf.
20. Global financial stability report 2024 / International Monetary Fund. Washington, D.C. : IMF, 2024.
21. Ukraine: Staff report for the extended fund facility / International Monetary Fund. Washington, D.C. : IMF, 2024.
22. Kshetri N. Cybersecurity and cyberwar: What everyone needs to know about financial cyber risks. *Journal of Cybersecurity*. 2023. Vol. 9(1). Art. tyad012. https://doi.org/10.1093/cybsec/tyad012.
23. Lyons R. K., Viswanath-Natraj G. What keeps stablecoins stable? *Journal of International Money and Finance*. 2023. Vol. 131. Art. 102777. https://doi.org/10.1016/j.jimonfin.2022.102777.
24. Maciejewski J. Dispositional groups: A sociological analysis. Wrocław : Wydawnictwo Uniwersytetu Wrocławskiego, 2014.
25. Maciejewski J. Dispositional groups: A sociological analysis. 3rd expanded ed. Wrocław : Wydawnictwo Uniwersytetu Wrocławskiego; Szermierz, 2025.
26. Moschella M., Tsingou E. Regulating finance in the digital age: Global governance challenges. *Review of International Political Economy*. 2022. Vol. 29(6). P. 1942–1965. https://doi.org/10.1080/09692290.2021.1903780.
27. National security strategy of the Republic of Poland. Warsaw : National Security Bureau, 2025.
28. Mapping Ukraine's financial markets and corporate governance framework for a sustainable recovery / OECD. Paris : OECD Publishing, 2025. URL: https://www.oecd.org/en/publications/mapping-ukraine-s-financial-markets-and-corporate-governance-framework-for-a-sustainable-recovery_866c5c44-en.html.
29. Pieczywok A. Social security under asymmetric threats. Warsaw : Difin, 2018.
30. Редзюк Є. Провідні ризики геополітики та геоекономіки для діяльності бізнесу в Україні під час війни. *Актуальні проблеми міжнародних відносин*. 2024. Вип. 1 (159). С. 138–145. https://doi.org/10.17721/apmv.2024.159.1.138-145.
31. Редзюк Є. Механізми зовнішнього фінансування економіки України під час війни та підходи до їх оптимізації. *Економіка України*. 2024. № 68 (12). С. 51–66. https://doi.org/10.15407/economyukr.2024.12.051.
32. Редзюк Є. В. Формування конкурентоспроможних кластерів України в умовах глобальних викликів. *Стратегія економічного розвитку України*. 2023. Вип. 53. С. 63–77. https://doi.org/10.33111/sedu.2023.53.063.077.
33. Rogoff K. The digitalization of money. *Journal of Economic Perspectives*. 2021. Vol. 35(2). P. 5–28.
34. Рибак М. Оцінка ефективності та факторів розвитку бізнесу в Україні. *Економіка та суспільство*. 2022. Вип. 45. https://doi.org/10.32782/2524-0072/2022-45-72.
35. Schär F. Decentralized finance: On blockchain- and smart contract-based financial markets. *Federal Reserve Bank of St. Louis Review*. 2021. Vol. 103(2). P. 153–174.
36. Ścibiorek Z. State security: An outline of key issues. Warsaw : Akademia Obrony Narodвої, 2013.
37. Stiglitz J. E. Globalization and its discontents. New York : Norton, 2003. https://doi.org/10.1002/jid.1134.
38. Digital public infrastructure and resilience in conflict-affected states / World Bank. Washington, D.C. : World Bank, 2023.
39. Resilience of financial systems in fragile and conflict-affected states / World Bank. Washington, D.C. : World Bank, 2023.
40. Social impacts of economic crises and conflict / World Bank. Washington, D.C. : World Bank, 2023.
41. Cybersecurity and financial sector stability in conflict-affected states / World Bank. Washington, D.C. : World Bank, 2024.
42. Global economic prospects 2024 / World Bank. Washington, D.C. : World Bank, 2024.
43. Ukraine rapid damage and needs assessment 2024 / World Bank. Washington, D.C. : World Bank, 2024.
44. Global cybersecurity outlook 2024 / World Economic Forum. Geneva : WEF, 2024.
45. Global risks report 2024 / World Economic Forum. Geneva : WEF, 2024.
46. Global risks report 2025 / World Economic Forum. Geneva : WEF, 2025.
47. Annual meeting 2026: A spirit of dialogue / World Economic Forum. Geneva : WEF, 2026.

Стаття надійшла до редакції 06.11.2025 *Статтю рекомендовано до друку 10.03.2026*
Стаття надійшла після рецензування 11.02.2026 *Статтю опубліковано 31.03.2026*

Внесок авторів: *всі автори зробили рівний внесок у цю роботу*
Конфлікт інтересів: *автори повідомляють про відсутність конфлікту інтересів*