UDC 005.334:005.21:004.9

О. В. КИССА[1]
А. С. КРАЄВСЬКА[2]

СТРАТЕГІЧНА СТІЙКІСТЬ ПІДПРИЄМСТВА ЧЕРЕЗ УПРАВЛІННЯ РИЗИКАМИ У МІЖНАРОДНИХ КОМАНДАХ ІТ-ПОСЛУГ

[1]Вінницький національний технічний університет
[2]Вінницький національний технічний університет

Анотація

Прискорення геополітичної нестабільності, тривалі перебої в ланцюгах постачання та зростаюча залежність компаній від розподілених цифрових сервісних інфраструктур трансформували стійкість з захисної організаційної властивості у стратегічний управлінський потенціал. У цій роботі досліджується, яким чином управління ризиками може посилювати стійкість підприємств у багатонаціональних ІТ-командах сервісної підтримки. Аргументація ґрунтується на концептуальному синтезі сучасних досліджень, присвячених невизначеності інвестицій в умовах війни, операційній залежності, вразливості глобальних ланцюгів постачання, кризовому управлінню в проєктно-орієнтованих організаціях, адаптивному управлінню проєктами, психологічній безпеці, організаційному навчанню та управлінню даними. У роботі обґрунтовується, що стійкість у багатонаціональних командах з надання ІТ-послуг не зводиться лише до реагування на інциденти чи планування безперебійності бізнесу. Вона формується як результат узгодженої конфігурації виявлення ризиків, повноважень щодо прийняття рішень, управління даними, процедур навчання, психологічної безпеки та адаптивного розподілу ресурсів. Запропонована аналітична позиція підкреслює, що багатонаціональні ІТ-команди сервісної підтримки слід розглядати як соціотехнічні системи, які одночасно зазнають впливу геополітичних, операційних, когнітивних ризиків та ризиків, пов'язаних із даними. У зв'язку з цим управління ризиками перетворюється на механізм забезпечення безперервності надання послуг, прискорення відновлення та трансформації дестабілізуючих факторів в організаційне навчання.

Ключові слова: стійкість підприємства, управління ризиками, міжнародні ІТ-команди, кризове управління, організаційне навчання, управління даними.

STRATEGIC ENTERPRISE RESILIENCE THROUGH RISK MANAGEMENT IN MULTINATIONAL IT SERVICE TEAMS

Abstract

The acceleration of geopolitical volatility, the persistence of supply-chain disruptions, and the growing dependence of firms on distributed digital service infrastructures have transformed resilience from a protective organizational property into a strategic management capability. These theses examine how risk management can strengthen enterprise resilience in multinational IT service teams. The argument is built on a conceptual synthesis of recent research on war-induced investment uncertainty, operational lock-in, global supply-chain vulnerability, crisis management in project-based organizations, adaptive project management, psychological safety, organizational learning, and data governance. The paper substantiates that resilience in multinational IT service teams is not reducible to incident response or business continuity planning. It emerges from a coordinated configuration of risk sensing, decision authority, data governance, learning routines, psychological safety, and adaptive resource allocation. The proposed analytical position emphasizes that multinational IT service teams should be managed as socio-technical systems exposed simultaneously to geopolitical, operational, cognitive, and data-related risks. Risk management therefore becomes a mechanism for preserving service continuity, accelerating recovery, and converting disturbance into organizational learning.

Keywords: enterprise resilience, risk management, multinational IT teams, crisis management, organizational learning, data governance.

Contemporary multinational enterprises increasingly depend on IT service teams that operate across jurisdictions, time zones, regulatory environments, cloud platforms and vendor ecosystems. In such conditions, technical support, service delivery, infrastructure maintenance and project execution can no longer be interpreted as merely operational functions. They become part of a broader resilience architecture because disruption in one region, supplier chain or data environment may rapidly affect the continuity of services delivered to users in another institutional context. The relevance of the topic is intensified by the Russia-Ukraine war, the long aftereffects of the COVID-19 crisis, the fragmentation of global markets and the growing exposure of firms to cyber, geopolitical, staffing and knowledge-continuity risks. Recent business research shows that inter-state war changes managerial decision-making and investment expectations rather than remaining an external political background [7]. For multinational IT service teams, this means that risk management must be embedded into service governance, not added as a secondary compliance procedure after incidents occur.

The object of these theses is enterprise resilience in multinational IT service teams. The subject is the system of risk-management mechanisms through which such teams maintain service continuity, preserve organizational learning and support strategic adaptability under uncertainty. The purpose is to substantiate a conceptual approach in which risk management functions as a strategic capability for resilience rather than as a narrow instrument of loss prevention. This purpose is achieved through three interconnected analytical tasks: first, to clarify how geopolitical and supply-chain disturbances reshape the risk environment of multinational service teams; second, to identify the organizational conditions that allow distributed teams to respond without losing coordination; third, to outline the managerial logic by which risk assessment, data governance, adaptive project management and team learning can be integrated into a coherent resilience model.

The methodological basis of the study is a conceptual synthesis of recent international literature. The analysis does not claim to present a new empirical survey of IT teams. Instead, it draws a theoretically grounded analogy from research on geopolitical risk, global supply chains, project-based crisis management, organizational learning and data governance. Such a design is methodologically appropriate because enterprise resilience in multinational IT service teams is an interdisciplinary phenomenon. It cannot be explained only through technical incident management, nor only through strategic management theory. The literature on operations locked in amid geopolitical conflicts is particularly relevant because it shows that enterprises may be unable to exit high-risk regions quickly and may therefore need capabilities for functioning under constrained strategic choice [8]. The implication for IT service teams is direct: resilience should be designed for conditions in which ideal risk avoidance is impossible and controlled continuation becomes the real managerial problem.

Geopolitical instability affects multinational IT service teams through several channels. It changes the cost and availability of infrastructure, complicates access to local talent, disrupts contractual relations with suppliers, increases compliance uncertainty and raises the probability of service fragmentation between regional units. Research on the Russia-Ukraine conflict and global supply chains indicates that conflict can produce bottlenecks, cost increases and availability shocks that move far beyond the immediate conflict zone [9]. Although this literature is often focused on physical logistics, its analytical significance for IT services lies in the same structural principle: globally distributed systems create efficiency under stable conditions but generate hidden dependencies under crisis conditions. Cloud service concentration, outsourcing chains, cross-border data flows and distributed support centers may therefore become sources of fragility if risk ownership is unclear.

The strategic meaning of enterprise resilience lies in the ability to preserve essential functions while adapting the configuration of resources, processes and decisions. In this sense, resilience differs from ordinary robustness. Robustness assumes that the existing system can absorb disturbance without major transformation, whereas resilience includes anticipation, absorption, recovery and learning. The work of T. G. Bas on globalization and glocalization is useful here because it demonstrates that global crisis experience encourages hybrid arrangements that combine the efficiency of global integration with the adaptability of local responses [1]. Transferred carefully to multinational IT service teams, this logic suggests that a resilient service model should not rely exclusively on centralized governance or fully decentralized autonomy. It requires a calibrated

balance: common standards for risk visibility and data quality, combined with regional authority to respond to locally specific disruptions.

Risk management in multinational IT service teams should therefore operate at three levels. At the strategic level, it identifies exposures that may affect enterprise continuity, such as geopolitical dependence, cloud concentration, regulatory fragmentation and vendor lock-in. At the organizational level, it defines decision rights, escalation paths, accountability and learning mechanisms. At the team level, it supports psychological safety, knowledge sharing and rapid problem framing. This multilevel view is consistent with research on crisis management in project-based organizations, where crisis response is not treated as a single event but as a process involving preparation, response, recovery and learning [4]. For IT service teams, the same processual logic is especially relevant because incidents rarely remain isolated. A service outage may quickly become a reputational issue, a compliance issue, a staffing issue and a client-retention issue.

Adaptive project management strengthens resilience because it permits controlled adjustment without abandoning accountability. L. Gutheil's analysis of adaptive project management emphasizes that such approaches are used in complex, changing and politicized environments where fixed planning logic is insufficient [2]. In multinational IT service teams, adaptive management should not be confused with improvisation. Its value lies in creating disciplined flexibility: short feedback loops, transparent assumptions, scenario-based planning, iterative prioritization and rapid reassessment of dependencies. A team that can revise its delivery sequence, redistribute workload across regions and reframe service priorities in response to emerging risk is strategically more resilient than a team that follows an obsolete plan with formal precision.

A central condition of such flexibility is psychological safety. S. Kim, H. Lee and T. P. Connerton show that psychological safety affects team performance through the mediating role of efficacy and learning behavior [6]. This finding has direct significance for multinational IT service teams because risk information is often dispersed among engineers, support specialists, service managers and local coordinators. If team members fear blame, reputational damage or managerial retaliation, early warning signals remain unreported until they become incidents. Conversely, psychologically safe teams can discuss weak signals, operational mistakes, ambiguous dependencies and client-side vulnerabilities before they generate systemic failure. In this regard, psychological safety is not a soft cultural addition to risk management. It is an information infrastructure that enables earlier detection and more accurate interpretation of risk.

Organizational learning converts disruption into resilience only when lessons are captured and reused. P. Jiao and W. Bu argue that organizational learning contributes to organizational resilience by enriching managerial cognition and strengthening the capacity to respond to uncertainty [5]. For multinational IT service teams, learning should be institutionalized through post-incident reviews, shared knowledge bases, architecture decision records, updated runbooks and cross-regional communities of practice. These instruments matter because resilience declines when knowledge remains personal, local or undocumented. A team may recover from an incident once through individual heroism, but enterprise resilience requires repeatable learning routines that reduce dependence on a small number of experts.

Data governance is the second structural foundation of strategic resilience. Y. Hua, M. Kang, H. Yao and Y. Fu demonstrate that data governance capabilities are related to project organization resilience and identify dimensions such as top-level design, data standards, data collection, storage and application [3]. In IT service teams, the relevance of this approach is even more pronounced because risk visibility depends on the quality, comparability and timeliness of data. Incident logs, service-level indicators, dependency maps, vulnerability records, client-impact assessments and escalation histories must be governed as strategic data assets. Without stable data definitions and accountable data ownership, multinational teams may produce many reports but fail to generate usable risk intelligence. Data governance therefore transforms fragmented operational signals into managerial evidence.

The proposed conceptual model can be formulated as a sequence of mutually reinforcing capabilities. Risk sensing detects weak signals across geopolitical, operational, technical and human domains. Risk interpretation translates these signals into scenarios and priorities. Coordinated response allocates authority and resources without destroying accountability. Learning consolidation captures lessons and changes the organizational memory of the team. Data governance connects all four stages by ensuring that decisions are based on reliable and shared information. This model is not a universal recipe; it is a strategic logic that helps multinational IT service teams avoid two typical failures: excessive centralization, which slows local response, and excessive fragmentation, which prevents enterprise-level learning.

The practical value of the proposed approach is that it gives managers a more precise understanding of what should be strengthened before a crisis rather than after it. A multinational IT service enterprise can use the model to audit cross-regional dependencies, clarify escalation rights, evaluate vendor concentration, design crisis communication channels, improve data-quality rules, and build learning routines after incidents. The relevance of this practical orientation is reinforced by recent evidence that firms may continue investing and operating under wartime conditions when economic, institutional and ethical motives interact in complex ways [7]. In such contexts, the objective is not to eliminate uncertainty, since this is impossible, but to prevent uncertainty from becoming organizational paralysis.

Strategic enterprise resilience through risk management in multinational IT service teams should thus be understood as a socio-technical capability. Its technical dimension includes service architecture, cybersecurity controls, monitoring systems, cloud continuity, data quality and documented procedures. Its organizational dimension includes decision rights, adaptive planning, psychological safety, learning routines and managerial cognition. Its strategic dimension concerns the ability to align these mechanisms with enterprise continuity under geopolitical and market turbulence. The main conclusion is that resilience is produced not by isolated emergency plans, but by the disciplined integration of risk management, data governance and team learning into everyday service operations. Such integration allows multinational IT service teams to remain operational under disruption, recover faster after failure and transform crisis experience into sustainable organizational competence.

REFERENCES

1. Bas, T. G. (2025). Globalization vs. glocalization: Learn lessons from two global crises, such as the Russia-Ukraine conflict and the COVID-19 pandemic, for the agro-food and agro-industrial sector. Agriculture, 15(2), 155. URL: https://doi.org/10.3390/agriculture15020155
2. Gutheil, L. (2021). Adaptive project management for the civil society sector: Towards an academic research agenda. International Development Planning Review, 43(3), 393-418. URL: https://doi.org/10.3828/idpr.2020.17
3. Hua, Y., Kang, M., Yao, H., & Fu, Y. (2025). How to foster project organization resilience in the construction industry: The role of data governance capabilities. Buildings, 15(8), 1219. URL: https://doi.org/10.3390/buildings15081219
4. Iftikhar, R., Majeed, M., & Drouin, N. (2023). Crisis management process for project-based organizations. International Journal of Managing Projects in Business, 16(8), 100-125. URL: https://doi.org/10.1108/IJMPB-10-2020-0306
5. Jiao, P., & Bu, W. (2024). The impact of organizational learning on organizational resilience in construction projects. Buildings, 14(4), 975. URL: https://doi.org/10.3390/buildings14040975
6. Kim, S., Lee, H., & Connerton, T. P. (2020). How psychological safety affects team performance: Mediating role of efficacy and learning behavior. Frontiers in Psychology, 11, 1581. URL: https://doi.org/10.3389/fpsyg.2020.01581
7. Nowińska, A., & Olesen, T. R. (2025). Inter-state war dynamics and investment: Insights from the Russia-Ukraine war. Journal of Business Research, 186, 114911. URL: https://doi.org/10.1016/j.jbusres.2024.114911
8. Shu, W., Fan, D., Zhang, X., & Li, G. (2025). Operations locked-in amid geopolitical conflicts: A study of the 2022 Russo-Ukrainian war. Transportation Research Part E: Logistics and Transportation Review, 199, 104147. URL: https://doi.org/10.1016/j.tre.2025.104147
9. Toygar, A., & Yildirim, U. (2023). Examining the effects of the Russia-Ukraine conflict on global supply chains. In Handbook of Research on War Policies, Strategies, and Cyber Wars (pp. 184-199). IGI Global. URL: https://doi.org/10.4018/978-1-6684-6741-1.ch010

Кисса Олександр Вікторович – аспірант, кафедра підприємництва, логістики та менеджменту, Вінницький національний технічний університет, Вінниця, Україна, ol.kyssa@gmail.com

Краєвська Алла Станіславівна – к.е.н, доцент, доцент кафедри підприємництва, логістики та менеджменту, Вінницький національний технічний університет, м. Вінниця, Україна, kraevska@vntu.edu.ua

Kyssa Oleksandr Viktorovych – Postgraduate student, Department of Entrepreneurship, Logistics and Management, Vinnytsia National Technical University, Vinnytsia, Ukraine, ol.kyssa@gmail.com

Kraievska Alla Stanislavivna – Candidate of Economic Science, Associate Professor, Associate Professor of the Department of Entrepreneurship, Logistics and Management, Vinnytsia National Technical University, Vinnytsia, Ukraine, kraevska@vntu.edu.ua